Generators and relations for 3-qubit Clifford+*CS* operators

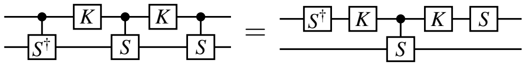
Xiaoning Bian and Peter Selinger
Dalhousie University

We give a presentation by generators and relations of the group of 3-qubit Clifford+*CS* operators. The proof roughly consists of two parts: (1) applying the Reidemeister-Schreier theorem recursively to an earlier result of ours; and (2) the simplification of thousands of relations into 17 relations. Both (1) and (2) have been formally verified in the proof assistant Agda. The Reidemeister-Schreier theorem gives a constructive method for computing a presentation of a sub-monoid given a presentation of the super-monoid. To achieve (2), we devise an almost-normal form for Clifford+*CS* operators. Along the way, we also identify several interesting structures within the Clifford+*CS* group. Specifically, we identify three different finite subgroups for whose elements we can give unique normal forms. We show that the 3-qubit Clifford+*CS* group, which is of course infinite, is the amalgamated product of these three finite subgroups. This result is analogous to the fact that the 1-qubit Clifford+*T* group is an amalgamated product of two finite subgroups.

1 Introduction

Just like Clifford+*T* circuits, the class of Clifford+*CS* circuits is universal for quantum computing [2]. Here, *CS* denotes the controlled-*S* gate. Amy, Glaudell, and Ross gave a characterization of the group of n-qubit Clifford+*CS* operators, showing that, up to a trivial condition on the determinant, a matrix is in this group if and only if it is unitary and its matrix entries belong to the ring $\mathbb{Z}[\frac{1}{2}, i]$ [2]. As a consequence of this, or alternatively since the *CS* gate is representable as a Clifford+*T* circuit with *T*-count 3, the Clifford+*CS* group is a subgroup of Clifford+*T*; see also [3]. Glaudell, Ross, and Taylor gave a normal form for 2-qubit Clifford+*CS* circuits [8]. In [9], Haah and Hastings showed how to construct a fault-tolerant *CS*-gate via magic state distillation. In [7], Garion and Cross described a *CS*- and *CX*-optimal canonical form for the 2-qubit group generated by the gates $\{X, T, CX, CS\}$.

This paper is motivated by the problem of optimizing Clifford+*CS* circuits. Like the *T*-gate, the *CS*-gate is a non-Clifford gate that is relatively expensive to perform in a fault-tolerant regime, requiring a magic state to be distilled [7]. It therefore makes sense to try to minimize the number of *CS*-gates. For example, one of the relations we found,



,

can sometimes be used to reduce the *CS*-count. Although we do not provide a method for minimizing the *CS*-count, we solve the important sub-problem of finding a complete set of relations for 3-qubit Clifford+*CS* circuits. This guarantees that any 3-qubit Clifford+*CS* circuit can be transformed into any other equivalent Clifford+*CS* circuit by the repeated application of a finite known set of relations.

Apart from giving a presentation of the group of 3-qubit Clifford+*CS* circuits by generators and relations, we also identify several interesting structures within this group along the way. Specifically, we identify three different finite subgroups for whose elements we can give unique normal forms. We show that the 3-qubit Clifford+*CS* group, which is of course infinite, is the amalgamated product of these three finite subgroups.

The paper is organized as follows. In Section 2, we provide the necessary background, including the definition of the Clifford+CS group. We also recall a presentation of the group of unitary matrices over the ring $\mathbb{Z}[\frac{1}{2},i]$ from our earlier work. In Section 3, we state our main result and give an outline of the proof. In Section 4, we present normal forms for three finite subgroups of the Clifford+CS operators, as well as an almost-normal form for Clifford+CS operators. In Section 5, we show that the 3-qubit Clifford+CS group is the amalgamated product of these three finite subgroups. This result is analogous to the fact that the 1-qubit Clifford+T group is an amalgamated product of two of its finite subgroups. In Section 6, we give a brief overview of the accompanying Agda code. We conclude the paper with some ideas for future work in Section 7.

2 Background

2.1 Clifford+CS operators

Consider the following unitary operators:

$$i, \qquad K = e^{-i\pi/4}H = \frac{1}{1+i}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \qquad CZ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

Here, i is a scalar, namely the usual complex unit. H is the Hadamard gate, and K is a scaled version of the Hadamard gate. S is sometimes called the *phase gate*, and CZ is the controlled-Z gate. When closed under multiplication, identities, and tensor products, these operators generate the *Clifford group* (possibly up to scalars, depending which scalars are included in the Clifford group — for our purposes, the scalars ± 1 and $\pm i$ are sufficient).

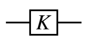
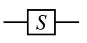
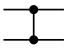
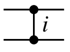
Every operator U obtained in this way is of size $2^n \times 2^n$ for some natural number n, and as usual, we say that U is an operator on n qubits. We write $\mathscr{C}(n)$ for the group of n-qubit Clifford operators. It is well-known that this group is finite for any given n (see, e.g., [12]), and therefore not universal for quantum computing. We can obtain a universal gate set by adding the controlled phase gate

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

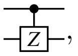
The resulting operators are called the Clifford+CS operators, and we write $\mathscr{CS}(n)$ for the n-qubit Clifford+CS group.

