Number-Theoretic Characterizations of Some Restricted Clifford+T Circuits

Matthew Amy[1], Andrew N. Glaudell[2,3], and Neil J. Ross[1]

[1]Department of Mathematics and Statistics, Dalhousie University, Halifax, NS, Canada

[2]Institute for Advanced Computer Studies and Joint Center for Quantum Information and Computer Science, University of Maryland, College Park, MD, USA

[3]Joint Quantum Institute, University of Maryland, College Park, MD, USA

Kliuchnikov, Maslov, and Mosca proved in 2012 that a 2×2 unitary matrix V can be exactly represented by a single-qubit Clifford+T circuit if and only if the entries of V belong to the ring $\mathbb{Z}[1/\sqrt{2}, i]$. Later that year, Giles and Selinger showed that the same restriction applies to matrices that can be exactly represented by a multi-qubit Clifford+T circuit. These number-theoretic characterizations shed new light upon the structure of Clifford+T circuits and led to remarkable developments in the field of quantum compiling. In the present paper, we provide number-theoretic characterizations for certain restricted Clifford+T circuits by considering unitary matrices over subrings of $\mathbb{Z}[1/\sqrt{2}, i]$. We focus on the subrings $\mathbb{Z}[1/2]$, $\mathbb{Z}[1/\sqrt{2}]$, $\mathbb{Z}[1/i\sqrt{2}]$, and $\mathbb{Z}[1/2, i]$, and we prove that unitary matrices with entries in these rings correspond to circuits over well-known universal gate sets. In each case, the desired gate set is obtained by extending the set of classical reversible gates $\{X, CX, CCX\}$ with an analogue of the Hadamard gate and an optional phase gate.

1 Introduction

Kliuchnikov, Maslov, and Mosca showed in [26] that a 2-dimensional unitary matrix V can be exactly represented by a single-qubit Clifford+T circuit if and only if the entries of V belong to the ring $\mathbb{Z}[1/\sqrt{2}, i]$. This result gives a number-theoretic characterization of single-qubit Clifford+T circuits. In [17], Giles and Selinger extended the characterization of Kliuchnikov et al. to multi-qubit Clifford+T circuits by proving that a 2^n-dimensional unitary matrix can be exactly represented by an n-qubit Clifford+T circuit if and only if its entries belong to $\mathbb{Z}[1/\sqrt{2}, i]$.

These number-theoretic characterizations provide great insight into the structure of Clifford+T circuits. As a result, single-qubit Clifford+T circuits are now very well understood [13, 18, 28, 29, 34], and some of these results have even been extended to single-qubit circuits beyond the Clifford+T gate set [12, 16, 25, 27, 32, 33]. In contrast, our understanding of multi-qubit Clifford+T circuits remains more limited, despite interesting results [11, 15, 19, 20, 39]. One of the reasons for this limitation is that large unitary matrices over $\mathbb{Z}[1/\sqrt{2}, i]$ are hard to analyze. In order to circumvent the difficulties associated with multi-qubit Clifford+T circuits, restricted gate sets have been considered in the literature. This led to important developments in the study of multi-qubit Clifford, CNOT+T, and CNOT-dihedral circuits [3–6, 23, 30, 36]. Unfortunately, the simpler structure of these restricted gate sets comes at a cost: they are not universal for quantum computing.

In the present paper, our goal is to address both of these limitations by considering restrictions of the Clifford+T gate set which are nevertheless universal for quantum computing. To this end, we study circuits corresponding to unitary matrices over proper subrings of $\mathbb{Z}[1/\sqrt{2}, i]$, focusing on $\mathbb{Z}[1/2]$, $\mathbb{Z}[1/\sqrt{2}]$, $\mathbb{Z}[1/i\sqrt{2}]$, and $\mathbb{Z}[1/2, i]$. For each subring, we find a set of quantum gates G with the property that circuits over G correspond to unitary matrices over the given ring. Writing $U_{2^n}(R)$ for the group of $2^n \times 2^n$ unitary matrices over a ring R, our main results can then be summarized in the following theorem.

Theorem. *A $2^n \times 2^n$ unitary matrix V can be exactly represented by an n-qubit circuit over*

(i) $\{X, CX, CCX, H \otimes H\}$ *if and only if* $V \in U_{2^n}(\mathbb{Z}[1/2])$,

(ii) $\{X, CX, CCX, H, CH\}$ *if and only if* $V \in U_{2^n}(\mathbb{Z}[1/\sqrt{2}])$,

(iii) $\{X, CX, CCX, F\}$ *if and only if* $V \in U_{2^n}(\mathbb{Z}[1/i\sqrt{2}])$, *and*

(iv) $\{X, CX, CCX, \omega H, S\}$ *if and only if* $V \in U_{2^n}(\mathbb{Z}[1/2, i])$,

where $\omega = e^{i\pi/4}$ *and* $F \propto \sqrt{H}$. *Moreover, in (i)-(iv), a single ancilla is sufficient.*

The gate sets in items (i)–(iv) of the above theorem are all universal for quantum computing [2, 37], and we sometimes refer to circuits over these gate sets as *integral*, *real*, *imaginary*, and *Gaussian* Clifford+T circuits, respectively. As a corollary to the above theorem, we also obtain two additional characterizations of universal gate sets.

Corollary. *A $2^n \times 2^n$ unitary matrix V can be exactly represented by an n-qubit circuit over*

(i) $\{X, CX, CCX, H\}$ *if and only if* $V = W/\sqrt{2}^q$ *for some matrix W over $\mathbb{Z}$ and some $q \in \mathbb{N}$, and*

(ii) $\{X, CX, CCX, H, S\}$ *if and only if* $V = W/\sqrt{2}^q$ *for some matrix W over $\mathbb{Z}[i]$ and some $q \in \mathbb{N}$.*

Moreover, in (i) and (ii), a single ancilla is sufficient.

As a final corollary to the theorem above, we refine the characterizations (iii) and (iv) by showing that in these cases a matrix can be represented by an ancilla-free circuit if and only if it has determinant 1.

Corollary. *Let $n \geq 4$. A $2^n \times 2^n$ unitary matrix V can be exactly represented by an n-qubit ancilla-free circuit over*

(i) $\{X, CX, CCX, F\}$ *if and only if* $V \in U_{2^n}(\mathbb{Z}[1/i\sqrt{2}])$ *and* $\det V = 1$, *and*

(ii) $\{X, CX, CCX, \omega H, S\}$ *if and only if* $V \in U_{2^n}(\mathbb{Z}[1/2, i])$ *and* $\det V = 1$.

In (i) and (ii), the requirement that $\det V = 1$ *can be dropped for* $n < 4$.

The characterization of ancilla-free real and integral Clifford+T circuits remains an open question but we conjecture that they correspond to a strict subgroup of the group of unitaries with determinant 1.

Restrictions similar to the ones considered here were previously studied in the context of foundations [35], randomized benchmarking [22], and graphical languages for quantum computing [8, 24, 38]. Furthermore, our study fits within a larger program, initiated by Aaronson and others, which aims at classifying quantum operations. Such classifications exist for classical reversible operations [1], for stabilizer operations [21], and for beam-splitter interactions [14], but no classification is known for a universal family of quantum operations suited for fault-tolerant quantum computing. In this context, our work can be seen as a partial classification of the universal extensions of the set of classical reversible gates $\{X, CX, CCX\}$. This perspective is illustrated in Figure 1, which depicts a fragment of the lattice of subgroups of $U_n(\mathbb{Z}[1/\sqrt{2}, i])$ where, for conciseness, we wrote $\mathbb{D}$ for the ring $\mathbb{Z}[1/2]$ so that the rings $\mathbb{Z}[1/\sqrt{2}]$, $\mathbb{Z}[1/i\sqrt{2}]$, $\mathbb{Z}[1/2, i]$ and $\mathbb{Z}[1/\sqrt{2}, i]$ are denoted by $\mathbb{D}\left[\sqrt{2}\right]$, $\mathbb{D}\left[i\sqrt{2}\right]$, $\mathbb{D}[i]$, and $\mathbb{D}\left[\omega\right]$, respectively.

The rest of the paper is organized as follows. In Section 2, we give an overview of our methods. In Section 3, we introduce the rings and matrices which will be used throughout the paper. In Section 4, we show that certain useful matrices can be exactly represented by restricted Clifford+T circuits. Section 5 contains the proofs of our various number-theoretic characterizations. We conclude in Section 6.

