Relations for Clifford+T operators on two qubits

Peter Selinger and Xiaoning Bian

Dalhousie University

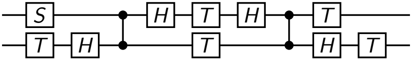
Contents

Why do we need relations?

- For 1 qubit Clifford+T operators
  - Exact synthesis algorithm (T-optimal)
  - *Matsumoto-Amano normal form* (T-optimal, unique)

$$THTSHTHTHTSHTSHTHTZ$$

- For n qubits Clifford+T operators
  - Exact synthesis – Giles-Selinger algorithm (but not T-optimal)
  - No normal form so far
  - How to minimize the T-count?

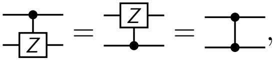


Clifford+T operators

The class of Clifford+T operators is the smallest class of unitary operators that includes the operators

$$\omega = e^{i\pi/4}, \quad H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 0 \\ 0 & \omega \end{pmatrix}$$

$$Z_c = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} =$$



and is closed under composition and tensor product.

The main theorem

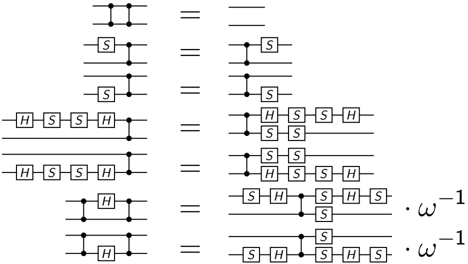
Theorem. *The following set of relations is complete for 2-qubit Clifford+T circuits:*

$$\omega^8 = 1$$

$$H^2 = 1$$

$$S^4 = 1$$

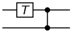
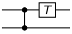
$$SHSHSH = \omega$$

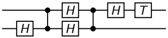
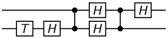


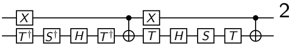
The main theorem, continued:

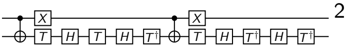
$$TT = S$$

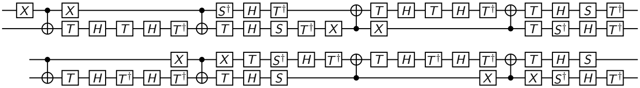
$$(THSSH)^2 = \omega$$

 $=$ 

 $=$ 

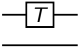
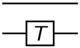
 $= \epsilon$

 $= \epsilon$

 $= \epsilon$

Clifford+T operators on 2 qubits

- Notations for 2 qubits Clifford+T operators:

$T_0 = T \otimes I =$ , $\quad T_1 = I \otimes T =$ 

Similarly for H_0, H_1, S_0, S_1.

- The group of 2 qubit Clifford+T operators is the smallest group containing

$$\omega, Z_c, T_0, T_1, H_0, H_1, S_0, S_1$$

Clifford+T and $U_4(\mathbb{Z}[\frac{1}{\sqrt{2}}, i])$

Theorem (Giles and Selinger, arXiv:1212.0506)**.** *The group of 2 qubits Clifford+T operators is the index 2 subgroup of $U_4(\mathbb{Z}[\frac{1}{\sqrt{2}}, i])$ consisting of operators with determinant $\pm 1, \pm i$.*

Here, $U_4(\mathbb{Z}[\frac{1}{\sqrt{2}}, i])$ is the group of unitary 4×4 matrices with entries in $\mathbb{Z}[\frac{1}{\sqrt{2}}, i]$.

Greylyn's result

Theorem (Greylyn, arXiv:1408.6204). *The group $U_4(\mathbb{Z}[\frac{1}{\sqrt{2}}, i])$ can be presented by 16 generators*

$$X_{[i,j]}, H_{[i,j]}, \omega_{[k]} \quad (1 \leqslant i < j \leqslant 4, 1 \leqslant k \leqslant 4)$$

and 123 equations.

