Algebraic Coding Problems from Quantum Fault Tolerance

Application-Driven Coding Theory Workshop
March 5, 2024
Simons Institute, UC Berkeley, CA

NARAYANAN RENGASWAMY
DEPT. OF ELECTRICAL AND COMPUTER ENGINEERING
UNIVERSITY OF ARIZONA
Quantum Circuits

Universal set of “gates”

$k = 1$ qubit

$k = 3$ qubits
QEC: Quantum Error Correction

Universal set of “gates”

$H$

$T$

$k$ qubits $|\psi\rangle_L$

$\langle \psi \rangle$

$n$ qubits

Noisy Logical gates

Translate (Synthesize)

Physical gates

Fault-tolerant

$|\phi\rangle_L$

$|\phi\rangle$

Non-Clifford gate

QECC: Quantum Error Correcting Code

QECC: Quantum Error Correcting Code

Universal set of “gates”

$H$

$T$

$k$ qubits $|\psi\rangle_L$

$\langle \psi \rangle$

$n$ qubits

Noisy Logical gates

Translate (Synthesize)

Physical gates

Fault-tolerant

$|\phi\rangle_L$

$|\phi\rangle$

Non-Clifford gate

QECC: Quantum Error Correcting Code
QEC: Syndrome-Based Error Correction

\[ |\psi\rangle = \alpha |0\rangle + \beta |1\rangle \]

\[ k = 1 \]

Logical Qubit

\[ |00\rangle \]

Physical Qubits

\[ n = 3 \]

Measure the stabilizer generators

\[ S_1 = ZZI \] and \[ S_2 = IZZZ \]

\[ +1\text{-Eigenvectors of} \]

\[ S_1 |\psi\rangle = |\psi\rangle , \quad S_2 |\psi\rangle = |\psi\rangle \]
Towards QEC with Constant Overhead

**Topological Codes** | **Optimal QLDPC Codes**
---|---

\([[[n, 1, \Theta(\sqrt{n})]]\) | \([[[n, \Theta(n), \Theta(n)]]\)

High error thresholds | Promising thresholds

\(~\) Linear-time decoder | Linear-time decoder*

Logical gates known | Very little research

Nearest-neighbor | Long-range interactions

**Not scalable; large overhead** | Scalable with constant overhead???

QLDPC: Quantum Low-Density Parity-Check

- vertex checks \((H_X)\)
- plaquette checks \((H_Z)\)
Calderbank-Shor-Steane (CSS) Codes

\[
[n, k_Z, d_Z] \quad C_Z \xrightarrow{\text{LDPC}} \quad [n, k_X, d_X] \quad C_X
\]

X-logicals
\[\bar{X} \equiv G_Z/H_X\]
\[X\]-logicals
\[\bar{X} \equiv G_Z/H_X\]
\[Z\]-logicals
\[\bar{Z} \equiv G_X/H_Z\]
\[C_X^\perp \]
\[C_Z^\perp \]

X-stabilizers
\[H_X\]
\[\langle 0 \rangle\]
\[Z\]-stabilizers
\[H_Z\]
\[\langle 0 \rangle\]

How to implement logical non-Clifford gate fault-tolerantly?

\[
H_S = \begin{bmatrix} H_X & 0 \\ 0 & H_Z \end{bmatrix}
\]

\[H_X H_Z^T = 0\]

\[k = n - \text{rank}(H_X) - \text{rank}(H_Z)\]

\[d = \text{minimum weight of } \bar{X}, \bar{Z}\]
Magic State Distillation and Injection

“Triorthogonal” Codes: https://arxiv.org/abs/1209.2426
Triorthogonal Codes

\[
\begin{bmatrix}
C_Z \mid C_X \\
\tilde{X} \mid \tilde{Z} \\
C_H \perp C_Z \perp H_Z \\
\langle 0 \rangle \mid \langle 0 \rangle
\end{bmatrix}
\]

\([15,1,3]\) Code: Transversal \(T\) induces logical \(T^\dagger\)

\[
H_X =
\begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & x_1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & x_2 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & x_3 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & x_4
\end{bmatrix}
\]

\[
H_Z =
\begin{bmatrix}
1 & 1 & 1 & 1 & 1 & x_1 x_2 \\
1 & 1 & 1 & 1 & 1 & x_1 x_3 \\
1 & 1 & 1 & 1 & 1 & x_1 x_4 \\
1 & 1 & 1 & 1 & 1 & x_2 x_3 \\
1 & 1 & 1 & 1 & 1 & x_2 x_4 \\
1 & 1 & 1 & 1 & 1 & x_3 x_4
\end{bmatrix}
\]

\(C_Z = \text{Punctured RM}(1,4)\)

\(C_X = [15,11,3]\) Hamming

\(C_Z^\perp = \text{Even weight subcode}\)

\(C_X^\perp = [15,4,8]\) Simplex

“Triorthogonal” Codes: https://arxiv.org/abs/1209.2426
Transversal $T$: Naturally Fault-Tolerant

When does this preserve the CSS code space?

Consider the projector $\Pi_S$ to the code space. For transversal $T$ to fix the code space, we need

$$T \otimes^n \Pi_S (T \otimes^n)^\dagger = \Pi_S.$$ 

Solving this equality leads to necessary and sufficient conditions that the code must meet.

