Generators and relations for 2-qubit Clifford+T operators

Xiaoning Bian and Peter Selinger
Dalhousie University

We give a presentation by generators and relations of the group of Clifford+T operators on two qubits. The proof relies on an application of the Reidemeister-Schreier theorem to an earlier result of Greylyn, and has been formally verified in the proof assistant Agda.

1 Introduction

The simplification of Clifford+T circuits is a topic of current interest in quantum computing [4, 5, 6, 15, 16, 17]. The Clifford+T gate set is both universal [18] and convenient for quantum error correction [9], and is therefore the preferred gate set for fault-tolerant quantum computing. Generally, in a fault-tolerant regime, applying a Clifford gate is some orders of magnitude cheaper than applying a T-gate, and therefore, it is sensible to try to simplify circuits so as to minimize the T-count [3]. Many methods for doing so have been proposed in the recent literature, including methods based on matroid partitioning [2], Reed-Muller codes [4], and ZX calculus [5, 6, 16]. Regardless of which method is used, the objective is to replace a Clifford+T circuit by a simpler, but equivalent circuit. This requires being able to tell when two circuits are equivalent. Surprisingly, no complete set of relations for ancilla-free Clifford+T circuits is currently known, i.e., there is no known set of relations by which any two equivalent Clifford+T circuits can be transformed into each other.

In this paper, we give such a complete set of relations for the case of 2-qubit Clifford+T circuits. We do this in several steps. First, a presentation of the group $U_4(\mathbb{Z}[\frac{1}{\sqrt{2}},i])$ of all unitary 4×4-matrices over the ring $\mathbb{Z}[\frac{1}{\sqrt{2}},i]$ is known due to the work of Greylyn [13]. Second, it is known that the group of 2-qubit Clifford+T circuits is exactly the subgroup of this group consisting of matrices whose determinant is in $\{\pm 1,\pm i\}$ [10]. Third, there is a theorem in group theory called the Reidemeister-Schreier theorem, by which a complete set of relations for a subgroup can be derived from a complete set of relations for the supergroup. Fourth, since the resulting relations are very long and complicated, we simplify them.

The last two steps of this procedure (applying the Reidemeister-Schreier theorem and simplifying the resulting relations) require a large amount of algebraic manipulations. Our longest equational proof has 480 steps, each of which in turns requires a lemma or rewrite procedure whose proof itself requires many equational steps. Such proofs would be impossible to verify by hand, and even verifying them by software is error-prone since it is hard to guarantee that no unwarranted assumptions were used. For this reason, we encoded our proof in machine-checkable form, using the proof assistant Agda [1].

The rest of this paper is organized as follows. In Section 2, we state our main result. Section 3 gives a brief overview of the proof. In Section 4, we present the required background material, including Greylyn's presentation of $U_4(\mathbb{Z}[\frac{1}{\sqrt{2}},i])$, the Reidemeister-Schreier theorem, and the Pauli rotation representation, which is an important tool for manipulating Clifford+T circuits. We also briefly describe our reasons for formalizing our proof in a proof assistant. Section 5 describes our formal proof of the main result. In Section 6, we briefly discuss the meaning of the Clifford+T relations, and especially of the three "non-obvious" relations. Section 7 contains some concluding remarks and ideas for future work.

2 Statement of the main result

Recall that 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, 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 [21], and therefore not universal for quantum computing. 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, and we write $\mathscr{C}\mathscr{T}(n)$ for the n-qubit Clifford+T group.

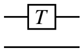
In this paper, we focus on the case $n = 2$. Our goal is to give a complete presentation of the 2-qubit Clifford+T group in terms of generators and relations. To ensure that all of our generators are 4×4-matrices, we introduce the following notation: we write $T_0 = T \otimes I$ and $T_1 = I \otimes T$, and similarly for H_0, H_1, S_0, and S_1. We also identify the scalar ω with the 4×4-matrix ωI. Our main result is the following:

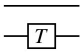
Theorem 2.1. *The 2-qubit Clifford+T group is presented by* $(\mathscr{X}, \Gamma)$*, where the set of generators is*

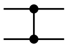
$$\mathscr{X} = \{\omega, H_0, H_1, S_0, S_1, T_0, T_1, CZ\},$$

and the set of relations Γ *is shown in Figure 1.*

In Figure 1, we have used circuit notation to express some of the relations; for example, we have written



,


, and


for T_0, T_1, and CZ, respectively. Note that the qubits are numbered from top to bottom. We write circuits in the same order as matrix multiplication. Moreover, in relations (C18)–(C20), we have used a number of abbreviations; these are defined in Figure 2. The empty word is denoted ε.

3 Proof outline

In a nutshell, the proof can be described in a few sentences. It proceeds as follows. 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. Then it is clear that $\mathscr{C}\mathscr{T}(2)$ is a subgroup of G, because all of its generators belong to G. Moreover, from [10], it is known that $\mathscr{C}\mathscr{T}(2)$ is precisely equal to the subgroup of G consisting of matrices whose determinant is a power of i. A presentation of G by generators and relations was given by Greylyn [13]. There is a general procedure, called the Reidemeister-Schreier procedure [19, 20], for finding generators and relations of a subgroup, given generators and relations of the supergroup. Applying this procedure therefore yields a complete set of relations for $\mathscr{C}\mathscr{T}(2)$.

While in principle, the above proof outline suffices to prove Theorem 2.1, in practice there is a large amount of non-trivial work involved in generating and simplifying the actual relations. For this reason, we have formalized Theorem 2.1 and its proof in the proof assistant Agda. This allows the proof to be independently checked without too much manual work.

(a) Monoidal relations:

$$\omega A = A\omega, \quad \text{where } A \in \{H_i, S_i, T_i, CZ\} \tag{C1}$$

$$A_0 B_1 = B_1 A_0, \quad \text{where } A, B \in \{H, S, T\} \tag{C2}$$

(b) Order of Clifford group elements:

$$\omega^8 = \varepsilon \tag{C3}$$

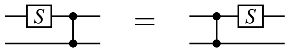
$$H_i^2 = \varepsilon \tag{C4}$$

$$S_i^4 = \varepsilon \tag{C5}$$

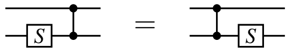
$$(S_i H_i)^3 = \omega \tag{C6}$$

$$CZ^2 = \varepsilon \tag{C7}$$

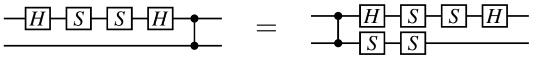
(c) Remaining Clifford relations:



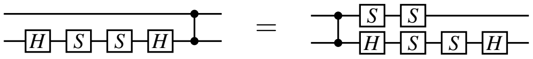
(C8)