Here, $\omega_{[k]}$, and $X_{[i,j]}, H_{[i,j]}$ are *one*- and *two-level operators*, e.g.:

$$\omega_{[4]} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \omega \end{pmatrix}, \quad X_{[2,3]} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

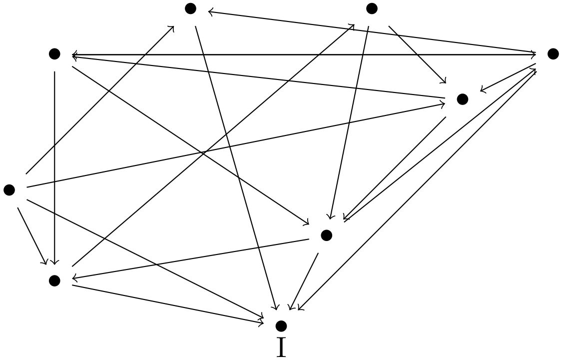
Greylyn's 123 relations

(1)	$\omega_{[j]}^8$	$\approx$	ϵ	
(2)	$H_{[j,k]}^2$	$\approx$	ϵ	$(j < k)$
(3)	$X_{[j,k]}^2$	$\approx$	ϵ	$(j < k)$
(4)	$\omega_{[j]}\omega_{[k]}$	$\approx$	$\omega_{[k]}\omega_{[j]}$	$(j \neq k)$
(5)	$\omega_{[\ell]}H_{[j,k]}$	$\approx$	$H_{[j,k]}\omega_{[\ell]}$	$(j < k, \ell \neq j, k)$
(6)	$\omega_{[\ell]}X_{[j,k]}$	$\approx$	$X_{[j,k]}\omega_{[\ell]}$	$(j < k, \ell \neq j, k)$
(7)	$H_{[j,k]}H_{[\ell,t]}$	$\approx$	$H_{[\ell,t]}H_{[j,k]}$	$(j < k, \ell < t, \{\ell,t\} \cap \{j,k\} = \emptyset)$
(8)	$H_{[j,k]}X_{[\ell,t]}$	$\approx$	$X_{[\ell,t]}H_{[j,k]}$	$(j < k, \ell < t, \{\ell,t\} \cap \{j,k\} = \emptyset)$
(9)	$X_{[j,k]}X_{[\ell,t]}$	$\approx$	$X_{[\ell,t]}X_{[j,k]}$	$(j < k, \ell < t, \{\ell,t\} \cap \{j,k\} = \emptyset)$
(10)	$X_{[j,k]}\omega_{[k]}$	$\approx$	$\omega_{[j]}X_{[j,k]}$	$(j < k)$
(11)	$X_{[j,k]}\omega_{[j]}$	$\approx$	$\omega_{[k]}X_{[j,k]}$	$(j < k)$
(12)	$X_{[j,k]}X_{[j,\ell]}$	$\approx$	$X_{[k,\ell]}X_{[j,k]}$	$(j < k < \ell)$
(13)	$X_{[j,k]}X_{[\ell,j]}$	$\approx$	$X_{[\ell,k]}X_{[j,k]}$	$(\ell < j < k)$
(14)	$X_{[j,k]}H_{[j,\ell]}$	$\approx$	$H_{[k,\ell]}X_{[j,k]}$	$(j < k < \ell)$
(15)	$X_{[j,k]}H_{[\ell,j]}$	$\approx$	$H_{[\ell,k]}X_{[j,k]}$	$(\ell < j < k)$
(16)	$\omega_{[j]}\omega_{[k]}X_{[j,k]}$	$\approx$	$X_{[j,k]}\omega_{[j]}\omega_{[k]}$	$(j < k)$
(17)	$\omega_{[j]}\omega_{[k]}H_{[j,k]}$	$\approx$	$H_{[j,k]}\omega_{[j]}\omega_{[k]}$	$(j < k)$
(18)	$H_{[j,k]}X_{[j,k]}$	$\approx$	$\omega_{[k]}^4 H_{[j,k]}$	$(j < k)$
(19)	$H_{[j,k]}\omega_{[j]}^2 H_{[j,k]}$	$\approx$	$\omega_{[j]}^6 H_{[j,k]}\omega_{[j]}^3\omega_{[k]}^5$	$(j < k)$
(20)	$H_{[j,k]}H_{[\ell,t]}H_{[j,\ell]}H_{[k,t]}$	$\approx$	$H_{[j,\ell]}H_{[k,t]}H_{[j,k]}H_{[\ell,t]}$	$(j < k < \ell < t)$

