Classical Coding Approaches to Quantum Applications

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

Ph.D. Final Defense

March 18, 2020

Classical Coding Approaches to Quantum Applications

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

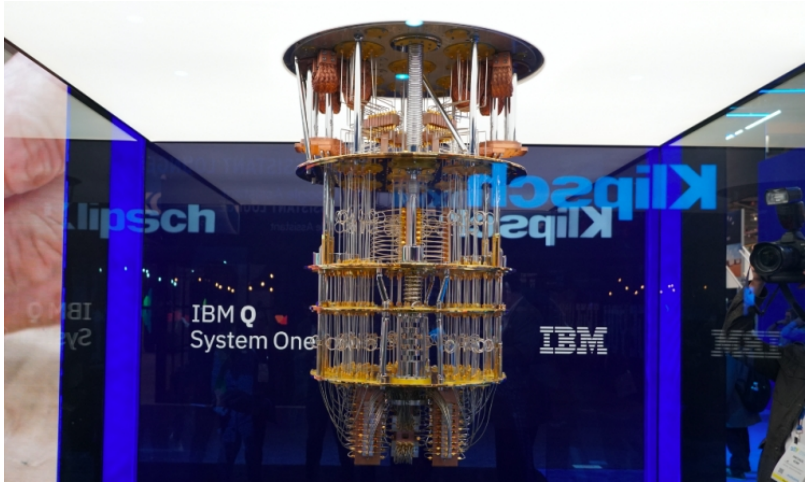
Joint Work: Michael Newman, Kaushik Seshadreesan, Swanand Kadhe, Saikat Guha, Robert Calderbank and Henry Pfister

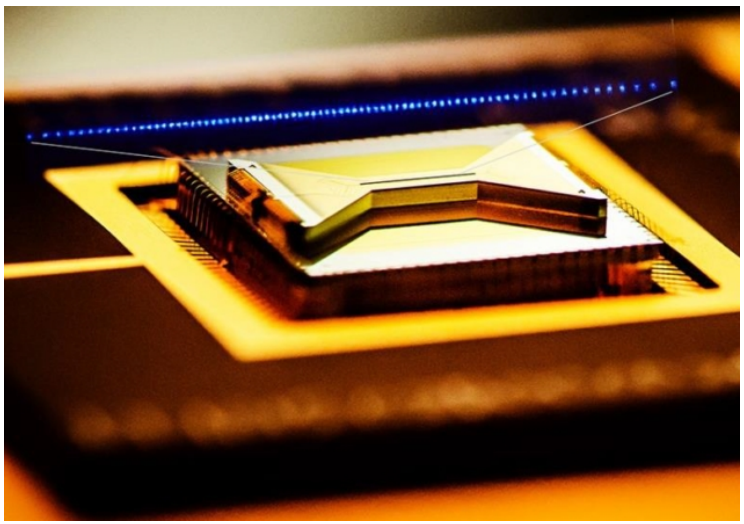
Ph.D. Final Defense

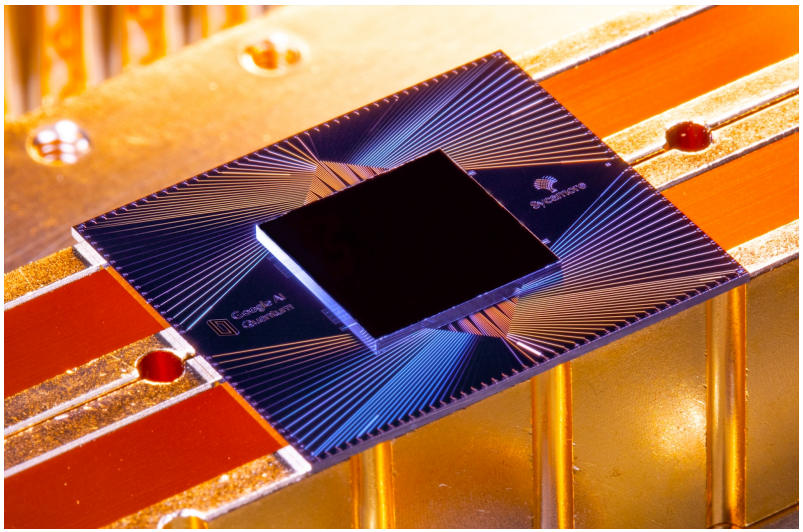
arXiv: 2003.04356, 1910.09333, 1904.07842, 1902.04022, 1907.00310

March 18, 2020

Quantum Technologies Today







Courtesy (clockwise from top-left): D-Wave, IBM, Google, IonQ

Recent Exciting Result

Article

Quantum supremacy using a programmable superconducting processor

https://doi.org/10.1038/s41586-019-1666-5

Received: 22 July 2019

Accepted: 20 September 2019

Published online: 23 October 2019

Frank Arute[1], Kunal Arya[1], Ryan Babbush[1], Dave Bacon[1], Joseph C. Bardin[1,2], Rami Barends[1], Rupak Biswas[3], Sergio Boixo[1], Fernando G. S. L. Brandao[1,4], David A. Buell[1], Brian Burkett[1], Yu Chen[1], Zijun Chen[1], Ben Chiaro[5], Roberto Collins[1], William Courtney[1], Andrew Dunsworth[1], Edward Farhi[1], Brooks Foxen[1,5], Austin Fowler[1], Craig Gidney[1], Marissa Giustina[1], Rob Graff[1], Keith Guerin[1], Steve Habegger[1], Matthew P. Harrigan[1], Michael J. Hartmann[1,6], Alan Ho[1], Markus Hoffmann[1], Trent Huang[1], Travis S. Humble[7], Sergei V. Isakov[1], Evan Jeffrey[1], Zhang Jiang[1], Dvir Kafri[1], Kostyantyn Kechedzhi[1], Julian Kelly[1], Paul V. Klimov[1], Sergey Knysh[1], Alexander Korotkov[1,8], Fedor Kostritsa[1], David Landhuis[1], Mike Lindmark[1], Erik Lucero[1], Dmitry Lyakh[9], Salvatore Mandrà[3,10], Jarrod R. McClean[1], Matthew McEwen[5], Anthony Megrant[1], Xiao Mi[1], Kristel Michielsen[11,12], Masoud Mohseni[1], Josh Mutus[1], Ofer Naaman[1], Matthew Neeley[1], Charles Neill[1], Murphy Yuezhen Niu[1], Eric Ostby[1], Andre Petukhov[1], John C. Platt[1], Chris Quintana[1], Eleanor G. Rieffel[3], Pedram Roushan[1], Nicholas C. Rubin[1], Daniel Sank[1], Kevin J. Satzinger[1], Vadim Smelyanskiy[1], Kevin J. Sung[1,13], Matthew D. Trevithick[1], Amit Vainsencher[1], Benjamin Villalonga[1,14], Theodore White[1], Z. Jamie Yao[1], Ping Yeh[1], Adam Zalcman[1], Hartmut Neven[1] & John M. Martinis[1,5]*

The promise of quantum computers is that certain computational tasks might be executed exponentially faster on a quantum processor than on a classical processor[1]. A fundamental challenge is to build a high-fidelity processor capable of running quantum algorithms in an exponentially large computational space. Here we report the use of a processor with programmable superconducting qubits[2–7] to create quantum states on 53 qubits, corresponding to a computational state-space of dimension 2^{53} (about 10^{16}). Measurements from repeated experiments sample the resulting probability distribution, which we verify using classical simulations. Our Sycamore processor takes about 200 seconds to sample one instance of a quantum circuit a million times—our benchmarks currently indicate that the equivalent task for a state-of-the-art classical supercomputer would take approximately 10,000 years. This dramatic increase in speed compared to all known classical algorithms is an experimental realization of quantum supremacy[8–14] for this specific computational task, heralding a much-anticipated computing paradigm.

Theme of the Dissertation

Quantum technologies promise significant advances in several practical applications, but the hardware remains noisy

Question: What prominent applications and how to tackle noise?

Here we consider two applications:

- Computing: Classical coding in dual bases; borrowed decoders
- Communications: Polar codes for classical-quantum channels

This Talk

Further strengthening the bridge to classical coding theory

Contributions via Classical Coding

- Computing: Classical coding in dual bases $\Rightarrow$ quantum error correction is even possible; classical decoders can be borrowed
  - New classical coding problem under quantum fault-tolerance
  - Classical codes for quantum unitary 2-designs in benchmarking
- Communications: Classical polar codes for classical-input quantum-output channels; decoder infeasible in practice
  - Borrow belief-propagation algorithm with a quantum twist
  - Optimality, new application for photonic quantum computing

Overview

1. Synthesizing Logical Operators for Stabilizer Codes
   - Motivation and Strategy
   - Logical Clifford Synthesis (LCS)
   - Quadratic Form Diagonal (QFD) Gates
   - Stabilizer Codes Matched to QFD Gates

2. Classical Communications over Pure-State Channels
   - Introduction and Motivation
   - Classical Belief-Propagation (BP)
   - Belief-Propagation with Quantum Messages (BPQM)

Overview

1. Synthesizing Logical Operators for Stabilizer Codes
   - Motivation and Strategy
   - Logical Clifford Synthesis (LCS)
   - Quadratic Form Diagonal (QFD) Gates
   - Stabilizer Codes Matched to QFD Gates
2. Classical Communications over Pure-State Channels
   - Introduction and Motivation
   - Classical Belief-Propagation (BP)
   - Belief-Propagation with Quantum Messages (BPQM)

Goal: Logical Operations from Physical Gates

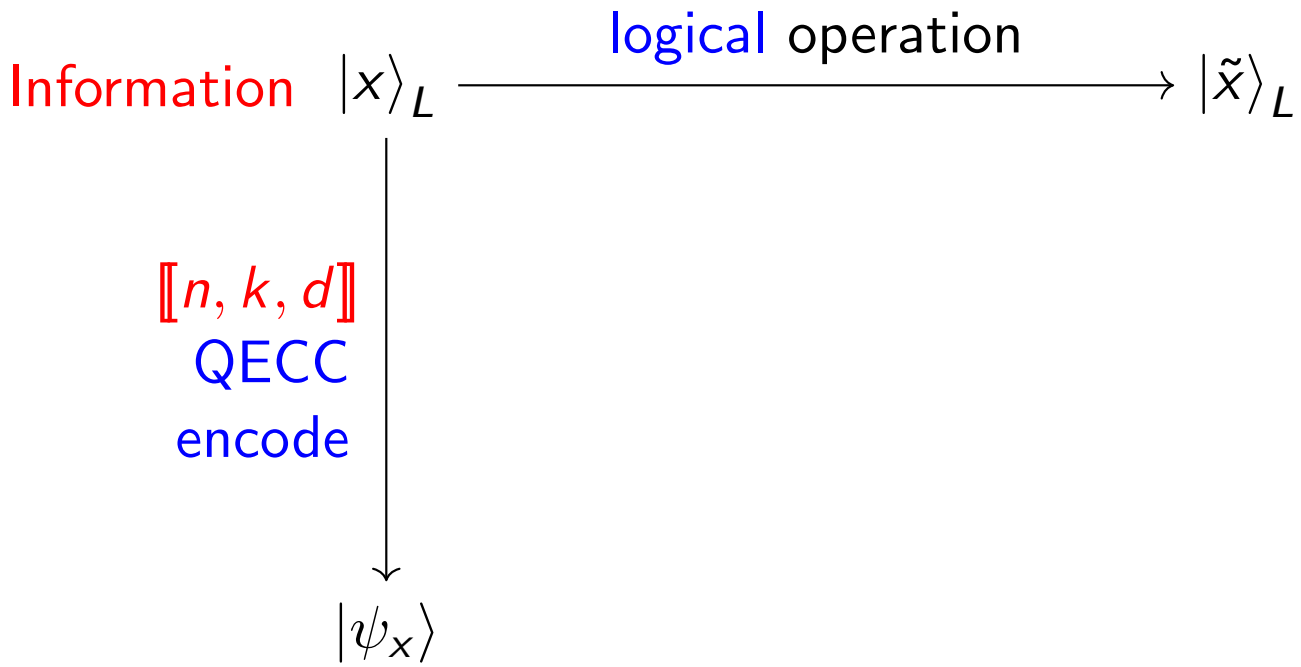
Information $|x\rangle_L$

Goal: Logical Operations from Physical Gates

Information $|x\rangle_L \xrightarrow{\text{logical operation}} |\tilde{x}\rangle_L$

