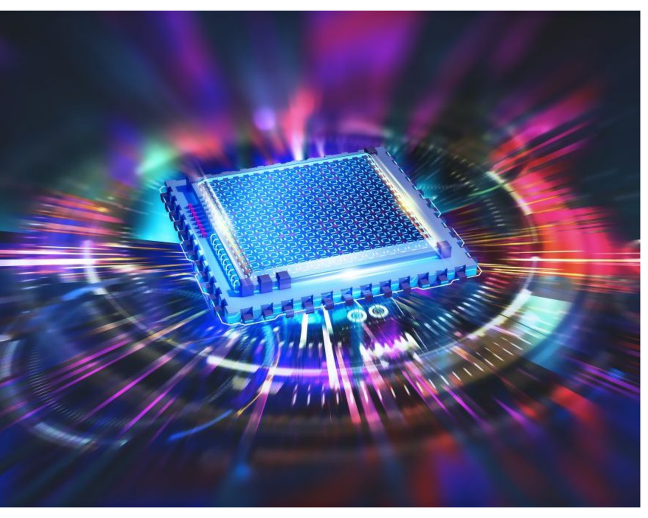
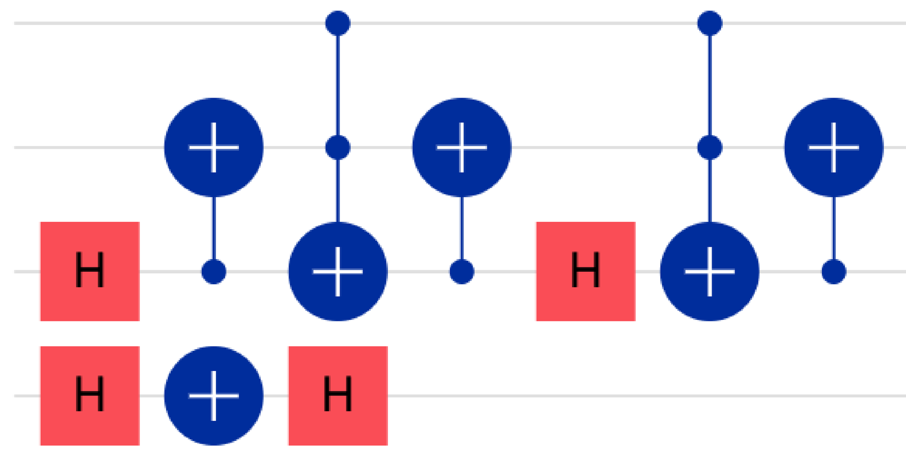


Improved Synthesis of Restricted Clifford+T Circuits

Sarah Meng Li[1] · Neil J. Ross[2]

[1]Institute for Quantum Computing, University of Waterloo, Canada

[2]Department of Mathematics and Statistics, Dalhousie University, Canada



1. Background

Algorithm: Carrying out a well-defined task.

Compilation: Translating a program to a sequence of elementary quantum gates.

Implementation: Mapping unitary operations to physical architectures.

Restricted Clifford+T Circuits

Quantum circuits over the gate set $\{X, CX, CCX, K\}$.

The Circuit-Matrix Correspondence

- A family of quantum circuits corresponds to a group of matrices.
- Studying matrix groups is a way to study quantum circuits.

2. Preliminaries

The ring of dyadic fractions: $\mathbb{Z}[\frac{1}{2}] = \{\frac{u}{2^q} | u \in \mathbb{Z}, q \in \mathbb{N}\}$.

The group of orthogonal dyadic matrices: $\mathrm{O}_n(\mathbb{Z}[\frac{1}{2}])$, or $\mathcal{O}_n$.

Denominator exponent k: $t = \frac{a}{2^k} \in \mathbb{Z}[\frac{1}{2}]$, $a \in \mathbb{Z}$, $k \in \mathbb{N}$.

The least denominator exponent lde: The minimal k of t is $\mathbf{lde}(t)$.

