Clifford Circuits for Encoded Quantum Gates with Low Error Spread

Todd A. Brun and R. Scout Kingery
tbrun@usc.edu and kingery@usc.edu

USC Viterbi School of Engineering
Ming Hsieh Department of Electrical Engineering

Abstract

It may be possible to utilize certain families of block codes for fault-tolerant quantum computation. For this to be done, we must be capable of implementing encoded logical operations such that small, single errors in the input do not spread to large, uncorrectable errors in the output. To this end we develop a linear algebraic representation for these Clifford circuits and explore the relationships between the distinct circuits for a given encoded quantum gate. In addition to the analytical description, we consider numerical methods to determine useful circuits and test these methods on small codes.

Describing a Logical Operation

Using the symplectic representation [1, 2], we may describe a code by writing its stabilizer generators, g_i, symplectic partners, h_i, and logical operators, $\overline{X}_i$ and $\overline{Z}_i$, as rows in a $2n \times 2n$ binary matrix:

$$M = \begin{pmatrix} h_1 \\ \vdots \\ h_{n-k} \\ \overline{X}_1 \\ \vdots \\ \overline{X}_k \\ g_1 \\ \vdots \\ g_{n-k} \\ \overline{Z}_1 \\ \vdots \\ \overline{Z}_k \end{pmatrix}$$

for example, the Steane code will have the matrix

$$M = \left(\begin{array}{ccccccc|ccccccc} 0&0&0&0&0&0&0&0&0&0&0&0&1&1 \\ 0&0&0&0&0&0&0&0&0&0&0&1&0&1 \\ 0&0&0&0&0&0&0&0&0&0&1&0&0&1 \\ 0&1&1&1&1&1&1&0&0&0&0&0&0&0 \\ 1&0&1&1&1&1&1&0&0&0&0&0&0&0 \\ 1&1&0&1&1&1&1&0&0&0&0&0&0&0 \\ 1&1&1&1&1&1&1&0&0&0&0&0&0&0 \\ 1&0&0&1&1&0&1&0&0&0&0&0&0&0 \\ 0&1&0&1&0&1&1&0&0&0&0&0&0&0 \\ 0&0&1&0&1&1&1&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&1&0&0&1&1&0&1 \\ 0&0&0&0&0&0&0&0&1&0&1&0&1&1 \\ 0&0&0&0&0&0&0&0&0&1&0&1&1&1 \\ 0&0&0&0&0&0&0&1&1&1&1&1&1&1 \end{array}\right)$$

Thus an encoded gate may be described by the transformation

$$M \longrightarrow M' = RMC$$

where C acts on the columns of M, representing the Clifford circuit acting on the physical qubits, and R acts on the rows of M, representing purely mental operations that do not affect the code itself.

The Canonical Code

If our information is stored in the k-qubit state, $|\psi\rangle$, then before encoding, our "codeword" is the state

$$|\Psi\rangle = |0\rangle^{\otimes n-k} \otimes |\psi\rangle$$

and our "code" is described by the matrix

$$M_0 = \left(\begin{array}{cc|cc} I_{n-k} & 0 & 0 & 0 \\ 0 & I_k & 0 & 0 \\ 0 & 0 & I_{n-k} & 0 \\ 0 & 0 & 0 & I_k \end{array}\right) \equiv I_{2n}$$

The encoding Clifford circuit, described by column operations on M_0, will have the effect

$$M = R_E M_0 C_E = R_E C_E$$

and we get back to the canonical code by

$$M_0 = R_E^{-1} M C_E^{-1}$$

So for the canonical code, the Clifford operation is the simple Clifford circuit

$$M_0' = M_0 C_0$$

which is equivalent to

$$M_0' = R_E^{-1} M' C_E^{-1} = R_E^{-1} RMC C_E^{-1} = R_E^{-1} R R_E M_0 C_E C C_E^{-1} \equiv R' M_0 C'$$

which implies that

$$C = C_E^{-1} (R')^{-1} C_0 C_E$$

That is, all circuits describing an encoded logical operation differ from the simple Clifford circuit only by some allowable row operations, $(R')^{-1}$.