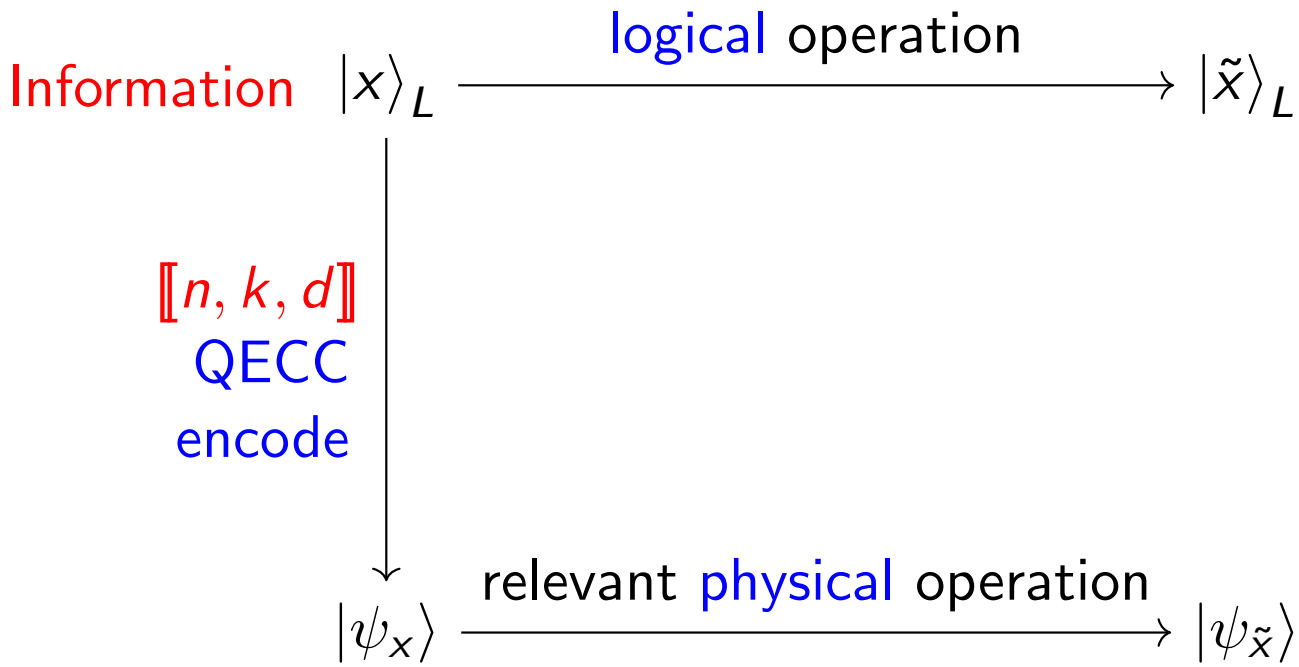
Goal: Logical Operations from Physical Gates

QECC: Quantum Error Correcting Code



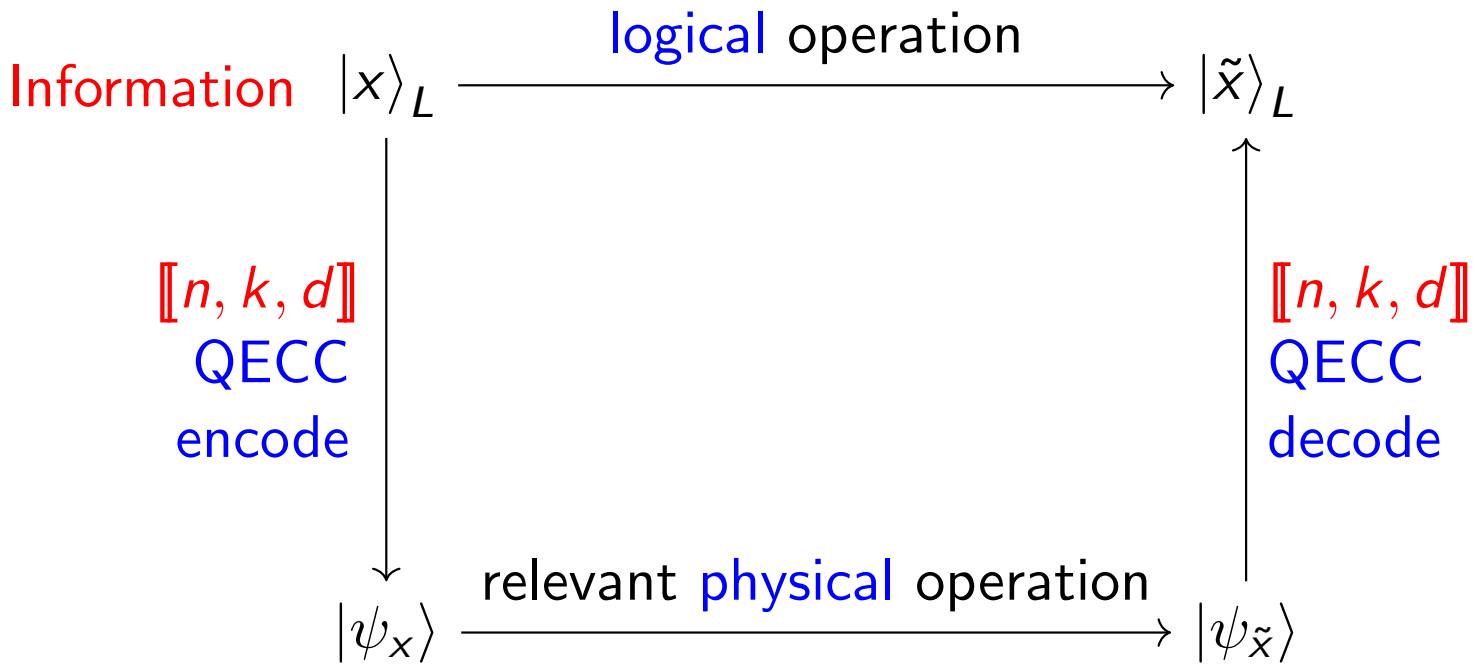
Goal: Logical Operations from Physical Gates

QECC: Quantum Error Correcting Code



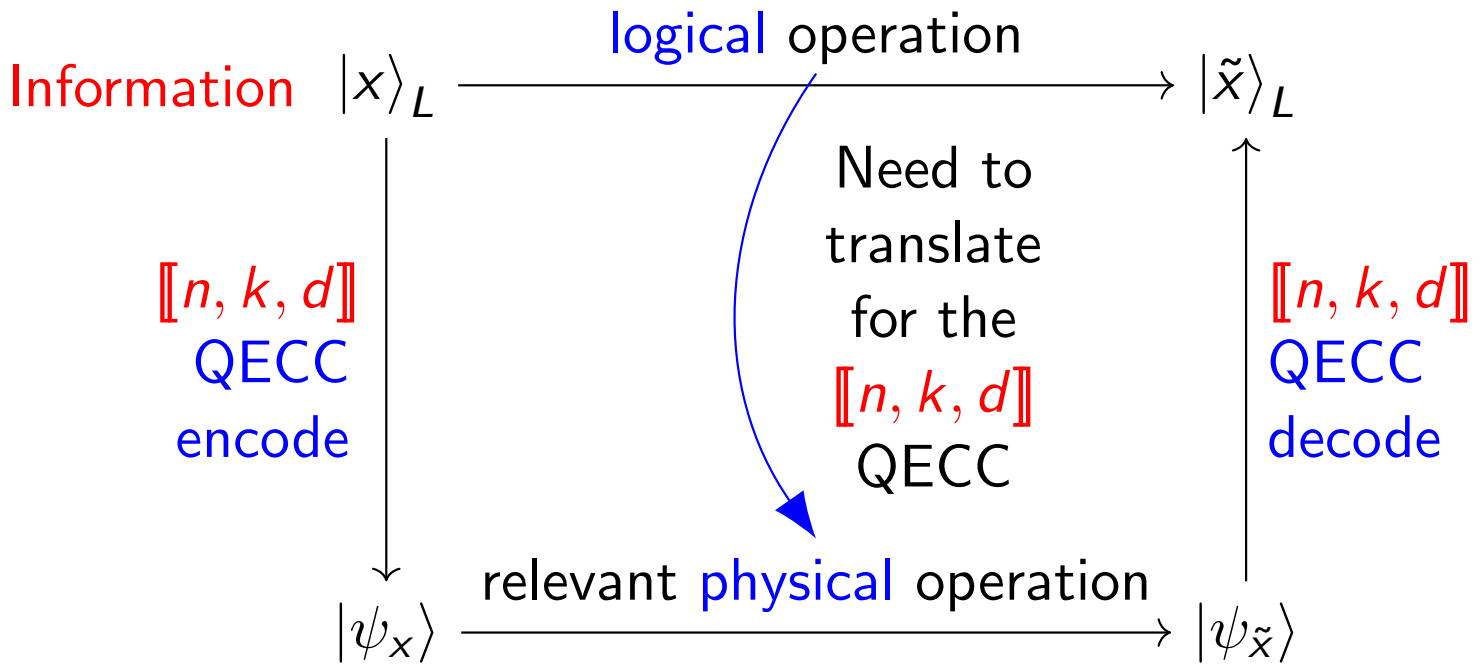
Goal: Logical Operations from Physical Gates

QECC: Quantum Error Correcting Code



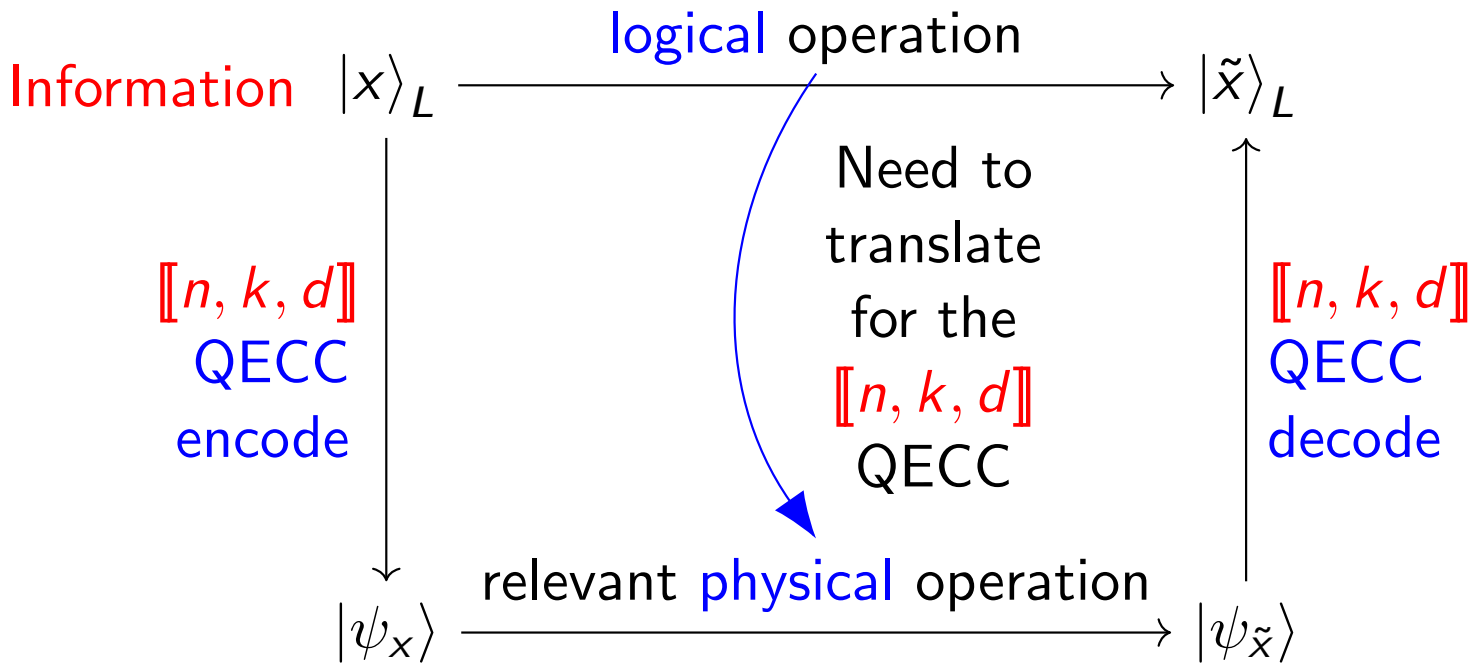
Goal: Logical Operations from Physical Gates

QECC: Quantum Error Correcting Code



Goal: Logical Operations from Physical Gates

QECC: Quantum Error Correcting Code



What QECC structure is required so that
the physical application of certain gates preserves the code subspace?