Figure from Greylyn's master thesis arXiv:1408.6204

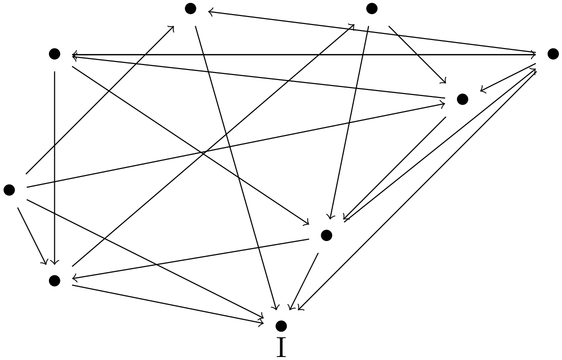
Proof idea of Greylyn's theorem

1. Build the *Cayley graph* of the group. Vertices = group elements, edges = generators.



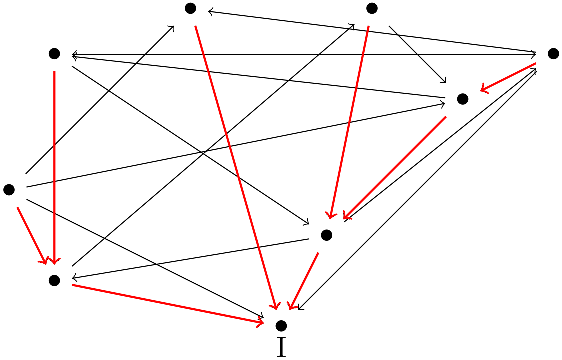
Proof idea of Greylyn's theorem

1. Build the *Cayley graph* of the group. Vertices = group elements, edges = generators. Cycles = relations.



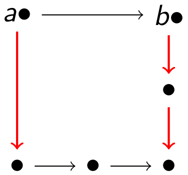
Proof idea of Greylyn's theorem

1. Build the *Cayley graph* of the group. Vertices = group elements, edges = generators. Cycles = relations.
2. The Giles-Selinger algorithm gives a *canonical path* from each group element to the identity. This forms a *spanning tree*.



Proof idea of Greylyn's theorem, continued

3. Find finitely many relations of the form



such that any arbitrary path can be transformed to the equivalent canonical path. By induction on the "height" of a and b.

Presentation of a subgroup

We have Clifford+$T \subset U_4(\mathbb{Z}[\frac{1}{\sqrt{2}}, i])$. Greylyn's result gives us generators and relations for the bigger group.

We face the following problem:

Problem. *Let H be a subgroup of G, and suppose we have a presentation of G by generators and relations. Can we find a presentation of H by generators and relations?*

Presentation of a subgroup

We have Clifford+$T \subset U_4(\mathbb{Z}[\frac{1}{\sqrt{2}}, i])$. Greylyn's result gives us generators and relations for the bigger group.

We face the following problem:

Problem. *Let H be a subgroup of G, and suppose we have a presentation of G by generators and relations. Can we find a presentation of H by generators and relations?*

Example.

$$G = \langle A, B, C \mid A^2, B^2, C^2, (BC)^3, (AC)^2, (AB)^4 \rangle$$

Let $X = AC$, $Y = BA$.

$$H = \langle X, Y \mid \qquad \qquad \rangle$$

Presentation of a subgroup

We have Clifford+$T \subset U_4(\mathbb{Z}[\frac{1}{\sqrt{2}}, i])$. Greylyn's result gives us generators and relations for the bigger group.

