Generators and relations for 3-qubit Clifford+CS Operators

Xiaoning Bian and Peter Selinger

Dalhousie University

Presented at 30th FMCS workshop
Mount Allison University
June 9, 2023

Contents

Clifford operators

- The set of Clifford operators is generated by the operators

$$i, \quad K = \frac{1-i}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \quad CZ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix},$$

  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. We write $\mathcal{C}(n)$ for the set of n-qubit Clifford operators.

- Peter found normal forms and complete relations for $\mathcal{C}(n)$.

Clifford+CS operators

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

$$CS = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \end{pmatrix}.$$

  The resulting operators are called the Clifford+CS operators.

- We focus on the case when $n = 3$. Let I be the 2×2 identity operator. We write

$$K_0 = K \otimes I \otimes I\,, \quad K_1 = I \otimes K \otimes I\,, \quad K_2 = I \otimes I \otimes K,$$

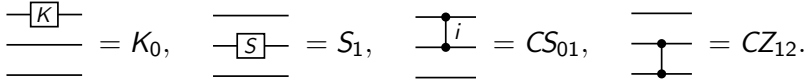
  and similarly for $S_0, ..., S_2$. We write

$$CS_{01} = CS \otimes I\,, \quad CS_{12} = I \otimes CS,$$

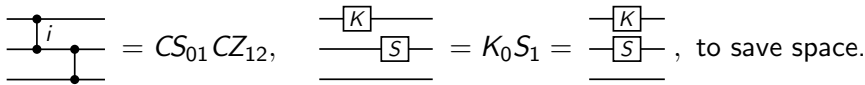
  and similarly for CZ_{01}, CZ_{12}. We also identify the scalar i with the 8×8-matrix $i(I \otimes I \otimes I)$.

Clifford+CS operators

- We use circuit notation, for example



- Circuit composition is matrix multiplication, i.e.,



- We use $\mathcal{CS}(n)$ to denote n-qubit Clifford+CS operators.

Monoid presentation

- 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.

Group presentation

- A *congruence relation* is a relation that satisfies *reflexivity*, *symmetry*, *transitivity* and *congruence* i.e.

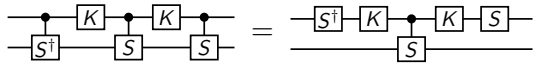
$$a = a' \text{ and } b = b' \implies ab = a'b'$$

- Given a set X and a congurence relation R over X, then X^* modulo R is also a monoid. Call it M. We say (X, R) is an *presentation* of M in terms of *generators* X and *relations* R.

- When R includes relations of the form $xy = \epsilon$ for all $x \in X$, M is also a group, and (X, R) also is a group presentation.

Motivation

- The result could potentially be used to minimize the CS-count and find normal forms,



- For Clifford+T operators, where $T = \begin{pmatrix} 1 & 0 \\ 0 & \omega \end{pmatrix}$, and $\omega = \frac{\sqrt{2}}{2}(1+i)$.
  - Matsumoto and Amano gave a T-optimal normal form for 1-qubit case.

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

  - Bian and Selinger gave a generator and relation result for 2-qubit case.
  - Li et al. gave an almost T-optimal norm form for 2-qubit case in April, 2023.

- For Clifford+CS operators, which is a proper subgroup of Clifford+T.
  - Glaudell et al. gave a CS-optimal normal form for 2-qubit case.

A known result and a known procedure

- A finite presentation of a supergroup $U_n(\mathbb{Z}[\frac{1}{2}, i])$ of Clifford+CS is known [2].
  - Here $\mathbb{Z}[\frac{1}{2}, i]$ is the smallest subring of the complex numbers containing $\frac{1}{2}$ and i.
  - $U_n(\mathbb{Z}[\frac{1}{2}, i])$ is the group of unitary $n \times n$-matrices with entries in $\mathbb{Z}[\frac{1}{2}, i]$.
  - The index is 2.
- The Reidemeister-Schreier procedure [7, 8] is used for finding generators and relations of a subgroup, given generators and relations of the supergroup.
  - Computationally efficient.
  - Formally verified in proof assistant Agda [3].