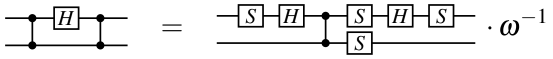
(C9)



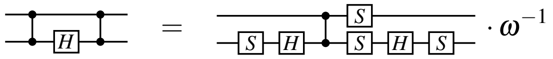
(C10)



(C11)



(C12)

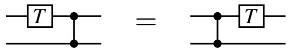


(C13)

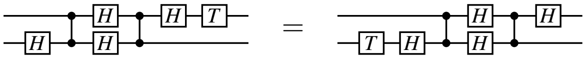
(d) "Obvious" relations involving T:

$$T_i^2 = S_i \tag{C14}$$

$$(T_i H_i S_i S_i H_i)^2 = \omega \tag{C15}$$

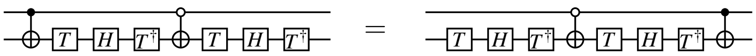


(C16)

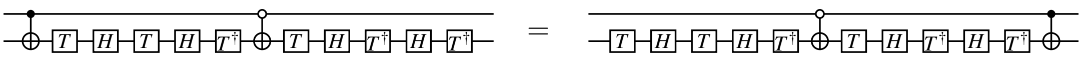


(C17)

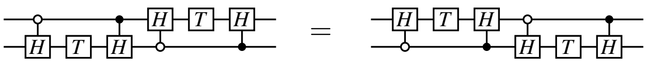
(e) "Non-obvious" relations involving T:



(C18)



(C19)



(C20)

Figure 1: Relations for 2-qubit Clifford+T operators. Here $i \in \{0, 1\}$.

$$\begin{aligned} T^{\dagger} &= T^{7} \\ S^{\dagger} &= S^{3} \end{aligned}$$

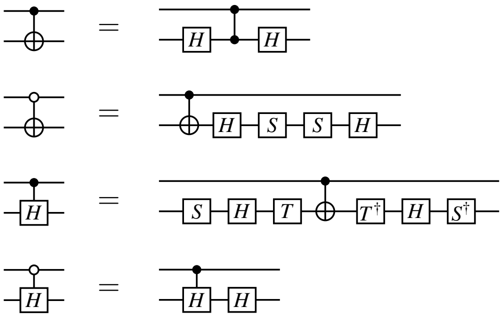


Figure 2: Abbreviations used in circuit notations

4 Background

4.1 Presentation of $U_4(\mathbb{Z}[\frac{1}{\sqrt{2}},i])$

As usual, $\mathbb{Z}$ is the ring of integers. Let $R = \mathbb{Z}[\frac{1}{\sqrt{2}},i]$ be the smallest subring of the complex numbers containing $\frac{1}{\sqrt{2}}$ and i. Let $\omega = e^{i\pi/4}$ be an 8th root of unity, and note that $\omega = \frac{1+i}{\sqrt{2}} \in R$. As before, $U_4(R)$ is the group of unitary 4×4-matrices with entries in R.

Greylyn [13] gave a presentation of $U_4(R)$ by generators and relations. His generators are $\omega_{[j]}$, $X_{[j,k]}$, and $H_{[j,k]}$, where $j,k \in \{0,...,3\}$ and $j<k$. The relations are shown in Figure 3. The intended interpretation of the generators is as 1- and 2-level matrices; specifically, $\omega_{[j]}$ is like the identity matrix, except with ω in the jth row and column, and $X_{[j,k]}$ and $H_{[j,k]}$ are like identity matrices, except with the entries of X, respectively H, in the jth and kth rows and columns, like this:

$$\omega_{[j]} = \begin{array}{c|ccc|} & \cdots & j & \cdots \\ \hline \vdots & I & 0 & 0 \\ j & 0 & \omega & 0 \\ \vdots & 0 & 0 & I \\ \hline \end{array}, \quad X_{[j,k]} = \begin{array}{c|ccccc|} & \cdots & j & \cdots & k & \cdots \\ \hline \vdots & I & 0 & 0 & 0 & 0 \\ j & 0 & 0 & 0 & 1 & 0 \\ \vdots & 0 & 0 & I & 0 & 0 \\ k & 0 & 1 & 0 & 0 & 0 \\ \vdots & 0 & 0 & 0 & 0 & I \\ \hline \end{array}, \quad H_{[j,k]} = \begin{array}{c|ccccc|} & \cdots & j & \cdots & k & \cdots \\ \hline \vdots & I & 0 & 0 & 0 & 0 \\ j & 0 & \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} & 0 \\ \vdots & 0 & 0 & I & 0 & 0 \\ k & 0 & \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} & 0 \\ \vdots & 0 & 0 & 0 & 0 & I \\ \hline \end{array}.$$

Note that we index rows and columns of matrices starting from 0, whereas Greylyn indexed them starting from 1. Greylyn's result is the following:

Theorem 4.1 (Greylyn [13])**.** *A presentation of the group $U_4(R)$ is given by $(\mathscr{Y},\Delta)$, where the set of generators is $\mathscr{Y} = \{\omega_{[j]}, X_{[j,k]}, H_{[j,k]} \mid j,k \in \{1,...,4\}$ and $j<k\}$, and the set of relations Δ is shown in Figure 3.*

4.2 The Reidemeister-Schreier theorem for monoids

The Reidemeister-Schreier theorem is a theorem in group theory that allows one to derive a complete set of relations for a subgroup from a complete set of relations for the supergroup, given enough information about the cosets. We will use a version of the Reidemeister-Schreier theorem that works for monoids,

(a) Order of generators:

$$\begin{array}{rcll}
\omega_{[j]}^{8} & = & \varepsilon & \text{(G1)} \\
H_{[j,k]}^{2} & = & \varepsilon & \text{(G2)} \\
X_{[j,k]}^{2} & = & \varepsilon & \text{(G3)}
\end{array}$$

(b) Disjoint generators commute:

$$\begin{array}{rcll}
\omega_{[j]}\omega_{[k]} & = & \omega_{[k]}\omega_{[j]}, & \text{where } j \neq k \quad \text{(G4)} \\
\omega_{[\ell]}H_{[j,k]} & = & H_{[j,k]}\omega_{[\ell]}, & \text{where } \ell \neq j,k \quad \text{(G5)} \\
\omega_{[\ell]}X_{[j,k]} & = & X_{[j,k]}\omega_{[\ell]}, & \text{where } \ell \neq j,k \quad \text{(G6)} \\
H_{[j,k]}H_{[\ell,t]} & = & H_{[\ell,t]}H_{[j,k]}, & \text{where } \{\ell,t\} \cap \{j,k\} = \emptyset \quad \text{(G7)} \\
H_{[j,k]}X_{[\ell,t]} & = & X_{[\ell,t]}H_{[j,k]}, & \text{where } \{\ell,t\} \cap \{j,k\} = \emptyset \quad \text{(G8)} \\
X_{[j,k]}X_{[\ell,t]} & = & X_{[\ell,t]}X_{[j,k]}, & \text{where } \{\ell,t\} \cap \{j,k\} = \emptyset \quad \text{(G9)}
\end{array}$$