We face the following problem:

Problem. *Let H be a subgroup of G, and suppose we have a presentation of G by generators and relations. Can we find a presentation of H by generators and relations?*

Example.

$$G = \langle A, B, C \mid A^2, B^2, C^2, (BC)^3, (AC)^2, (AB)^4 \rangle$$

Let $X = AC$, $Y = BA$.

$$H = \langle X, Y \mid X^2, Y^4, (XY)^3 \rangle$$

Fortunately, there is a method for computing this.

Presentation of a subgroup

Lemma. *If* $(G_0, \mathcal{S})$ *is a presentation of group* G*, and* $H = \langle H_0 \rangle$ *is a subgroup of* G*, and if* C*,* f*, and* $\overline{h}$ *are chosen as below, then* $(H_0, \mathcal{R})$ *is a presentation of* H*, where* $\mathcal{R}$ *consists of the following relations:*

(A) For each generator $x \in H_0$*, a relation* $x = \overline{g}(f_x) \in \mathcal{R}$*; and*

(B) For each coset representative $c \in C$ *and each relation* $s = t \in \mathcal{S}$*, a relation* $u = v \in \mathcal{R}$*, where* $(u, d) = \overline{h}(c, s)$*, and* $(v, e) = \overline{h}(c, t)$*.*

C, f, and $\overline{h}$

- Coset representative C
- $x \in H_0$ can be written as a finite product f_x of elements in G_0
- Define a map (where w and d satisfy $cy = wd$)

$$h : C \times G_0 \to \vec{H}_0 \times C$$
$$(c, y) \mapsto (w, d)$$

- Since $G = \langle G_0 \rangle$, extend h, where $h(c_{i-1}, y_i) = (w_i, c_i)$

$$\overline{h} : C \times \vec{G}_0 \to \vec{H}_0 \times C$$
$$\overline{h}(c_0, y_1 y_2 ... y_n) = (w_1 w_2 ... w_n, c_n)$$

- Define $\overline{g} : H \to H$ given by $\overline{g}(u) = v$ iff $\overline{h}(1, u) = (v, 1)$

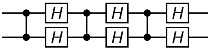
Choice of C, f, and h

- $C = \{1, \omega_{[4]}\}$
- Choice of f_x

x	f_x
H_0	$H_{[1,3]} H_{[0,2]}$
H_1	$H_{[2,3]} H_{[0,1]}$
S_0	$\omega_{[3]}^2 \omega_{[2]}^2$
S_1	$\omega_{[3]}^2 \omega_{[1]}^2$

x	f_x
Z_c	$\omega_{[3]}^4$
ω	$\omega_{[0]}\omega_{[1]}\omega_{[2]}\omega_{[3]}$
T_0	$\omega_{[2]}\omega_{[3]}$
T_1	$\omega_{[3]}\omega_{[1]}$

- Choice of h, using the following abbreviations

$Swap =$ 

, $\quad T^\dagger = T^7, \quad CX_0 = H_0 Z_c H_0$

$$X_0 = H_0 S_0 S_0 H_0, \quad X_1 = H_1 S_1 S_1 H_1, \quad S^\dagger = S^3, \quad CX_1 = H_1 Z_c H_1$$