2 Overview

Unrestricted Clifford+T circuits are generated by

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad CX = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad \text{and} \quad T = \begin{bmatrix} 1 & 0 \\ 0 & \omega \end{bmatrix}.$$

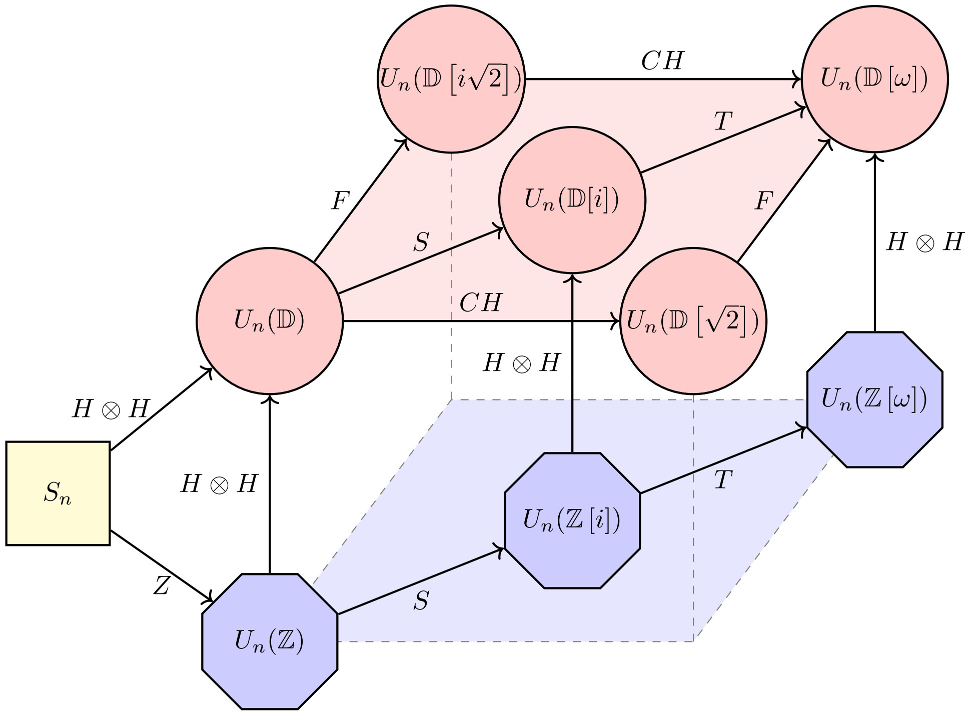


Figure 1: Some subgroups of $U_n(\mathbb{D}[\omega])$. To the left of the cube, in yellow, the symmetric group S_n corresponds to circuits over the gate set $\{X, CX, CCX\}$. On the bottom face of the cube, in blue, are generalized symmetric groups, and on the top face of the cube, in red, are universal subgroups of $U_n(\mathbb{D}[\omega])$. The edges of the lattice denote inclusion. The gates labeling the edges are sufficient to extend the expressive power of a gate set from one subgroup to the next (and no further). For example, the edge labeled Z going from S_n to $U_n(\mathbb{Z})$ indicates that adding the Z gate to $\{X, CX, CCX\}$ produces a gate set expressive enough to represent every matrix in $U_n(\mathbb{Z})$ (but not every matrix in $U_n(\mathbb{Z}[i])$).

Since $\omega = (1+i)/\sqrt{2}$, the entries of all the generators belong to the ring $\mathbb{Z}[1/\sqrt{2}, \omega] = \mathbb{Z}[1/\sqrt{2}, i] = \mathbb{D}[\omega]$. Hence, if a matrix V can be represented exactly by an n-qubit Clifford+T circuit, then $V \in U_{2^n}(\mathbb{D}[\omega])$, the group of $2^n \times 2^n$ unitary matrices with entries in $\mathbb{D}[\omega]$. Showing that the ring $\mathbb{D}[\omega]$ characterizes Clifford+T circuits thus amounts to proving the converse implication. An algorithm establishing that every element of $U_{2^n}(\mathbb{D}[\omega])$ can be exactly represented by a Clifford+T circuit is known as an exact synthesis algorithm.

The original insight of Kliuchnikov, Maslov and Mosca in the single-qubit Clifford+T case was to reduce the problem of exact synthesis to the problem of state preparation. The latter problem is to find, given a target vector $v \in \mathbb{D}[\omega]^n$, a sequence $G_1, \ldots, G_\ell$ of Clifford+T gates such that $G_\ell \cdots G_1 e_1 = v$ or, equivalently, such that $G_1^\dagger \cdots G_\ell^\dagger v = e_1$. Kliuchnikov et al. realized that this sequence of gates can be found by first writing v as $v = u/\sqrt{2}^q$ for some $u \in \mathbb{Z}[\omega]$ and then iteratively reducing the exponent q.

This basic premise was extended by Giles and Selinger to the multi-qubit context by adding an outer induction over the columns of an n-qubit unitary. This method amounts to performing a constrained Gaussian elimination where the row operations are restricted to a few basic moves. The Giles-Selinger algorithm proceeds by reducing the leftmost column of an $n \times n$ unitary matrix to the first standard basis vector by applying a sequence of one- and two-level matrices, which act non-trivially on at most two components of a vector, before recursively dealing with the remaining submatrix. If the target unitary is $V = \left[\begin{array}{c|c} v & V' \end{array}\right]$, then the Giles-Selinger algorithm first constructs a sequence of matrices $G_1, \ldots, G_\ell$ such that $G_1 \cdots G_\ell v = e_1$. Left-multiplying V by this sequence of matrices then yields

$$G_1 \cdots G_\ell \left[\begin{array}{c|c} v & \quad V' \quad \end{array}\right] = \left[\begin{array}{c|ccc} 1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & V'' & \\ 0 & & & \end{array}\right]$$

where V'' is unitary. The fact that the matrices used in this reduction act non-trivially on no more than two rows of the matrix ensures that when the algorithm recursively reduces the columns of V'' it does so without perturbing the previously fixed columns. The Giles-Selinger algorithm thus relies on the following two facts.

1. A unit vector in $\mathbb{D}[\omega]^n$ can be reduced to a standard basis vector by using one- and two-level matrices and
2. the required one- and two-level matrices can be exactly represented by Clifford+T circuits.

While there are subtle differences between the various cases discussed below, our method in characterizing restricted Clifford+T circuits follows this general structure.

3 Rings and Matrices

In this section, we discuss the rings and matrices that will be used throughout the paper. For further details, the reader is encouraged to consult [7].

3.1 Rings

We write $\mathbb{N}$ for the set of nonnegative integers and if $n \in \mathbb{N}$ we write $[n]$ for the set $\{1, \ldots, n\}$. We use $\mathbb{Z}$ to denote the ring of integers and i to denote the imaginary unit. We define ω as $\omega = e^{i\pi/4} = (1+i)/\sqrt{2}$. Note that i is a 4-th root of unity and that ω is an 8-th root of unity.

We will use the extensions of $\mathbb{Z}$ defined below.

Definition 3.1. Let

- $\mathbb{Z}\left[\sqrt{2}\right] = \left\{x_0 + x_1\sqrt{2} \mid x_0, x_1 \in \mathbb{Z}\right\}$,
- $\mathbb{Z}\left[i\sqrt{2}\right] = \left\{x_0 + x_1 i\sqrt{2} \mid x_0, x_1 \in \mathbb{Z}\right\}$,
- $\mathbb{Z}[i] = \{x_0 + x_1 i \mid x_0, x_1 \in \mathbb{Z}\}$, and
- $\mathbb{Z}[\omega] = \left\{x_0 + x_1\omega + x_2\omega^2 + x_3\omega^3 \mid x_0, x_1, x_2, x_3 \in \mathbb{Z}\right\}$.

The rings $\mathbb{Z}\left[\sqrt{2}\right]$, $\mathbb{Z}\left[i\sqrt{2}\right]$, $\mathbb{Z}[i]$, and $\mathbb{Z}[\omega]$ are known as the ring of *quadratic integers with radicand 2*, the ring of *quadratic integers with radicand -2*, the ring of *Gaussian integers*, and the ring of *cyclotomic integers of degree 8*, respectively. All of these rings are distinct subrings of $\mathbb{Z}[\omega]$ and we have the inclusions depicted in the lattice of subrings below.

$$\begin{tikzcd}
& \mathbb{Z}[\omega] & \\
\mathbb{Z}\left[i\sqrt{2}\right] \arrow[ur] & \mathbb{Z}[i] \arrow[u] & \mathbb{Z}\left[\sqrt{2}\right] \arrow[ul] \\
& \mathbb{Z} \arrow[ul] \arrow[u] \arrow[ur] &
\end{tikzcd}$$

Further to the rings introduced in Definition 3.1, we will consider extensions of the ring of *dyadic fractions*, i.e., fractions whose denominator is a power of 2.

Definition 3.2. The ring of *dyadic fractions* $\mathbb{D}$ is defined as $\mathbb{D} = \left\{\frac{u}{2^q} \mid u \in \mathbb{Z}, q \in \mathbb{N}\right\}$.

Definition 3.3. Let

- $\mathbb{D}\left[\sqrt{2}\right] = \left\{x_0 + x_1\sqrt{2} \mid x_0, x_1 \in \mathbb{D}\right\}$,
- $\mathbb{D}\left[i\sqrt{2}\right] = \left\{x_0 + x_1 i\sqrt{2} \mid x_0, x_1 \in \mathbb{D}\right\}$,
- $\mathbb{D}[i] = \{x_0 + x_1 i \mid x_0, x_1 \in \mathbb{D}\}$, and
- $\mathbb{D}[\omega] = \left\{x_0 + x_1\omega + x_2\omega^2 + x_3\omega^3 \mid x_0, x_1, x_2, x_3 \in \mathbb{D}\right\}$.

If $v \in \mathbb{D}\left[\sqrt{2}\right]$, then v can be written as $v = u/2^q$ for some $q \in \mathbb{N}$ and some $u \in \mathbb{Z}\left[\sqrt{2}\right]$. A similar property holds for elements of $\mathbb{D}\left[i\sqrt{2}\right]$, $\mathbb{D}[i]$, and $\mathbb{D}[\omega]$.