(c) X permutes indices:

$$\begin{array}{rcll}
X_{[j,k]}\omega_{[k]} & = & \omega_{[j]}X_{[j,k]} & \text{(G10)} \\
X_{[j,k]}\omega_{[j]} & = & \omega_{[k]}X_{[j,k]} & \text{(G11)} \\
X_{[j,k]}X_{[j,\ell]} & = & X_{[k,\ell]}X_{[j,k]} & \text{(G12)} \\
X_{[j,k]}X_{[\ell,j]} & = & X_{[\ell,k]}X_{[j,k]} & \text{(G13)} \\
X_{[j,k]}H_{[j,\ell]} & = & H_{[k,\ell]}X_{[j,k]} & \text{(G14)} \\
X_{[j,k]}H_{[\ell,j]} & = & H_{[\ell,k]}X_{[j,k]} & \text{(G15)}
\end{array}$$

(d) $\omega_{[j]}\omega_{[k]}$ is diagonal:

$$\begin{array}{rcll}
\omega_{[j]}\omega_{[k]}X_{[j,k]} & = & X_{[j,k]}\omega_{[j]}\omega_{[k]} & \text{(G16)} \\
\omega_{[j]}\omega_{[k]}H_{[j,k]} & = & H_{[j,k]}\omega_{[j]}\omega_{[k]} & \text{(G17)}
\end{array}$$

(e) Relations for H:

$$\begin{array}{rcll}
H_{[j,k]}X_{[j,k]} & = & \omega_{[k]}^{4}H_{[j,k]} & \text{(G18)} \\
H_{[j,k]}\omega_{[j]}^{2}H_{[j,k]} & = & \omega_{[j]}^{6}H_{[j,k]}\omega_{[j]}^{3}\omega_{[k]}^{5} & \text{(G19)} \\
H_{[j,k]}H_{[\ell,t]}H_{[j,\ell]}H_{[k,t]} & = & H_{[j,\ell]}H_{[k,t]}H_{[j,k]}H_{[\ell,t]}, \quad \text{where } k < \ell & \text{(G20)}
\end{array}$$

Figure 3: Greylyn's relations for $U_4(\mathbb{Z}[\frac{1}{\sqrt{2}},i])$. Whenever we use a generator $X_{[j,k]}$ or $H_{[j,k]}$, we implicitly assume that $j < k$.

which we now describe. To our knowledge, this monoid formulation of the Reidemeister-Schreier theorem does not appear in the literature.

If X is a set, let us 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.

Let G be a monoid and let $X \subseteq G$ be a subset of G. We write $\langle X \rangle$ for the smallest submonoid of G containing X, and we say that X *generates* G if $\langle X \rangle = G$. Given any word $w \in X^*$, we write $[w]_G \in G$ for the canonical interpretation of w in G, i.e., $[-]_G : X^* \to G$ is the unique monoid homomorphism such that $[x]_G = x$ for all $x \in X$.

A *relation* over X is an element of $X^* \times X^*$, i.e., an ordered pair of words. We say that a relation (w,v) is *valid* in G if $[w]_G = [v]_G$. If Γ is a set of relations over X, we write $\sim_\Gamma$ for the smallest congruence relation on X^* containing Γ. Here, as usual, a congruence relation is an equivalence relation that is compatible with the monoid operation, i.e., such that $w \sim v$ and $w' \sim v'$ implies $ww' \sim vv'$. Given a set X of generators for a monoid G and a set Γ of valid relations, we say that Γ is *complete* if for all $w,v \in X^*$, $[w]_G = [v]_G$ implies $w \sim_\Gamma v$. In that case, we also say that (X,Γ) is a *presentation by generators and relations* (or simply *presentation*) of G.

Definition 4.2. Given sets X,Y and a function $f : X \to Y^*$, let $f^* : X^* \to Y^*$ be the unique monoid homomorphism extending f. Concretely, f^* is given by $f^*(x_1 \ldots x_n) = f(x_1) \cdot \ldots \cdot f(x_n)$.

More generally, given sets C,X,Y and a function $f : C \times X \to Y^* \times C$, let $f^{**} : C \times X^* \to Y^* \times C$ be the function defined by $f^{**}(c_0, x_1 \ldots x_n) = (w_1 \cdot \ldots \cdot w_n, c_n)$, where $f(c_{i-1}, x_i) = (w_i, c_i)$ for all $i = 1, \ldots, n$.

Note that in case C is a singleton, the functions f^* and f^{**} are essentially the same. In general, the difference is that f^{**} also keeps a "state" in the form of an element of C.

Theorem 4.3 (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 $v \sim_\Gamma v'$.

To better understand the utility of this theorem, let us briefly provide some context. First, we note that we will be using this theorem in the case where G is a monoid, H is a submonoid of G, (Y,Δ) is a presentation of G, X is a set of generators for H, and we wish to show that some proposed set of relations Γ is complete for H. Assuming that all hypotheses of Theorem 4.3 are satisfied, and further assuming that f represents the inclusion function of H into G, i.e., that for all $x \in X$, $[f(x)]_G = [x]_H$, the completeness of Γ then follows. Namely, $[v]_H = [v']_H$ implies $[f^*(v)]_G = [f^*(v')]_G$, which implies $f^*(v) \sim_\Delta f^*(v')$ by completeness of Δ, which implies $v \sim_\Gamma v'$ by Theorem 4.3.

To see how the theorem works, it is useful to further concentrate on the case where G and H are groups, although the theorem itself does not require this. In the case of groups, one would typically consider the set $H\backslash G = \{Hc \mid c \in G\}$ of right cosets of H in G, and one would let C be a set of chosen coset representatives. The function f is then chosen to assign to each $x \in X$ some word $w \in Y^*$ such that $[x]_H = [w]_G$. The function h is chosen to assign to each pair of a coset representative $c \in C$ and generator $y \in Y$ the unique coset representative $c' \in C$ and some word $v \in X^*$ such that $c[y]_G = [v]_H c'$. Conditions (a) and (b) are then sufficient for the set of relations Γ to be complete. In the more general case of monoids, G is not necessarily partitioned into cosets, but the method works anyway, provided that appropriate C, f, and h can be chosen.