Example: $U \in \mathcal{O}_5$, $\mathbf{lde}(U) = 2$.

$$U = \begin{bmatrix} 3/4 & 1/4 & -1/4 & 1/4 & 1/2 \\ 1/4 & 3/4 & 1/4 & -1/4 & -1/2 \\ -1/4 & 1/4 & 3/4 & 1/4 & 1/2 \\ 1/4 & -1/4 & 1/4 & 3/4 & -1/2 \\ -1/2 & 1/2 & -1/2 & 1/2 & 0 \end{bmatrix} = \frac{1}{2^2}\begin{bmatrix} 3 & 1 & -1 & 1 & 2 \\ 1 & 3 & 1 & -1 & -2 \\ -1 & 1 & 3 & 1 & 2 \\ 1 & -1 & 1 & 3 & -2 \\ -2 & 2 & -2 & 2 & 0 \end{bmatrix}$$

3. Basic Gates

$$(-1) = [-1], \quad H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad K = H \otimes H = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad CX = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = \left[\begin{array}{c|c} I_2 & 0 \\ \hline 0 & X \end{array}\right], \quad CCX = \left[\begin{array}{c|c} I_6 & 0 \\ \hline 0 & X \end{array}\right]$$

Two-level Operators: $U_{[\alpha,\beta]}$

Let $U = \begin{bmatrix} x_{1,1} & x_{1,2} \\ x_{2,1} & x_{2,2} \end{bmatrix}$. The action of $U_{[\alpha,\beta]}$, $1 \leq \alpha < \beta \leq n$, is defined as

$$U_{[\alpha,\beta]} v = w, \text{ where } \begin{cases} \begin{bmatrix} w_\alpha \\ w_\beta \end{bmatrix} = U \begin{bmatrix} v_\alpha \\ v_\beta \end{bmatrix}, \\ w_i = v_i, i \notin \{\alpha, \beta\}. \end{cases}$$

Example: Construct $X_{[2,3]}$ by embedding X into a 4×4 identity matrix.

$$X_{[2,3]} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \text{ such that } X_{[2,3]} \begin{bmatrix} v_1 \\ v_2 \\ v_3 \\ v_4 \end{bmatrix} = \begin{bmatrix} v_1 \\ v_3 \\ v_2 \\ v_4 \end{bmatrix}.$$

4. Constructive Membership Problem (CMP)

Let $\mathcal{G}$ be a group of matrices with entries over some ring, $S = \{a_1, \ldots, a_k\}$ be a set of generators for $\mathcal{G}$.

$\forall U \in \mathcal{G}$, find a sequence of generators $a_1, \ldots, a_\ell$ such that $a_1 \cdot \ldots \cdot a_\ell = U$.

- The smaller the ℓ, the better the solution.
- A solution is optimal if the sequence is a shortest possible sequence.
- The algorithm to solve CMP is called the **exact synthesis algorithm**.

The Circuit-Matrix Correspondence (Amy et al., 2020)

Let $\mathcal{T} = \{(-1)_{[\alpha]}, X_{[\alpha,\beta]}, K_{[\alpha,\beta,\gamma,\delta]} : 1 \leq \alpha < \beta < \gamma < \delta \leq n\}$.

- U can be exactly represented by a circuit over $\{X, CX, CCX, K\}$ iff $U \in \mathcal{O}_n$.
- U can be exactly represented by a circuit over $\mathcal{T}$ iff $U \in \mathcal{O}_n$.

5. The Local Synthesis Algorithm: $O(2^n k)$

Input: $v \in \mathbb{Z}[\frac{1}{2}]^8$ Output: G_1, G_2, G_3 Result: $G_3 \cdot G_2 \cdot G_1 \cdot v = e_1$