If R is a ring and $r \in R$ we write $R/(r)$ for the quotient of the ring R by the ideal generated by the element r. Two elements s and s' of R are congruent modulo r if $s - s'$ belongs to the ideal (r), in which case we write $s \equiv s' \pmod{r}$. We sometimes refer to the elements of the ring $R/(r)$ as residues. Some quotient rings are well-known. For example, $\mathbb{Z}/(2) = \{0, 1\}$ and $\mathbb{Z}/(4) = \{0, 1, 2, 3\}$. The following proposition gives an explicit description of certain lesser-known rings of residues which will be useful in what follows.

Proposition 3.4. *We have*

- $\mathbb{Z}\left[\sqrt{2}\right]/(2) = \left\{0, 1, \sqrt{2}, 1 + \sqrt{2}\right\}$,
- $\mathbb{Z}\left[i\sqrt{2}\right]/(2) = \left\{0, 1, i\sqrt{2}, 1 + i\sqrt{2}\right\}$,
- $\mathbb{Z}\left[i\sqrt{2}\right]/(2i\sqrt{2}) = \left\{0, 1, 2, 3, i\sqrt{2}, 1 + i\sqrt{2}, 2 + i\sqrt{2}, 3 + i\sqrt{2}\right\}$, *and*
- $\mathbb{Z}[i]/(2) = \{0, 1, i, 1 + i\}$.

Proof. To see, for example, that $\mathbb{Z}\left[\sqrt{2}\right]/(2) = \left\{0, 1, \sqrt{2}, 1 + \sqrt{2}\right\}$, note that $u = x_0 + x_1\sqrt{2}$ and $u' = x_0' + x_1'\sqrt{2}$ are congruent modulo 2 if there exists an element $t = y_0 + y_1\sqrt{2}$ such that $u - u' = 2t$. This is the case if and only if $(x_0 - x_0') + (x_1 - x_1')\sqrt{2} = 2y_0 + 2y_1\sqrt{2}$ which in turn holds if and only if $x_0 \equiv x_0' \pmod{2}$ and $x_1 \equiv x_1' \pmod{2}$. $\square$

We will often take advantage of properties of residues. Some of these properties are generic. For example, if u and v are two elements of a ring R and $u \equiv v \pmod{2}$, then $u \pm v \equiv 0 \pmod{2}$. Other properties of residues are specific to a particular ring. For example, an integer $u \in \mathbb{Z}$ is odd if and only if $u^2 \equiv 1 \pmod{4}$. Similarly, for an integer $u \in \mathbb{Z}$, we have $u \equiv 3 \pmod{4}$ if and only if $-u \equiv 1 \pmod{4}$. We now state important properties of residues in $\mathbb{Z}\left[i\sqrt{2}\right]$ and $\mathbb{Z}[i]$ for future reference. They can be established by reasoning using residue tables in the relevant quotient rings. In the following, we denote the complex conjugate of an element u by $u^\dagger$. For uniformity, we sometimes write $u^\dagger$ even when u belongs to a real subring of $\mathbb{D}[\omega]$. In this case, $u^\dagger = u$.

Proposition 3.5. *The following statements hold.*

- *In* $\mathbb{Z}\left[i\sqrt{2}\right]/(2)$, $u^\dagger u \equiv 0$ *or* 1.
- *If* $u^\dagger u \equiv 1$ *in* $\mathbb{Z}\left[i\sqrt{2}\right]/(2)$, *then* $u \equiv 1, 3, 1 + i\sqrt{2},$ *or* $3 + i\sqrt{2}$ *in* $\mathbb{Z}\left[i\sqrt{2}\right]/(2i\sqrt{2})$.
- *In* $\mathbb{Z}\left[i\sqrt{2}\right]/(2i\sqrt{2})$, $u \equiv 3$ *if and only if* $-u \equiv 1$ *and* $u \equiv 3 + i\sqrt{2}$ *if and only if* $-u \equiv 1 + i\sqrt{2}$.

Proposition 3.6. *The following statements hold.*

- *In* $\mathbb{Z}[i]/(2)$, *if* $u^2 \equiv 1$, *then* $u \equiv 1$ *or* i.
- *In* $\mathbb{Z}[i]/(2)$, $u \equiv i$ *if and only if* $iu \equiv 1$.

3.2 Matrices

We write e_j for the j-th standard basis vector and $M^\dagger$ for the conjugate transpose of the matrix M. If R is a ring, we sometimes write $R^{n \times n'}$ for the collection of $n \times n'$ matrices over R. We will use one-, two-, and four-level matrices which act non-trivially on only one, two, or four of the components of their input. These matrices will be defined using basic matrices. The construction is best explained with an example. If

$$V = \begin{bmatrix} v_{1,1} & v_{1,2} \\ v_{2,1} & v_{2,2} \end{bmatrix}$$

is a 2-dimensional unitary matrix, then in 3 dimensions the two-level operator of type V, denoted by $V_{[1,3]}$, is the matrix given below.

$$V_{[1,3]} = \begin{bmatrix} v_{1,1} & 0 & v_{1,2} \\ 0 & 1 & 0 \\ v_{2,1} & 0 & v_{2,2} \end{bmatrix}$$

Definition 3.7. Let W be an $n \times n$ unitary matrix, let $n \leq n'$, and let $a_1, \ldots, a_n \in [n']$. The *$n$-level matrix of type W* is the $n' \times n'$ unitary matrix $W_{[a_1,\ldots,a_n]}$ defined by

$$W_{[a_1,\ldots,a_n]\,j,k} = \begin{cases} W_{j',k'} \text{ if } j = a_{j'} \text{ and } k = a_{k'} \\ I_{j,k} \text{ otherwise.} \end{cases}$$

Let R be one of $\mathbb{Z}$, $\mathbb{Z}\left[\sqrt{2}\right]$, $\mathbb{Z}\left[i\sqrt{2}\right]$, $\mathbb{Z}\left[i\right]$ or $\mathbb{Z}\left[\omega\right]$ and let p be an element of $\mathbb{Z}\left[\omega\right]$. We will be interested in matrices of the form

$$V = \frac{1}{p^q} W \tag{1}$$

where W is a matrix over R and $q \in \mathbb{N}$.

Definition 3.8. Fix $R \in \left\{\mathbb{Z}, \mathbb{Z}\left[\sqrt{2}\right], \mathbb{Z}\left[i\sqrt{2}\right], \mathbb{Z}\left[i\right], \mathbb{Z}\left[\omega\right]\right\}$. If V is a matrix of the form (1) and $q' \in \mathbb{N}$, then we say that q' is a *p-denominator exponent* of V if

$$p^{q'} V \in R^{m \times n}.$$

The smallest such q' is the *least p-denominator exponent* of V, denoted $\mathrm{lde}_p(V)$.

We sometimes omit p when the base of the exponent is clear from the context. Note that the notion of denominator exponent applies to matrices of any dimension and we can therefore talk about the denominator exponent of a vector or scalar.

4 Circuits

In this section, we review basic circuit constructions which will be useful below. A more detailed discussion of quantum circuits can be found in Chapter 4 of [31].

Let ζ be an m-th root of unity. We sometimes call ζ a *global phase of order m*. We think of these global phases as gates acting on 0 qubits and in what follows we will be especially interested in the global phases of order 2, 4, and 8, which we denote -1, i, and ω, respectively. The single-qubit *phase gate of order m* is defined as

$$P_\zeta = \begin{bmatrix} 1 & 0 \\ 0 & \zeta \end{bmatrix}.$$

We will be particularly interested in phase gates of order 2, 4, and 8 which we call the Z, S, and T gates, respectively. Hence

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}, \quad \text{and} \quad T = \begin{bmatrix} 1 & 0 \\ 0 & \omega \end{bmatrix}.$$

In addition to phase gates, we will also use the single-qubit gates H and X defined by

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad \text{and} \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

The H gate is the *Hadamard* gate and the X gate is the *NOT* gate. The last single-qubit gate we will use is the F gate defined below.

$$F = \frac{1}{2} \begin{bmatrix} 1 + i\sqrt{2} & 1 \\ 1 & -1 + i\sqrt{2} \end{bmatrix}.$$

The F gate is not as common as the other single-qubit gates introduced above. We note that $F^2 = iH$ and that F can be expressed as a product of better-known gates in Matsumoto-Amano normal form [29],

$$F = SHTSHTSHS\omega^{-1}.$$

We will also make use of the two-qubit $H \otimes H$ gate as well as the *controlled* gates defined below.

$$CH = I_2 \oplus H, \qquad CX = I_2 \oplus X, \quad \text{and} \qquad CCX = I_6 \oplus X.$$

We will refer to these gates as the *controlled-H* gate, *controlled-X* or *CNOT* gate, and the *doubly-controlled-X* or *Toffoli* gate, respectively. In general, if G is a gate, then we write $C^n G$ for the *n-control-G* gate.