In this paper, we focus on the case $n = 3$. Our goal is to give a complete presentation of the 3-qubit Clifford+CS group in terms of generators and relations. To ensure that all of our generators are 8×8-matrices, we introduce the following notations: we write $CS_{01} = CS \otimes I, CS_{12} = I \otimes CS, K_0 = K \otimes I \otimes I, K_1 = I \otimes K \otimes I, K_2 = I \otimes I \otimes K$, and similarly for S_0, S_1, and S_2, where I is the 2×2 identity operator. We identify the scalar i with the 8×8-matrix iI. In the notation for controlled gates, we use the convention that the target is the last index. For example, CX_{01} is a controlled X-gate with control qubit 0 and target qubit 1. Note that the controlled S- and Z-gates are symmetric, in the sense that $CS_{jk} = CS_{kj}$ and $CZ_{jk} = CZ_{kj}$, and therefore the order of indices does not matter for them.

We use the following circuit notations for K, S, CZ, and CS, respectively:

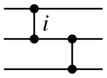
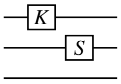
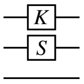
$K =$ , $S =$ , $CZ =$ , $CS =$ .

The CZ gate is usually denoted

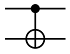
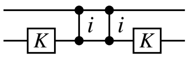


but since it is symmetric with respect to its two qubits, we prefer the more symmetric notation shown above. We also use a similar notation for the CS gate, except that we label it with an "i".

We number the qubits from top to bottom, and we write the circuits in the same order as matrix multiplication, i.e., from right to left. For example,

$CS_{01}CZ_{12} =$  , $K_0S_1 =$  $=$  .

Note that the X-gate and the controlled X-gate are definable as follows:

$X = KSSKi,$  $=$  $\cdot i.$

When we use the X- and controlled X-gates, for example in Figure 2, they are to be understood as abbreviations for these definitions.

2.2 A presentation of $U_n(\mathbb{Z}[\frac{1}{2},i])$

We briefly recall a result from our earlier work [4]. As usual, $\mathbb{Z}$ is the ring of integers. Let $\mathbb{Z}[\frac{1}{2},i]$ be the smallest subring of the complex numbers containing $\frac{1}{2}$ and i. Let $U_n(\mathbb{Z}[\frac{1}{2},i])$ be the group of unitary $n \times n$-matrices with entries in $\mathbb{Z}[\frac{1}{2},i]$.

In [4], we proved that the following is a presentation of $U_n(\mathbb{Z}[\frac{1}{2},i])$ by generators and relations. The generators are $i_{[j]}$, $X_{[j,k]}$, and $K_{[j,k]}$, where $j,k \in \{0,\ldots,n-1\}$ and $j < k$. The relations are shown in Figure 1. These relations are between words in the generators, and we write ε for the empty word (corresponding to the identity element of the group). The intended interpretation of the generators is as 1- and 2-level matrices; specifically, $i_{[j]}$ is like the identity matrix, except with i in the jth row and column, and $X_{[j,k]}$ and $K_{[j,k]}$ are like identity matrices, except with the entries of X, respectively K, in the jth and kth rows and columns, like this:

$$
i_{[j]} = \begin{array}{c} \\ \vdots \\ j \\ \vdots \end{array}\!\!\begin{array}{c} \begin{array}{ccc} \cdots & j & \cdots \end{array} \\ \begin{bmatrix} I & 0 & 0 \\ 0 & i & 0 \\ 0 & 0 & I \end{bmatrix} \end{array},\quad
X_{[j,k]} = \begin{array}{c} \\ \vdots \\ j \\ \vdots \\ k \\ \vdots \end{array}\!\!\begin{array}{c} \begin{array}{ccccc} \cdots & j & \cdots & k & \cdots \end{array} \\ \begin{bmatrix} I & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & I & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & I \end{bmatrix} \end{array},\quad
K_{[j,k]} = \begin{array}{c} \\ \vdots \\ j \\ \vdots \\ k \\ \vdots \end{array}\!\!\begin{array}{c} \begin{array}{ccccc} \cdots & j & \cdots & k & \cdots \end{array} \\ \begin{bmatrix} I & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{1+i} & 0 & \frac{1}{1+i} & 0 \\ 0 & 0 & I & 0 & 0 \\ 0 & \frac{1}{1+i} & 0 & \frac{-1}{1+i} & 0 \\ 0 & 0 & 0 & 0 & I \end{bmatrix} \end{array}.
$$

Theorem 2.1 ([4]). *Let $\mathcal{G}$ be the set of one- and two-level matrices $i_{[j]}$, $X_{[j,k]}$, and $K_{[j,k]}$, where $j,k \in \{0,\ldots,n-1\}$ and $j < k$. Let Δ be the set of relations shown in Figure 1. Then $(\mathcal{G},\Delta)$ is a presentation of $U_n(\mathbb{Z}[\frac{1}{2},i])$. In other words, the relations in Figure 1 are sound and complete for $U_n(\mathbb{Z}[\frac{1}{2},i])$.*

2.3 The Reidemeister-Schreier theorem

We will also make use of a result known as the Reidemeister-Schreier theorem for monoids [10, 11, 5]. In a nutshell, if G is a monoid and H is a submonoid of G, the Reidemeister-Schreier theorem, under suitable assumptions, gives a method for deriving generators and relations for H from generators and relations for G. Giving a complete account of the Reidemeister-Schreier theorem is beyond the scope of this paper, but we refer the interested reader to Section 4.2 of [5] for a detailed explanation.