Choice of C, f, and h

y	$h(1, y)$	$h(\omega_{[4]}, y)$
$X_{[0,1]}$	$(X_0 CX_1 X_0, 1)$	$(X_0 CX_1 X_0, \omega_{[4]})$
$X_{[0,2]}$	$(SwapX_0 CX_1 X_0 Swap, 1)$	$(SwapX_0 CX_1 X_0 Swap, \omega_{[4]})$
$X_{[0,3]}$	$(CX_0 X_0 CX_1 X_0 CX_0, 1)$	$(CX_0 X_0 T_1 CX_1 T_1^\dagger X_0 CX_0, \omega_{[4]})$
$X_{[1,2]}$	$(CX_0 X_1 CX_1 X_1 CX_0, 1)$	$(CX_0 X_1 CX_1 X_1 CX_0, \omega_{[4]})$
$X_{[1,3]}$	$(SwapCX_1 Swap, 1)$	$(Swap T_1 CX_1 T_1^\dagger Swap, \omega_{[4]})$
$X_{[2,3]}$	$(CX_1, 1)$	$(T_1 CX_1 T_1^\dagger, \omega_{[4]})$
$H_{[0,1]}$	$(X_0 S_1^\dagger H_1 T_1^\dagger CX_1 T_1 H_1 S_1 X_0, 1)$	$(X_0 S_1^\dagger H_1 T_1^\dagger CX_1 T_1 H_1 S_1 X_0, \omega_{[4]})$
$H_{[0,2]}$	$(SwapX_0 S_1^\dagger H_1 T_1^\dagger CX_1 T_1 H_1 S_1 X_0 Swap, 1)$	$(SwapX_0 S_1^\dagger H_1 T_1^\dagger CX_1 T_1 H_1 S_1 X_0 Swap, \omega_{[4]})$
$H_{[0,3]}$	$(CX_0 X_0 S_1^\dagger H_1 T_1^\dagger CX_1 T_1 H_1 S_1 X_0 CX_0, 1)$	$(CX_0 X_0 T_1 S_1^\dagger H_1 T_1^\dagger CX_1 T_1 H_1 S_1 T_1^\dagger X_0 CX_0, \omega_{[4]})$
$H_{[1,2]}$	$(CX_0 X_1 S_1^\dagger H_1 T_1^\dagger CX_1 T_1 H_1 S_1 X_1 CX_0, 1)$	$(CX_0 X_1 S_1^\dagger H_1 T_1^\dagger CX_1 T_1 H_1 S_1 X_1 CX_0, \omega_{[4]})$
$H_{[1,3]}$	$(SwapS_1^\dagger H_1 T_1^\dagger CX_1 T_1 H_1 S_1 Swap, 1)$	$(Swap T_1 S_1^\dagger H_1 T_1^\dagger CX_1 T_1 H_1 S_1 T_1^\dagger Swap, \omega_{[4]})$
$H_{[2,3]}$	$(S_1^\dagger H_1 T_1^\dagger CX_1 T_1 H_1 S_1, 1)$	$(T_1 S_1^\dagger H_1 T_1^\dagger CX_1 T_1 H_1 S_1 T_1^\dagger, \omega_{[4]})$
$\omega_{[0]}$	$(CX_0 X_0 T_1^\dagger CX_1 T_1 CX_1 X_0 CX_0, \omega_{[4]})$	$(CX_0 X_0 T_0 X_0 CX_0, 1)$
$\omega_{[1]}$	$(Swap T_1^\dagger CX_1 T_1 CX_1 Swap, \omega_{[4]})$	$(Swap T_0 Swap, 1)$
$\omega_{[2]}$	$(T_1^\dagger CX_1 T_1 CX_1, \omega_{[4]})$	$(T_0, 1)$
$\omega_{[3]}$	$(\epsilon, \omega_{[4]})$	$(T_1 T_0 CX_1 T_1^\dagger CX_1, 1)$

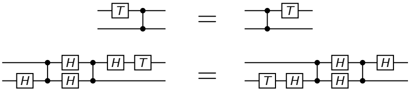
Reduction of equations

- Apply this lemma, we get $8 + 246 = 254$ equations, all very long.

Reduction of equations

- Apply this lemma, we get $8 + 246 = 254$ equations, all very long.
- We already know some "obvious" equations:
  - All Clifford equations
  - Obvious Clifford+T equations

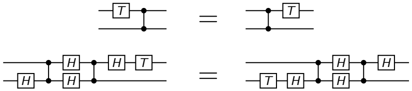
$$
\begin{aligned}
TT &= S \\
(THSSH)^2 &= \omega
\end{aligned}
$$



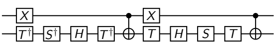
Reduction of equations

- Apply this lemma, we get $8 + 246 = 254$ equations, all very long.
- We already know some "obvious" equations:
  - All Clifford equations
  - Obvious Clifford+T equations