Line of Thought

What QECC structure is required so that
the physical application of certain gates preserves the code subspace?

Key Idea

Pauli operators form an orthonormal basis for all operators!

- Understand action of those gates on Pauli operators
- Use the action to study effect on quantum error correcting codes
- Finally, restrict to gates that are reliable in the lab

In this talk . . .

1. Synthesizing Logical Operators for Stabilizer Codes
   - Motivation and Strategy
   - Logical Clifford Synthesis (LCS)
   - Quadratic Form Diagonal (QFD) Gates
   - Stabilizer Codes Matched to QFD Gates

2. Classical Communications over Pure-State Channels
   - Introduction and Motivation
   - Classical Belief-Propagation (BP)
   - Belief-Propagation with Quantum Messages (BPQM)

Overview

1. Synthesizing Logical Operators for Stabilizer Codes
   - Motivation and Strategy
   - Logical Clifford Synthesis (LCS)
   - Quadratic Form Diagonal (QFD) Gates
   - Stabilizer Codes Matched to QFD Gates
2. Classical Communications over Pure-State Channels
   - Introduction and Motivation
   - Classical Belief-Propagation (BP)
   - Belief-Propagation with Quantum Messages (BPQM)

Pure (Quantum) States

Qubit: Mathematically, it is a 2-dimensional vector space over $\mathbb{C}$

Pure state: $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,,$ with $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$

$$\text{Example } (n = 2 \text{ qubits}): \quad |0\rangle \otimes |1\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = |01\rangle$$

$$|1\rangle \otimes |0\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = |10\rangle$$

Pure state (n qubits): $|\phi\rangle = \sum_{v \in \mathbb{F}_2^n} \alpha_v\,|v\rangle$, $\alpha_v \in \mathbb{C}$, $\sum_{v \in \mathbb{F}_2^n} |\alpha_v|^2 = 1$

Heisenberg-Weyl (or Pauli) Group HW_N

Pure state (n qubits): $|\phi\rangle = \sum_{v \in \mathbb{F}_2^n} \alpha_v |v\rangle$, $\alpha_v \in \mathbb{C}$, $\sum_{v \in \mathbb{F}_2^n} |\alpha_v|^2 = 1$

$$HW_2 := \langle \imath^\kappa I, X, Z, Y \mid \ \imath := \sqrt{-1},\ \kappa \in \mathbb{Z}_4 \rangle,\ I, X, Y, Z \in \mathbb{C}^{2\times 2}$$

$$\begin{aligned} \text{Bit-Flip}: &\quad X|0\rangle = |1\rangle,\ X|1\rangle = |0\rangle \\ \text{Phase-Flip}: &\quad Z|0\rangle = |0\rangle,\ Z|1\rangle = -|1\rangle \\ \text{Bit-Phase Flip}: &\quad Y := \imath \cdot XZ,\quad XZ = -ZX \end{aligned}$$

For n Qubits: $HW_N :=$ Kronecker products of n HW_2 matrices ($N = 2^n$)

Example ($n = 3$): $(X \otimes Z \otimes Y)(|0\rangle \otimes |1\rangle \otimes |1\rangle) = |1\rangle \otimes (-|1\rangle) \otimes (-\imath|0\rangle)$

Important Fact

Pauli operators form an orthonormal basis for all $N \times N$ matrices

Pauli Group, Clifford Group and Symplectic Matrices

Heisenberg-Weyl Group $HW_N := \{i^\kappa E(a,b) \colon a, b \in \mathbb{F}_2^n, \kappa \in \mathbb{Z}_4\}$

$E(a,b), a, b \in \mathbb{F}_2^n$: $\underbrace{X \otimes Z \otimes Y}_{n=3 \text{ qubits}} = E(\underbrace{1\,0\,1}_{a}, \underbrace{0\,1\,1}_{b})$

$a =$	1	0	1
$b =$	0	1	1
$E(a,b) =$	X_1	Z_2	Y_3

Symplectic Inner Product: $\langle [a,b], [c,d] \rangle_s := [a,b]\,\Omega\,[c,d]^T, \Omega := \begin{bmatrix} 0 & I_n \\ I_n & 0 \end{bmatrix}$

Pauli Group, Clifford Group and Symplectic Matrices

Heisenberg-Weyl Group $HW_N := \{i^\kappa E(a,b) \colon a, b \in \mathbb{F}_2^n, \kappa \in \mathbb{Z}_4\}$

$E(a,b), a, b \in \mathbb{F}_2^n$: $\underbrace{X \otimes Z \otimes Y}_{n=3 \text{ qubits}} = E(\underbrace{1\,0\,1}_{a}, \underbrace{0\,1\,1}_{b})$

$a =$	1	0	1
$b =$	0	1	1
$E(a,b) =$	X_1	Z_2	Y_3

Symplectic Inner Product: $\langle [a,b],[c,d] \rangle_s := [a,b]\,\Omega\,[c,d]^T, \Omega := \begin{bmatrix} 0 & I_n \\ I_n & 0 \end{bmatrix}$

Clifford Group: All unitaries that map Paulis to Paulis under conjugation

Symplectic Matrices: If $g \in \text{Cliff}_N$ (Cliffords on $n = \log_2 N$ qubits) then

$$g\,E(a,b)\,g^\dagger = \pm E\left([a,b]F_g\right), \text{ where } F_g \Omega F_g^T = \Omega$$

$F_g \in \mathbb{F}_2^{2n \times 2n}$ is symplectic: preserves the symplectic inner product

Pauli Group, Clifford Group and Symplectic Matrices

Heisenberg-Weyl Group $HW_N := \{i^\kappa E(a,b) : a, b \in \mathbb{F}_2^n, \kappa \in \mathbb{Z}_4\}$

$E(a,b), a, b \in \mathbb{F}_2^n$: $\underbrace{X \otimes Z \otimes Y}_{n=3 \text{ qubits}} = E(\underbrace{1\,0\,1}_{a}, \underbrace{0\,1\,1}_{b})$

$a =$	1	0	1
$b =$	0	1	1
$E(a,b) =$	X_1	Z_2	Y_3

Clifford Group: All unitaries that map Paulis to Paulis under conjugation

$$g\,E(a,b)\,g^\dagger = \pm E\left([a,b]F_g\right), \text{ where } F_g \Omega F_g^T = \Omega$$

$F_g \in \mathbb{F}_2^{2n \times 2n}$ is symplectic

Two-Qubit Clifford: The Controlled-Z (CZ) Gate

$$g = \mathrm{CZ} = \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & -1 \end{bmatrix},$$

Symplectic Representation: $gE(a,b)g^\dagger = \pm E\left([a,b]F_g\right)$

$$g(X \otimes I)g^\dagger$$

$$= X \otimes Z$$

$$\text{(or) } \mathrm{CZ}(X \otimes I) = (X \otimes Z)\mathrm{CZ}$$

Two-Qubit Clifford: The Controlled-Z (CZ) Gate

$$g = \mathrm{CZ} = \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & -1 \end{bmatrix},$$

Symplectic Representation: $gE(a,b)g^\dagger = \pm E\left([a,b]F_g\right)$

$$\begin{aligned} g(X \otimes I)g^\dagger &= gE(10,00)g^\dagger \\ &= E\left([10,00]F_g\right) \\ &= E(10,01) \\ &= X \otimes Z \\ \text{(or) } \mathrm{CZ}(X \otimes I) &= (X \otimes Z)\mathrm{CZ} \end{aligned}$$

Two-Qubit Clifford: The Controlled-Z (CZ) Gate

$$g = \mathrm{CZ} = \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & -1 \end{bmatrix}, F_g = \begin{bmatrix} I_2 & B_g \\ 0 & I_2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ & & 1 & 0 \\ & & 0 & 1 \end{bmatrix}$$

Symplectic Representation: $gE(a,b)g^\dagger = \pm E\left([a,b]F_g\right)$

$$\begin{aligned} g(X \otimes I)g^\dagger &= gE(10,00)g^\dagger \\ &= E\left([10,00]F_g\right) \\ &= E(10,01) \\ &= X \otimes Z \\ \text{(or) } \mathrm{CZ}(X \otimes I) &= (X \otimes Z)\mathrm{CZ} \end{aligned}$$

Stabilizer Codes ($N = 2^n$)

r-dimensional Stabilizer: Generated by r commuting Pauli operators:

$$S = \langle \epsilon_i E(a_i, b_i) \,;\, i = 1, \ldots, r \rangle, \;\; \epsilon_i \in \{\pm 1\}, \;\; -I_N \notin S$$

$[\![n, k = n - r, d]\!]$ Stabilizer Code: The 2^k dimensional subspace, $V(S)$, jointly fixed by all elements of S

$$V(S) := \left\{ |\psi\rangle \in \mathbb{C}^N : g\,|\psi\rangle = |\psi\rangle \;\text{ for all } g \in S \right\}$$

Example:

$[\![6, 4, 2]\!]$ CSS Code: $S := \langle X^{\otimes 6} = E(a, 0), Z^{\otimes 6} = E(0, a) \rangle$, $a := [1\,1\,1\,1\,1\,1]$

Generator Matrix: $G_S = \left[\begin{array}{cccccc|cccccc} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right]$

Universal Quantum Computation

Goal: Implement arbitrary unitary operations on the k encoded qubits

Break-it-down: Need to implement all Clifford gates and at least one non-Clifford gate on the k logical qubits

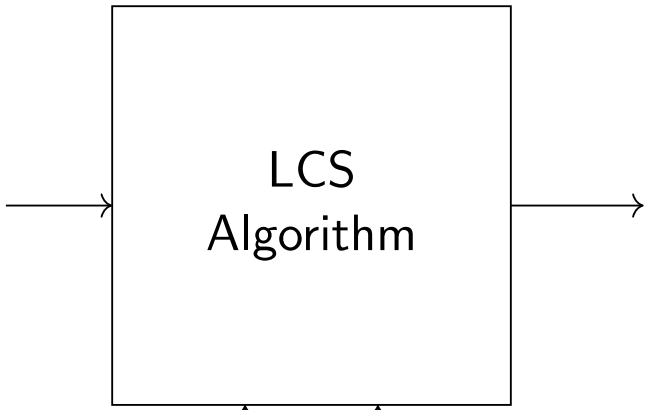
Starting Point

Algorithm for implementing any logical Clifford gate on any stabilizer code

- Understand action of Clifford gates on Pauli operators
- Use the action to study effect on quantum error correcting codes