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 $f^{***}(c, x) = \mathit{fst}(f^{**}(c, x))$.

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 $1 \in C$,*
- *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 $h^{**}(1, f(x)) = (v, c)$, then $v \sim_\Gamma x$ and $c = 1$.*

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 3-qubit Clifford+CS group is presented by* $(\mathcal{X}, \Gamma_X)$*, where the set of generators is*

$$\mathcal{X} = \{i, K_0, K_1, K_2, S_0, S_1, S_2, CS_{01}, CS_{12}\},$$

and the set of relations Γ_X *is shown in Figure 2.*

(a) Relations for $n \geq 0$:

$$i^4 = \varepsilon \tag{C1}$$

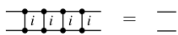
(b) Relations for $n \geq 1$:

$$K^2 = i^3 \tag{C2}$$

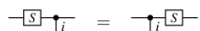
$$S^4 = \varepsilon \tag{C3}$$

$$SKSKSK = i^3 \tag{C4}$$

(c) Relations for $n \geq 2$:



(C5)



(C6)

(C7)

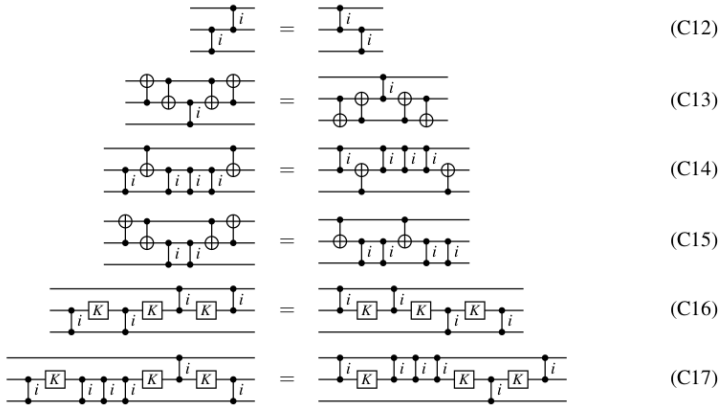
(C8)

(C9)

(C10)

(C11)

(d) Relations for $n = 3$:



(e) Monoidal relations: the scalar i commutes with everything, and non-overlapping gates commute.

Figure 2: Complete relations for $\mathscr{CS}(3)$. Each relation in (b) denotes three relations (one for each qubit), and each relation in (c) denotes two relations (one for each pair of adjacent qubits).

Main theorem proof outline

- G is the subgroup of $U_8(\mathbb{Z}[\frac{1}{2}, i])$ consisting of matrices whose determinant is a power of -1, which has index 2.
- A presentation of $U_8(\mathbb{Z}[\frac{1}{2}, i])$ by generators and relations was given by [6].
- Apply the Reidemeister-Schreier procedure.
- Simplify the output.

Relation simplification

- The Reidemeister-Schreier procedure produces thousands of Clifford+*CS* relations. We must verify that each of them is derivable from relations (a) - (e). This task is too much to do "by hand". We use some automation.

- We define an *almost normal form* to simplify relations. Most of the relations simplify to trivial.

- The almost normalization procedure only uses relations in Fig 2.

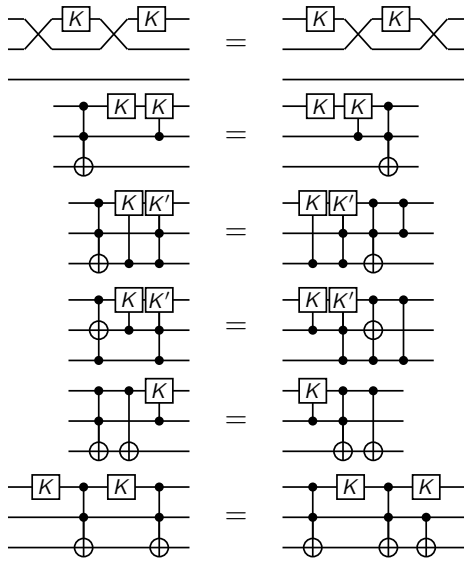
- We formalized the Main Theorem and its proof in the proof assistant Agda [1].

```
soundness-property : Set
soundness-property = ∀ {w v} -> Clifford+CS.Rel ⊢ w === v -> TwoLevel.Rel ⊢ (f *) w === (f *) v

completeness-property : Set
completeness-property = ∀ {w v} -> TwoLevel.Rel ⊢ (f *) w === (f *) v -> Clifford+CS.Rel ⊢ w === v
□
```