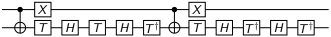
$$
\begin{aligned}
TT &= S \\
(THSSH)^2 &= \omega
\end{aligned}
$$



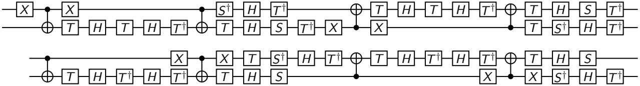
- After automatic reduction, we have 40 left
- After manual reduction, we have 3 left



$$\left(\cdots \right)^2 = \epsilon$$



$$\left(\cdots \right)^2 = \epsilon$$



$$= \epsilon$$

Sketch of the automated reduction

Following Gosset, Kliuchnikov, Mosca, and Russo (arXiv:1308.4134), we define, for any Pauli operators P, Q:

$$R(P \otimes Q) = \frac{1+\omega}{2} I + \frac{1-\omega}{2} (P \otimes Q).$$

Sketch of the automated reduction

Following Gosset, Kliuchnikov, Mosca, and Russo (arXiv:1308.4134), we define, for any Pauli operators P, Q:

$$R(P \otimes Q) = \frac{1+\omega}{2} I + \frac{1-\omega}{2} (P \otimes Q).$$

Then every Clifford$+T$ operator can be written (not uniquely) as

$$R(P_1 \otimes Q_1) \cdots R(P_k \otimes Q_k)\, C,$$

where P_j, Q_j are Pauli and C is Clifford.

Sketch of the automated reduction

Following Gosset, Kliuchnikov, Mosca, and Russo (arXiv:1308.4134), we define, for any Pauli operators P, Q:

$$R(P \otimes Q) = \frac{1+\omega}{2} I + \frac{1-\omega}{2} (P \otimes Q).$$

Then every Clifford+T operator can be written (not uniquely) as

$$R(P_1 \otimes Q_1) \cdots R(P_k \otimes Q_k)\, C,$$

where P_j, Q_j are Pauli and C is Clifford. We can use the "obvious" equations to convert any Clifford+T operator to this form. Also, $R(P \otimes Q)$ and $R(P' \otimes Q')$ commute iff $P \otimes Q$ and $P' \otimes Q'$ commute. Using these techniques, most of the 254 equations can be automatically proven.

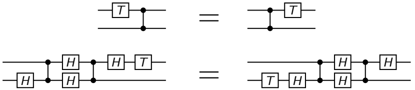
This concludes the proof of the main theorem!

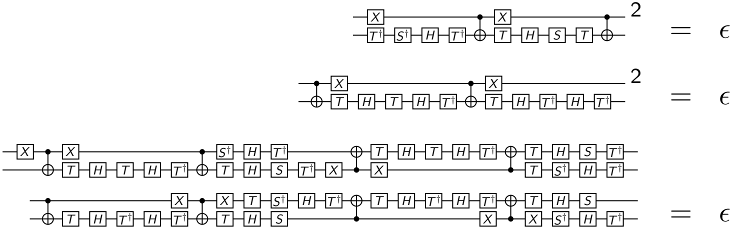
Theorem. *The following set of relations is complete for 2-qubit Clifford+T circuits:*

Clifford equations

$$TT = S$$

$$(THSSH)^2 = \omega$$





References

B. Giles and P. Selinger.
Exact synthesis of multiqubit Clifford+T circuits.
Physical Review A, 87(3):032332, 2013.

D. Gosset, V. Kliuchnikov, M. Mosca, and V. Russo.
An algorithm for the t-count.
Quantum Information & Computation, 14(15-16):1261–1276, 2014.

S. E. M. Greylyn.
Generators and relations for the group $U_4(\mathbb{Z}[\frac{1}{\sqrt{2}}, i])$.
arXiv preprint arXiv:1408.6204, 2014.

P. Selinger.
Generators and relations for n-qubit Clifford operators.
arXiv preprint arXiv:1310.6813, 2013.

Thank You!