Logical Clifford Synthesis (LCS)

Synthesis of CZ_{12}^{L} for $[\![6,4,2]\!]$ Code



Logical Clifford
$g^L = \mathrm{CZ}_{12}^L$

Stabilizer
$S = \langle X^{\otimes 6}, Z^{\otimes 6} \rangle$
$= \langle E(\underline{1}, \underline{0}), E(\underline{0}, \underline{1}) \rangle$

All* circuits $\bar{g} \in \mathrm{Cliff}_{2^6}$
that realize g^L and fix S
(stabilizer freedom ignored)
* up to an equivalence class

Logical Pauli Operators
$\bar{X}_j = X_1 X_{j+1} = E(\underline{e}_1 + \underline{e}_{j+1}, \underline{0})$
$\bar{Z}_j = Z_{j+1} Z_6 = E(\underline{0}, \underline{e}_{j+1} + \underline{e}_6)$
$(j = 1, 2, 3, 4)$

Implementation: https://github.com/nrenga/symplectic-arxiv18a

Paper: https://arxiv.org/abs/1907.00310

Kerdock (Logical) Unitary 2-Design

2-Design: Unitary ensemble, matches Haar measure up to second moment

Kerdock Set $P_{\mathrm{K}}(n)$: A specific collection of $N = 2^n$ symmetric matrices

Kerdock Code $K(n)$: Each (classical) codeword $c_{P,w,\kappa} \in \mathbb{Z}_4^N$ is indexed by $P \in P_{\mathrm{K}}(n)$, $w \in \mathbb{F}_2^n$, and $\kappa \in \mathbb{Z}_4$; so, totally 2^{2n+2} codewords

Obtain graph states from all $c_{P,w,\kappa}$ by mapping $\mathbb{Z}_4 \mapsto \{1, \imath, -1, -\imath\}$!

Main Result

The symmetry group of the graph states produces a unitary 2-design

Combining with the LCS algorithm produces a logical unitary 2-design!
See https://arxiv.org/abs/1904.07842 for details

LCS: Exploit Action on Pauli Operators

Main Ideas in LCS: Use $\bar{g}\, E(a,b)\, \bar{g}^\dagger = \pm E([a,b]F_{\bar{g}})$

- Implied logical action: $g^L X_j^L (g^L)^\dagger, g^L Z_j^L (g^L)^\dagger \Rightarrow \bar{g}\bar{X}_j\bar{g}^\dagger, \bar{g}\bar{Z}_j\bar{g}^\dagger$
- $\bar{g} \in \text{Cliff}_N$ must map stabilizers to stabilizers under conjugation
- Translate conjugation relations into symplectic constraints on $F_{\bar{g}}$

LCS: Exploit Action on Pauli Operators

Main Ideas in LCS: Use $\bar{g}\, E(a,b)\, \bar{g}^\dagger = \pm E([a,b]F_{\bar{g}})$

- Implied logical action: $g^L X_j^L (g^L)^\dagger, g^L Z_j^L (g^L)^\dagger \Rightarrow \bar{g}\bar{X}_j\bar{g}^\dagger, \bar{g}\bar{Z}_j\bar{g}^\dagger$
- $\bar{g} \in \text{Cliff}_N$ must map stabilizers to stabilizers under conjugation
- Translate conjugation relations into symplectic constraints on $F_{\bar{g}}$

Issues in generalizing to non-Clifford gates:

- Translating logical non-Cliffords to physical non-Cliffords is hard: there is no clear symplectic connection
- Physical operation is not Clifford $\Rightarrow$ does not necessarily map stabilizers to stabilizers under conjugation

Overview

1. Synthesizing Logical Operators for Stabilizer Codes
   - Motivation and Strategy
   - Logical Clifford Synthesis (LCS)
   - Quadratic Form Diagonal (QFD) Gates
   - Stabilizer Codes Matched to QFD Gates
2. Classical Communications over Pure-State Channels
   - Introduction and Motivation
   - Classical Belief-Propagation (BP)
   - Belief-Propagation with Quantum Messages (BPQM)

Gates for Universal Computation

$\text{Cliff}_N = \langle H, P, \text{CZ or CNOT (on all qubits)} \rangle \longleftarrow$ Not universal!

Gate	Unitary Matrix	Action on Paulis	Symplectic Matrix
Hadamard	$H := \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$	$HXH^\dagger = Z$ $HZH^\dagger = X$	$F_H = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Phase	$P := \begin{bmatrix} 1 & 0 \\ 0 & \imath \end{bmatrix} = \sqrt{Z}$	$PXP^\dagger = Y$ $PZP^\dagger = Z$	$F_P = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$
Phase (P), Ctrl-Z (CZ)	$t_R := \sum_{v \in \mathbb{F}_2^n} \imath^{vRv^T} \lvert v \rangle \langle v \rvert$ (vRv^T computed over $\mathbb{Z}$)	CZ: $X_a \mapsto X_a Z_b$ $Z_a \mapsto Z_a$	$T_R = \begin{bmatrix} I_n & R \\ 0 & I_n \end{bmatrix}$ with R symmetric
T	$T := \begin{bmatrix} 1 & 0 \\ 0 & e^{\imath\pi/4} \end{bmatrix} = \sqrt{P}$	$TXT^\dagger = \frac{X+Y}{\sqrt{2}}$ $TZT^\dagger = Z$	?

Gates for Universal Computation

Gate	Unitary Matrix	Action on Paulis	Symplectic Matrix
Phase (P), Ctrl-Z (CZ)	$t_R := \sum_{v \in \mathbb{F}_2^n} \imath^{vRv^T} \lvert v \rangle \langle v \rvert$ (vRv^T computed over $\mathbb{Z}$)	CZ: $X_a \mapsto X_a Z_b$, $Z_a \mapsto Z_a$	$T_R = \begin{bmatrix} I_n & R \\ 0 & I_n \end{bmatrix}$ with R symmetric
T	$T := \begin{bmatrix} 1 & 0 \\ 0 & e^{\imath\pi/4} \end{bmatrix} = \sqrt{P}$	$TXT^\dagger = \frac{X+Y}{\sqrt{2}}$, $TZT^\dagger = Z$	?

Quadratic Form Diagonal (QFD) Gates

S.X. Cui, D. Gottesman and A. Krishna, Phys. Rev. A, 2017
If $U \in \mathcal{C}^{(\ell)}$ is diagonal, then all entries are 2^{ℓ}-th roots of unity.

Examples:

$$P \in \mathcal{C}^{(2)} \leftrightarrow R = [1] \text{ over } \mathbb{Z}_4$$

$$\mathcal{C}^{(2)}: t_R = \sum_{v \in \mathbb{F}_2^n} i^{vRv^T} |v\rangle \langle v|$$

R is $n \times n$ symmetric with entries in $\mathbb{Z}_2$

$$\mathcal{C}^{(1)} = HW_N$$

$$\text{CZ} = \text{diag}[1, 1, 1, -1] \in \mathcal{C}^{(2)}$$

$$\leftrightarrow R = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ over } \mathbb{Z}_4$$

Quadratic Form Diagonal (QFD) Gates

S.X. Cui, D. Gottesman and A. Krishna, Phys. Rev. A, 2017
If $U \in \mathcal{C}^{(\ell)}$ is diagonal, then all entries are 2^ℓ-th roots of unity.

$\mathcal{C}^{(\ell)}$: $\tau_R^{(\ell)} = \sum_{v \in \mathbb{F}_2^n} \xi^{vRv^T} |v\rangle \langle v|$

- R is $n \times n$ symmetric with entries in $\mathbb{Z}_{2^\ell}$, $\xi = \exp\left(\frac{2\pi\imath}{2^\ell}\right)$

$\mathcal{C}^{(2)}$: $t_R = \sum_{v \in \mathbb{F}_2^n} \imath^{vRv^T} |v\rangle \langle v|$

- R is $n \times n$ symmetric with entries in $\mathbb{Z}_2$

$\mathcal{C}^{(1)} = HW_N$

Examples:

$P \in \mathcal{C}^{(2)} \leftrightarrow R = [1]$ over $\mathbb{Z}_4$

$T \in \mathcal{C}^{(3)} \leftrightarrow R = [1]$ over $\mathbb{Z}_8$

$$\mathrm{CZ} = \mathrm{diag}[1,1,1,-1] \in \mathcal{C}^{(2)}$$
$$\leftrightarrow R = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ over } \mathbb{Z}_4$$

Quadratic Form Diagonal (QFD) Gates

S.X. Cui, D. Gottesman and A. Krishna, Phys. Rev. A, 2017
If $U \in \mathcal{C}^{(\ell)}$ is diagonal, then all entries are 2^ℓ-th roots of unity.

$\mathcal{C}^{(\ell)}$: $\tau_R^{(\ell)} = \sum_{v \in \mathbb{F}_2^n} \xi^{vRv^T} |v\rangle \langle v|$

R is $n \times n$ symmetric with entries in $\mathbb{Z}_{2^\ell}$, $\xi = \exp\left(\frac{2\pi\imath}{2^\ell}\right)$

$\mathcal{C}^{(2)}$: $t_R = \sum_{v \in \mathbb{F}_2^n} \imath^{vRv^T} |v\rangle \langle v|$

R is $n \times n$ symmetric with entries in $\mathbb{Z}_2$

$\mathcal{C}^{(1)} = HW_N$

Examples:

$P \in \mathcal{C}^{(2)} \leftrightarrow R = [1]$ over $\mathbb{Z}_4$

$T \in \mathcal{C}^{(3)} \leftrightarrow R = [1]$ over $\mathbb{Z}_8$

$$\mathrm{CZ} = \mathrm{diag}[1,1,1,-1] \in \mathcal{C}^{(2)}$$
$$\leftrightarrow R = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ over } \mathbb{Z}_4$$
$$\mathrm{CP} = \mathrm{diag}[1,1,1,\imath] \in \mathcal{C}^{(3)}$$
$$\leftrightarrow R = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ over } \mathbb{Z}_8$$

Diagonal Recursion for QFD Gates

Recollect: Clifford g acts as $g\,E(a,b)\,g^\dagger = \pm E([a,b]F_g)$, F_g symplectic

How do QFD gates act on Pauli matrices under conjugation?

$$\tau_R^{(\ell)} E(a,b) \left(\tau_R^{(\ell)}\right)^\dagger = \phi(R,a,b,\ell) \cdot E\left([a,b]\begin{bmatrix} I_n & R \\ 0 & I_n \end{bmatrix}\right) \cdot \tau_{\tilde{R}(R,a,\ell)}^{(\ell-1)}$$

$\phi(R,a,b,\ell)$: Deterministic global phase

$\tilde{R}(R,a,\ell)$: New symmetric matrix with entries in $\mathbb{Z}_{2^{\ell-1}}$

Diagonal Recursion for QFD Gates

Recollect: Clifford g acts as $g\,E(a,b)\,g^\dagger = \pm E([a,b]F_g)$, F_g symplectic

How do QFD gates act on Pauli matrices under conjugation?

$$\tau_R^{(\ell)} E(a,b) \left(\tau_R^{(\ell)}\right)^\dagger = \phi(R,a,b,\ell) \cdot E\left([a,b]\begin{bmatrix} I_n & R \\ 0 & I_n \end{bmatrix}\right) \cdot \tau^{(\ell-1)}_{\tilde{R}(R,a,\ell)}$$

$\phi(R,a,b,\ell)$: Deterministic global phase

$\tilde{R}(R,a,\ell)$: New symmetric matrix with entries in $\mathbb{Z}_{2^{\ell-1}}$

All 1- and 2-local diagonal gates in $\mathcal{C}^{(\ell)}$ are QFD for any $\ell \geq 1$

Mølmer-Sørensen gates MS($\frac{\pi}{2^\ell}$) are QFD up to Hadamards

For details see: https://arxiv.org/abs/1902.04022

Overview

1. Synthesizing Logical Operators for Stabilizer Codes
   - Motivation and Strategy
   - Logical Clifford Synthesis (LCS)
   - Quadratic Form Diagonal (QFD) Gates
   - Stabilizer Codes Matched to QFD Gates
2. Classical Communications over Pure-State Channels
   - Introduction and Motivation
   - Classical Belief-Propagation (BP)
   - Belief-Propagation with Quantum Messages (BPQM)

Universal Quantum Computation

Goal: Implement arbitrary unitary operations on the k encoded qubits

Break-it-down: Need to implement all Clifford gates and at least one non-Clifford gate on the k logical qubits

Synthesizing logical non-Cliffords is hard

First explore how physical non-Clifford gates affect the code subspace

- Understand action of non-Clifford gates on Pauli operators
- Use the action to study effect on quantum error correcting codes

LCS: Exploit Action on Pauli Operators

Main Ideas in LCS:

- Implied logical action: $g^L X_j^L (g^L)^\dagger, g^L Z_j^L (g^L)^\dagger \Rightarrow \bar{g} \bar{X}_j \bar{g}^\dagger, \bar{g} \bar{Z}_j \bar{g}^\dagger$
- $\bar{g} \in \text{Cliff}_N$ must map stabilizers to stabilizers under conjugation
- Translate conjugation relations into symplectic constraints on $F_{\bar{g}}$

Issues in generalizing to $\mathcal{C}^{(\ell)}, \ell > 2$:

- Translating logical non-Cliffords to physical non-Cliffords is hard: there is no clear symplectic connection.
- Physical operation is not Clifford $\Rightarrow$ does not necessarily map stabilizers to stabilizers.