As usual, *circuits* are built from gates through composition and tensor product. An *ancilla* is a qubit used locally within a circuit but on which the global action of the circuit is trivial. We say that a $2^n \times 2^n$ unitary matrix W is exactly represented by a circuit D using m *clean* ancillas if for any n-qubit state $|\psi\rangle$,

$$D|\psi\rangle|0\rangle^{\otimes m} = (W|\psi\rangle)|0\rangle^{\otimes m}.$$

If the circuit is independent of the initial state of the ancilla, it is said to accept a *dirty* ancilla. In particular, we say that a $2^n \times 2^n$ unitary matrix W is exactly represented by a circuit D using m *dirty* ancillas if for any n-qubit state $|\psi\rangle$ and any m-qubit state $|\phi\rangle$,

$$D|\psi\rangle|\phi\rangle = (W|\psi\rangle)|\phi\rangle.$$

Note that a clean ancilla can always be used in place of a dirty ancilla.

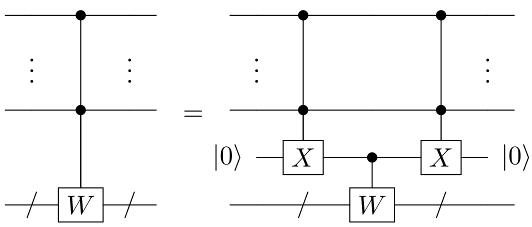
In order to characterize restricted Clifford+T circuits, it is helpful to establish some basic facts about the construction of multi-level matrices over gate sets including the Toffoli gate.

Proposition 4.1. *Any $2^n \times 2^n$ permutation matrix V can be exactly represented by a circuit over the gate set $\{X, CX, CCX\}$ with at most one dirty ancilla.*

Proof. By the Giles-Selinger algorithm [17] restricted to permutation matrices, V can be represented by a circuit over two-level X gates. Likewise, each two-level X gate can be implemented over fully-controlled X and single-qubit gates by using a Gray code (see, e.g., [31, Sec. 4.5.2]). Each fully-controlled X gate can be implemented with one dirty ancilla by [9], which completes the proof. □

Proposition 4.2. *Let W be a $2^m \times 2^m$ unitary matrix and let $\mathcal{G}$ be a set of gates. If CW can be exactly represented over $\{X, CX, CCX\} \cup \mathcal{G}$ using at most one dirty ancilla, then, for any $n \geq 1$, $C^n W$ can also be exactly represented over $\{X, CX, CCX\} \cup \mathcal{G}$. Moreover, a single clean ancilla suffices.*

Proof. This follows from standard techniques, e.g. [9]. If $n = 1$, then CW can be implemented with a single dirty ancilla and thus also with a clean one. If $n > 1$, then the $C^n W$ gate can be implemented as follows, where each gate on the right has at least one dirty ancilla available for use.



□

Corollary 4.3. *Let W be a $2^m \times 2^m$ unitary matrix and let $\mathcal{G}$ be a set of gates. If CW can be exactly represented over $\{X, CX, CCX\} \cup \mathcal{G}$ with at most one dirty ancilla, then $W_{[a_1, a_2 \ldots, a_{2^m}]}$ is representable over $\{X, CX, CCX\} \cup \mathcal{G}$ with at most one clean ancilla.*

Proof. Follows from Propositions 4.1 and 4.2 by noting that there exists a 2^{n+m}-dimensional permutation matrix V such that

$$W_{[a_1, a_2 \ldots, a_{2^m}]} = V^\dagger (C^n W) V.$$

□

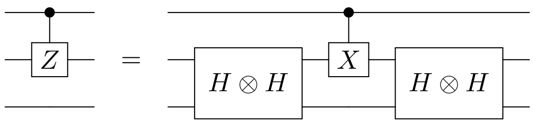
We can now use Corollary 4.3 to give constructions of multi-level matrices of different types over their uncontrolled versions in the presence of the Toffoli gate.

Proposition 4.4. *The operators*

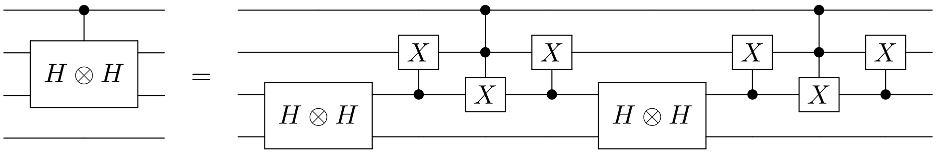
$$\left\{(-1)_{[a]}, X_{[a,b]}, (H \otimes H)_{[a,b,c,d]}\right\},$$

where a, b, c, and d are distinct elements of $[n]$, can be exactly represented by quantum circuits over the gate set $\{X, CX, CCX, H \otimes H\}$ using at most one clean ancilla.

Proof. By Corollary 4.3 it suffices to give constructions for the singly-controlled Z and $H \otimes H$ gates using at most a single dirty ancilla. We have



and it can be verified that the equality below holds.



□

Corollary 4.5. *The operators*

$$\left\{(-1)_{[a]}, X_{[a,b]}, (H \otimes H)_{[a,b,c,d]}, I_{2^{n-1}} \otimes H\right\},$$

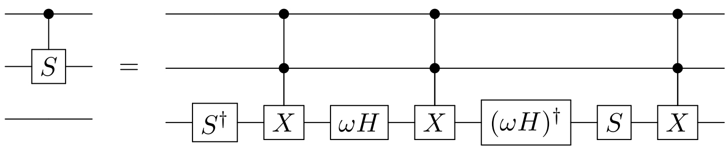
where a, b, c, and d are distinct elements of $[n]$, can be exactly represented by quantum circuits over the gate set $\{X, CX, CCX, H\}$ using at most one clean ancilla.

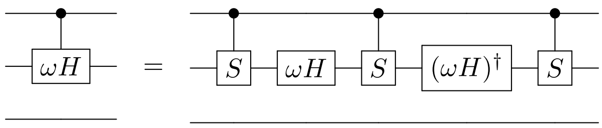
Proposition 4.6. *The operators*

$$\left\{i_{[a]}, X_{[a,b]}, \omega H_{[a,b]}\right\},$$

where a and b are distinct elements of $[n]$, can be exactly represented by quantum circuits over the gate set $\{X, CX, CCX, \omega H, S\}$ using at most one clean ancilla.

Proof. Again, it suffices to give constructions for the singly-controlled S and ωH gates. In this case it can be verified that both of the equalities below hold.





□

Corollary 4.7. *The operators*

$$\left\{i_{[a]}, X_{[a,b]}, \omega H_{[a,b]}, \omega I_n\right\},$$

where a and b are distinct elements of $[n]$, can be exactly represented by quantum circuits over the gate set $\{X, CX, CCX, H, S\}$ using at most one clean ancilla.

Proof. Follows from Proposition 4.6 and the fact that $\omega = SHSHSH$. □

Proposition 4.8. *The operators*

$$\left\{(-1)_{[a]}, X_{[a,b]}, H_{[a,b]}\right\},$$

where a and b are distinct elements of $[n]$, can be exactly represented by quantum circuits over the gate set $\{X, CX, CCX, H, CH\}$ using at most one clean ancilla.

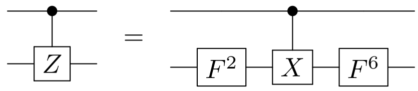
Proof. By Proposition 4.4, $(-1)_{[a]}$ can be represented by a quantum circuit over $\{X, CX, CCX, H \otimes H\}$ and hence also $\{X, CX, CCX, H, CH\}$. Since CH is already in the generating set the proof is complete.
□

Proposition 4.9. *The operators*

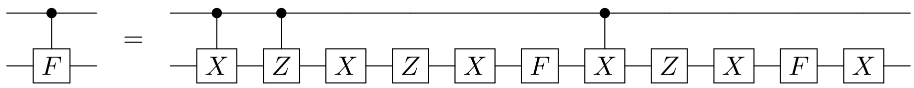
$$\left\{(-1)_{[a]}, X_{[a,b]}, F_{[a,b]}\right\},$$

where a and b are distinct elements of $[n]$, can be exactly represented by quantum circuits over the gate set $\{X, CX, CCX, F\}$ using at most one clean ancilla.

Proof. To show that CZ is representable over the gate set, it can be observed that the equality below holds, since $F^2 = iH$ and $F^6 = -iH$.



The construction of CF is somewhat more involved, but can be obtained from standard constructions (e.g., [9]) by first noting that $(ZXF)^2$ and $X(ZXF)X(ZXF)X = ZXF$. The CF gate can then be constructed as below.



$\square$

5 Number-Theoretic Characterizations

5.1 The $\mathbb{D}$ case

We start by studying the group of $n \times n$ unitary matrices over $\mathbb{D}$. Since X, CX, CCX, and $H \otimes H$ have entries in $\mathbb{D}$, any circuit over the gate set $\{X, CX, CCX, H \otimes H\}$ must represent a unitary matrix over $\mathbb{D}$. Here, we show the converse: any unitary matrix over $\mathbb{D}$ can be represented by a circuit over $\{X, CX, CCX, H \otimes H\}$. To prove this, it is sufficient to establish that every unitary over $\mathbb{D}$ can be expressed as a product of the following generators

$$\left\{(-1)_{[a]}, X_{[a,b]}, (H \otimes H)_{[a,b,c,d]}\right\}, \tag{2}$$

where a, b, c, and d are distinct elements of $[n]$. Indeed, by Proposition 4.4, all of the above generators can be exactly represented by quantum circuits over the gate set $\{X, CX, CCX, H \otimes H\}$.

