Number-Theoretic Characterizations of Some Restricted Clifford+T Circuits

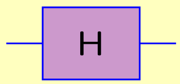
QPL 2020

M. Amy, A. N. Glaudell, & N. J. Ross

I. The Clifford+T Gate Set and its Restrictions

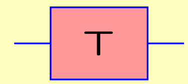
The Clifford+T Gate Set

Let $\omega = e^{i\pi/4} = (1+i)/\sqrt{2}$. The *Clifford+T gate set* consists of the H and T gates below



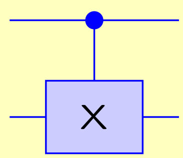
$$= \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

and



$$= \begin{bmatrix} 1 & 0 \\ 0 & \omega \end{bmatrix}$$

together with the CX gate



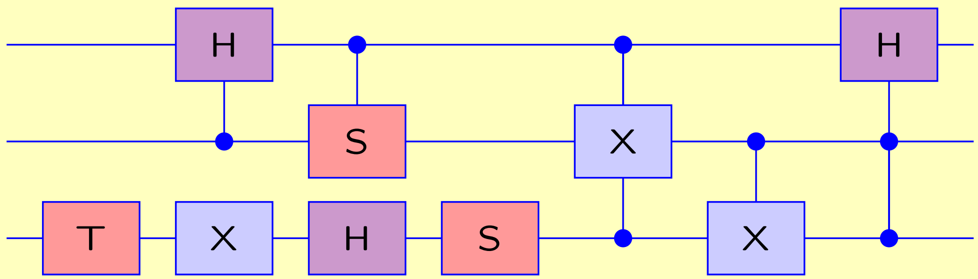
$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

The set $\{H, T, CX\}$ forms a *universal* and *fault-tolerant* set of quantum gates.

Clifford+T Circuits

Clifford+T circuits are generated from Clifford+T gates via *composition* and *tensor product* (and *ancillas*).

The circuit below is a Clifford+T circuit.

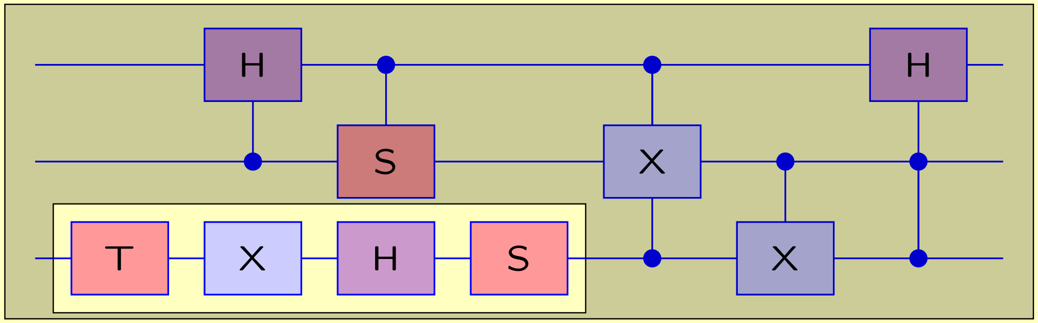


Some of the gates in the above circuit are *derived gates*.

Because they are universal and well-suited for fault-tolerant quantum computing, Clifford+T circuits have received a lot of attention.

Single-Qubit Clifford+T Circuits

Single-qubit Clifford+T circuits are **very well** understood.

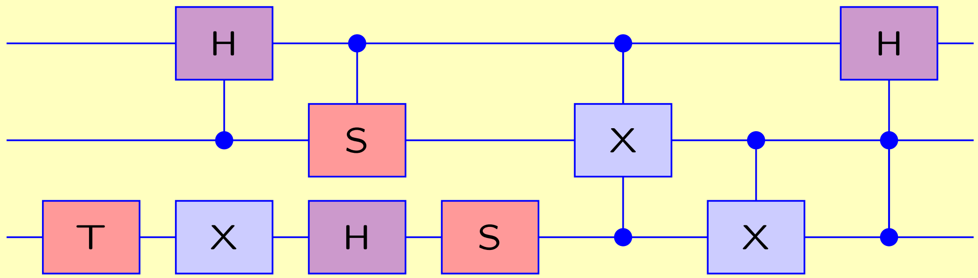


For single qubit Clifford+T operators we have:

- generators and relations [M.A. 2008],
- optimal normal forms [M.A. 2008],
- a number-theoretic characterization [K.M.M. 2013], and
- optimal approximations [R.S. 2014].