Transversal $T$: Classical Coding Problem

**“CSS-T” Problem for Quantum Codes**

Construct pair $(C_Z, C_X)$ of classical codes s.t.:

1. All codewords of $C_X^\perp$ have even Hamming weight

2. For each $x \in C_X^\perp$, the code $C_Z^\perp$ contains a self-dual code $Z_x$ supported only on $x \in C_X^\perp$

$(Z_x$ is essentially a $[w_H(x), \frac{w_H(x)}{2}]$ self-dual code)

CSS-T Example 1

Construct pair \((C_Z, C_X)\) of classical (LDPC) codes s.t.:
1. All codewords of \(C_X^\perp\) have even Hamming weight
2. For each \(x \in C_X^\perp\), the code \(C_Z^\perp\) contains a self-dual code \(Z_x\) supported only on \(x \in C_X^\perp\)

\[\text{[[8,3,2]] Code: Transversal } T \text{ induces logical } CCZ\]

\[H_X = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}\]

8-bit Repetition

\[H_Z = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}\]

Reed-Muller RM(1,3)
a.k.a.
Extended Hamming
CSS-T Example 2 (Triorthogonal Code)

$$\begin{array}{|c|c|}
\hline
C_Z & C_X \\
\hline
\tilde{X} & \tilde{Z} \\
\hline
C_Z^\perp & C_X^\perp \\
\hline
H_X & H_Z \\
\hline
\langle 0 \rangle & \langle 0 \rangle \\
\hline
\end{array}$$

$[[15,1,3]]$ Code: Transversal $T$ induces logical $T^\dagger$

$$H_Z = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\end{bmatrix}$$

$$H_X = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\end{bmatrix}$$

- $C_Z = \text{Punctured RM}(1,4)$
- $C_X = [[15,11,3]] \text{ Hamming}$
- $C_Z^\perp = \text{Even weight subcode}$
- $C_X^\perp = [[15,4,8]] \text{ Simplex}$

CSS-T Example 3

[[16,3,2]] Code: Transversal $T$ induces logical $CCZ$

$H_X = \{1, x_1, x_2\}$

$G_Z = H_X \cup \{x_3, x_4, x_1x_2\}$

$H_Z = G_Z \cup \{x_1x_3, x_1x_4, x_2x_3, x_2x_4\}$

$G_X = H_Z \cup \{x_3x_4, x_1x_2x_3, x_1x_2x_4\}$

Related Work (Partial List)

Magic state distillation with low overhead
Sergey Bravyi\textsuperscript{1} and Jeongwan Haah\textsuperscript{2}

Codes and Protocols for Distilling $T$, controlled-$S$, and Toffoli Gates
Jeongwan Haah\textsuperscript{1} and Matthew B. Hastings\textsuperscript{2,1}

Towers of generalized divisible quantum codes
Jeongwan Haah\textsuperscript{*}

Classification of Small Triorthogonal Codes
Sepehr Nezami\textsuperscript{1} and Jeongwan Haah\textsuperscript{2}

Quantum Pin Codes
Christophe Vuillot and Nikolas P. Breuckmann

Divisible Codes for Quantum Computation
Jingzhen Hu\textsuperscript{*}, Qingzhong Liang\textsuperscript{*}, and Robert Calderbank

CSS-T Codes From Reed Muller Codes
Emma Andrade\textsuperscript{1}, Jessalyn Bolkema\textsuperscript{2}, Thomas Dexter\textsuperscript{3}, Harrison Eggers\textsuperscript{4}, Victoria Luongo\textsuperscript{4}, Felice Manganiello\textsuperscript{4}, and Luke Szramowski\textsuperscript{1}

THE POSET OF BINARY CSS-T QUANTUM CODES AND CYCLIC CODES
EDUARDO CAMPS-MORENO, HIRAM H. LÓPEZ, GRETCHEN L. MATTHEWS, DIEGO RUANO, RODRIGO SAN-JOSÉ, AND IVAN SOPRUNOV

Classical Coding Theorists!
CSS-T: Search for Good Codes

Construct pair \((C_Z, C_X)\) of classical (LDPC) codes s.t.:
1. All codewords of \(C_X^\perp\) have even Hamming weight
2. For each \(x \in C_X^\perp\), the code \(C_Z^\perp\) contains a self-dual code \(Z_x\) supported only on \(x \in C_X^\perp\)

\([n, k, d]\) CSS-T Codes:
1. **Current solution:** polynomial evaluation codes
2. **Problem:** high-weight checks, poor parameters
3. **Towards optimality:** need \(k = \Theta(n)\), \(d = \Theta(n)\)
4. **Practicality:** need both \(C_Z\) and \(C_X\) to be LDPC
1st Quantum Information Knowledge (QuIK) Workshop

- **Date:** July 7, 2024 @ ISIT (full day)
- **Venue:** Athens, Greece
- **Theme:** Quantum Error Correction
- **Goal:** Interactions between QEC community and coding theorists
- **Components:** Tutorial, Invited Talks, Poster Session, Panel Discussion
- **Submit posters by 3/17!!**

Details: [https://isit-quik24.com](https://isit-quik24.com)
Thank you!


narayananr@arizona.edu
https://ece.arizona.edu
https://cqn-erc.org
https://sqmscenter.fnal.gov/