If V is a matrix over $\mathbb{D}$, then V can be written as

$$V = \frac{1}{2^q} W \tag{3}$$

where $q \in \mathbb{N}$ and W is a matrix over $\mathbb{Z}$. We will consider 2-denominator exponents of such matrices.

The following four lemmas are devoted to proving the analogue of Giles and Selinger's *Column Lemma* (Lemma 5 in [17]). Here, the goal is to establish that any unit vector over $\mathbb{D}$ can be reduced to a standard basis vector by multiplying it on the left by an appropriately chosen sequence of generators. We consider the case of vectors of dimension $n < 4$ first, before moving on to higher dimensions.

Lemma 5.1. *Let $n < 4$ and let $j \in [n]$. If v is an n-dimensional unit vector over $\mathbb{D}$, then there exist generators $G_1, \ldots, G_\ell$ from (2) such that $G_1 \cdots G_\ell v = e_j$.*

Proof. Write v as $v = u/2^q$ with $u \in \mathbb{Z}^n$ and $q = \operatorname{lde}_2(v)$. Since v is a unit vector, we have $v^\dagger v = 1$ and thus $4^q = \sum u_k^\dagger u_k = \sum u_k^2$. The square of any odd number is congruent to 1 modulo 4. Thus when $n < 4$, we have $\sum u_k^2 \equiv 0 \pmod 4$ only if every u_k is even. This implies that $\operatorname{lde}_2(v) = 0$ when $n < 4$ and therefore that $v = \pm e_{j'}$ for some $j' \in [n]$. Hence one of

$$v = e_j, \quad (-1)_{[j]} v = e_j, \quad X_{[j,j']} v = e_j, \quad \text{or} \quad X_{[j,j']}(-1)_{[j']} v = e_j$$

must hold, which completes the proof. $\square$

Because $(H \otimes H)_{[a,b,c,d]}$ is a four-level matrix, we consider its action on certain 4-dimensional vectors in the lemma below. This is in contrast with Giles and Selinger's algorithm, for which only one- and two-level matrices are needed.

Lemma 5.2. *If $u_1, \ldots, u_4 \in \mathbb{Z}$ are such that $u_1^2 \equiv \ldots \equiv u_4^2 \equiv 1 \pmod 4$, then there exist $m_1, \ldots, m_4$ such that*

$$(H \otimes H)(-1)^{m_1}_{[1]}(-1)^{m_2}_{[2]}(-1)^{m_3}_{[3]}(-1)^{m_4}_{[4]} \begin{bmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \end{bmatrix} = \begin{bmatrix} u_1' \\ u_2' \\ u_3' \\ u_4' \end{bmatrix}$$

for some $u_1', \ldots, u_4' \in \mathbb{Z}$ such that $u_1' \equiv \ldots \equiv u_4' \equiv 0 \pmod 2$.

Proof. If $u \in \mathbb{Z}$ is such that $u^2 \equiv 1 \pmod 4$, then $u \equiv 1 \pmod 4$ or $u \equiv 3 \pmod 4$. Furthermore, if $u \equiv 3 \pmod 4$, then $-u \equiv 1 \pmod 4$. Hence, given $u_1, \ldots, u_4 \in \mathbb{Z}$ such that $u_1^2 \equiv \ldots \equiv u_4^2 \equiv 1 \pmod 4$, we can find $m_1, \ldots, m_4$ such that $(-1)^{m_1} u_1 \equiv \ldots \equiv (-1)^{m_4} u_4 \equiv 1 \pmod 4$. It can then be verified that

$$(H \otimes H) \begin{bmatrix} (-1)^{m_1} u_1 \\ (-1)^{m_2} u_2 \\ (-1)^{m_3} u_3 \\ (-1)^{m_4} u_4 \end{bmatrix} = \begin{bmatrix} u_1' \\ u_2' \\ u_3' \\ u_4' \end{bmatrix}$$

for some $u_1' \equiv \ldots \equiv u_4' \equiv 0 \pmod 2$. □

Lemma 5.3. *Let $n \geq 4$. If v is an n-dimensional unit vector over $\mathbb{D}$ and $\mathrm{lde}_2(v) > 0$, then there exist generators $G_1, \ldots, G_\ell$ from (2) such that $G_1 \cdots G_\ell v = v'$ and $\mathrm{lde}_2(v') < \mathrm{lde}_2(v)$.*

Proof. Write v as $v = u/2^q$ where $u \in \mathbb{Z}^n$ and $q > 1$. Since v is a unit vector we have $v^\dagger v = 1$ and thus $4^q = \sum u_k^\dagger u_k = \sum u_k^2$ since u is real. The number of u_k such that $u_k^2 \equiv 1 \pmod 4$ is therefore congruent to 0 modulo 4. Hence, we can group these entries in sets of size 4 and apply Lemma 5.2 to each such set in order to reduce the 2-denominator exponent of the vector. □

Lemma 5.4. *Let $j \in [n]$. If v is an n-dimensional unit vector over $\mathbb{D}$, then there exist generators $G_1, \ldots, G_\ell$ from (2) such that $G_1 \cdots G_\ell v = e_j$.*

Proof. The case of vectors of dimension $n < 4$ was treated in Lemma 5.1 so we assume that $n \geq 4$ and we proceed by induction on the least 2-denominator exponent of v.

- If $\mathrm{lde}_2(v) = 0$, then v is a unit vector in $\mathbb{Z}^n$. Hence $v = \pm e_{j'}$ for some $j' \in [n]$ and one of

  $$v = e_j, \quad (-1)_{[j]} v = e_j, \quad X_{[j,j']} v = e_j, \quad \text{or} \quad X_{[j,j']}(-1)_{[j']} v = e_j$$

  must hold.

- If $\mathrm{lde}_2(v) > 0$, apply Lemma 5.3 to reduce the 2-denominator exponent of v. □

We can now use Lemma 5.4 to prove that every unitary matrix with entries in $\mathbb{D}$ can be written as a product of generators. This, together with Proposition 4.4 establishes our characterization of circuits over the gate set $\{X, CX, CCX, H \otimes H\}$.

Theorem 5.5. *If V is an n-dimensional unitary matrix with entries in $\mathbb{D}$, then there exist generators $G_1, \ldots, G_\ell$ from (2) such that $G_1 \cdots G_\ell V = I$.*

Proof. By iteratively applying Lemma 5.4 to the columns of V. □

Corollary 5.6. *A matrix V can be exactly represented by an n-qubit circuit over $\{X, CX, CCX, H \otimes H\}$ if and only if $V \in U_{2^n}(\mathbb{D})$. Moreover, a single ancilla always suffices to construct a circuit for V.*

5.1.1 Super-integral Clifford+T operators

One might wonder whether the $H \otimes H$ gate can be replaced with the H gate. Since the H gate lies strictly outside of $U_{2^n}(\mathbb{D})$, having denominator $\sqrt{2}$, we get a slightly more general gate set. Circuits over this gate set generate matrices of the form

$$V = \frac{1}{\sqrt{2}^q} W \tag{4}$$

where $q \in \mathbb{N}$ and W is a matrix over $\mathbb{Z}$.

We now leverage Theorem 5.5 and Corollary 4.5 to show that every unitary matrix of the form in Eq. (4) can be represented by a circuit over $\{X, CX, CCX, H\}$. For these matrices, we use $\sqrt{2}$-denominator exponents. We extend the set of generators from (2) with a matrix of the form $I \otimes H$. Thus the relevant generators are now

$$\left\{(-1)_{[a]}, X_{[a,b]}, (H \otimes H)_{[a,b,c,d]}, I_{n/2} \otimes H\right\} \tag{5}$$

where a, b, c, and d are distinct elements of $[n]$, and $I_{n/2} \otimes H$ is only well-defined when n is even. As the extra generator is only available in even dimensions, we start by showing that there are no odd-dimension unitary matrices of the form of Eq. (4) with odd q. The proof of this fact is due to Xiaoning Bian [10].

Lemma 5.7. *If $V \neq 0$ is as in (4), then all the $\sqrt{2}$-denominator exponents of V are congruent modulo 2.*

Proof. Suppose that $q < q'$ are two $\sqrt{2}$-denominator exponents of V. Then $V = W/\sqrt{2}^q = W'/\sqrt{2}^{q'}$ for some integer matrices W and W'. Assume without loss of generality that $q < q'$. Then

$$W' = \sqrt{2}^{q'} V = \sqrt{2}^{q'-q} W$$

so that $\sqrt{2}^{q'-q} W$ is an integer matrix. Hence $q \equiv q' \pmod 2$, since $V \neq 0$ and $\sqrt{2} \notin \mathbb{Z}$. □

Lemma 5.8. *If v is an n-dimensional unit vector of the form $v = (1/\sqrt{2})^q u$ where u is an integer vector and q is odd, then there exist generators $G_1, \ldots, G_\ell$ from (5) such that*

$$G_1 \cdots G_\ell v = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Proof. By induction on q. For the base case, it suffices to observe that since $\sum u_k^2 = 2$, there exist j, j' such that $u_j = (-1)^{m_j}$ and $u_{j'} = (-1)^{m_{j'}}$ and the other entries of u are all 0. It can then be verified that

$$X_{[0,j]} X_{[1,j']} (-1)_{[j]}^{m_j} (-1)_{[j']}^{m_{j'}} v = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Now suppose $q \geq 3$. Then $\sum u_k^2 = 2^q = 4^{q'}$ and hence the number of $u_k^2 \equiv 1 \pmod 4$ is congruent to 0 modulo 4. Then, as in Lemma 5.3, we can group these entries in sets of size 4 and apply Lemma 5.2 to each set to reduce the $\sqrt{2}$-denominator exponent of the vector by 2. □

Note also that the proof of Lemma 5.8 implies that there are no unit vectors of the form $v = u/\sqrt{2}^q$ with odd $q \geq 3$ and dimension $n < 4$.