Proof of Theorem 4.3. Let us say that a word $w \in Y^*$ is *special* if $h^{**}(I,w) = (v,I)$ for some $v \in X^*$. Let Y_s^* be the set of special words. By definition of h^{**}, the empty word is special and special words are closed under concatenation, so Y_s^* is a submonoid of Y^*. Moreover, the image of f is special by property (a), and therefore the image of f^* is also special. Finally, there is a translation back from special words in Y to words in X: define $g : Y_s^* \to X^*$ by letting $g(w) = v$ where $h^{**}(I,w) = (v,I)$. Clearly, g is a monoid homomorphism.

Claim A: for all $v \in X^*$, we have $v \sim_\Gamma g(f^*(v))$. Proof: Since both g and f^* are monoid homomorphisms and $\sim_\Gamma$ is a congruence, it suffices to show this in the case when $v \in X$ is a generator. But in that case, it holds by assumption (a).

Claim B: for all $w,w' \in Y^*$ and $c \in C$, if $w \sim_\Delta w'$ and $h^{**}(c,w) = (v,d)$ and $h^{**}(c,w') = (v',d')$, then $v \sim_\Gamma v'$ and $d = d'$. Proof: define a relation $\sim$ on Y^* by $w \sim w'$ if for all $c \in C$, $h^{**}(c,w) = (v,d)$ and $h^{**}(c,w') = (v',d')$ implies $v \sim_\Gamma v'$ and $d = d'$. We must show that $w \sim_\Delta w'$ implies $w \sim w'$. Since $\sim_\Delta$ is, by definition, the smallest congruence containing Δ, it suffices to show that $\sim$ is a congruence containing Δ. The fact that $\sim$ is reflexive, symmetric, and transitive is obvious from its definition. The fact that it is a congruence follows from the definition of h^{**} and the fact that $\sim_\Gamma$ is a congruence. Finally, $\sim$ contains Δ by assumption (b).

Note that, as a special case of claim B, we also have the following: if $w,w' \in Y_s^*$ are special words, then $w \sim_\Delta w'$ implies $g(w) \sim_\Gamma g(w')$. This follows directly from the definition of g.

To finish the proof of the Reidemeister-Schreier theorem, let $v,v' \in X^*$ and assume that $f^*(v) \sim_\Delta f^*(v')$. Then we have:

$$v \;\sim_\Gamma\; g(f^*(v)) \;\sim_\Gamma\; g(f^*(v')) \;\sim_\Gamma\; v',$$

where the first and last congruence holds by claim A, and the middle one holds by the special case of claim B. Therefore, $v \sim_\Gamma v'$ as claimed. □

Corollary 4.4. *Let G be a monoid with presentation (Y,Δ), where $Y \subseteq G$. Suppose $H \subseteq G$ is a submonoid and X is a set of generators for H. Let Γ be a set of valid relations for H. Assume a set C and functions f and h are given, satisfying the hypotheses of Theorem 4.3, and assume that f represents the inclusion function of H into G, i.e., that $x \in X$, $[f(x)]_G = [x]_H$. Then Γ is a complete set of relations for H.* □

4.3 Pauli rotation representation

One of the problems we face in applying the Reidemeister-Schreier theorem is that we must show that a large number of (computer-generated) Clifford+T relations follow from the relations in Figure 1. It would be very useful if this task could be automated. Ideally, the relations in Figure 1 could be turned into a set of rewrite rules with the property that every Clifford+T circuit can be rewritten to a unique *normal form*; in that case, to show that a given relation follows from the ones in Figure 1, it would be sufficient to reduce the left-hand and right-hand sides to normal form and check that they are equal.

Unfortunately, no such rewrite system or normal form is known. Instead, the best we can do is a semi-automated process in which words are rewritten to something that is “almost” a normal form, i.e., not quite unique, but close enough so that many relations can be proved automatically, and the rest are more easily solvable by hand.

For this, the *Pauli rotation representation* of Clifford+T operators turns out to be useful. This representation was first described in [12, Section 3]. We start by noting that the T-gate is a linear combination of the identity I and the Pauli operator Z. Specifically:

$$T \;=\; \begin{pmatrix} 1 & 0 \\ 0 & \omega \end{pmatrix} \;=\; \frac{1+\omega}{2}I + \frac{1-\omega}{2}Z. \tag{1}$$

Therefore, an operator A commutes with T if and only if it commutes with Z. More generally, given any n-qubit Pauli operator P, define

$$R_P \;=\; \frac{1+\omega}{2}I + \frac{1-\omega}{2}P. \tag{2}$$

Note that $R_Z = T$. We refer to the operators R_P as *(45 degree) Pauli rotations*. Note that R_P is not a Pauli operator; we call it a Pauli rotation because it is a rotation about a Pauli axis. By (2), it is again obvious that an operator A commutes with R_P if and only if it commutes with P. Moreover, from (2), we get the following fundamental property of Pauli rotations:

$$CPC^{-1} = Q \quad \text{if and only if} \quad CR_PC^{-1} = R_Q. \tag{3}$$

Let $Z_{(i)} = I \otimes \ldots \otimes I \otimes Z \otimes I \otimes \ldots \otimes I$ be the n-qubit Pauli operator with Z acting on the ith qubit, and similarly $T_{(i)} = I \otimes \ldots \otimes I \otimes T \otimes I \otimes \ldots \otimes I = R_{Z_{(i)}}$. Since the Clifford operators act transitively on the set of non-trivial self-adjoint Pauli operators by conjugation, for every such n-qubit Pauli operator P, there exists a (non-unique) Clifford operator C such that $CZ_{(1)}C^{-1} = P$, and therefore $CT_{(1)}C^{-1} = R_P$. We therefore see that all of the Pauli rotations are Clifford conjugates of the $T_{(1)}$-gate.