LCS: Exploit Action on Pauli Operators

Main Ideas in LCS:

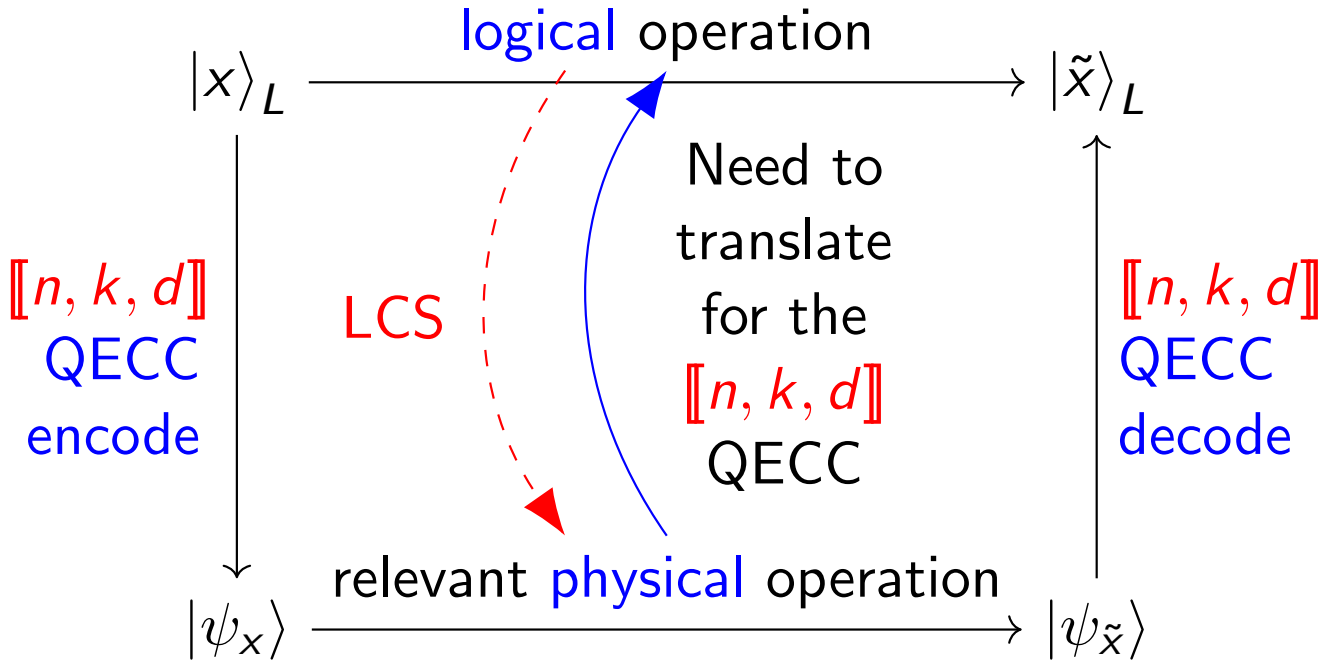
- Implied logical action: $g^L X_j^L (g^L)^\dagger, g^L Z_j^L (g^L)^\dagger \Rightarrow \bar{g} \bar{X}_j \bar{g}^\dagger, \bar{g} \bar{Z}_j \bar{g}^\dagger$
- $\bar{g} \in \text{Cliff}_N$ must map stabilizers to stabilizers under conjugation
- Translate conjugation relations into symplectic constraints on $F_{\bar{g}}$

Issues in generalizing to $\mathcal{C}^{(\ell)}, \ell > 2$:

- Translating logical non-Cliffords to physical non-Cliffords is hard: there is no clear symplectic connection. QFD Gates!
- Physical operation is not Clifford $\Rightarrow$ does not necessarily map stabilizers to stabilizers. Preserve projector onto code subspace!

Reverse LCS Strategy for Physical T Gates

QECC: Quantum Error Correcting Code



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

Transversal T as a Logical Operator

Question: When is transversal T a logical operator for a stabilizer code? What is the induced logical operation?

Stabilizer: $S = \langle \epsilon_i E(a_i, b_i)\,;\, i = 1, 2, \ldots, r \rangle,\ \epsilon_i \in \{\pm 1\}$

Code Projector: $\Pi_s = \prod_{i=1}^{r} \frac{I_N + \epsilon_i E(a_i, b_i)}{2} = \frac{1}{2^r} \sum_{a,b \in S} \epsilon_{a,b} E(a, b)$

Transversal T as a Logical Operator

Question: When is transversal T a logical operator for a stabilizer code? What is the induced logical operation?

Stabilizer: $S = \langle \epsilon_i E(a_i, b_i)\,;\, i = 1, 2, \ldots, r \rangle,\ \epsilon_i \in \{\pm 1\}$

Code Projector: $\Pi_s = \prod_{i=1}^{r} \frac{I_N + \epsilon_i E(a_i, b_i)}{2} = \frac{1}{2^r} \sum_{a,b \in S} \epsilon_{a,b} E(a, b)$

Calculation using QFD recursion [hard for general QFD!]

$$T^{\otimes n} E(a, b) \left(T^{\otimes n}\right)^{\dagger} = \frac{1}{2^{\mathrm{wt}_H(a)/2}} \sum_{y \preceq a} (-1)^{by^T} E(a, b \oplus y)$$

Transversal T as a Logical Operator

Question: When is transversal T a logical operator for a stabilizer code? What is the induced logical operation?

Stabilizer: $S = \langle \epsilon_i E(a_i, b_i)\,;\, i = 1, 2, \ldots, r \rangle,\ \epsilon_i \in \{\pm 1\}$

Code Projector: $\Pi_s = \prod_{i=1}^{r} \frac{I_N + \epsilon_i E(a_i, b_i)}{2} = \frac{1}{2^r} \sum_{a,b \in S} \epsilon_{a,b} E(a, b)$

Calculation using QFD recursion [hard for general QFD!]

$$T^{\otimes n} E(a, b) \left(T^{\otimes n}\right)^{\dagger} = \frac{1}{2^{\mathrm{wt}_H(a)/2}} \sum_{y \preceq a} (-1)^{by^T} E(a, b \oplus y)$$

$T^{\otimes n}$ is a logical operator iff $T^{\otimes n} \Pi_S (T^{\otimes n})^{\dagger} = \Pi_S$: [also hard in general!]

$$\frac{1}{2^r} \sum_{a,b \in S} \frac{\epsilon_{a,b}}{2^{\mathrm{wt}_H(a)/2}} \sum_{y \preceq a} (-1)^{by^T} E(a, b \oplus y) = \frac{1}{2^r} \sum_{a,b \in S} \epsilon_{a,b} E(a, b)$$

CSS-T Codes and Two Corollaries

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 $[\![n, k_1 - k_2, d \geq \min(d_1, d_2^{\perp})]\!]$.

CSS-T Codes and Two Corollaries

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 $[\![n, k_1 - k_2, d \geq \min(d_1, d_2^{\perp})]\!]$.

Two Corollaries: (Non-degenerate $\Rightarrow$ each stabilizer has weight $\geq d$)

1. Triorthogonal codes form the only CSS family with $T^{\otimes n} \equiv \bar{T}^{\otimes k}$.
2. For each $[\![n, k, d]\!]$ non-degenerate stabilizer code that supports transversal T, there is an $[\![n, k, d]\!]$ CSS-T code that does too.

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 Problem

A CSS-T family with $\frac{(k_1 - k_2)}{n} = \Omega(1)$ and $\frac{d}{n} = \Omega(1)$

Would imply constant overhead magic state distillation! $\left[\gamma = \frac{\log(n/k)}{\log d}\right]$

(see arXiv:1910.09333, or arXiv:2001.04887 for shorter version)

Summary and Future Work

- Reviewed the Logical Clifford Synthesis (LCS) algorithm

Summary and Future Work

- Reviewed the Logical Clifford Synthesis (LCS) algorithm
- Characterized QFD gates in the Clifford hierarchy
  - All 1- and 2-local diagonal gates in the hierarchy are QFD
  - Rigorously derived their action on Pauli matrices by conjugation

Summary and Future Work

- Reviewed the Logical Clifford Synthesis (LCS) algorithm
- Characterized QFD gates in the Clifford hierarchy
  - All 1- and 2-local diagonal gates in the hierarchy are QFD
  - Rigorously derived their action on Pauli matrices by conjugation
- Used QFD framework to construct codes matched to T gates
  - Triorthogonal codes form the only CSS family with $T^{\otimes n} \equiv \bar{T}^{\otimes k}$
  - CSS-T optimal for $T^{\otimes n}$ among non-degenerate stabilizer codes
  - Paper: Extensions to finer angle Z-rotations and Reed-Muller codes

Summary and Future Work

- Reviewed the Logical Clifford Synthesis (LCS) algorithm
- Characterized QFD gates in the Clifford hierarchy
  - All 1- and 2-local diagonal gates in the hierarchy are QFD
  - Rigorously derived their action on Pauli matrices by conjugation
- Used QFD framework to construct codes matched to T gates
  - Triorthogonal codes form the only CSS family with $T^{\otimes n} \equiv \bar{T}^{\otimes k}$
  - CSS-T optimal for $T^{\otimes n}$ among non-degenerate stabilizer codes
  - Paper: Extensions to finer angle Z-rotations and Reed-Muller codes
- Use our recipe to find codes supporting any reliable QFD gate?