Lemma 5.9. *There are no odd-dimensional unitary matrices $V = W/\sqrt{2}^q$ such that W is an integer matrix and q is odd.*

Proof. By induction on n. If $n = 1$, then the only possibility is $V = 1$, hence there is no such unitary with odd least $\sqrt{2}$-denominator exponent. Now consider $n \geq 3$ and assume that $V = W/\sqrt{2}^q$ where q is odd and W is an integer matrix. Let v be the first column of V. By Lemma 5.7, all the $\sqrt{2}$-denominator exponents of v are odd and by Lemma 5.8 there exists a unitary transformation $G = G_1 \cdots G_\ell U$ such that

$$GV = \left[\begin{array}{c|c} \frac{1}{\sqrt{2}} & \\ \frac{1}{\sqrt{2}} & \\ 0 & V' \\ \vdots & \\ 0 & \end{array}\right].$$

Let u_1, u_2 be the first two columns of $(GV)^\dagger$. Since $(GV)^\dagger$ is unitary, we know that $u_1^\dagger u_1 = u_2^\dagger u_2 = 1$, and $u_1^\dagger u_2 = u_2^\dagger u_1 = 0$. In can then be observed from the unit condition on u_1 and u_2, that they each have one additional $\pm(1/\sqrt{2})$ entry, and are 0 everywhere else. Further, by the orthogonality condition it follows that these entries both occur on the same row j. Hence there exists m such that

$$(-1)^m_{[2]} X_{[2,j]} \begin{bmatrix} u_1 & u_2 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \\ 0 & 0 \\ \vdots & \vdots \\ 0 & 0 \end{bmatrix}.$$

Thus

$$UV((-1)^m_{[2]} X_{[2,j]})^\dagger = \left[\begin{array}{c|c} H & 0 \\ \hline 0 & V'' \end{array}\right]$$

where V'' is a unitary matrix of the form of Eq. (4) that has odd dimension and, by Lemma 5.7, odd least $\sqrt{2}$-denominator exponent, a contradiction. $\square$

Having ruled out matrices with odd dimension and odd $\sqrt{2}$-denominator exponent, we can now prove our theorem.

Theorem 5.10. *If $V = W/\sqrt{2}^q$ is an n-dimensional unitary matrix such that W is an integer matrix, then there exist generators $G_1, \ldots, G_\ell$ from (5) such that $G_1 \cdots G_\ell V = I$.*

Proof. If q is even, the result follows from Theorem 5.5. If q is odd, then by Lemma 5.9 n must be even, and so $(I_{n/2} \otimes H)V$ is a matrix with entries in $\mathbb{D}$. Hence the result follows by applying Theorem 5.5 to $(I_{n/2} \otimes H)V$. $\square$

Corollary 5.11. *A matrix V can be exactly represented by an n-qubit circuit over $\{X, CX, CCX, H\}$ if and only if V is a 2^n-dimensional unitary matrix such that $V = W/\sqrt{2}^q$ for some integer matrix W and some $q \in \mathbb{N}$. Moreover, a single ancilla always suffices to construct a circuit for V.*

5.2 The $\mathbb{D}\left[\sqrt{2}\right]$ case

We now focus on the group of $n \times n$ unitary matrices with entries in $\mathbb{D}\left[\sqrt{2}\right]$. The elements of this group can be written as

$$V = \frac{1}{\sqrt{2}^q} W \tag{6}$$

where $q \in \mathbb{N}$ and W is a matrix over $\mathbb{Z}\left[\sqrt{2}\right]$. We now use $\sqrt{2}$-denominator exponents and the relevant generators are

$$\left\{(-1)_{[a]}, X_{[a,b]}, H_{[a,b]}\right\} \tag{7}$$

where a and b are distinct elements of $[n]$. By Proposition 4.8, all of the above generators can be exactly represented by quantum circuits over the gate set $\{X, CX, CCX, H, CH\}$. As in the previous cases, we prove our characterization by showing that any unitary matrix of the form (6) can be expressed as a product of generators from (7).

Lemma 5.12. *If $u_1, u_2 \in \mathbb{Z}\left[\sqrt{2}\right]$ are such that $u_1 \equiv u_2 \pmod{2}$, then*

$$H \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} = \begin{bmatrix} u_1' \\ u_2' \end{bmatrix}$$

for some $u_1', u_2' \in \mathbb{Z}\left[\sqrt{2}\right]$ such that $u_1' \equiv u_2' \equiv 0 \pmod{\sqrt{2}}$.

Proof. Since $u_1 \equiv u_2 \pmod{2}$, we have $u_1 + u_2 \equiv u_1 - u_2 \equiv 0 \pmod{2}$. It can then be verified that

$$H \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} = \begin{bmatrix} u_1' \\ u_2' \end{bmatrix}$$

for some $u_1' \equiv u_2' \equiv 0 \pmod{2}$. □

Lemma 5.13. *If v is an n-dimensional unit vector over $\mathbb{D}\left[\sqrt{2}\right]$ and $\operatorname{lde}_{\sqrt{2}}(v) > 0$, then there exist generators $G_1, \ldots, G_\ell$ from (7) such that $G_1 \cdots G_\ell v = v'$ and $\operatorname{lde}_{\sqrt{2}}(v') < \operatorname{lde}_{\sqrt{2}}(v)$.*

Proof. Write v as $v = u/\sqrt{2}^q$ where $u \in \mathbb{Z}\left[\sqrt{2}\right]$ and $q > 0$. Since v is a unit vector we have $v^\dagger v = 1$ and thus $2^q = \sum u_j^\dagger u_j = \sum u_j^2$ since u is real. Letting $u_j = x_j + y_j\sqrt{2}$, this yields the following equation

$$2^q = \sum x_j^2 + 2y_j^2 + x_j y_j 2\sqrt{2}.$$

Thus $\sum x_j^2 \equiv 0 \pmod{2}$ and $\sum x_j y_j = 0$. It follows that $u_j \equiv 1 \pmod{2}$ for evenly many j and $u_j \equiv 1 + \sqrt{2} \pmod{2}$ for evenly many j. We can therefore group these entries in sets of size 2 and apply Lemma 5.12 to each such set in order to reduce the $\sqrt{2}$-denominator exponent of the vector. □

The following three statements are established like the corresponding ones in the previous section. For this reason, we omit their proofs.

Lemma 5.14. *Let $j \in [n]$. If v is an n-dimensional unit vector over $\mathbb{D}\left[\sqrt{2}\right]$, then there exist generators $G_1, \ldots, G_\ell$ from (7) such that $G_1 \cdots G_\ell v = e_j$.*

Theorem 5.15. *If V is an n-dimensional unitary matrix with entries in $\mathbb{D}\left[\sqrt{2}\right]$, then there exist generators $G_1, \ldots, G_\ell$ from (7) such that $G_1 \cdots G_\ell V = I$.*

Corollary 5.16. *A matrix V can be exactly represented by an n-qubit quantum circuit over the gate set $\{X, CX, CCX, H, CH\}$ if and only if $V \in U_{2^n}\left(\mathbb{D}\left[\sqrt{2}\right]\right)$. Moreover, a single ancilla always suffices to construct a circuit for V.*

5.3 The $\mathbb{D}\left[i\sqrt{2}\right]$ case

We now consider the group of $n \times n$ unitary matrices with entries in $\mathbb{D}\left[i\sqrt{2}\right]$. Such matrices can be written as

$$V = \frac{1}{(i\sqrt{2})^q} W \tag{8}$$

where $q \in \mathbb{N}$ and W is a matrix over $\mathbb{Z}\left[i\sqrt{2}\right]$. We now use $i\sqrt{2}$-denominator exponents and the relevant generators are

$$\left\{(-1)_{[a]}, X_{[a,b]}, F_{[a,b]}\right\} \tag{9}$$

where a and b are distinct elements of $[n]$. By Proposition 4.9, all of the above generators can be exactly represented by quantum circuits over the gate set $\{X, CX, CCX, F\}$. As in the previous cases, we establish our characterization by showing that any unitary matrix of the form (8) can be expressed as a product of generators from (9).

Lemma 5.17. *If $u_1, u_2 \in \mathbb{Z}\left[i\sqrt{2}\right]$ are such that $u_1^\dagger u_1 \equiv u_2^\dagger u_2 \equiv 1 \pmod{2}$, then there exist m_0, m_1, m_2, and m_3 such that*

$$F^{m_0}(-1)_{[1]}^{m_1}(-1)_{[2]}^{m_2} X^{m_3} \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} = \begin{bmatrix} u_1' \\ u_2' \end{bmatrix}$$

for some $u_1', u_2' \in \mathbb{Z}\left[i\sqrt{2}\right]$ such that $u_1' \equiv u_2' \equiv 0 \pmod{i\sqrt{2}}$.