Multi-Qubit Clifford+T Circuits

Multi-qubit Clifford+T circuits are **not** very well understood.

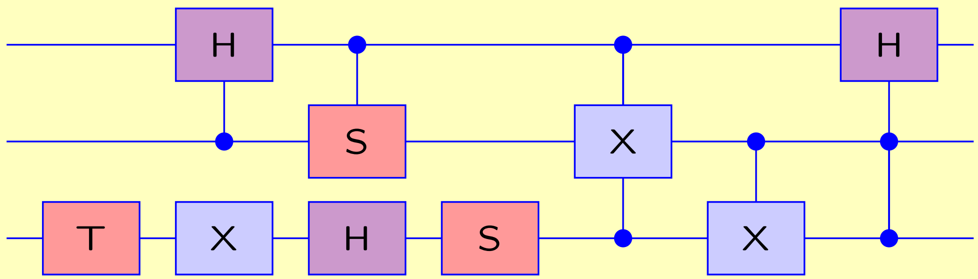


For multi-qubit qubit Clifford+T operators we have:

- a number-theoretic characterization [G.S. 2013] and
- generators and relations for 2-qubit circuits [B.S. 2015].

Multi-Qubit Clifford+T Circuits

Multi-qubit Clifford+T circuits are **not** very well understood.



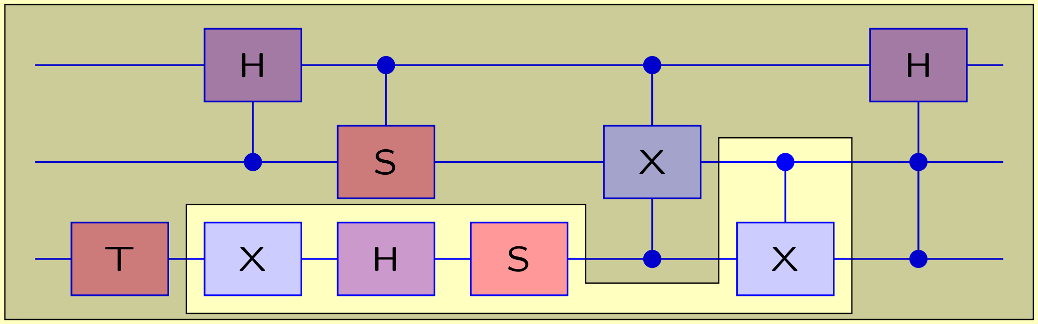
For multi-qubit qubit Clifford+T operators we have:

- a number-theoretic characterization [G.S. 2013] and
- generators and relations for 2-qubit circuits [B.S. 2015].

To circumvent the difficulties associated with multi-qubit Clifford+T circuits **restricted gate sets** have been considered.

Restricted Clifford+T Circuits

Several types of *restricted* Clifford+T circuits have been studied.



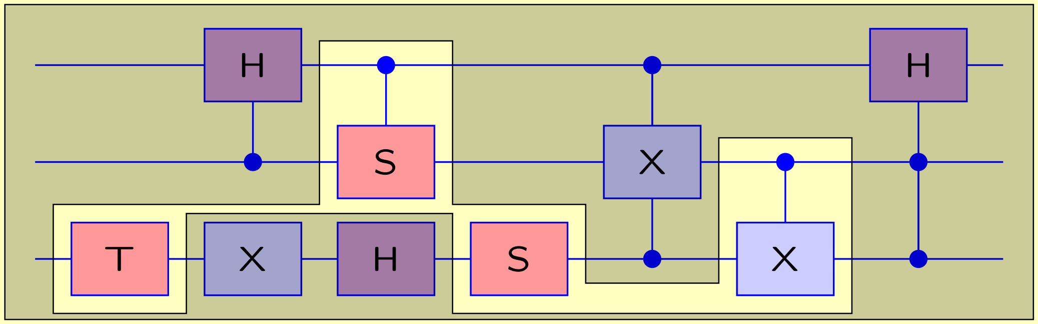
These include:

- Clifford circuits [S. 2015],
- CX+T circuits [A.M. 2016, C.H. 2017, A.C.R. 2017], and
- CX-dihedral circuits [A.C.R. 2017].