$$
\begin{aligned}
i_{[j]}^{4} &\sim \varepsilon \qquad (1)\\
X_{[j,k]}^{2} &\sim \varepsilon \qquad (2)\\
K_{[j,k]}^{8} &\sim \varepsilon \qquad (3)\\[1em]
i_{[j]}i_{[k]} &\sim i_{[k]}i_{[j]} \qquad (4)\\
i_{[j]}X_{[k,\ell]} &\sim X_{[k,\ell]}i_{[j]} \qquad (5)\\
i_{[j]}K_{[k,\ell]} &\sim K_{[k,\ell]}i_{[j]} \qquad (6)\\
X_{[j,k]}X_{[\ell,m]} &\sim X_{[\ell,m]}X_{[j,k]} \qquad (7)\\
X_{[j,k]}K_{[\ell,m]} &\sim K_{[\ell,m]}X_{[j,k]} \qquad (8)\\
K_{[j,k]}K_{[\ell,m]} &\sim K_{[\ell,m]}K_{[j,k]} \qquad (9)
\end{aligned}
$$

$$
\begin{aligned}
i_{[k]}X_{[j,k]} &\sim X_{[j,k]}i_{[j]} \qquad (10)\\
X_{[k,\ell]}X_{[j,k]} &\sim X_{[j,k]}X_{[j,\ell]} \qquad (11)\\
X_{[j,\ell]}X_{[k,\ell]} &\sim X_{[k,\ell]}X_{[j,k]} \qquad (12)\\
K_{[k,\ell]}X_{[j,k]} &\sim X_{[j,k]}K_{[j,\ell]} \qquad (13)\\
K_{[j,\ell]}X_{[k,\ell]} &\sim X_{[k,\ell]}K_{[j,k]} \qquad (14)\\[1em]
K_{[j,k]}i_{[k]}^{2} &\sim X_{[j,k]}K_{[j,k]} \qquad (15)\\
K_{[j,k]}i_{[k]}^{3} &\sim i_{[k]}K_{[j,k]}i_{[k]}K_{[j,k]} \qquad (16)\\
K_{[j,k]}i_{[j]}i_{[k]} &\sim i_{[j]}i_{[k]}K_{[j,k]} \qquad (17)\\
K_{[j,k]}^{2}i_{[j]}i_{[k]} &\sim \varepsilon \qquad (18)\\
K_{[j,k]}K_{[\ell,m]}K_{[j,\ell]}K_{[k,m]} &\sim K_{[j,\ell]}K_{[k,m]}K_{[j,k]}K_{[\ell,m]} \qquad (19)
\end{aligned}
$$

Figure 1: A sound and complete set of relations for $U_n(\mathbb{Z}[\frac{1}{2},i])$. In each relation, the indices are assumed to be distinct; moreover, whenever a generator $X_{[a,b]}$ or $K_{[a,b]}$ is mentioned, we assume $a<b$.

3 A presentation of Clifford+*CS* operators

In this section, we state our main result and give an outline of the proof. The full proof can be found in the accompanying Agda code [6].

Theorem 3.1. *The* 3*-qubit Clifford+CS group is presented by* $(\mathscr{X},\Gamma_X)$*, where the set of generators is*

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

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

One interesting feature of the axioms in Figure 2 is that the upside-down version of each relation is also a relation, except for (C15). The upside-down version of (C15) is provable, so we do not require it as an axiom.

3.1 Proof outline

Our proof follows a similar general outline as the corresponding proof for 2-qubit Clifford+T operators in [5]. Let $G=U_8(\mathbb{Z}[\frac{1}{2},i])$ be the group of unitary 8×8-matrices with entries in $\mathbb{Z}[\frac{1}{2},i]$. An exact synthesis algorithm for G was given by Amy, Glaudell, and Ross [2]. Based on this, we gave a presentation of G by generators and relations in [4]. It is clear that $\mathscr{CS}(3)$ is a subgroup of G, because all of its generators belong to G. Moreover, by a result of Amy et al. [2], we know that $\mathscr{CS}(3)$ is precisely the subgroup of G consisting of matrices whose determinant is ± 1. The only other possible values for the determinant are $\pm i$, and therefore $\mathscr{CS}(3)$ is a subgroup of G of index 2. We can therefore apply the Reidemeister-Schreier procedure [10, 11] to find generators and relations for $\mathscr{CS}(3)$, given the known generators and relations for G. Applying this procedure yields a complete set of relations for $\mathscr{CS}(3)$.

The application of the Reidemeister-Schreier method produces thousands of relations, compared to the 17 cleaned-up relations in Figure 2. Moreover, these relations are very large. In our code, which

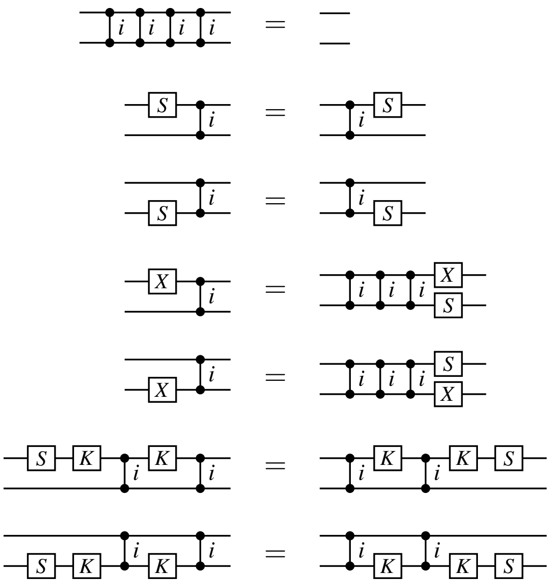
(a) Relations for $n \geq 0$:

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

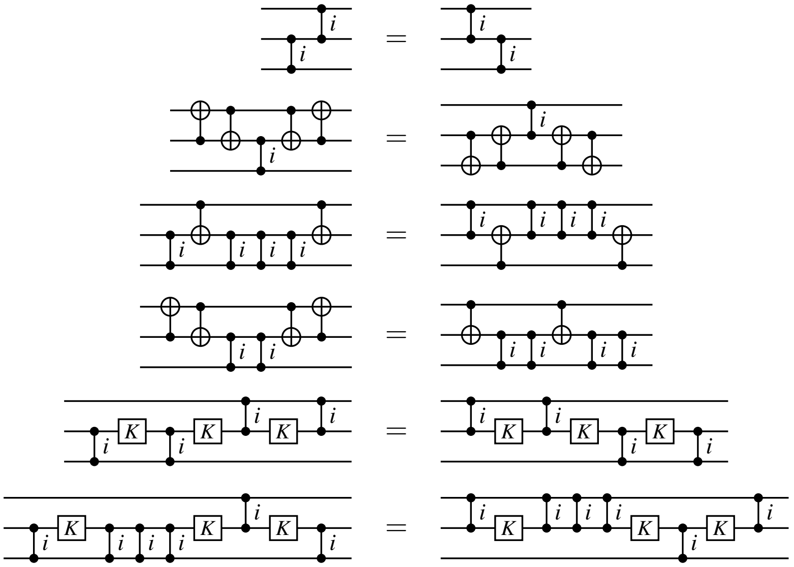
(b) Relations for $n \geq 1$:

$$\begin{aligned} K^2 &= i^3 && \text{(C2)} \\ S^4 &= \varepsilon && \text{(C3)} \\ SKSKSK &= i^3 && \text{(C4)} \end{aligned}$$

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



(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).

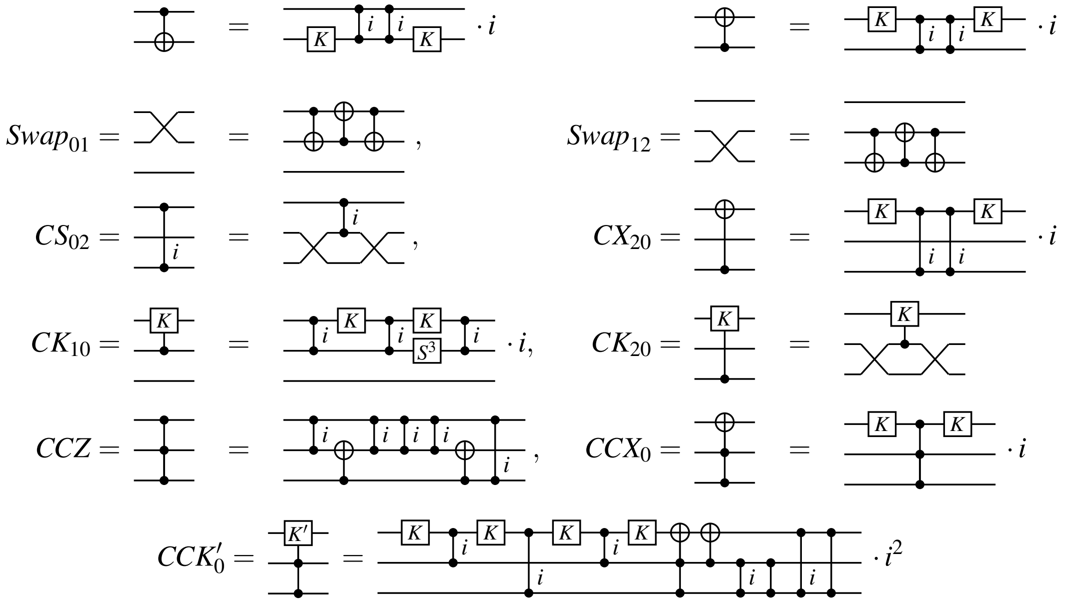
actually uses a sequence of multiple applications of the Reidemeister-Schreier theorem passing through a number of intermediate representations, some of the longest relations involve more than 50,000 generators. Our main contribution is the simplification of these relations. Due to the sheer magnitude of this task, we must rely on a computer to expedite the computation. However, we also require the simplification process to be trustworthy, as it is very easy in a computer program to accidentally use a relation that has not yet been proved. To this end, we have formalized Theorem 3.1 and its proof in the proof assistant Agda. This allows the proof to be verified independently and with a high degree of confidence in its correctness, despite the magnitude of the proof.

The main idea of the simplification is to use the 17 relations from Figure 2, along with some of their easy consequences, to rewrite the thousands of relations until they are all eliminated. We define several rewrite systems for this task. Some of these rewrite systems are confluent and terminating, and others are just heuristics. All of these rewrite systems are implemented in Agda and the computations are verified within Agda.

4 Normal forms and an almost-normal form

4.1 Notations

For convenience, we will use the following notations:



The first two notations extend to 3-qubit circuits, giving us the definitions of, for example, CX_{01}, and CX_{21}. The definitions for a Toffoli gate with target on the second, respectively first, qubit are given by $CCX_1 = Swap_{01}\, CCX_0\, Swap_{01}$ and $CCX_2 = Swap_{12}\, CCX_1\, Swap_{12}$. The last notation uses a twice-controlled K' gate. Here $K' = KS^\dagger$ is a variant of the K-gate that has determinant 1. The reason we are not using a twice-controlled K-gate is that it has determinant i and is therefore not an element of $\mathscr{CS}(3)$.