Almost normal form

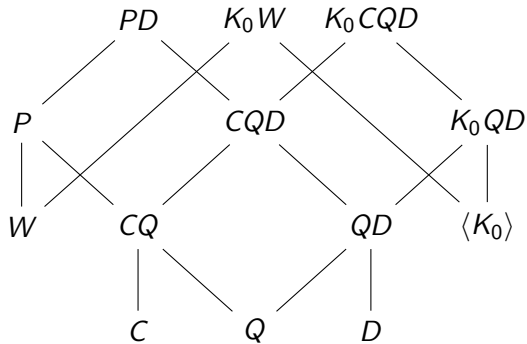
- We found normal forms for many finite subgroups. In particular, we are interested in three of them (each is maximal in some sense and finite).
- Each group element is the product of elements from the three subgroups.
- Normalize each factor and then simplify the result using the following relations.


K
K
=
K
K
K
K
=
K
K
K
K'
=
K
K'
K
K'
=
K
K'
K
K
=
K
K
K
K
=
K
K
K

Normal forms for many finite subgroups

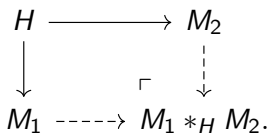
- W, the subgroup of permutation matrices generated by $\mathcal{X}_W = \{Swap_{01}, Swap_{12}\}$.
- Q, the subgroup of permutation matrices generated by $\mathcal{X}_Q = \{X_0, CX_{10}, CX_{20}, CCX_0\}$.
- C, the subgroup of permutation matrices generated by $\mathcal{X}_C = \{X_1, CX_{12}, CX_{21}\}$.
- CQ, the subgroup generated by $\mathcal{X}_C$ and $\mathcal{X}_Q$.
- P, the subgroup of permutation matrices generated by $\mathcal{X}_P = \{CX_{01}, CX_{10}, CX_{12}, CX_{21}, CCX_0, X_0\}$.
- D, the diagonal subgroup generated by $\mathcal{X}_D = \{i, S_0, S_1, S_2, CS_{01}, CS_{12}, CS_{02}, CCZ\}$.
- PD, the subgroup generated by $\mathcal{X}_P$ and $\mathcal{X}_D$.
- QD, the subgroup generated by $\mathcal{X}_Q$ and $\mathcal{X}_D$.
- CQD, the subgroup generated by $\mathcal{X}_C$, $\mathcal{X}_Q$ and $\mathcal{X}_D$.
- K_0D the subgroup generated by $\{K_0\} \cup \mathcal{X}_D$. Note that this group contains Q, so it can also be denoted by K_0QD.
- K_0CD, the subgroup generated by $\{K_0\} \cup \mathcal{X}_C \cup \mathcal{X}_D$. Since this group contains Q, it can also be denoted by K_0CQD.
- K_0W, the subgroup generated by K_0 and $\mathcal{X}_W$.