Next, we note that every Clifford+T operator can be written as a product of Pauli rotations followed by a single Clifford operator. Specifically, by definition, every Clifford+T operator can be written as

$$C_1T_{(i_1)}C_2T_{(i_2)}C_3\cdots C_nT_{(i_n)}C_{n+1}.$$

For all k, let $D_k = C_1C_2\cdots C_k$, so that $C_k = D_{k-1}^{-1}D_k$. Then the above can be rewritten as

$$\begin{aligned}
C_1T_{(i_1)}C_2T_{(i_2)}C_3\cdots C_nT_{(i_n)}C_{n+1} \;&=\; C_1R_{Z_{(i_1)}}C_2R_{Z_{(i_2)}}C_3\cdots C_nR_{Z_{(i_n)}}C_{n+1} \\
&=\; D_1R_{Z_{(i_1)}}D_1^{-1}D_2R_{Z_{(i_2)}}D_2^{-1}D_3\cdots D_{n-1}^{-1}D_nR_{Z_{(i_n)}}D_n^{-1}D_{n+1} \\
&=\; R_{D_1Z_{(i_1)}D_1^{-1}}R_{D_2Z_{(i_2)}D_2^{-1}}\cdots R_{D_nZ_{(i_n)}D_n^{-1}}D_{n+1} \\
&=\; R_{P_1}R_{P_2}\cdots R_{P_n}D_{n+1},
\end{aligned}$$

where $P_k = D_kZ_{(i_k)}D_k^{-1}$. Therefore, every Clifford+T operator can be written as a product of Pauli rotations followed by a single Clifford operator, as claimed. It also shows that the number of required Pauli rotations is at most equal to the T-count of the original circuit. In fact, since every Pauli rotation has T-count 1, it is clear that every product of n Pauli rotations can be converted to a circuit of T-count n, and vice versa. In particular, the minimal T-count of a circuit is equal to the minimal number of Pauli rotations required to express it.

The Pauli rotation representation is not unique. There are some obvious relations:

(a) R_P and R_Q commute if and only if P and Q commute. This follows from (2).

(b) For any P, the operator R_P^2 is Clifford, and therefore can be eliminated, resulting in a shorter word. To see why, recall that there exists a Clifford operator C such that $R_P = CT_{(1)}C^{-1}$; therefore $R_P^2 = CT_{(1)}^2 C^{-1}$. Since $T_{(1)}^2 = S_{(1)}$ is a Clifford gate, it follows that R_P^2 is Clifford.

(c) For any P, there exists a Clifford operator D such that $R_{(-P)} = R_P D$. Indeed, let C be a Clifford operator such that $P = CZ_{(1)}C^{-1}$. Then $-P = C(-Z_{(1)})C^{-1} = CX_{(1)}Z_{(1)}X_{(1)}C^{-1}$. Therefore $R_{(-P)} = CX_{(1)}T_{(1)}X_{(1)}C^{-1}$. Using the relation $XTX = TS^\dagger\omega$, we have $R_{(-P)} = CT_{(1)}S_{(1)}^\dagger\omega C^{-1} = CT_{(1)}C^{-1}CS_{(1)}^\dagger\omega C^{-1} = R_P CS_{(1)}^\dagger\omega C^{-1}$. Thus, the claim holds with $D = CS_{(1)}^\dagger\omega C^{-1}$.

It is relatively easy to standardize the Pauli rotation representation modulo the above three relations: First, we eliminate any generators of the form $R_{(-P)}$. This can be done from left to right, using relations from (c); the resulting Clifford operator can be shifted all the way to the end of the word using relations of the form $DR_P = R_Q D$, where $Q = DPD^{-1}$, see (3). Next, we use relations from (a) to swap adjacent generators when possible, for example arriving at the lexicographically smallest word that is equal to the given word up to such commuting permutations. Next, we use relations from (b) to remove any duplicates. Should there be any such duplicates, the resulting word will need to be standardized again, but since it uses fewer Pauli rotations, the process eventually terminates.

However, even when the Pauli rotation representation is standardized modulo the relations (a), (b), and (c), it is still not unique. Indeed, there are some “non-obvious” relations. In a sense, the contribution of this paper is to state exactly what these non-obvious relations are. They turn out to be the following. Here, for brevity, we have omitted the tensor symbol $\otimes$, i.e., we wrote R_{IX} instead of $R_{I\otimes X}$.

$$\begin{array}{rcl} R_{IX}R_{IZ}R_{ZZ}R_{ZX} &=& R_{ZX}R_{IZ}R_{ZZ}R_{IX}, \\ R_{IX}R_{IZ}R_{IX}R_{ZX}R_{ZZ}R_{ZX} &=& R_{ZX}R_{IZ}R_{IX}R_{ZX}R_{ZZ}R_{IX}, \\ R_{XY}R_{YZ}R_{XZ}R_{IX}R_{ZI}R_{YX}R_{ZY}R_{ZX}R_{XI}R_{IZ} &=& R_{YX}R_{ZY}R_{ZX}R_{XI}R_{IZ}R_{XY}R_{YZ}R_{XZ}R_{IX}R_{ZI}. \end{array}$$

These turn out to be equivalent to relations (C18), (C19), and (C20) in Figure 1, respectively. We will address the question of what these relations might “mean” (i.e., how one might be able to see that they are true without computing the matrices) in Section 6.

4.4 Proof assistants

As outlined in Section 3, once we are armed with the Reidemeister-Schreier theorem, in theory there is a mechanical way to obtain a complete set of relations for $\mathscr{C}\mathscr{T}(2)$, given that $\mathscr{C}\mathscr{T}(2)$ is a subgroup of $U_4(\mathbb{Z}[\frac{1}{\sqrt{2}}, i])$ and we already have a complete set of relations for the latter due to Greylyn [13]. However, when applied in practice, this method yields a large number of very large relations, all of which must be shown to follow from the relations in Figure 1. Although Figure 3 appears to contain only 20 relations, they are actually parameterized by indices such as j,k, etc. After accounting for these indices, there are 123 distinct relations. Since there are two cosets of $\mathscr{C}\mathscr{T}(2)$ in $U_4(\mathbb{Z}[\frac{1}{\sqrt{2}}, i])$, under part (b) of the Reidemeister-Schreier theorem, each of these 123 relations yields two Clifford+T relations, plus another 8 relations (one for each generator) from part (a), giving a total of 254 Clifford+T relations that must be verified. This task is too daunting to do “by hand”.

Given the mechanical and repetitive nature of these calculations, we initially wrote a computer program to generate and verify the relations. However, this raised another issue: our program was large and complicated and used a variety of tactics to show that the given relations follow from the ones in Figure 1. We could not claim with mathematical certainty that our program was free of bugs, nor that it didn’t use some hidden assumptions that weren’t actually consequences of Figure 1. Moreover, it would have been unreasonable for any referee to verify our calculations.

For this reason, we decided to go one step further and formalize the soundness and completeness proofs in a *proof assistant*. A proof assistant is a piece of software in which one can write definitions, theorems, and proofs, and the software will check the correctness of the proofs. Purists might object that the proof assistant is itself a piece of software that might be buggy. But, as has been argued eloquently by [11, 14], current proof assistants can be scrutinized at many levels and are many orders of magnitude more reliable than the traditional way of checking paper-and-pencil proofs. The particular proof assistant we used in this work is Agda [1].