4.2 Normal forms for finite subgroups of Clifford+CS operators

We will define normal forms and discuss the structure of the following finite subgroups of Clifford+CS operators. The inclusion relations between these subgroups are visualized in Figure 3.

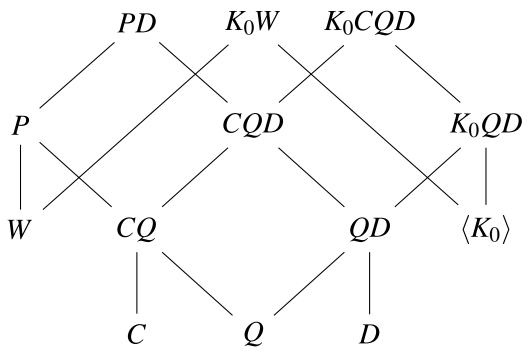


Figure 3: The inclusion graph of various finite subgroups of $\mathscr{CS}(3)$

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

Note that P is the group of all permutations of the computational basis vectors; we call its members "permutation operators". Q, C, and CQ are subgroups of P. Similarly, D is the group of all diagonal operators in $\mathscr{CS}(3)$. The remaining subgroups play a technical role in our proofs.

Given that all claims about finite groups can be proved by just enumerating the elements, we will not give proofs of the following claims about finite subgroups of $\mathscr{CS}(3)$. Instead, we will illustrate the proofs with examples. Some of the proofs can be found in the Agda code.

The group W is the group of permutations of 3 qubits.

The generators of Q all commute with each other and are self-inverse. Therefore, each element of Q can be uniquely written of the form $X_0^a CX_{10}^b CX_{20}^c CCX_0^d$, where $a,b,c,d \in \{0,1\}$. We say that the subgroup Q has the following normal form:

$$\overline{Q} \ ::= \ X_0^a CX_{10}^b CX_{20}^c CCX_0^d, \text{ where } a,b,c,d \in \{0,1\}. \tag{20}$$

We use $\overline{Q}$ to range over normal forms for Q. More generally, given any group G for which normal forms are defined, we use $\overline{G}$ to range over the normal forms of G. The group Q has $2^4 = 16$ distinct normal forms corresponding to 16 distinct elements.

It is easy to see that $Swap_{12} \in C$, and therefore also $X_2 \in C$. The group C has the following normal form:

$$\overline{C} \ ::= \ c_4 c_3 c_2 \tag{21}$$

where

$$\begin{aligned} c_2 &\in \{\varepsilon, CX_{12}\}, \\ c_3 &\in \{\varepsilon, CX_{21}, CX_{12}CX_{21}\}, \\ c_4 &\in \{X_1^a X_2^b \mid a,b \in \{0,1\}\}. \end{aligned}$$

There are $4! = 24$ distinct normal forms in C.

The group CQ is a semidirect product of C and Q with Q being normal. A semidirect product structure means that we have commuting relations of the form $qc = cq'$, or more precisely, for all $q \in Q$ and $c \in C$, there exists a unique $q' \in Q$ such that $qc = cq'$. Consequently, CQ has the following normal form:

$$\overline{CQ} \ ::= \ \overline{C}\,\overline{Q}.$$

The group P contains CQ as a subgroup with 105 cosets. We get the following normal form for P:

$$\overline{P} = c\overline{CQ}, \text{ where } c \text{ ranges over the set } V \text{ of 105 left coset representatives.} \tag{22}$$

One can easily spot a normal form for D, since all the generators commute with each other, CCZ has order 2, and all of the other generators have order 4. The normal form is:

$$\overline{D} \ ::= \ i^{n_0} S_0^{n_1} S_1^{n_2} S_2^{n_3} CS_{01}^{n_4} CS_{12}^{n_5} CS_{02}^{n_6} CCZ^{n_7}, \text{ where } n_0, \ldots, n_6 \in \{0,1,2,3\} \text{ and } n_7 \in \{0,1\}. \tag{23}$$

The group PD is a semidirect product of P and D, with D being normal. It therefore has the following normal form:

$$\overline{PD} \ ::= \ \overline{P}\,\overline{D}. \tag{24}$$

Since Q is a subgroup of P, it follows that QD is also a semidirect product. It enjoys a similar normal form as (24), with P replaced by Q.

It is easy to see the that group K_0D contains $\mathscr{X}_Q$, hence Q is a subgroup of K_0D. We have the following normal form:

$$\overline{K_0D} \ ::= \ e_4 e_3 e_2 e_1 \overline{D}\,\overline{Q}, \tag{25}$$

where

$$\begin{aligned} e_1 &\in \{\varepsilon, CCK_0', CCK_0'CCK_0'\}, \\ e_2 &\in \{\varepsilon, CK_{10}, S_0CK_{10}\}, \\ e_3 &\in \{\varepsilon, CK_{20}, S_0CK_{20}\}, \\ e_4 &\in \{\varepsilon, K_0, S_0K_0\}. \end{aligned}$$

Note that CK_{10}, CK_{20} and K_0 commute with each other but not with CCK_0'.