Proof. First consider the case in which $u_1 \equiv u_2 \pmod 2$. Then $u_1 + u_2 \equiv u_1 - u_2 \equiv 0 \pmod 2$ and it can be verified that

$$F^2 \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} = iH \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} = \begin{bmatrix} u_1' \\ u_2' \end{bmatrix}$$

for some $u_1' \equiv u_2' \equiv 0 \pmod{i\sqrt{2}}$. We now consider the case in which $u_1 \not\equiv u_2 \pmod 2$. In this case, the fact that $u_1^\dagger u_1 \equiv u_2^\dagger u_2 \equiv 1 \pmod 2$ implies that one of u_1 or u_2 is congruent to 1 or 3 modulo $2i\sqrt{2}$ while the other is congruent to $(1+i\sqrt{2})$ or $(3+i\sqrt{2})$ modulo $2i\sqrt{2}$. We can therefore find m_1, m_2, m_3 such that

$$(-1)_{[1]}^{m_1}(-1)_{[2]}^{m_2} X^{m_3} \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} = \begin{bmatrix} u_1'' \\ u_2'' \end{bmatrix}$$

where $u_1'' \equiv 1 + i\sqrt{2} \pmod{2i\sqrt{2}}$ and $u_2'' \equiv 1 \pmod{2i\sqrt{2}}$. Then

$$F \begin{bmatrix} u_1'' \\ u_2'' \end{bmatrix} = \frac{1}{2} \begin{bmatrix} (1+i\sqrt{2})u_1'' + u_2'' \\ u_1'' + (-1+i\sqrt{2})u_2'' \end{bmatrix}.$$

But $u_1'' \equiv 1 + i\sqrt{2} \pmod{2i\sqrt{2}}$ and $u_2'' \equiv 1 \pmod{2i\sqrt{2}}$ so that

$$(1+i\sqrt{2})u_1'' + u_2'' \equiv (1+i\sqrt{2})^2 + 1 \equiv 2i\sqrt{2} \equiv 0 \pmod{2i\sqrt{2}}.$$

and

$$u_1'' + (-1+i\sqrt{2})u_2'' \equiv (1+i\sqrt{2}) + (-1+i\sqrt{2}) \equiv 2i\sqrt{2} \equiv 0 \pmod{2i\sqrt{2}}.$$

Hence we can set $u_1' = ((1+i\sqrt{2})u_1'' + u_2'')/2$ and $u_2' = (u_1'' + (-1+i\sqrt{2})u_2'')/2$ to complete the proof. □

Lemma 5.18. *If v is an n-dimensional unit vector over $\mathbb{D}\left[i\sqrt{2}\right]$ and $\mathrm{lde}_{i\sqrt{2}}(v) > 0$, then there exist generators $G_1, \ldots, G_\ell$ from (9) such that $G_1 \cdots G_\ell v = v'$ and $\mathrm{lde}_{i\sqrt{2}}(v') < \mathrm{lde}_{i\sqrt{2}}(v)$.*

Proof. Write v as $v = u/i\sqrt{2}^q$ where $u \in \mathbb{Z}\left[i\sqrt{2}\right]$ and $q > 0$. Since v is a unit vector we have $v^\dagger v = 1$ and thus $(-2)^q = \sum u_j^\dagger u_j$. Thus $\sum u_j^\dagger u_j \equiv 0 \pmod 2$ and it follows that $u_j^\dagger u_j \equiv 1 \pmod 2$ for evenly many j, since modulo 2 we have $u_j^\dagger u_j \equiv 0$ or $u_j^\dagger u_j \equiv 1$. We can therefore group these entries in sets of size 2 and apply Lemma 5.17 to each such set in order to reduce the denominator exponent. □

Lemma 5.19. *Let $j \in [n]$. If v is an n-dimensional unit vector over $\mathbb{D}\left[i\sqrt{2}\right]$, then there exist generators $G_1, \ldots, G_\ell$ from (9) such that $G_1 \cdots G_\ell v = e_j$.*

Theorem 5.20. *If V is an n-dimensional unitary matrix with entries in $\mathbb{D}\left[i\sqrt{2}\right]$, then there exist generators $G_1, \ldots, G_\ell$ from (9) such that $G_1 \cdots G_\ell V = I$.*

Corollary 5.21. *A matrix V can be exactly represented by an n-qubit circuit over $\{X, CX, CCX, F\}$ if and only if $V \in U_{2^n}\left(\mathbb{D}\left[i\sqrt{2}\right]\right)$. Moreover, a single ancilla always suffices to construct a circuit for V.*

We close this section with a characterization of ancilla-free circuits over $\{X, CX, CCX, F\}$, focusing on circuits on four or more qubits. The required circuit constructions are relegated to Appendix A.1.

Corollary 5.22. *Let $n \geq 4$. A matrix $V \in U_{2^n}(\mathbb{D}\left[i\sqrt{2}\right])$ can be exactly represented by an ancilla-free n-qubit circuit over $\{X, CX, CCX, F\}$ if and only if $\det V = 1$.*

Proof. If $\det V \neq 1$, then V cannot be exactly represented over $\{X, CX, CCX, F\}$ without ancillas when $n \geq 4$, as each gate has determinant 1 in this case.

Now suppose $\det V = 1$. First observe that in Lemma 5.17, and consequently Lemma 5.18, the least $i\sqrt{2}$-denominator exponent can be reduced by substituting $F^{m_0}(-1)_{[1]}^{m_1}(-1)_{[2]}^{m_2}X^{m_3}$ as follows:

$$\begin{aligned}
F^2 &\to (FZ)(ZF), \\
F(-1)_{[1]} &\to (FZ)(XZ)(XZ), \\
F(-1)_{[2]} &\to (FZ), \\
F(-1)_{[1]}(-1)_{[2]} &\to (ZF)(XZ)(XZ), \\
FX &\to (FZ)(ZX), \\
F(-1)_{[1]}X &\to (ZF)(XZ), \\
F(-1)_{[2]}X &\to (ZF)(ZX), \text{ and} \\
F(-1)_{[1]}(-1)_{[2]}X &\to (FZ)(XZ).
\end{aligned}$$

Moreover, FZ, ZF, XZ and ZX have determinant 1 and can be represented over $\{X, CX, CCX, F\}$ without ancillas when $n \geq 4$ as shown in Appendix A.1. Likewise, an analogue of Lemma 5.19, where $G_1 \cdots G_\ell v = i^m e_j$, holds by using the two-level ZX operator, which has determinant 1 and is representable without ancillas as shown in Appendix A.1. It now suffices to note that there exist generators $G_1, \ldots, G_\ell$ from the set $\left\{XZ_{[a,b]}, ZX_{[a,b]}, FZ_{[a,b]}, ZF_{[a,b]}\right\}$ such that

$$G_1 \cdots G_\ell V = D$$

where D is a diagonal unitary with entries ± 1. Since $\det D = \det V = 1$, there are an even number of -1 entries, thus we can group them into pairs and use four-level $I \otimes Z$ operators to change each pair into $+1$ and obtain the identity matrix. □

5.4 The $\mathbb{D}[i]$ case

Finally, we turn our attention to the group of $n \times n$ unitary matrices with entries in $\mathbb{D}[i]$. The relevant set of generators is

$$\left\{i_{[a]}, X_{[a,b]}, \omega H_{[a,b]}\right\} \tag{10}$$

where a and b are distinct elements of $[n]$. We reason as in the previous cases, noting by Proposition 4.6 that all of the above generators can be exactly represented by circuits over $\{X, CX, CCX, \omega H, S\}$.

If V is a matrix over $\mathbb{D}[i]$, then V can be written as $V = W/2^q$ where $q \in \mathbb{N}$ and W is a matrix over $\mathbb{Z}[i]$. For our purposes, however, it is more convenient to express these matrices as

$$V = \frac{1}{(1+i)^q} W \tag{11}$$

where $q \in \mathbb{N}$ and W is a matrix over $\mathbb{Z}[i]$. This is equivalent since

$$\frac{1}{2^q} W = \frac{i^q}{(1+i)^{2q}} W = \frac{1}{(1+i)^{2q}} W'.$$

We therefore use matrices of the form (11) and use $(1+i)$-denominator exponents.

Lemma 5.23. *If $u_1, u_2 \in \mathbb{Z}[i]$ are such that $u_1^2 \equiv u_2^2 \equiv 1 \pmod 2$, then there exist m_1 and m_2 such that*

$$\omega H i_{[1]}^{m_1} i_{[2]}^{m_2} \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} = \begin{bmatrix} u_1' \\ u_2' \end{bmatrix}$$

for some $u_1', u_2' \in \mathbb{Z}[i]$ such that $u_1' \equiv u_2' \equiv 0 \pmod{1+i}$.