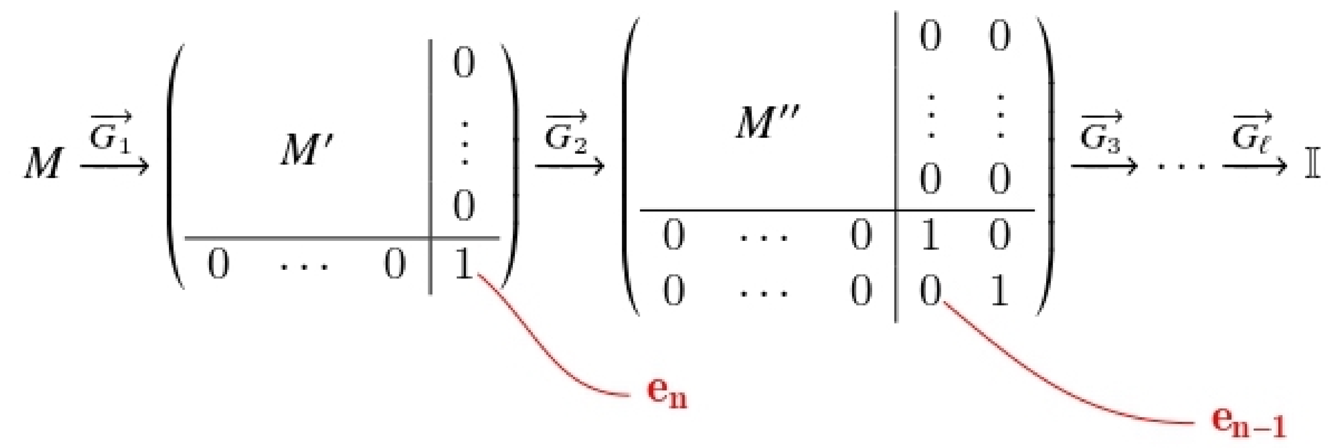
$$v : \frac{1}{4}\begin{pmatrix} -1 \\ 1 \\ -1 \\ -1 \\ 3 \\ 1 \\ 1 \\ 1 \end{pmatrix} \xrightarrow{G_1 = K_{[1,2,3,4]}(-1)_{[4]}(-1)_{[3]}(-1)_{[1]}} v' : \frac{1}{4}\begin{pmatrix} 2 \\ 0 \\ 0 \\ 0 \\ 3 \\ 1 \\ 1 \\ 1 \end{pmatrix} \xrightarrow{G_2 = K_{[5,6,7,8]}(-1)_{[5]}}$$

$\mathrm{lde}(v) = 2$ $\mathrm{lde}(v') = 2$

$$v'' : \frac{1}{4}\begin{pmatrix} 2 \\ 0 \\ 0 \\ 0 \\ 0 \\ -2 \\ -2 \\ -2 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ -1 \\ -1 \\ -1 \end{pmatrix} \xrightarrow{G_3 = K_{[1,6,7,8]}(-1)_{[8]}(-1)_{[7]}(-1)_{[6]}} v''' : \frac{1}{2}\begin{pmatrix} 2 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = e_1.$$

$\mathrm{lde}(v'') = 1$ $\mathrm{lde}(v''') = 0$

- The algorithm proceeds one column at a time, reducing each column to a corresponding basis vector.
- While outputting a word $\overrightarrow{G_\ell}$ after each iteration, the algorithm recursively acts on the input matrix until it is reduced to the identity matrix $\mathbb{I}$.



$$\overrightarrow{G_\ell} \cdot \ldots \cdot \overrightarrow{G_1} M = \mathbb{I} \Rightarrow M = \overrightarrow{G_1}^{-1} \cdot \ldots \cdot \overrightarrow{G_\ell}^{-1}$$

6. The Global Synthesis Algorithm for $\mathcal{L}_8 : O(k)$

Define a global synthesis for $\mathcal{L}_8$. Then, leverage this to find a global synthesis for $\mathcal{O}_8$.

Orthogonal Scaled Dyadic Matrices

$\mathcal{L}_8$ is the group of 8×8 orthogonal matrices of the form $M/\sqrt{2}^k$, where M is an integer matrix and k is a nonnegative integer.

- $\mathcal{O}_8 \subset \mathcal{L}_8$.
- $\mathcal{F} = \{(-1)_{[\alpha]}, X_{[\alpha,\beta]}, I_4 \otimes H : 1 \leq \alpha < \beta \leq 8\}$ generates $\mathcal{L}_8$.
- Let $U \in \mathcal{L}_n$. Write $U = \frac{1}{\sqrt{2}^k} M$ with k minimal. The residue mod 2 of M is called the **binary pattern** of U, denoted as $\overline{U}$.

Example: $U, V \in \mathcal{L}_8$, $U \in \mathcal{O}_8$, but $V \notin \mathcal{O}_8$

$$U = \frac{1}{\sqrt{2}^2}\begin{bmatrix} 1 & -1 & -1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & 1 \end{bmatrix}, \quad \overline{U} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}, \quad V = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 0 & -1 & 0 \\ 0 & -1 & 0 & -1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix}$$

Weight Lemma: Let $U \in \mathcal{L}_n$ and $\mathbf{lde}_{\sqrt{2}}(U) = k \geq 2$. Let u be an arbitrary column vector in $\overline{U}$. Then $|\{u_i; u_i = 1, 1 \leq i \leq n\}| \equiv 0(4)$. In other words, in each column of $\overline{U}$, the 1's occur in quadruples.