Notice that each element of $\mathscr{X}_C$ commutes with K_0. For any element of K_0CD, for example $w = X_1K_0CS_{01}K_0CCZ$, we can commute X_1 all the way to the right using the commuting relations and the semidirect product structure of QD. For example, we get $w = K_0CS_{01}CS_{01}CS_{01}S_0K_0CCZCS_{02}CS_{02}X_1$. We will use the following normal form for K_0CD:

$$\overline{K_0CD} = \overline{(K_0D)}\ \overline{C} = e_4e_3e_2e_1\overline{D}\,\overline{Q}\,\overline{C}. \tag{26}$$

Note that this also proves that K_0CD is finite, which perhaps wasn't obvious from its definition.

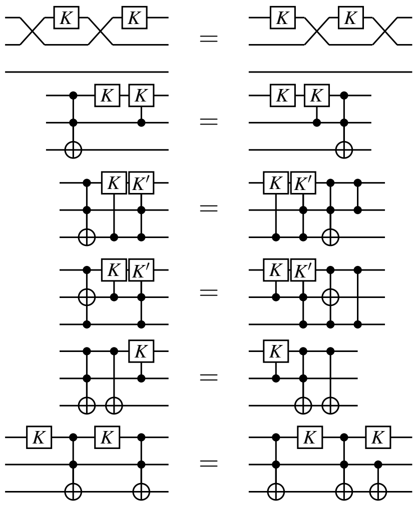


Figure 4: Some relations used to rewrite words of the form $ce_4e_3e_2e_1\,ce_4e_3e_2e_1\,\ldots\,ce_4e_3e_2e_1$.

4.3 An almost-normal form for $\mathscr{CS}(3)$

Consider a Clifford+*CS* circuit. After replacing the generators K_1 and K_2 by $Swap_{01}\,K_0\,Swap_{01}$ and $Swap_{12}\,Swap_{01}\,K_0\,Swap_{01}\,Swap_{12}$, respectively, the circuit can be written as an alternating sequence of elements of PD and K_0:

$$PD\,K_0\,PD\,K_0\ldots PD\,K_0\,PD.$$

By repeatedly converting subcircuits to normal forms of the form (24), (22), and (26), we can rewrite this circuit as follows:

$$\begin{array}{rl} & PD\,K_0\,PD\,K_0\ldots PD\,K_0\,PD \\ \overset{(24)(22)}{\to} & c\overline{CQD}K_0c\overline{CQD}K_0\ldots c\overline{CQD}K_0c\overline{CQD} \\ \overset{(26)}{\to} & ce_4e_3e_2e_1\overline{D}\,\overline{Q}\,\overline{C}c\overline{CQD}K_0\ldots c\overline{CQD}K_0c\overline{CQD} \\ \overset{(24)(22)}{\to} & ce_4e_3e_2e_1c\overline{CQD}K_0\ldots c\overline{CQD}K_0c\overline{CQD} \\ \overset{repeat}{\to} & ce_4e_3e_2e_1\,ce_4e_3e_2e_1\,\ldots\,ce_4e_3e_2e_1c\overline{CQD}. \end{array}$$

We can further rewrite the last expression, for example using relations in Figure 4. After this step, we might get some new gates that are not in V or of the form e_i. In this case, we continue with the first arrow step. We repeat the whole process until there is no further simplification. We call the resulting word an *almost-normal form*.

It turns out this almost-normal form is "canonical" enough. It can be used to show that a complete set of thousands of relations hold by rewriting both sides of each relation to almost-normal form. Moreover, all rewriting rules used to get an almost-normal form are consequences of the relations in Figure 2. This shows that the relations in Figure 2 are complete.

5 Clifford+*CS* is an amalgamated product of three finite groups

Let us first recall the definition of an amalgamated product of two monoids. For category theorists, this is simply a pushout: 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

$$\begin{tikzcd}
H \arrow[r] \arrow[d] & M_2 \arrow[d, dashed] \\
M_1 \arrow[r, dashed] & M_1 *_H M_2. \arrow[ul, phantom, "\ulcorner", very near start]
\end{tikzcd}$$

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:

$$\begin{tikzcd}
 & & H_{23} \arrow[dr] \arrow[dd] & \\
 & H_{13} \arrow[rr] \arrow[dd] & & M_3 \arrow[dd, dashed] \\
H_{12} \arrow[rr] \arrow[dr] & & M_2 \arrow[dr, dashed] & \\
 & M_1 \arrow[rr, dashed] & & P.
\end{tikzcd}$$

In terms of generators and relations, we have the following situation: Suppose we have three sets of generators X, Y, and Z, and three monoid presentations $M_1 = \langle X \cup Y \mid \Gamma_1 \rangle$, $M_2 = \langle X \cup Z \mid \Gamma_2 \rangle$, 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. In that case, the slogan "the only relations that hold in P are relations that hold in a finite submonoid of P" applies.

Using the results of this paper, we can show that $\mathscr{CS}(3)$ is an amalgamated product of three finite groups. We choose the sets of generators as follows:

$$\begin{aligned}
X &= \{K_0, i\}, \\
Y &= \{X_0, X_1, X_2, CX_{12}, CX_{21}, CX_{10}, CX_{20}, CCX_0, S_0, S_1, S_2, CS_{01}, CS_{12}, CS_{02}, CCZ, i\}, \\
Z &= \{Swap_{01}, Swap_{12}\}.
\end{aligned}$$

One can check that $\langle X \cup Y \rangle = K_0 CQD$, $\langle X \cup Z \rangle = K_0 W$, and $\langle Y \cup Z \rangle = PD$. Since $X \cup Y$, $X \cup Z$, and $Y \cup Z$ each generate a finite subgroup of $\mathscr{CS}(3)$, all that is left to show is that each relation of $\mathscr{CS}(3)$ is a consequence of relations in one of these three subgroups.