5 Proof of the main result

5.1 Soundness and completeness

Our goal is to prove that Theorem 4.1 implies Theorem 2.1. Recall that Greylyn's set of generators for $U_4(R)$ is $\mathscr{Y} = \{\omega_{[j]}, X_{[j,k]}, H_{[j,k]} \mid j,k \in \{1,...,4\}$ and $j < k\}$. Also recall that our target set of generators for $\mathscr{C}\mathscr{T}(2)$ is $\mathscr{X} = \{\omega, H_0, H_1, S_0, S_1, T_0, T_1, CZ\}$. We fix a translation from $\mathscr{X}$ to $\mathscr{Y}^*$ as follows:

$$\begin{aligned}
f(\omega) &= \omega_{[0]}\omega_{[1]}\omega_{[2]}\omega_{[3]}, \\
f(H_0) &= H_{[1,3]}H_{[0,2]}, \\
f(H_1) &= H_{[2,3]}H_{[0,1]}, \\
f(S_0) &= \omega_{[2]}^2\omega_{[3]}^2, \\
f(S_1) &= \omega_{[1]}^2\omega_{[3]}^2, \\
f(T_0) &= \omega_{[2]}\omega_{[3]}, \\
f(T_1) &= \omega_{[1]}\omega_{[3]}, \\
f(CZ) &= \omega_{[3]}^4.
\end{aligned}$$

We prove the following soundness and completeness theorems for this translation:

Theorem 5.1 (Soundness)**.** *For all $w, v \in \mathscr{X}^*$, $w \sim_\Gamma v$ implies $f^*(w) \sim_\Delta f^*(v)$.*

Theorem 5.2 (Completeness)**.** *For all $w, v \in \mathscr{X}^*$, $f^*(w) \sim_\Delta f^*(v)$ implies $w \sim_\Gamma v$.*

As already noted in Section 4.2, these two theorems, together with Theorem 4.1, immediately imply Theorem 2.1. Specifically, we have $w \sim_\Gamma v$ if and only if $f^*(w) \sim_\Delta f^*(v)$ if and only if $[f^*(w)] = [f^*(v)]$ if and only if $[w] = [v]$, where the first equivalence follows from Theorems 5.1 and 5.2, the second equivalence follows from Theorem 4.1, and the last equivalence holds because the function f respects the interpretation.

5.2 The formal proof

Soundness and completeness are formally proved in the Agda code accompanying this paper [8]. We organized the code to make it hopefully as easy as possible to verify the result. The code consists of 67 files that are listed in Figure 4, and which we now briefly describe.

(a) Background. The eight files in the "background" section contain general-purpose definitions of the kind that are usually found in the Agda standard library, i.e., basic properties of booleans, integers, equality, propositional connectives, etc. The reason we did not use the actual Agda standard library is that it is very large and changes frequently. We felt that it is better for our code to be self-contained rather than depending on a particular library version.

(b) Statement of the result. In these two files, we give a minimal set of definitions that allows us to *state* the soundness and completeness theorems. The file `Word.agda` defines what it means to be a word over a set of generators, as well as the inference rules we use for deriving relations from a set of axioms (such as reflexivity, symmetry, transitivity, congruence, associativity, and the left and right unit laws). Note that in the Agda code, we define a word as a term in the language of monoids, rather than as a sequence of generators. In other words, associativity and the unit laws are treated as laws, rather than being built into the definition. The file `Word.agda` also defines the f^* operation used in the statement of the soundness and completeness theorems. The file `Generator.agda` defines the Clifford+T generators and the relations from Figure 1, Greylyn's generators and the relations from Figure 3, and the translation function f from Section 5.1. It also contains the statement of the soundness and completeness theorems, but not their proofs. The reason we state these theorems separately from their proofs is to make sure that Agda (and a human reviewer) can verify that the statement of these theorems only depends on the relatively small number of definitions given so far, and not on the much larger number of definitions and tactics used in the proof.

(c) Details of the proof. The proof of the soundness and completeness theorems relies on a large number of auxiliary definitions and lemmas, and comprises the bulk of our code with 56 files. This includes a formal proof of the Reidemeister-Schreier theorem; several tactics for automating steps in certain equational proofs; a simplified presentation of Greylyn's generators and relations, using only 5 generators and 19 relations (instead of Greylyn's original 16 generators and 123 relations), along with the proof of its completeness; a formalization of Pauli rotations and their relevant properties; as well as 46 step-by-step proofs of individual relations. These details are primarily intended to be machine-readable, and can safely be skipped by readers who trust Agda and merely want to check the proof rather than reading it. However, all of the files are documented and human-readable.

The relations in the files `Equation1.agda` to `Equation46.agda` are at the heart of the completeness proof. These are the relations that must be proved to satisfy the hypotheses of the Reidemeister-Schreier theorem. Some of these relations are trivial, such as `Equation13.agda`. Others are highly non-trivial and require almost a thousand proof steps, such as `Equation44.agda`. In particular, the proofs that require relations (C18)–(C20) from Figure 1 tend to be non-obvious; in fact, this is how we discovered relations (C18)–(C20) in the first place. We did not write these equational proofs by hand; instead, we used a semi-automated process where most of the proofs were generated by a separate Haskell program and output in a format that is convenient and efficient for Agda to check. Originally, we also attempted to write Agda tactics that would allow Agda to derive these relations fully automatically; however, this failed due to performance issues with Agda.

(d) Proof witness. Finally, the file `Proof.agda` contains nothing but a witness of the fact that the soundness and completeness theorems have been formally proven. A reader who wants to skip the details of the formal proof only needs to check two things: the statement of the main result in `Generator.agda` (to make sure the statement correctly captures what we said it does), and the fact that the Agda proof checker accepts `Proof.agda`.

6 Discussion of the axioms

Here, we give some further perspectives on what the axioms of Figure 1 might "mean", and in particular, how one might convince oneself that the relations are true without having to compute the corresponding

(a) Background:

`Boolean.agda`	The type of booleans.
`Proposition.agda`	Basic definitions in propositional logic.
`Equality.agda`	Basic properties of equality.
`Decidable.agda`	Some definitions to deal with decidable properties.
`Inspect.agda`	Agda's "inspect" paradigm, to assist with pattern matching.
`Nat.agda`	Basic properties of the natural numbers.
`Maybe.agda`	The "Maybe" type.
`List.agda`	Basic properties of lists.

(b) Statement of the result

`Word.agda`	Basic properties of words.
`Generator.agda`	Generators and relations for our two groups, and statement of main result.