References

[1] Calderbank, A R and Rains, E M and Shor, P W and Sloane, N J A. *Quantum Error Correction and Orthogonal Geometry.* arXiv.org, quant-ph, May 1996.

[2] Daniel Gottesman. *Stabilizer Codes and Quantum Error Correction.* arXiv.org, quant-ph, February 1997

[3] Mark M Wilde. *Qantum Coding with Entanglement.* arXiv.org, quant-ph, June 2008.

Row Operations

Row operations must preserve the code: the stabilizer generators may change so long as they generate the same group, and the logical operators may be multiplied by an element of the stabilizer. Row operations must preserve the commutation relations, which is equivalent to satisfying $RJR^T = J$, where

$$J = \left(\begin{array}{c|c} 0 & I_n \\ I_n & 0 \end{array}\right)$$

In general, R has the form

$$R = \left(\begin{array}{cc|cc} A_1 & Q_1 & A_2 & Q_2 \\ 0 & I_k & R_1 & 0 \\ 0 & 0 & B & 0 \\ 0 & 0 & R_2 & I_k \end{array}\right)$$

such that

$$\begin{aligned} A_1 &= (B^T)^{-1} \\ Q_1 &= (B^T)^{-1} R_2^T \\ Q_2 &= (B^T)^{-1} R_1^T \\ A_2 &= (B^T)^{-1} R_1^T R_2 + SB. \end{aligned}$$

The Spread of Errors

We write all single qubit errors in the matrix

$$E = \left(\begin{array}{c|c} I_n & 0 \\ 0 & I_n \\ I_n & I_n \end{array}\right)$$

A given encoded operation, C, may spread these single qubit errors to multiple qubit errors. This spread is given by the weight of the Pauli operators represented by the rows of the matrix EC.

Examples

Consider a simple $[[4, 2, 2]]$ error-detecting code encoding 2 qubits into 4:

$$M = \left(\begin{array}{cccc|cccc} 0&0&0&1&0&0&0&0 \\ 0&0&0&0&1&1&1&0 \\ 1&1&0&0&0&0&0&0 \\ 1&0&1&0&0&0&0&0 \\ 0&0&0&0&1&1&1&1 \\ 1&1&1&1&0&0&0&0 \\ 0&0&0&0&1&0&1&0 \\ 0&0&0&0&1&1&0&0 \end{array}\right)$$

An encoded Hadamard on logical qubit 1 results in a swap of $\overline{X}_1$ and $\overline{Z}_1$:

$$M' = RMC_{H_1} = \left(\begin{array}{cccc|cccc} 0&0&0&1&0&0&0&0 \\ 0&0&0&0&1&1&1&0 \\ 0&0&0&0&1&0&1&0 \\ 1&0&1&0&0&0&0&0 \\ 0&0&0&0&1&1&1&1 \\ 1&1&1&1&0&0&0&0 \\ 1&1&0&0&0&0&0&0 \\ 0&0&0&0&1&1&0&0 \end{array}\right)$$

One such circuit, with maximum spread 3 and average spread 2 is given by

$$C_{H_1} = \begin{pmatrix} 0&1&0&0&1&0&1&0 \\ 0&1&0&0&0&0&0&0 \\ 1&1&1&0&1&0&1&0 \\ 0&0&0&1&0&0&0&0 \\ 1&1&0&0&0&0&1&0 \\ 1&1&0&0&1&1&1&0 \\ 0&0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&0&1 \end{pmatrix}$$

Numerical Solutions

For small codes one may search over the space of all encodings, C, by iterating through all allowable row operations $(R')^{-1}$. However this has a prohibitive exponential time complexity.

The space of solutions is rife with local minima, and thus an iterative descent method does not converge on the optimal solution for all but the smallest codes. We have considered simulated annealing and genetic algorithms to find good solutions for larger codes, though these approaches require further development.

Future Work

- Further explore optimization methods to search for good solutions.
- Find an efficient algorithm to extract the Clifford circuit for a given matrix C [3].
- Include a non-Clifford gate for universal quantum computation.
- Explore code families and look for analytical solutions for encoded Clifford operations.
- Search for efficient encodings of common sub-circuits which may have improved spread over encoding each operation separately.