Key Takeaway

Expressing unitaries in the Pauli basis seems like an under-utilized trick

Overview

1. Synthesizing Logical Operators for Stabilizer Codes
   - Motivation and Strategy
   - Logical Clifford Synthesis (LCS)
   - Quadratic Form Diagonal (QFD) Gates
   - Stabilizer Codes Matched to QFD Gates

2. Classical Communications over Pure-State Channels
   - Introduction and Motivation
   - Classical Belief-Propagation (BP)
   - Belief-Propagation with Quantum Messages (BPQM)

Message Passing Algorithms

- To compute quantities related to problems defined on graphs
- They work by passing messages between nodes of the graph

Belief-Propagation (BP)

A message passing algorithm to efficiently compute posterior marginal distributions in statistical inference problems

- BP exactly performs bit-wise (or variable-wise) maximum-a-posteriori (bit-MAP) estimation when the underlying graph is a tree
- When the graph has cycles, usually run BP for a fixed number of iterations; it converges in many cases, e.g., LDPC codes

Extending BP to the Quantum World

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. Synthesizing Logical Operators for Stabilizer Codes
   - Motivation and Strategy
   - Logical Clifford Synthesis (LCS)
   - Quadratic Form Diagonal (QFD) Gates
   - Stabilizer Codes Matched to QFD Gates

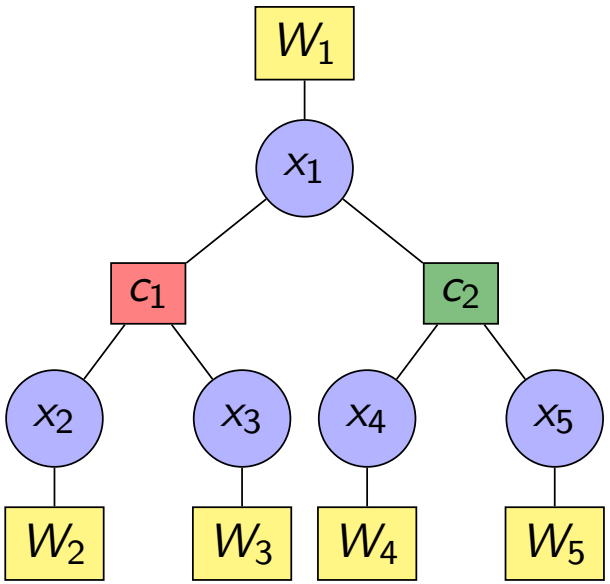
2. Classical Communications over Pure-State Channels
   - Introduction and Motivation
   - Classical Belief-Propagation (BP)
   - Belief-Propagation with Quantum Messages (BPQM)

Binary Linear Codes and Factor Graphs

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

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

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



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

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

Maximum-a-Posteriori (MAP) Decoding

Problem: Transmit codeword $\underline{x} \in \mathcal{C}$ through W^n, receive vector $\underline{y} \in \mathcal{Y}^n$, optimally estimate the sent codeword $\hat{\underline{x}} \in \mathcal{C}$ given observation $\underline{y}$

$$p(\underline{x}|\underline{y}) = \frac{p(\underline{y}|\underline{x}) \cdot p(\underline{x})}{\sum_{\underline{x} \in \{0,1\}^5} p(\underline{y}|\underline{x}) \cdot p(\underline{x})}$$

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

Maximum-a-Posteriori (MAP) Decoding

Problem: Transmit codeword $\underline{x} \in \mathcal{C}$ through W^n, receive vector $\underline{y} \in \mathcal{Y}^n$, optimally estimate the sent codeword $\hat{\underline{x}} \in \mathcal{C}$ given observation $\underline{y}$

$$p(\underline{x}|\underline{y}) = \frac{p(\underline{y}|\underline{x}) \cdot p(\underline{x})}{\sum_{\underline{x} \in \{0,1\}^5} p(\underline{y}|\underline{x}) \cdot p(\underline{x})}$$

$$= \frac{\prod_{k=1}^{5} W(y_k|x_k) \cdot \frac{1}{|\mathcal{C}|} \mathbb{I}(\underline{x} \in \mathcal{C})}{p(\underline{y})}$$

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

Maximum-a-Posteriori (MAP) Decoding

Problem: Transmit codeword $\underline{x} \in \mathcal{C}$ through W^n, receive vector $\underline{y} \in \mathcal{Y}^n$, optimally estimate the sent codeword $\hat{\underline{x}} \in \mathcal{C}$ given observation $\underline{y}$

$$p(\underline{x}|\underline{y}) = \frac{p(\underline{y}|\underline{x}) \cdot p(\underline{x})}{\sum_{\underline{x} \in \{0,1\}^5} p(\underline{y}|\underline{x}) \cdot p(\underline{x})}$$

$$= \frac{\prod_{k=1}^{5} W(y_k|x_k) \cdot \frac{1}{|\mathcal{C}|} \mathbb{I}(\underline{x} \in \mathcal{C})}{p(\underline{y})}$$

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

$$\propto \prod_{k=1}^{5} W(y_k|x_k) \cdot [\mathbb{I}(x_1 \oplus x_2 \oplus x_3 = 0)\, \mathbb{I}(x_1 \oplus x_4 \oplus x_5 = 0)]$$

Maximum-a-Posteriori (MAP) Decoding

Problem: Transmit codeword $\underline{x} \in \mathcal{C}$ through W^n, receive vector $\underline{y} \in \mathcal{Y}^n$, optimally estimate the sent codeword $\hat{\underline{x}} \in \mathcal{C}$ given observation $\underline{y}$

$$p(\underline{x}|\underline{y}) = \frac{p(\underline{y}|\underline{x}) \cdot p(\underline{x})}{\sum_{\underline{x} \in \{0,1\}^5} p(\underline{y}|\underline{x}) \cdot p(\underline{x})}$$

$$= \frac{\prod_{k=1}^{5} W(y_k|x_k) \cdot \frac{1}{|\mathcal{C}|} \mathbb{I}(\underline{x} \in \mathcal{C})}{p(\underline{y})}$$

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

$$\propto \prod_{k=1}^{5} W(y_k|x_k) \cdot [\mathbb{I}(x_1 \oplus x_2 \oplus x_3 = 0)\, \mathbb{I}(x_1 \oplus x_4 \oplus x_5 = 0)]$$

$$= W(y_1|x_1) \cdot [\mathbb{I}(x_1 \oplus x_2 \oplus x_3 = 0) W(y_2|x_2) W(y_3|x_3)]$$
$$\cdot [\mathbb{I}(x_1 \oplus x_4 \oplus x_5 = 0) W(y_4|x_4) W(y_5|x_5)],$$

Maximum-a-Posteriori (MAP) Decoding

Problem: Transmit codeword $\underline{x} \in \mathcal{C}$ through W^n, receive vector $\underline{y} \in \mathcal{Y}^n$, optimally estimate the sent codeword $\hat{\underline{x}} \in \mathcal{C}$ given observation $\underline{y}$

$$p(\underline{x}|\underline{y}) = \frac{p(\underline{y}|\underline{x}) \cdot p(\underline{x})}{\sum_{\underline{x} \in \{0,1\}^5} p(\underline{y}|\underline{x}) \cdot p(\underline{x})}$$

$$= \frac{\prod_{k=1}^{5} W(y_k|x_k) \cdot \frac{1}{|\mathcal{C}|} \mathbb{I}(\underline{x} \in \mathcal{C})}{p(\underline{y})}$$

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

$$\propto \prod_{k=1}^{5} W(y_k|x_k) \cdot [\mathbb{I}(x_1 \oplus x_2 \oplus x_3 = 0)\, \mathbb{I}(x_1 \oplus x_4 \oplus x_5 = 0)]$$

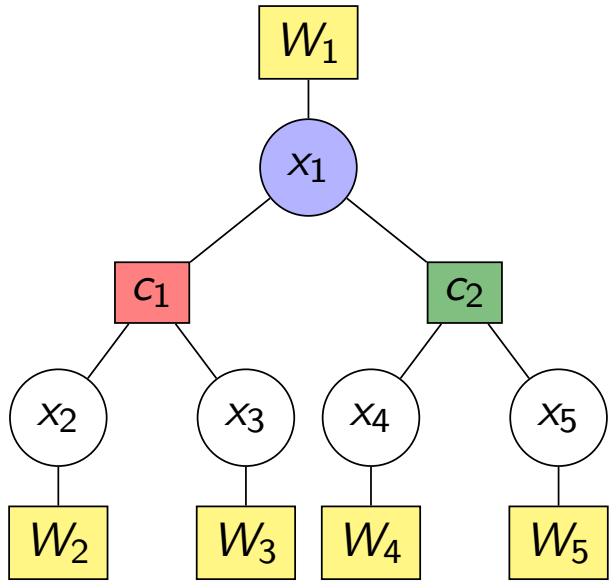
$$= W(y_1|x_1) \cdot [\mathbb{I}(x_1 \oplus x_2 \oplus x_3 = 0) W(y_2|x_2) W(y_3|x_3)]$$
$$\cdot [\mathbb{I}(x_1 \oplus x_4 \oplus x_5 = 0) W(y_4|x_4) W(y_5|x_5)],$$

$$\hat{\underline{x}}^{\text{MAP}} := \underset{\underline{x} \in \{0,1\}^5}{\text{argmax}}\ p(\underline{x}|\underline{y}) \longleftarrow \text{Block-MAP}$$

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:

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

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

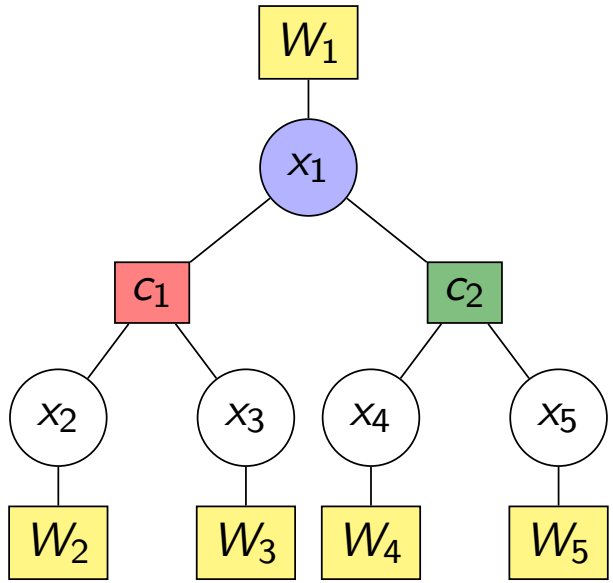
$$\left. \cdot \left[\sum_{x_4,x_5 \in \{0,1\}^2} \mathbb{I}(x_1 \oplus x_4 \oplus x_5 = 0) W(y_4|x_4) W(y_5|x_5) \right] \right\}$$

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:

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

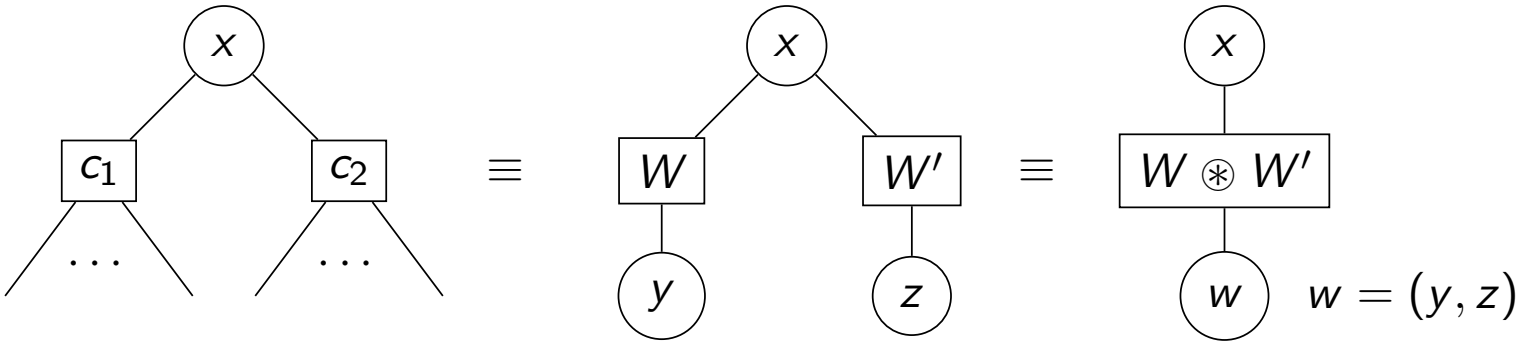
$$= \underset{x_1 \in \{0,1\}}{\text{argmax}} \left\{ W(y_1|x_1) \cdot \left[\sum_{x_2,x_3 \in \{0,1\}^2} \mathbb{I}(x_1 \oplus x_2 \oplus x_3 = 0) W(y_2|x_2) W(y_3|x_3) \right] \right.$$

