Generators and relations for 2-qubit Clifford+T operators

Xiaoning Bian and Peter Selinger

Dalhousie University

Presented at 29th FMCS workshop, Kananaskis
June 25, 2022

Contents

Clifford operators

- The set of Clifford operators is generated by the operators

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

  and is closed under multiplication and tensor product.

- Every such operator U is of size $2^n \times 2^n$ for some natural number n. We say that U is an operator on n qubits.

Clifford+T operators

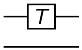
- We obtain a universal gate set by also adding the T-gate as a generator

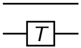
$$T = \begin{pmatrix} 1 & 0 \\ 0 & \omega \end{pmatrix}.$$

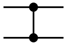
  The resulting operators are called the Clifford+T operators.

- We focus on the case $n = 2$. We write $T_0 = T \otimes I$ and $T_1 = I \otimes T$, and similarly for H_0, H_1, S_0, and S_1. We also identify the scalar ω with the 4×4-matrix ωI.

- We use circuit notation, for example



$= T_0$,


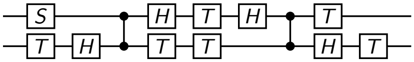
$= T_1$, and

$= CZ$.

Motivation

- For 1-qubit Clifford+T operators:
  - Generators and relations for 1-qubit Clifford+T operators.
  - Matsumoto-Amano normal form (T-optimal, unique)

$$(T \mid \varepsilon)(HT \mid SHT)^* C, \text{ where } C \text{ is some Clifford operator.}$$

- For n-qubit Clifford+T operators:
  - No finite presentation so far.
  - No normal form so far.
- The result could potentially be used to minimize the T-count.



Reidemeister-Schreier theorem — notations

The Reidemeister-Schreier procedure [5, 6] is used for finding generators and relations of a subgroup, given generators and relations of the supergroup.

- Let X be a set. We write X^* for the set of finite sequences of elements of X, which we also call *words* over the alphabet X.
- We write $w \cdot v$ or simply wv for the concatenation of words, making X^* into a monoid. The unit of this monoid is the empty word ϵ. As usual, we identify X with the set of one-letter words.
- A *relation* over X is an element of $X^* \times X^*$, i.e., an ordered pair of words, written as $w = v$, by a slight abuse of notation.

Reidemeister-Schreier theorem — special case

- Let G be a group, presented by $(\mathcal{X}, \Gamma)$. Let $\mathcal{Y}$ be another generating set.
- We have back-forth translations: define

  $$f : \mathcal{X} \to \mathcal{Y}^*, \; g : \mathcal{Y} \to \mathcal{X}^*,$$

  then extend them to

  $$f^* : \mathcal{X}^* \to \mathcal{Y}^*, \; g^* : \mathcal{Y}^* \to \mathcal{X}^*.$$

- Then $(\mathcal{Y}, \Delta)$ is another presentation of G, where

  $$\Delta = \{f^*(g(y)) = y \; : \; y \in \mathcal{Y}\} \cup \{f^*(u) = f^*(t) \; : \; u = t \in \Gamma\}.$$

Reidemeister-Schreier theorem — full version

- Let G be a group, presented by $(\mathcal{X}, \Gamma)$. Let H be a subgroup of G generated by $\mathcal{Y}$.
- One direction of the translation $g : \mathcal{Y} \to \mathcal{X}^*$ still works. Let C be the set of coset representatives, define, in a proper way

$$f : C \times \mathcal{X} \to \mathcal{Y}^* \times C,$$

then, we can extend f to $\quad f^{**} : C \times \mathcal{X}^* \to \mathcal{Y}^* \times C,$

$$f^{**}(c_0, x_1 \dots x_n) = (w_1 \cdot \dots \cdot w_n, c_n), \text{ where } f(c_{i-1}, x_i) = (w_i, c_i).$$

- Then $(\mathcal{Y}, \Delta)$ is a presentation of H, where

$$\begin{aligned} \Delta &= \{f^{***}(I, g(y)) = y \,:\, y \in \mathcal{Y}\} \\ &\cup \{f^{***}(c, u) = f^{***}(c, t) \,:\, u = t \in \Gamma,\, c \in C\}, \end{aligned}$$

and where $f^{***}(c, x) = fst(f^{**}(c, x))$.

Reidemeister-Schreier theorem — monoid version

Theorem 2.1 (Reidemeister-Schreier theorem for monoids). *Let X and Y be sets, and let Γ and Δ be sets of relations over X and Y, respectively. Suppose that the following additional data is given:*

- *a set C with a distinguished element $I \in C$,*
- *a function $f : X \to Y^*$,*
- *a function $h : C \times Y \to X^* \times C$,*

subject to the following conditions:

a. *For all $x \in X$, if $h^{**}(I, f(x)) = (v, c)$, then $v \sim_\Gamma x$ and $c = I$.*
b. *For all $c \in C$ and $w, w' \in Y^*$ with $(w, w') \in \Delta$, if $h^{**}(c, w) = (v, c')$ and $h^{**}(c, w') = (v', c'')$ then $v \sim_\Gamma v'$ and $c' = c''$.*

Then for all $v, v' \in X^*$, $f^*(v) \sim_\Delta f^*(v')$ implies $v \sim_\Gamma v'$.