(c) Proof of the result

`Word-Lemmas.agda`	Basic lemmas about monoids and groups, and equational reasoning.
`Reidemeister-Schreier.agda`	Two versions of the Reidemeister-Schreier theorem.
`Word-Tactics.agda`	Some tactics for proving properties of words.
`Clifford-Lemmas.agda`	A decision procedure for equality of 2-qubit Clifford operators.
`CliffordT-Lemmas.agda`	Properties and tactics for Clifford+T operators.
`Greylyn-Lemmas.agda`	Some automation for Greylyn's 1- and 2-level operators.
`Soundness.agda`	Proof of soundness.
`Greylyn-Simplified.agda`	A smaller set of generators and relations for Greylyn's operators.
`PauliRotations.agda`	Definitions, properties, and tactics for Pauli rotations.
`Equation1.agda` – `Equation46.agda`	Explicit proofs of 46 relations required for completeness.
`Completeness.agda`	Proof of completeness.

(d) Top-level proof witness

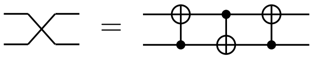
`Proof.agda`	The final witness for soundness and completeness.

Figure 4: List of Agda files. The files are listed in order of dependency, i.e., each file only imports earlier files.

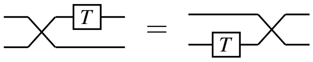
matrices.

Note that we are not claiming that axioms (C1)–(C20) are independent; for example, (C8) clearly follows from (C14) and (C16); however, we found it useful to separate the Clifford relations from the rest, which is why (C8) was included. It would be nice to know whether axioms (C18)–(C20) are independent from the others and from each other, and this seems likely to be true, but we do not know.

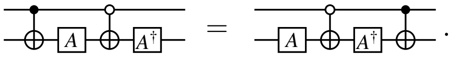
The axioms in groups (a)–(c) are well-known; they merely express the Clifford relations [21] and the fact that operators on disjoint qubits commute. Relations (C14) and (C15) express the well-known facts that $T^2 = S$ and $(TX)^2 = \omega$, whereas relation (C16) holds because diagonal operators commute. Note that the upside-down version of relation (C16) was not included among our axioms; this is because it is actually derivable from the remaining axioms. Relation (C17) becomes obvious once one realizes that the swap gate can be expressed as a sequence of three controlled-not gates:



Relation (C17) is then obtained by simplifying the following, which expresses the fact that a T-gate can be moved past a swap-gate:



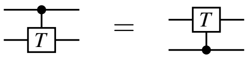
We will now focus on the "non-obvious" relations (C18)–(C20). Relations (C18) and (C19) are of the form



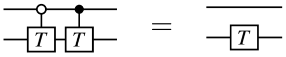
(4)

They hold because positively controlled gates commute with negatively controlled gates. Note that there are infinitely many relations of the form (4), where A is any single-qubit Clifford+T operator, but our completeness proof shows that, in the presence of the remaining axioms, two of them are sufficient to prove all the others.

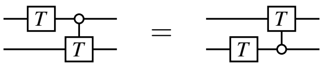
Relation (C20) is more interesting. It, too, states that two operators commute, but it is less obvious why this is so. Ideally, we would be able to find some simpler and more obvious relations that imply (C20). While we have not been able to find such simpler relations in the Clifford+T generators, we can do this if we permit ourselves a controlled T-gate. Note that the controlled T-gate is not itself a member of the 2-qubit Clifford+T group, since representing it as a Clifford+T operator requires an ancilla [10]. But the use of controlled T-gates is nevertheless helpful in explaining relation (C20). We start by noting that the controlled T-gate satisfies the following obvious circuit identities (and their upside-down versions):



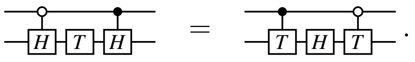
(5)



(6)

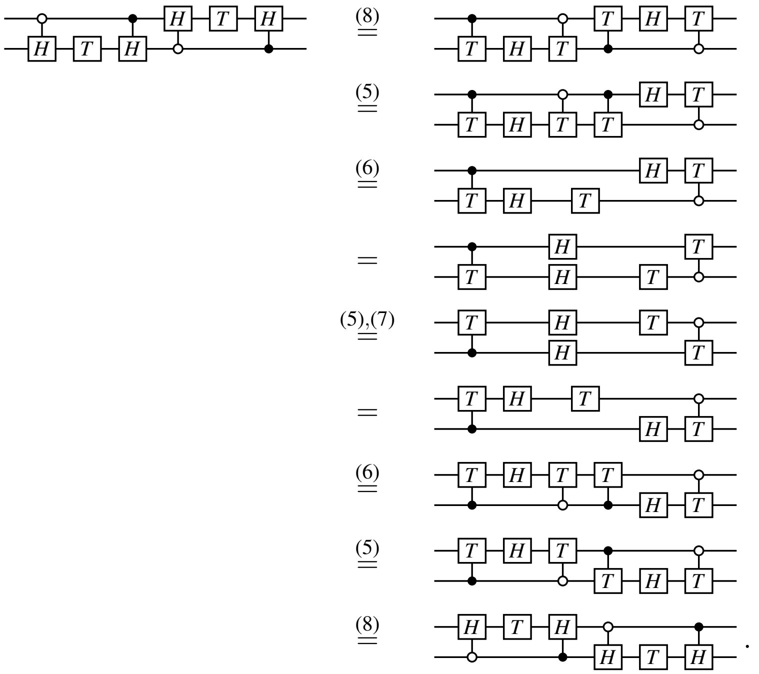


(7)



(8)

Identities (5)–(7) are obvious because all of the operators in them are diagonal. Identity (8) holds by case distinction: this circuit applies either HT or TH to the bottom qubit, depending on whether the top qubit is $|0\rangle$ or $|1\rangle$. Using these identities, we can easily prove (C20):



Note that there is again an infinite family of such relations, because in the above derivation, we could have used any gate in place of H. However, due to completeness, all other such relations are consequences of (C18)–(C20) and the remaining axioms.

Another way to look at relations (C18)–(C20) is in terms of their Pauli rotation representations. As we already mentioned in Section 4.3, up to basis changes, the three relations can be written in terms of Pauli rotations, respectively as follows:

$$\begin{array}{rcl} R_{IX}R_{IZ}R_{ZZ}R_{ZX} & = & R_{ZX}R_{IZ}R_{ZZ}R_{IX}, \\ R_{IX}R_{IZ}R_{IX}R_{ZX}R_{ZZ}R_{ZX} & = & R_{ZX}R_{IZ}R_{IX}R_{ZX}R_{ZZ}R_{IX}, \\ R_{XY}R_{YZ}R_{XZ}R_{IX}R_{ZI}R_{YX}R_{ZY}R_{ZX}R_{XI}R_{IZ} & = & R_{YX}R_{ZY}R_{ZX}R_{XI}R_{IZ}R_{XY}R_{YZ}R_{XZ}R_{IX}R_{ZI}. \end{array}$$

When written in this form, the first two of these relations only use X and Z Paulis, and use only Z on the left qubit. This indicates that these relations are about controlled gates. We can also see that in both cases, the relation exchanges the positions of the leftmost R_{IX} and the rightmost R_{ZX}. The first relation can also be seen to express the fact that $R_{IZ}R_{ZZ}$ commutes with $R_{ZX}R_{IX}^{-1}$, and similarly for the second relation. The third relation again takes the form of an operator commuting with its upside-down version.