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

Induced Channels in BP

Variable Node Convolution: The transition probabilities of this channel are

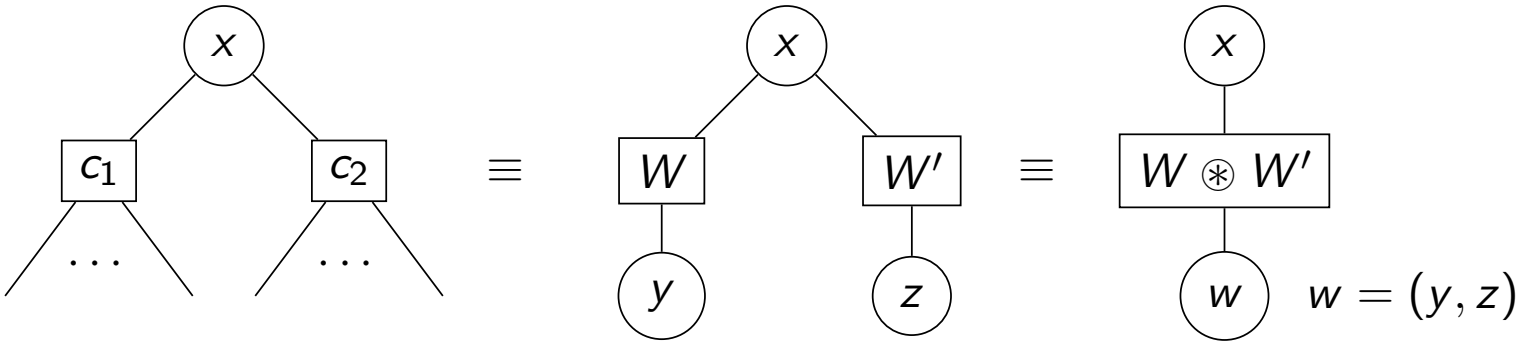
$$[W \circledast W'](y, z|x) = W(y|x) \cdot W'(z|x, y) = W(y|x) \cdot W'(z|x)$$



Induced Channels in BP

Variable Node Convolution: The transition probabilities of this channel are

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



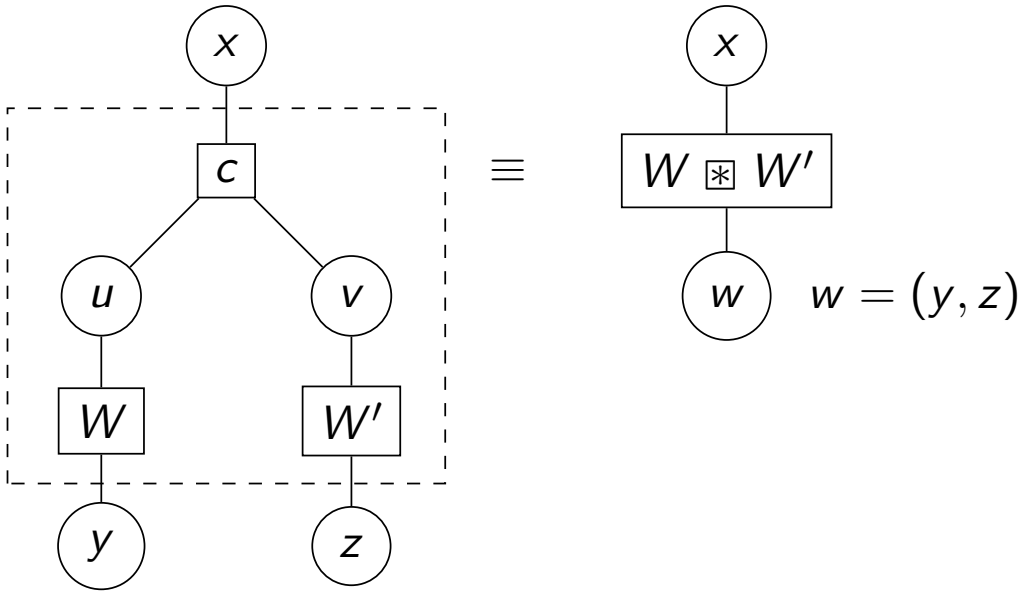
$$\text{At } x_1 \longrightarrow W(y_1|x_1) \cdot \left[\sum_{x_2, x_3 \in \{0,1\}^2} \mathbb{I}(x_1 \oplus x_2 \oplus x_3 = 0) W(y_2|x_2) W(y_3|x_3) \right]$$

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

Induced Channels in BP

Factor Node Convolution: The transition probabilities of this channel are

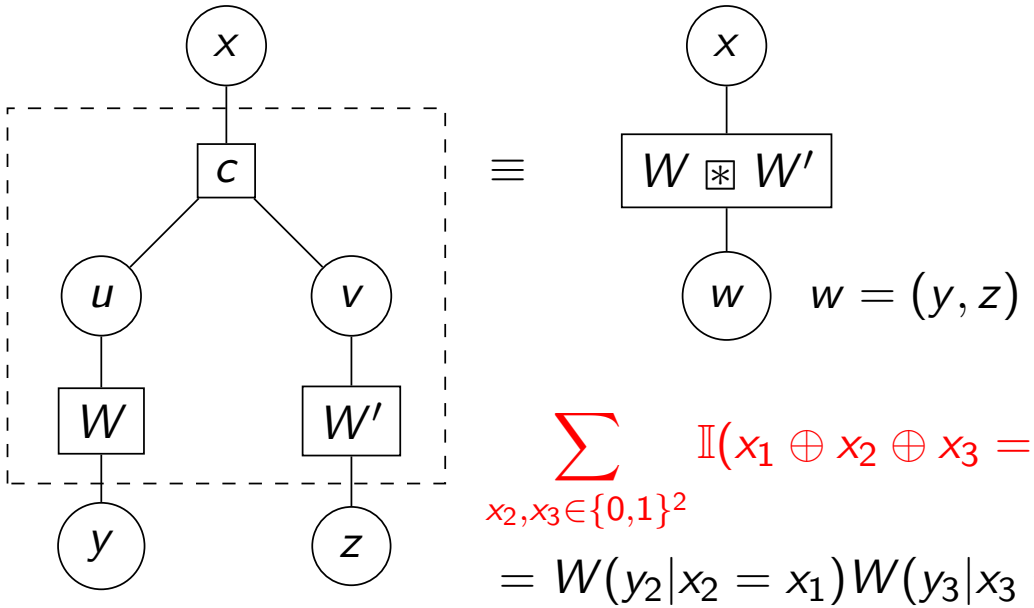
$$[W \circledast W'](y,z|x) = \frac{1}{2}W(y|u=x)\cdot W'(z|v=0) + \frac{1}{2}W(y|u=x\oplus 1)\cdot W'(z|v=1)$$
$$= \frac{1}{2}W(y|x)\cdot W'(z|0) + \frac{1}{2}W(y|x\oplus 1)\cdot W'(z|1)$$



Induced Channels in BP

Factor Node Convolution: The transition probabilities of this channel are

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



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

Generalized Channel Convolutions [Ren17; Ren18]

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

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

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

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

Generalized Channel Convolutions [Ren17; Ren18]

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

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

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

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

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

Overview

1. Synthesizing Logical Operators for Stabilizer Codes
   - Motivation and Strategy
   - Logical Clifford Synthesis (LCS)
   - Quadratic Form Diagonal (QFD) Gates
   - Stabilizer Codes Matched to QFD Gates

2. Classical Communications over Pure-State Channels
   - Introduction and Motivation
   - Classical Belief-Propagation (BP)
   - Belief-Propagation with Quantum Messages (BPQM)

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

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

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

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]

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

Helstrom Measurement [Hel69; HLG70]

An optimal measurement to distinguish between any two states ρ_0, ρ_1. It is defined by the projectors $\{\Pi_{\text{Hel}}, \mathbb{I} - \Pi_{\text{Hel}}\}$:

$$\Pi_{\text{Hel}} := \sum_{i\,:\,\lambda_i \geq 0} |i\rangle\langle i|, \quad (\rho_0 - \rho_1)\,|i\rangle = \lambda_i\,|i\rangle\,.$$

For the pure state channel, for any θ, easy to see that

$$\rho_0 - \rho_1 = |\theta\rangle\langle\theta| - |-\theta\rangle\langle-\theta| = \sin\theta \cdot X,$$

so the Helstrom measurement is projecting onto the Pauli X basis, i.e., the projectors are $\{|+\rangle\langle+|, |-\rangle\langle-|\}$.

Helstrom Measurement [Hel69; HLG70]

An optimal measurement to distinguish between any two states ρ_0, ρ_1. It is defined by the projectors $\{\Pi_{\text{Hel}}, \mathbb{I} - \Pi_{\text{Hel}}\}$:

$$\Pi_{\text{Hel}} := \sum_{i\,:\,\lambda_i \geq 0} |i\rangle\langle i|, \quad (\rho_0 - \rho_1)\,|i\rangle = \lambda_i\,|i\rangle\,.$$

For the pure state channel, for any θ, easy to see that

$$\rho_0 - \rho_1 = |\theta\rangle\langle\theta| - |-\theta\rangle\langle-\theta| = \sin\theta \cdot X,$$

so the Helstrom measurement is projecting onto the Pauli X basis, i.e., the projectors are $\{|+\rangle\langle+|, |-\rangle\langle-|\}$. Optimal error probability: ([Dol73])

$$P_{\text{min}} = \frac{1}{2} - \frac{1}{4}\|\rho_0 - \rho_1\|_1 = \frac{1 - \sqrt{1 - F(W)}}{2} = \frac{1 - \sin\theta}{2}.$$

Hence, the Helstrom measurement induces the channel BSC(P_{min}).

Optimal Processing for Pure-State Channel

Capacity under symbol-by-symbol Helstrom Measurement:

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

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

Classical-Quantum Polar Codes close this gap but the quantum successive cancellation decoder is infeasible to realize in practice [WG13].

Optimal Processing for Pure-State Channel

Capacity under symbol-by-symbol Helstrom Measurement:

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

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

Classical-Quantum Polar Codes close this gap but the quantum successive cancellation decoder is infeasible to realize in practice [WG13].