Main theorem

Theorem 3.1. *The 2-qubit Clifford+T group is presented by* $(\mathcal{X}, \Gamma)$*, where the set of generators is*

$$\mathcal{X} = \{\omega, H_0, H_1, S_0, S_1, T_0, T_1, CZ\},$$

and the set of relations Γ *is shown in the following two slides.*

Relations

(a) Monoidal relations:

$$\omega A = A\omega, \quad \text{where } A \in \{H_i, S_i, T_i, CZ\} \tag{1}$$

$$A_0 B_1 = B_1 A_0, \quad \text{where } A, B \in \{H, S, T\} \tag{2}$$

(b) Order of Clifford group elements:

$$\omega^8 = \epsilon \tag{3}$$

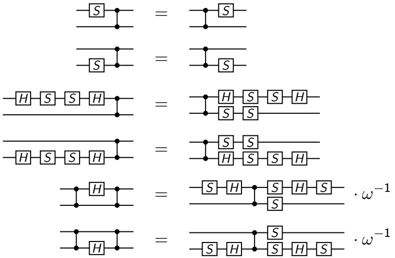
$$H_i^2 = \epsilon \tag{4}$$

$$S_i^4 = \epsilon \tag{5}$$

$$(S_i H_i)^3 = \omega \tag{6}$$

$$CZ^2 = \epsilon \tag{7}$$

(c) Remaining Clifford relations:



(8)
(9)
(10)
(11)
(12)
(13)

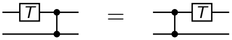
Here $i \in \{0, 1\}$

Relations — T part

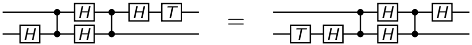
(d) "Obvious" relations involving T:

$$T_i^2 = S_i \tag{14}$$

$$(T_i H_i S_i S_i H_i)^2 = \omega \tag{15}$$

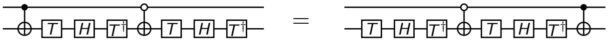


(16)

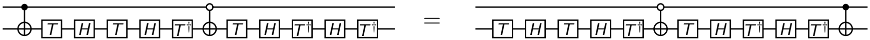


(17)

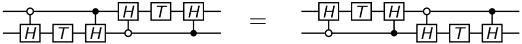
(e) "Non-obvious" relations involving T:



(18)



(19)

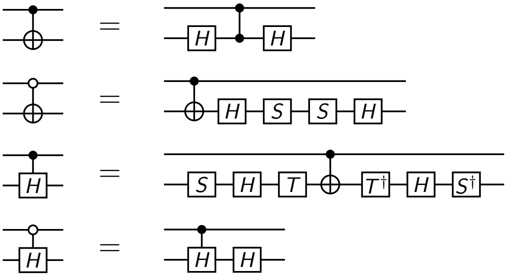


(20)

Abbreviations

In relations (18)–(20), we have used abbreviations:

$$T^\dagger = T^7$$
$$S^\dagger = S^3$$



Proof outline

Let $R = \mathbb{Z}[\frac{1}{\sqrt{2}}, i]$ be the smallest subring of the complex numbers containing $\frac{1}{\sqrt{2}}$ and i, and let $G = U_4(R)$ be the group of unitary 4×4-matrices with entries in R.

- 2-qubit Clifford+T operators is the subgroup of G consisting of matrices whose determinant is a power of i [2].
- A presentation of G by generators and relations was given by Greylyn [4].
- Apply the Reidemeister-Schreier procedure.

Relation simplification

- The Reidemeister-Schreier procedure produces 254 Clifford+T relations. We must verify that each of them is derivable from relations (1) - (20). This task is too much to do “by hand”.
- We formalize the Main Theorem and its proof in the proof assistant Agda [1].
- Naively hard-coding the proof is also too much, we use some automation.
- Automation takes care most of 254 proof obligations.

Automation

- We use the *Pauli rotation representation* of Clifford+T operators [3, Section 3].
- Every Clifford+T operator can be written as a product of Pauli rotations followed by a single Clifford operator.

$$C_1 T_{(i_1)} C_2 T_{(i_2)} C_3 \cdots C_n T_{(i_n)} C_{n+1} \quad = \quad R_{P_1} R_{P_2} \cdots R_{P_n} D_{n+1},$$

where R-syllable R_P is indexed by Pauli operators (finite many). E.g. $R_{Z \otimes I} = T_0$.

Automation

- The representation can be standardized using:
  (a) R_P and R_Q commute if and only if P and Q commute.
  (b) R_P^2 is Clifford, and therefore can be "eliminated".
  (c) $R_{(-P)} = R_P D$, for some Clifford operator D.
- To show $L = R$, we show $P(L) = P(R)$, where $P(X)$ is the standardized Pauli rotation representation of X.
- Easy to code the above rewriting.
- Easy to code the proofs of the rewriting rules are devrivable from our relations.

Future work

- Using proof assistant for some computation-heavy proofs might be a good idea.
- Complete relations for 3-qubit Clifford+T operators.
- Another project that is currently in progress is to apply the method of this paper to restrictions of the Clifford+T group.

References

- Agda documentation.
  `https://agda.readthedocs.io/`.
  Accessed: 2022-02-15.
- B. Giles and P. Selinger.
  Exact synthesis of multiqubit Clifford+T circuits.
  Physical Review A, 87(3):032332 (7 pages), 2013.
  Also available from arXiv:1212.0506.
- D. Gosset, V. Kliuchnikov, M. Mosca, and V. Russo.
  An algorithm for the T-count.
  Quantum Information and Computation, 14(15–16):1261–1276, 2014.
  Also available from arXiv:1308.4134.
- S. E. M. Greylyn.
  Generators and relations for the group $U_4(\mathbb{Z}[\frac{1}{\sqrt{2}}, i])$.
  M.Sc. thesis, Dalhousie University, 2014.
  Available from arXiv:1408.6204.
- K. Reidemeister.
  Knoten und Gruppen.
  Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg, 5(1):7–23, 1927.
- O. Schreier.
  Die Untergruppen der freien Gruppen.
  Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg, 5(1):161–183, 1927.