Unfortunately, **these restrictions are not universal**.

Restricted Clifford+T Circuits

Several types of *restricted* Clifford+T circuits have been studied.



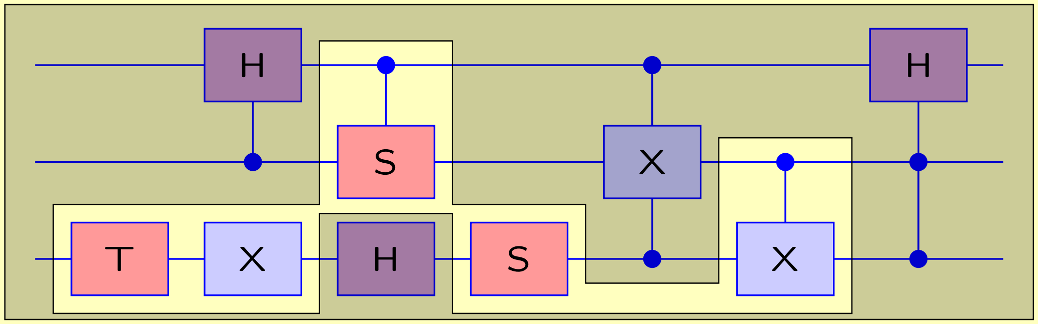
These include:

- Clifford circuits [S. 2015],
- CX+T circuits [A.M. 2016, C.H. 2017, A.C.R. 2017], and
- CX-dihedral circuits [A.C.R. 2017].

Unfortunately, **these restrictions are not universal**.

Restricted Clifford+T Circuits

Several types of *restricted* Clifford+T circuits have been studied.



These include:

- Clifford circuits [S. 2015],
- CX+T circuits [A.M. 2016, C.H. 2017, A.C.R. 2017], and
- CX-dihedral circuits [A.C.R. 2017].

Unfortunately, **these restrictions are not universal**.

Goal: study restricted <u>and</u> universal Clifford+T circuits.

II. Number-Theoretic Characterizations

Characterizing Clifford+T Operators

Let $\mathbb{D} = \{\frac{a}{2^k} \mid a \in \mathbb{Z}, k \in \mathbb{N}\}$ be the ring of *Dyadic fractions* and let

$$\mathbb{D}[\omega] = \{a\omega^3 + b\omega^2 + c\omega + d \mid a, b, c, d \in \mathbb{D}\}$$

where $\omega = e^{i\pi/4} = (1+i)/\sqrt{2}$.

[G.S. 2013] A $2^n \times 2^n$ matrix V can be exactly represented by an n-qubit Clifford+T circuit if, and only if, $V \in U_{2^n}(\mathbb{D}[\omega])$.

This number-theoretic characterization proved extremely useful in the study of 1- and 2-qubit Clifford+T circuits.

Restricted Clifford+T Operators

We can restrict Clifford+T operators by considering unitary matrices over **subrings** of $\mathbb{D}[\omega]$.

$$\begin{tikzcd}
& \mathbb{D}[\omega] & & & U_n(\mathbb{D}[\omega]) & \\
\mathbb{D}[i\sqrt{2}] \arrow[ur] & \mathbb{D}[i] \arrow[u] & \mathbb{D}[\sqrt{2}] \arrow[ul] \arrow[r, Longrightarrow] & U_n(\mathbb{D}[i\sqrt{2}]) \arrow[ur] & U_n(\mathbb{D}[i]) \arrow[u] & U_n(\mathbb{D}[\sqrt{2}]) \arrow[ul] \\
& \mathbb{D} \arrow[ul] \arrow[u] \arrow[ur] & & & U_n(\mathbb{D}) \arrow[ul] \arrow[u] \arrow[ur] &
\end{tikzcd}$$

For sufficiently large n, each one of these subrings of $D[\omega]$ corresponds to a **universal** subgroup of $U_n(\mathbb{D}[\omega])$ (sometimes in an encoded sense).