Inclusion graph of various finite subgroups



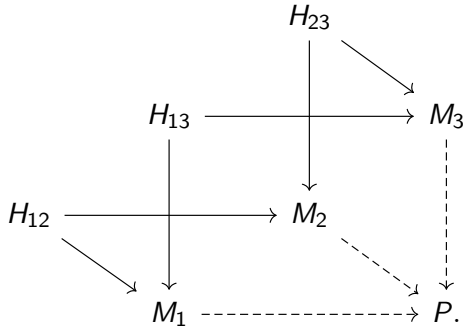
Amalgamation of two monoids

Given monoids M_1, M_2, and H with morphisms $H \to M_1$ and $H \to M_2$, the amalgamated product $M_1 *_H M_2$ is the pushout



Amalgamation of three monoids

The amalgamated product of three monoids is defined similarly. Suppose M_1, M_2, M_3, H_{12}, H_{23}, H_{13} are monoids with morphisms $H_{jk} \to H_j$ and $H_{jk} \to H_k$ for all relevant j and k. Then the amalgamated product P is the colimit of the following diagram, which generalizes a pushout:



Amalgamation in terms of generators and relations

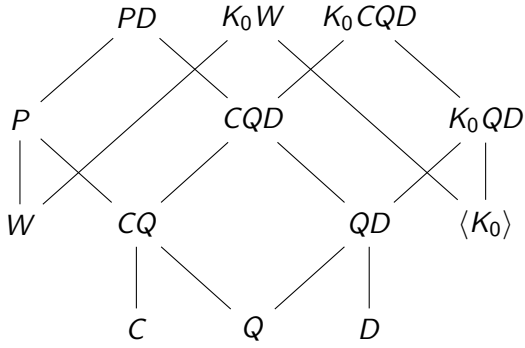
- Suppose we have three sets of generators X, Y, and Z, and three monoid presentations

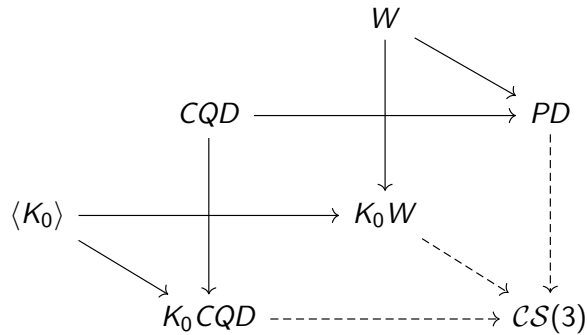
$$M_1 = \langle X \cup Y \mid \Gamma_1 \rangle, \quad M_2 = \langle X \cup Z \mid \Gamma_2 \rangle, \text{ and } M_3 = \langle Y \cup Z \mid \Gamma_3 \rangle.$$

- We can take $H_{12} = \langle X \rangle$, $H_{13} = \langle Y \rangle$ and $H_{23} = \langle Z \rangle$, with the obvious maps.
- Then the amalgamated product P has the presentation $\langle X \cup Y \cup Z \mid \Gamma_1 \cup \Gamma_2 \cup \Gamma_3 \rangle$.
- In cases where P is an infinite monoid or group, it is remarkable when M_1, M_2, and M_3 can be chosen to be finite.

$\mathcal{CS}(3)$ is an amalgamated product of three finite groups

Using the main theorem, we can show that $\mathcal{CS}(3)$ is an amalgamated product of three finite groups.





The slogan is "the only relations that hold in $\mathcal{CS}(3)$ are relations that hold in a finite subgroup of $\mathcal{CS}(3)$".

Future work

- Normal forms for 3-qubit Clifford+CS operators.
- Complete relations for 4-qubit Clifford+CS operators.
- Complete relations for 3-qubit Clifford+T operators.

Thank you

- Thank you for your attention.
- Looking for jobs. Expected graduation: 2023 Fall.

References

Agda documentation.
`https://agda.readthedocs.io/`.
Accessed: 2022-02-15.

X. Bian and P. Selinger.
Generators and relations for $U_n(\mathbb{Z}[1/2, i])$.
In *Proceedings of the 18th International Conference on Quantum Physics and Logic, QPL 2021, Gdansk, Poland*, volume 343 of *Electronic Proceedings in Theoretical Computer Science*, pages 145–164, 2021.
Also available from arXiv:2105.14047.

X. Bian and P. Selinger.
Generators and relations for 2-qubit Clifford+T operators.
To appear in *QPL 2022*. Available from arXiv:2204.02217, Apr. 2022.

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.