7 Conclusion and future work

We gave a presentation of the 2-qubit Clifford+T group by generators and relations. We did this by applying the Reidemeister-Schreier theorem to Greylyn's presentation of the group of unitary 4×4-matrices over the ring $\mathbb{Z}[\frac{1}{\sqrt{2}},i]$. Since there is a very large number of relations to check and simplify, and checking them by hand or by an unverified computer program would be error-prone, we used the proof assistant Agda to formalize our proof. The latter process is painstaking and took us more than 5 years to complete after our result was first announced in [7].

An obvious candidate for future work would be to find a complete set of relations for the Clifford+T group with 3 or more qubits. This is currently out of reach for two reasons: first, the computations required to simplify any potential set of relations will be even more labor-intensive than in the 2-qubit case. Second, and more seriously, there is no known presentation of the group of unitary $n \times n$-matrices over the ring $\mathbb{Z}[\frac{1}{\sqrt{2}}, i]$ for $n > 4$.

Another project that is currently in progress is to apply the method of this paper to restrictions of the Clifford+T group for which presentations of the corresponding matrix group are known. This includes the Clifford+Toffoli gate set and the Clifford+controlled-S gate set.

References

[1] *Agda Documentation*. `https://agda.readthedocs.io/`. Accessed: 2022-02-15.

[2] Matthew Amy, Dmitri Maslov & Michele Mosca (2014): *Polynomial-Time T-Depth Optimization of Clifford+T Circuits Via Matroid Partitioning*. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 33(10), pp. 1476–1489, doi:10.1109/TCAD.2014.2341953. Also available from arXiv:1303.2042.

[3] Matthew Amy, Dmitri Maslov, Michele Mosca & Martin Roetteler (2013): *A Meet-in-the-Middle Algorithm for Fast Synthesis of Depth-Optimal Quantum Circuits*. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 32(6), pp. 818–830, doi:10.1109/TCAD.2013.2244643. Also available from arXiv:1206.0758v2.

[4] Matthew Amy & Michele Mosca (2019): *T-count optimization and Reed-Muller codes*. IEEE Transactions on Information Theory 65(8), pp. 4771–4784, doi:10.1109/TIT.2019.2906374. Also available from arXiv:1601.07363.

[5] Niel de Beaudrap, Xiaoning Bian & Quanlong Wang (2020): *Fast and effective techniques for T-count reduction via spider nest identities*. In Steven T. Flammia, editor: 15th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2020), Leibniz International Proceedings in Informatics (LIPIcs) 158, Schloss Dagstuhl–Leibniz-Zentrum für Informatik, pp. 11:1–23, doi:10.4230/LIPIcs.TQC.2020.11. Also available from arXiv:2004.05164.

[6] Niel de Beaudrap, Xiaoning Bian & Quanlong Wang (2020): *Techniques to reduce $\pi/4$-parity-phase circuits, motivated by the ZX calculus*. Electronic Proceedings in Theoretical Computer Science 318, p. 131–149, doi:10.4204/eptcs.318.9. Available from arXiv:1911.09039.

[7] Xiaoning Bian & Peter Selinger (2015): *Relations for the 2-qubit Clifford+T operator group*. Slides presented at the Workshop on Quantum Programming and Circuits, Waterloo, Canada, June 8–11, 2015. Available from `https://mathstat.dal.ca/~xbian/talks/slide_cliffordt2.pdf`.

[8] Xiaoning Bian & Peter Selinger (2022): *Agda code accompanying this paper*. Available as ancillary material at arXiv:2204.02217.

[9] Harry Buhrman, Richard Cleve, Monique Laurent, Noah Linden, Alexander Schrijver & Falk Unger (2006): *New Limits on Fault-Tolerant Quantum Computation*. In: Proceedings of the 47th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2006), pp. 411–419, doi:10.1109/FOCS.2006.50. Also available from arXiv:quant-ph/0604141.

[10] Brett Giles & Peter Selinger (2013): *Exact synthesis of multiqubit Clifford+T circuits*. Physical Review A 87(3), p. 032332 (7 pages), doi:10.1103/PhysRevA.87.032332. Also available from arXiv:1212.0506.

[11] Georges Gonthier (2008): *Formal Proof — The Four Color Theorem*. Notices of the American Mathematical Society 55(11), pp. 1382–1393.

[12] David Gosset, Vadym Kliuchnikov, Michele Mosca & Vincent Russo (2014): *An Algorithm for the T-Count*. Quantum Information and Computation 14(15–16), pp. 1261–1276, doi:10.26421/QIC14.15-16-1. Also available from arXiv:1308.4134.

[13] Seth E. M. Greylyn (2014): *Generators and relations for the group $U_4(\mathbb{Z}[\frac{1}{\sqrt{2}},i])$*. M.Sc. thesis, Dalhousie University. Available from arXiv:1408.6204.

[14] Thomas C. Hales (2008): *Formal Proof*. Notices of the American Mathematical Society 55(11), pp. 1370–1380.

[15] Luke E. Heyfron & Earl T. Campbell (2018): *An efficient quantum compiler that reduces T count*. Quantum Science and Technology 4(1), p. 015004, doi:10.1088/2058-9565/aad604. Also available from arXiv:1712.01557.

[16] Aleks Kissinger & John van de Wetering (2020): *Reducing the number of non-Clifford gates in quantum circuits*. Phys. Rev. A 102, p. 022406, doi:10.1103/PhysRevA.102.022406. Preprint available from arXiv:1903.10477.

[17] Yunseong Nam, Neil J. Ross, Yuan Su, Andrew M. Childs & Dmitri Maslov (2018): *Automated optimization of large quantum circuits with continuous parameters*. NPJ Quantum Information 4(1), doi:10.1038/s41534-018-0072-4. Also available from arXiv:1710.07345.

[18] Michael A. Nielsen & Isaac L. Chuang (2002): *Quantum Computation and Quantum Information*. Cambridge University Press.

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

[20] 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.

[21] 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.