Before we prove this, we must adjust the relations of Figure 2 to fit the new set of generators $X \cup Y \cup Z$. This requires two adjustments. First, compared to the set of generators from Theorem 3.1, a number of new generators have been added, namely X_0, X_1, X_2, CX_{12}, CX_{21}, CX_{10}, CX_{20}, CCX_0, CS_{02}, CCZ, $Swap_{01}$, and $Swap_{12}$. For each of these, we must add a defining relation in terms of the old generators. These relations are as in Section 4.1. Second, the two generators K_1 and K_2 are no longer used, so where they appear in the relations, they must now be regarded as abbreviations for the words $Swap_{01}\, K_0\, Swap_{01}$ and $Swap_{12}\, Swap_{01}\, K_0\, Swap_{01}\, Swap_{12}$, respectively. With these adjustments, we still have a sound and complete presentation of $\mathscr{CS}(3)$ using the generators $X \cup Y \cup Z$.

Now we must show that each of the relations follows from relations that hold in $\langle X \cup Y \rangle$, $\langle X \cup Z \rangle$, or $\langle Y \cup Z \rangle$. many of the relations, such as (C1), (C3), (C5)–(C9), and (C12) are already in one of the three subgroups, so there is nothing else to show for them. The remaining relations must be proved individually; here, we give a proof of (C16) as a representative example. We have:

$$\begin{array}{rll}
\multicolumn{2}{l}{CS_{12}\,K_1\,CS_{12}\,K_1\,CS_{01}\,K_1\,CS_{01}} & \\
= & CS_{12}\,Swap_{01}\,K_0\,Swap_{01}\,CS_{12}\,Swap_{01}\,K_0\,Swap_{01}\,CS_{01}\,Swap_{01}\,K_0\,Swap_{01}\,CS_{01} & (1)\\
= & Swap_{01}\,CS_{02}\,K_0\,CS_{02}\,K_0\,CS_{01}\,K_0\,CS_{01}\,Swap_{01} & (2)\\
= & Swap_{01}\,CS_{01}\,K_0\,CS_{01}\,K_0\,CS_{02}\,K_0\,CS_{02}\,Swap_{01} & (3)\\
= & CS_{01}\,Swap_{01}\,K_0\,Swap_{01}\,CS_{01}\,Swap_{01}\,K_0\,Swap_{01}\,CS_{12}\,Swap_{01}\,K_0\,Swap_{01}\,CS_{12} & (4)\\
= & CS_{01}\,K_1\,CS_{01}\,K_1\,CS_{12}\,K_1\,CS_{12} & (5)
\end{array}$$

Here, steps (1) and (5) use the definition of K_1, which is at this point merely an abbreviation for $Swap_{01}\,K_0\,Swap_{01}$. Steps (2) and (4) uses the relations $Swap^2_{01} = \varepsilon$ and $Swap_{01}\,CS_{12}\,Swap_{01} = CS_{02}$ and $Swap_{01}\,CS_{01}\,Swap_{01} = CS_{01}$. All three of these relations come from $\langle Y \cup Z\rangle$. Step (3) uses the relation $CS_{02}\,K_0\,CS_{02}\,K_0\,CS_{01}\,K_0\,CS_{01} = CS_{01}\,K_0\,CS_{01}\,K_0\,CS_{02}\,K_0\,CS_{02}$, which comes from $\langle X \cup Y\rangle$. In addition to (C16), there are a number of other relations to be proved, but they all follow a similar pattern.

As mentioned in the introduction, there is an analogous result for the 1-qubit Clifford+T group, which is also an infinite group, and which is an amalgamated product of two finite subgroups. In this case, the finite subgroups are the Clifford group and the subgroup of diagonal and permutation operators, which is generated by T and X.

6 An overview of the accompanying Agda code

This paper is accompanied by a machine-checkable proof of Theorem 3.1 [6]. It has been formalized in the proof assistant Agda [1]. The proof assumes only the result of [4], i.e., the soundness and completeness of a certain set of relations for $U_n(\mathbb{Z}[\frac{1}{2}, i])$. Everything else is proved from first principles, including, for example, a complete proof of the version of the Reidemeister-Schreier theorem that we used.

Verifying the proof. Readers who are interested in verifying the proof only need to know the following: The *statement* of Theorem 3.1 is contained in the file `Theorem.agda`, and the final step of the *proof* of Theorem 3.1 is contained in the file `Proof.agda`. The reason we separated the statement of the theorem from its proof is to ensure that the statement assumes as little as possible: in fact, the file `Theorem.agda` is almost completely self-contained and only depends on a few definitions concerning generators, words, indices, and two-level relations. On the other hand, the proof requires a large number of auxiliary files with definitions, lemmas, tactics, and more. We checked the proof with Agda 2.6.4, and it took about 120 minutes on our laptop.