1. Is it possible to define a quantum BP decoder that closes this gap?

2. Given a code, how to define quantum BP for optimal 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?

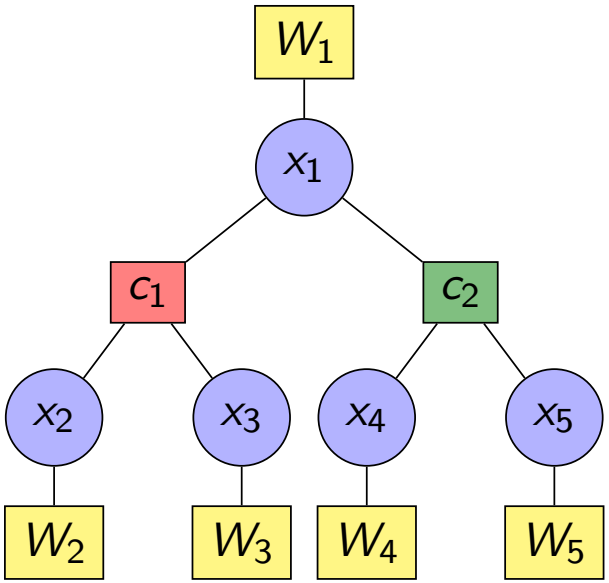
BPQM on the 5-bit Code

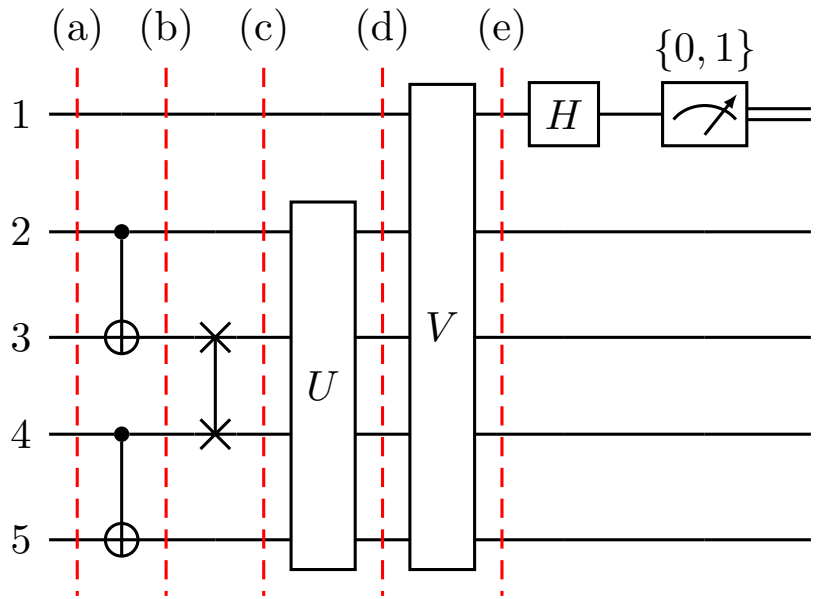
BPQM Node Operations:

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

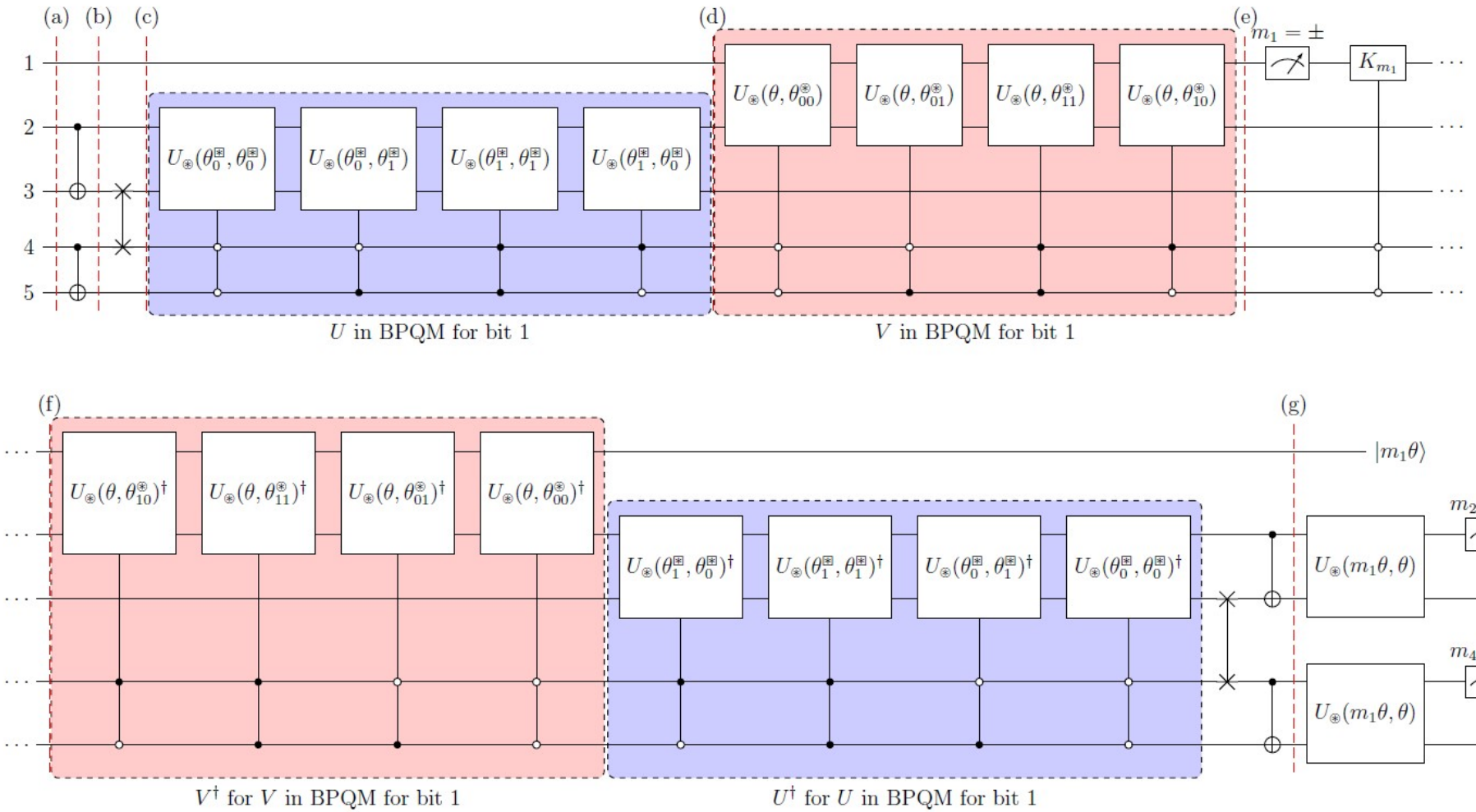
$$U_{\boxplus}\left([W \boxplus W'](x)\right)U_{\boxplus}^{\dagger} = \sum_{j\in\{0,1\}} p_j \left|\pm\theta_j^{\boxplus}\right\rangle\left\langle\pm\theta_j^{\boxplus}\right| \otimes |j\rangle\langle j|$$

Apply BPQM operations to decode bit x_1 of the code:



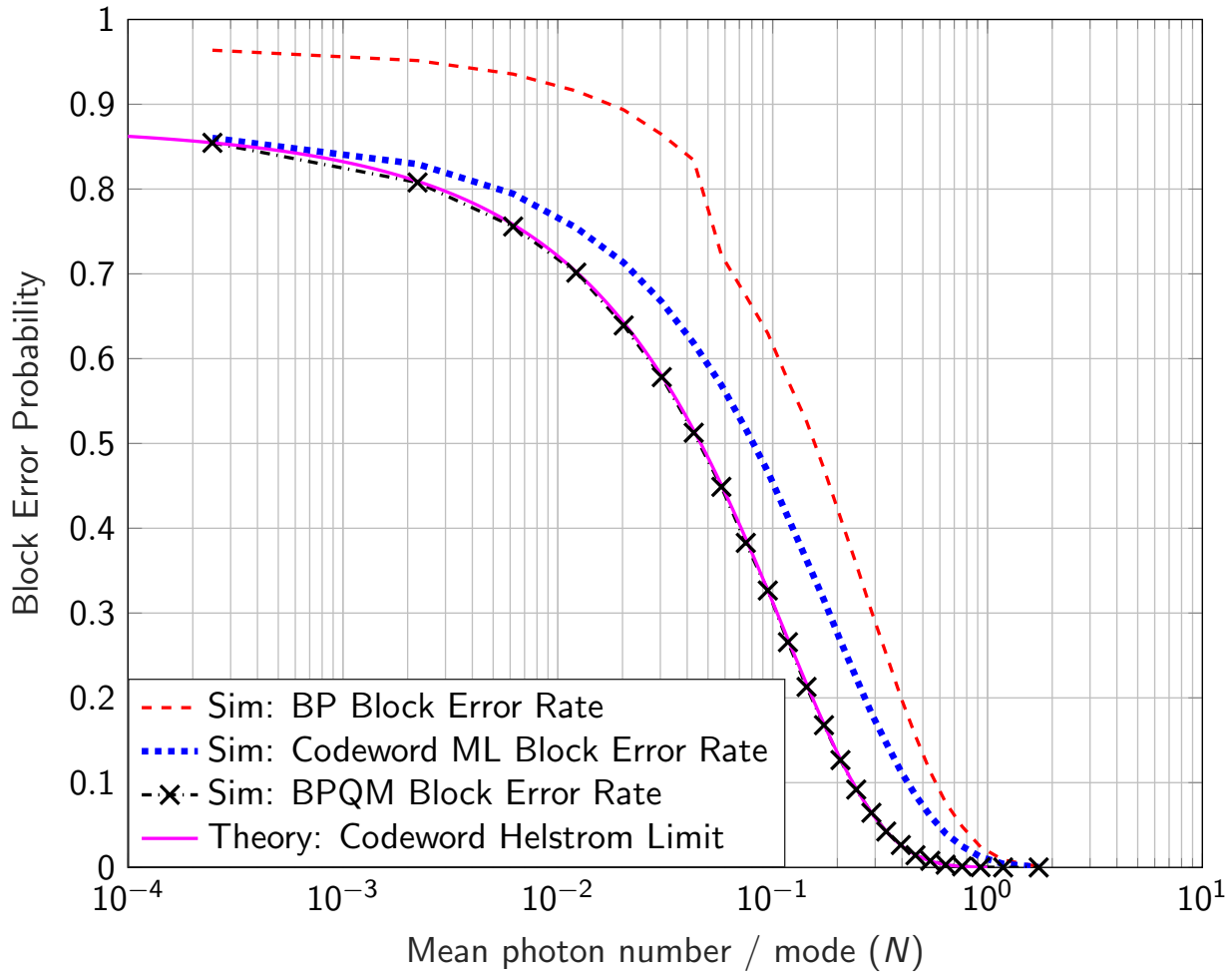


Full BPQM Circuit for the 5-bit Code



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 be quantum optimal 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 be quantum optimal for the 5-bit code
- Prove BPQM optimality for codes with tree factor graphs?
- Does the 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.

[Dol73] S.J. Dolinar Jr. "An Optimum Receiver for the Binary Coherent State Quantum Channel". In: *MIT Res. Lab. Electron. Q. Prog. Rep.* 111 (1973), pp. 115–120. URL: https://dspace.mit.edu/bitstream/handle/1721.1/56414/RLE%7B%5C_%7DQPR%7B%5C_%7D111%7B%5C_%7DVII.pdf?sequence=1.

References

[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.

[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.

References

[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.

[Can+19] Trung Can et al. "Kerdock Codes Determine Unitary 2-Designs". In: *Submitted to IEEE Trans. Inf. Theory, preprint arXiv:1904.07842* (2019). [Online]. Available: http://arxiv.org/abs/1904.07842.

References

[RCP19] Narayanan Rengaswamy, Robert Calderbank, and Henry D. Pfister. "Unifying the Clifford Hierarchy via Symmetric Matrices over Rings". In: *Phys. Rev. A* 100.2 (2019), p. 022304. DOI: 10.1103/PhysRevA.100.022304. URL: http://arxiv.org/abs/1902.04022.

[Ren+19a] Narayanan Rengaswamy et al. "Logical Clifford Synthesis for Stabilizer Codes". In: *arXiv preprint arXiv:1907.00310* (2019). URL: http://arxiv.org/abs/1907.00310.

[Ren+19b] Narayanan Rengaswamy et al. "On Optimality of CSS Codes for Transversal T". In: *arXiv preprint arXiv:1910.09333* (2019). URL: http://arxiv.org/abs/1910.09333.

[Ren+20] Narayanan Rengaswamy et al. "Quantum-Message-Passing Receiver for Quantum-Enhanced Classical Communications". In: *arXiv preprint arXiv:2003.04356* (2020). URL: http://arxiv.org/abs/2003.04356.

Thank you!

LCS Algorithm: https://arxiv.org/abs/1907.00310
Code at https://github.com/nrenga/symplectic-arxiv18a

QFD Gates: https://arxiv.org/abs/1902.04022

CSS-T Codes: https://arxiv.org/abs/1910.09333

Kerdock 2-Design: https://arxiv.org/abs/1904.07842
Code at https://github.com/nrenga/symplectic-arxiv18a

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