Results (I)

Theorem: A $2^n \times 2^n$ matrix V can be exactly represented by an n-qubit circuit over

- $\{X, CX, CCX, H \otimes H\}$ if and only if $V \in U_{2^n}(\mathbb{D})$,
- $\{X, CX, CCX, H, CH\}$ if and only if $V \in U_{2^n}(\mathbb{D}[\sqrt{2}])$,
- $\{X, CX, CCX, F\}$ if and only if $V \in U_{2^n}(\mathbb{D}[i\sqrt{2}])$, and
- $\{X, CX, CCX, \omega H, S\}$ if and only if $V \in U_{2^n}(\mathbb{D}[i])$,

where $F \propto \sqrt{H}$. Moreover, a single ancilla is always sufficient.

III. The Dyadic Case

Dyadic Matrices

In the *Dyadic* case we focus on matrices of the form

$$V = \frac{1}{2^k} U$$

where $k \in \mathbb{N}$, $U \in \mathbb{Z}^{n \times n}$.

The smallest k such that V can be written as above is called the *least denominator exponent* of V, written $\mathrm{lde}(V)$.

Our basic gates are X, CX, CCX, together with

$$H \otimes H = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}.$$

Exact Synthesis

Easy: If a $2^n \times 2^n$ matrix V can be exactly represented by an n-qubit circuit over $\{X, CX, CCX, H \otimes H\}$ then $V \in U_{2^n}(\mathbb{D})$.

Harder: If a $2^n \times 2^n$ matrix $V \in U_{2^n}(\mathbb{D})$ then V can be exactly represented by an n-qubit circuit over $\{X, CX, CCX, H \otimes H\}$.

To solve the harder problem, we follow [G.S. 2013] and introduce an *exact synthesis algorithm*.

The exact synthesis algorithm inputs $V \in U_{2^n}(\mathbb{D})$ and outputs an n-qubit circuit over $\{X, CX, CCX, H \otimes H\}$ for V.

Generators

The 1-, 2-, and 4-level operators

$$\{(-1)_{[\alpha]}, X_{[\alpha,\beta]}, H \otimes H_{[\alpha,\beta,\gamma,\delta]} \mid 1 \leq \alpha < \beta < \gamma < \delta \leq n\}$$

can be exactly represented over the gate set $\{X, CX, CCX, H \otimes H\}$.

Where, e.g.,

$$H \otimes H_{[1,3,4,5]} \begin{bmatrix} a \\ b \\ c \\ d \\ e \end{bmatrix} = \begin{bmatrix} (a+c+d+e)/2 \\ b \\ (a-c+d-e)/2 \\ (a+c-d-e)/2 \\ (a-c-d+e)/2 \end{bmatrix}.$$

We now forget circuits and we use the set

$$\{(-1)_{[\alpha]}, X_{[\alpha,\beta]}, H \otimes H_{[\alpha,\beta,\gamma,\delta]} \mid 1 \leq \alpha < \beta < \gamma < \delta \leq n\}$$

as our set of generators.

Some Lemmas (I)

Lemma 1: If $u_1, \ldots, u_4$ are odd integers, then there exists $m_1, \ldots, m_4$ such that

$$(H \otimes H)(-1)_{[1]}^{m_1}(-1)_{[2]}^{m_2}(-1)_{[3]}^{m_3}(-1)_{[4]}^{m_4} \begin{bmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \end{bmatrix} = \begin{bmatrix} w_1 \\ w_2 \\ w_3 \\ w_4 \end{bmatrix}$$

for some even integers $w_1, \ldots, w_4$.

Some Lemmas (I)

Lemma 1: If $u_1, \ldots, u_4$ are odd integers, then there exists $m_1, \ldots, m_4$ such that

$$(H \otimes H)(-1)^{m_1}_{[1]}(-1)^{m_2}_{[2]}(-1)^{m_3}_{[3]}(-1)^{m_4}_{[4]} \begin{bmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \end{bmatrix} = \begin{bmatrix} w_1 \\ w_2 \\ w_3 \\ w_4 \end{bmatrix}$$

for some even integers $w_1, \ldots, w_4$.

Lemma 2: If $v = u/2^k$ is a unit vector such that $u \in \mathbb{Z}^n$ and $\mathsf{lde}(v) \geq 1$ then the number of odd entries in u is a multiple of 4.

Proof. Let $k = \mathsf{lde}(v)$. Since v is a unit vector we have

$$4^k = u^\dagger u = \sum a_i^2$$

and since $k \geq 1$ the number of odd a_i must be a multiple of 4.