Reading the proof. For readers who are interested in inspecting our proof, here are some pointers. The folder `Lib` contains some general-purpose definitions, such as booleans and natural numbers, and some definitions and tactics related to monoids and relations. The main parts of the proof are contained in the folders `Step1` – `Step8`. Each of these steps transforms a set of generators and relations into an equivalent set of generators and relations, gradually simplifying the relations. The file `Gate.agda` provides the definitions for all gates used. The file `CosetNF.agda` contains definitions related to semidirect products and normal forms. The final proof witness is contained in the file `Proof.agda`.

7 Conclusion and future work

The main result of this paper is a presentation of the group of 3-qubit Clifford+CS operators by just 17 relatively simple relations. We proved this by a combination of a previous result from [4], the Reidemeister-Schreier method, and an Agda program that simplified several thousand large relations into the aforementioned 17 simple ones. Doing this simplification by brute force would not have been feasible. Instead, we proceeded by identifying a number of finite subgroups of the Clifford+CS operators, defining normal forms for these, and then combining them into carefully chosen rewrite rules. After months of fine-tuning, these rules eventually reduced the relations to a manageable size.

Unlike our previous work on generators and relations for 2-qubit Clifford+T operators [5], which used a *Pauli rotation decomposition* to guide the rewriting, we found that the analog of the Pauli rotation decomposition, i.e., taking syllables that are conjugates of the CS gate under the action of the Clifford operators, does not work very well. Instead, we were surprised to find that a more useful decomposition was to take conjugates of K_0 (basically a Hadamard gate) under the action of diagonal and permutation operators. We may call this the *Hadamard decomposition* of Clifford+CS. In the process, we learned many interesting facts about finite subgroups of Clifford+CS. One of these facts is that the 3-qubits Clifford+CS group is an amalgamated product of three of its finite subgroups. Concretely, this means that every relation that holds in this group follows from relations that already hold in some finite subgroup of Clifford+CS.

This work suggests some interesting directions for future work. Many of our results about finite subgroups of Clifford+CS are valid for n qubits, so one may ask whether our generators and relations can also be extended to circuits with 4 or more qubits. Currently, the limiting factor is the prohibitive computational cost of applying the Reidemeister-Schreier method to a set of 2-level relations for 16×16-matrices and then simplifying a massive set of relations. Perhaps a further study of the finite subgroups of Clifford+CS will open up an alternative path to this problem. For example, one may ask whether the n-qubit Clifford+CS group is an amalgamated product for all n. One may further ask the same question for the n-qubits Clifford+T group or its other subgroups of interest, such as the Clifford+Toffoli group.

The fact that the Hadamard decomposition turned out to be more useful than the analog of the Pauli rotation decomposition raises the question whether our earlier work on Clifford+T could benefit from the same insight. By applying these lessons, perhaps one can come up with a simpler complete set of relations. For example, our Clifford+T axiomatization involved a number of obvious relations and three "non-obvious" ones. We were never able to resolve the question of whether these non-obvious relations actually follow from something simpler.

Another intriguing question is whether one can find a unique normal form for 3-qubit Clifford+CS circuits, like the Matsumoto-Amano normal form for 1-qubit Clifford+T circuits. We currently only have an "almost-normal" form, but the fact that it efficiently reduced all of our relations is encouraging.

References

[1] *Agda Documentation*. `https://agda.readthedocs.io/`. Accessed: 2023-03-17.

[2] Matthew Amy, Andrew N. Glaudell & Neil J. Ross (2020): *Number-theoretic characterizations of some restricted Clifford+T circuits*. Quantum 4, p. 252, doi:10.22331/q-2020-04-06-252. Also available from arXiv:1908.06076.

[3] Michael Beverland, Earl Campbell, Mark Howard & Vadym Kliuchnikov (2020): *Lower bounds on the non-Clifford resources for quantum computations*. Quantum Science and Technology 5(3), p. 035009.

[4] Xiaoning Bian & Peter Selinger (2021): *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, Electronic Proceedings in Theoretical Computer Science* 343, pp. 145–164, doi:10.4204/EPTCS.343.8.

[5] Xiaoning Bian & Peter Selinger (2022): *Generators and relations for 2-qubit Clifford+T operators*. To appear in *QPL 2022*. Available from arXiv:2204.02217.

[6] Xiaoning Bian & Peter Selinger (2023): *Agda code accompanying this paper*. Available from `https://www.mathstat.dal.ca/~selinger/papers/downloads/cliffordcs3/`.

[7] Shelly Garion & Andrew W Cross (2020): *Synthesis of CNOT-dihedral circuits with optimal number of two qubit gates*. *Quantum* 4, p. 369.

[8] Andrew N. Glaudell, Neil J. Ross & Jacob M. Taylor (2021): *Optimal two-qubit circuits for universal fault-tolerant quantum computation*. *npj Quantum Information* 7(1), p. 103, doi:10.1038/s41534-021-00424-z.

[9] Jeongwan Haah & Matthew B Hastings (2018): *Codes and protocols for distilling T, controlled-S, and Toffoli gates*. *Quantum* 2, p. 71.

[10] Kurt Reidemeister (1927): *Knoten und Gruppen*. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg* 5(1), pp. 7–23, doi:10.1007/BF02952506.

[11] Otto Schreier (1927): *Die Untergruppen der freien Gruppen*. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg* 5(1), pp. 161–183, doi:10.1007/BF02952517.

[12] Peter Selinger (2015): *Generators and relations for n-qubit Clifford operators*. *Logical Methods in Computer Science* 11(2:10), pp. 1–17, doi:10.2168/LMCS-11(2:10)2015. Also available from arXiv:1310.6813.