Collision Lemma: Let $U \in \mathcal{L}_n$ and $\mathbf{lde}_{\sqrt{2}}(U) = k > 0$. Any two distinct columns in $\overline{U}$ must have evenly many 1's in common.

Pattern Theorem: There exists a set $\mathcal{P}$ of 14 binary patterns such that if $U \in \mathcal{L}_8$ and $\mathbf{lde}(U) \geq 2$, $\overline{U} \in \mathcal{P}$.
Up to row and column permutations, as well as taking transpose.

- Patterns $A \sim K$ are either row-paired or column-paired.
  $\exists P \in S_8$ such that $\mathbf{lde}_{\sqrt{2}}(U(P(I \otimes H))) < \mathbf{lde}_{\sqrt{2}}(U)$.

$$A = \begin{bmatrix} 1&1&1&1&1&1&1&1 \\ 1&1&1&1&1&1&1&1 \\ 1&1&1&1&1&1&1&1 \\ 1&1&1&1&1&1&1&1 \\ 1&1&1&1&1&1&1&1 \\ 1&1&1&1&1&1&1&1 \\ 1&1&1&1&1&1&1&1 \\ 1&1&1&1&1&1&1&1 \end{bmatrix}, \quad B = \begin{bmatrix} 1&1&1&1&1&1&1&1 \\ 1&1&1&1&1&1&1&1 \\ 1&1&1&1&1&1&1&1 \\ 1&1&1&1&1&1&1&1 \\ 1&1&1&1&0&0&0&0 \\ 1&1&1&1&0&0&0&0 \\ 1&1&1&1&0&0&0&0 \\ 1&1&1&1&0&0&0&0 \end{bmatrix}, \ldots, K = \begin{bmatrix} 1&1&1&1&1&1&1&1 \\ 1&1&1&1&1&1&1&1 \\ 1&1&1&1&1&1&1&1 \\ 1&1&1&1&1&1&1&1 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \end{bmatrix}$$

- Patterns $L \sim N$ are neither row-paired nor column-paired.
  Let $U' = (I \otimes H)\, U\, (I \otimes H)$. $\overline{U'}$ is row-paired with $\mathbf{lde}_{\sqrt{2}}(U') \leq \mathbf{lde}_{\sqrt{2}}(U)$.

$$L = \begin{bmatrix} 1&1&1&1&1&1&1&1 \\ 1&1&1&1&0&0&0&0 \\ 1&1&0&0&1&1&0&0 \\ 1&1&0&0&0&0&1&1 \\ 1&0&1&0&1&0&1&0 \\ 1&0&1&0&0&1&0&1 \\ 1&0&0&1&1&0&0&1 \\ 1&0&0&1&0&1&1&0 \end{bmatrix}, \quad M = \begin{bmatrix} 1&1&1&1&0&0&0&0 \\ 1&1&0&0&1&1&0&0 \\ 1&0&1&0&1&0&1&0 \\ 1&0&0&1&0&1&1&0 \\ 0&1&1&0&1&0&0&1 \\ 0&1&0&1&0&1&0&1 \\ 0&0&1&1&0&0&1&1 \\ 0&0&0&0&1&1&1&1 \end{bmatrix}, \quad N = \begin{bmatrix} 1&1&1&1&0&0&0&0 \\ 1&1&0&0&1&1&0&0 \\ 1&0&1&0&1&0&1&0 \\ 1&0&0&1&0&1&1&0 \\ 0&1&1&0&0&1&1&0 \\ 0&1&0&1&1&0&1&0 \\ 0&0&1&1&1&1&0&0 \\ 0&0&0&0&0&0&0&0 \end{bmatrix}$$

7. The Global Synthesis Algorithm for $\mathcal{O}_8 : O(k)$

Intuition: Commuting $I \otimes H$ with an element in $\mathcal{T}$ adds $O(1)$ gates.

$$\begin{aligned} (I \otimes H)(I \otimes H) &= \epsilon \\ (I \otimes H)(-1)_{[1]} &= (-1)_{[1]} X_{[1,2]} (-1)_{[1]} (I \otimes H) \\ (I \otimes H) X_{[a,a+1]} &= (-1)^{a+1}_{[a+1]} X^a_{[a,a+1]} K^a_{[a-1,a,a+1,a+2]} (I \otimes H) \\ (I \otimes H) K_{[1,2,3,4]} &= K_{[1,2,3,4]} (I \otimes H) \end{aligned}$$