Some Lemmas (II)

Column Lemma: If $v \in \mathbb{D}^n$ is a unit vector then there exists a sequence $G_1, \ldots, G_\ell$ of 1-, 2-, and 4-level operators of type (-1), X, and $H \otimes H$ such that

$$G_1 \cdots G_\ell v = e_j$$

where e_j is the j-th standard basis vector.

Proof. By induction on the least denominator exponent k of v.

- If $k = 0$ then $v = \pm e_q$ and we choose the appropriate operators of type (-1) and X.
- If $k > 0$ then we can apply 4-level operators of type (-1) and $H \otimes H$ to groups of 4 odd components until all the entries in our vector are even at which point the least denominator exponent decreases.

The Exact Synthesis Algorithm

Theorem: If $V \in \mathcal{U}_n(\mathbb{D})$ then there exists a sequence $G_1, \ldots, G_\ell$ of 1- and 2- level operators of type (-1), X, and $H \otimes H$ such that

$$G_1 \cdots G_\ell V = I$$

or, equivalently, $G_\ell^\dagger \cdots G_1^\dagger = V$.

Proof. Apply the Column Lemma iteratively to the columns of V until the matrix is reduced to I.

IV. Further Results

Results (II)

Theorem: A $2^n \times 2^n$ matrix V can be exactly represented by an n-qubit circuit over

- $\{X, CX, CCX, H\}$ if and only if $V = W/\sqrt{2}^q$ for some matrix W over $\mathbb{Z}$ and some $q \in \mathbb{N}$, and
- $\{X, CX, CCX, H, S\}$ if and only if $V = W/\sqrt{2}^q$ for some matrix W over $\mathbb{Z}[i]$ and some $q \in \mathbb{N}$.

Moreover, a single ancilla is always sufficient.

Results (III)

Theorem: Let $n \geq 4$. A $2^n \times 2^n$ matrix V can be exactly represented by an n-qubit ancilla-free circuit over

- $\{X, CX, CCX, F\}$ if and only if $V \in U_{2^n}(\mathbb{D}[i\sqrt{2}])$ and $\det(V) = 1$, and
- $\{X, CX, CCX, \omega H, S\}$ if and only if $V \in U_{2^n}(\mathbb{D}[i])$ and $\det(V) = 1$,

where $F \propto \sqrt{H}$. Moreover, the requirement that $\det(V) = 1$ can be dropped for $n < 4$.

V. Conclusion and Outlook

Contributions

- We showed that the groups $\mathcal{U}_n(\mathbb{D})$, $\mathcal{U}_n(\mathbb{D}[i\sqrt{2}])$, $\mathcal{U}_n(\mathbb{D}[i])$, and $\mathcal{U}_n(\mathbb{D}[\sqrt{2}])$ correspond to classes of restricted Clifford+T circuits.
- In each case, the circuits are associated to gate sets obtained by extending the set of classical reversible gates $\{X, CX, CCX\}$ with ananalogue of the Hadamard gate and an optional phase gate.

Looking Forward

- Can we further explore the lattice of subgroups of $U_n(\mathbb{D}[\omega])$ through the study of restricted Clifford+T circuits?

- Can we use these characterizations to find presentations for families of circuits?

- Can this work provide a foundation for the optimization and verification of quantum circuits?

References (I)

- [M.A. 2008]: Matsumoto and Amano, *Representation of quantum circuits with Clifford and* $\pi/8$ *gates*.

- [K.M.M. 2013]: Kliuchnikov, Maslov, and Mosca, *Fast and efficient exact synthesis of single-qubit unitaries generated by Clifford and* T *gates*.

- [G.S. 2013]: Giles and Selinger, *Exact synthesis of multiqubit Clifford+*T *circuits*.

- [B.S. 2015]: Bian and Selinger, *Relations for the group of 2-qubit Clifford+*T *T operators*.

- [S. 2015]: Selinger, *Generators and relations for* n*-qubit Clifford operators*.

References (II)

- [R.S. 2014]: Ross and Selinger, *Optimal ancilla-free Clifford+T approximation of z-rotations*.

- [A.M. 2016]: Amy and Mosca, T*-count optimization and Reed-Muller codes*.

- [C.H. 2017]: Campbell and Howard, *Unified framework for magic state distillation and multiqubit gate synthesis with reduced resource cost*.

- [A.C.R. 2017]: Amy, Chen, and Ross, *A finite presentation of CNOT-dihedral operators*.