Proof. If $u^2 \equiv 1 \pmod 2$, then $u \equiv 1 \pmod 2$ or $u \equiv i \pmod 2$. Furthermore, if $u \equiv i \pmod 2$, then $iu \equiv 1 \pmod 2$. Hence, given $u_1, u_2 \in \mathbb{Z}$ such that $u_1^2 \equiv u_2^2 \equiv 1 \pmod 2$, we can find m_1 and m_2 such that $i^{m_1} u_1 \equiv i^{m_2} u_2 \equiv 1 \pmod 2$. It can then be verified that

$$\omega H i_{[1]}^{m_1} i_{[2]}^{m_2} \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} = \begin{bmatrix} u_1' \\ u_2' \end{bmatrix}$$

for some $u_1' \equiv u_2' \equiv 0 \pmod{1+i}$. □

Lemma 5.24. *If v is an n-dimensional unit vector over $\mathbb{D}[i]$ and $\operatorname{lde}_{(1+i)}(v) > 0$, then there exist generators $G_1, \ldots, G_\ell$ from (10) such that $G_1 \cdots G_\ell v = v'$ and $\operatorname{lde}_{(1+i)}(v') < \operatorname{lde}_{(1+i)}(v)$.*

Proof. Write v as $v = u/(1+i)^q$ where $u \in \mathbb{Z}[i]$ and $q > 1$. Since $(1+i)^\dagger(1+i) = 2$ and v is a unit vector, we have $2^q = \sum u_j^\dagger u_j$. Thus $0 \equiv \sum u_j^\dagger u_j \equiv \sum u_j^2 \pmod 2$ and it follows that $u_j^2 \equiv 1 \pmod 2$ for evenly many j. We can therefore group these entries in sets of size 2 and apply Lemma 5.23 to each such set in order to reduce the denominator exponent. □

Lemma 5.25. *Let $j \in [n]$. If v is an n-dimensional unit vector over $\mathbb{D}[i]$, then there exist generators $G_1, \ldots, G_\ell$ from (10) such that $G_1 \cdots G_\ell v = e_j$.*

Theorem 5.26. *If V is an n-dimensional unitary matrix with entries in $\mathbb{D}[i]$, then there exist generators $G_1, \ldots, G_\ell$ from (10) such that $G_1 \cdots G_\ell V = I$.*

Corollary 5.27. *A matrix V can be exactly represented by an n-qubit circuit over $\{X, CX, CCX, \omega H, S\}$ if and only if $V \in U_{2^n}(\mathbb{D}[i])$. Moreover, a single ancilla always suffices to construct a circuit for V.*

Corollary 5.28. *Let $n \geq 4$. A matrix $V \in U_{2^n}(\mathbb{D}[i])$ can be exactly represented by an ancilla-free n-qubit circuit over $\{X, CX, CCX, \omega H, S\}$ if and only if $\det V = 1$.*

Proof. We proceed as in the proof of Corollary 5.22. In particular, the least $(1+i)$-denominator exponent can be reduced in Lemma 5.24 by substituting $\omega H i_{[1]}^{m_1} i_{[2]}^{m_2}$ with ancilla-free two-level generators as follows:

$$\begin{aligned} \omega H &\to (\omega SH), \\ \omega H i_{[1]} &\to (\omega HS)(iZ), \\ \omega H i_{[2]} &\to (\omega HS), \text{ and} \\ \omega H i_{[1]} i_{[2]} &\to (\omega SH)(iZ). \end{aligned}$$

Moreover, each parenthesized two-level operator on the right hand side has determinant 1 and can be exactly represented over $\{X, CX, CCX, \omega H, S\}$ without ancillas when $n \geq 4$ as shown in Appendix A.2.

An analogue of Lemma 5.25 where $G_1 \cdots G_\ell v = i^m e_j$ holds by using the two-level iX operator, which similarly has determinant 1 and is representable without ancillas as shown in Appendix A.2. Again, there exist generators $G_1, \ldots, G_\ell$ from the set $\left\{iZ_{[a,b]}, iX_{[a,b]}, \omega SH_{[a,b]}, \omega HS_{[a,b]}\right\}$ such that

$$G_1 \cdots G_\ell V = D$$

where D is a diagonal unitary with entries i^m. We can then use the n-qubit two-level iZ operator to remove the phases as follows. Suppose the jth diagonal entry is i^{m_j} and let $N = 2^n$. It can then be observed that

$$(iZ_{[1,2]})^{-m_1}(iZ_{[2,3]})^{-m_1-m_2} \ldots (iZ_{[N-1,N]})^{-m_1-m_2-\cdots-m_{N-1}} D = \begin{bmatrix} I_{N-1} & 0 \\ 0 & i^{\sum_{j=1}^{N} m_j} \end{bmatrix} = \begin{bmatrix} I_{N-1} & 0 \\ 0 & \det D \end{bmatrix}$$

Since $\det D = \det V = 1$, the proof is complete. □

5.4.1 Super-Gaussian Clifford+T operators

As in the integral case, the characterization of Gaussian Clifford+T circuits as unitaries over $\mathbb{D}[i]$ requires the unusual ωH gate as a generator. Replacing ωH with H yields a slightly larger set of unitaries with matrices of the form

$$V = \frac{1}{\sqrt{2}^q} W \tag{12}$$

where $q \in \mathbb{N}$ and W is a matrix over $\mathbb{Z}[i]$.

We use Corollary 5.27 together with Corollary 4.7 to show that any unitary of the form of Eq. (12) can be represented by a circuit over the gate set $\{X, CX, CCX, H, S\}$. In this case we use $\sqrt{2}$-denominator exponents and, as in Section 5.1, we make use of the fact that $\sqrt{2} \notin \mathbb{Z}[i]$. The relevant generators are now

$$\left\{ i_{[a]}, X_{[a,b]}, \omega H_{[a,b]}, \omega I_n \right\}. \tag{13}$$

Lemma 5.29. *If $V \neq 0$ is as in (12), then all the denominator exponents of V are congruent modulo 2.*

Proof. Similar to the proof of Lemma 5.7. □

Theorem 5.30. *If $V = W/\sqrt{2}^q$ is an n-dimensional unitary matrix such that W is a matrix over $\mathbb{Z}[i]$, then there exist generators $G_1, \ldots, G_\ell$ from (13) such that $G_1 \cdots G_\ell V = I$.*

Proof. If q is even, the result follows from Theorem 5.26. If q is odd, then $(\omega I_n)V$ is a matrix with entries in $\mathbb{D}[i]$. Hence the result follows by applying Theorem 5.26 to $(\omega I_n)V$. □

Corollary 5.31. *A matrix V can be exactly represented by an n-qubit circuit over $\{X, CX, CCX, H, S\}$ if and only if V is a 2^n-dimensional unitary matrix such $V = W/\sqrt{2}^q$ for some matrix W over $\mathbb{Z}[i]$ and some $q \in \mathbb{N}$. Moreover, a single ancilla always suffices to construct a circuit for V.*

6 Conclusion

In this paper, we provided number-theoretic characterizations for several classes of restricted but universal Clifford+T circuits, focusing on integral, real, imaginary, and Gaussian circuits. We showed that a unitary matrix can be exactly represented by an n-qubit integral Clifford+T circuit if and only if it is an element of the group $U_{2^n}(\mathbb{D})$. We then established that real, imaginary, and Gaussian circuits similarly correspond to the groups $U_{2^n}(\mathbb{D}\left[\sqrt{2}\right])$, $U_{2^n}(\mathbb{D}\left[i\sqrt{2}\right])$, and $U_{2^n}(\mathbb{D}[i])$, respectively.

An avenue for future research is to improve the performance, in runtime or gate count, of the algorithms introduced in the present paper. Further afield, it would be interesting to study restricted Clifford+T circuits in the context of fault-tolerance, randomized benchmarking, or simulation. While these and many other questions remain open, we hope that our characterizations will help deepen our understanding of Clifford+T circuits, restricted or not.

7 Acknowledgements

We would like to thank Alexandre Clément, Sarah Li, Rob Noble, and Kira Scheibelhut for their valuable insights as well as Xiaoning Bian, Simon Burton, and Peter Selinger for providing helpful feedback on an earlier version of the paper. We are especially indebted to Xiaoning Bian for the proof of Lemma 5.9 and to Peter Selinger for crucial observations on restrictions of the Clifford+T gate set.

References

[1] S. Aaronson, D. Grier, and L. Schaeffer. The classification of reversible bit operations. In *Proceedings of the 8th Innovations in Theoretical Computer Science Conference*, volume 67 of *LIPIcs*, pages 23:1–23:34, 2017. DOI: 10.4230/LIPIcs.ITCS.2017.23. Also available from `arXiv:1504.05155`.

[2] D. Aharonov. A simple proof that Toffoli and Hadamard are quantum universal. Preprint available from `arXiv:quant-ph/0301040`, Jan. 2003.

[3] M. Amy and M. Mosca. T-count optimization and Reed-Muller codes. *IEEE Transactions on Information Theory*, 65(8):4771–4784, 2019. DOI: 10.1109/TIT.2019.2906374. Also available from `arXiv:1601.07363`.

[4] M. Amy, D. Maslov, M. Mosca, and M. Roetteler. 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):818–830, 2013. DOI: 10.1109/TCAD.2013.2244643. Also available from `arXiv:1206.0758`.

[5] M. Amy, D. Maslov, and M. Mosca. 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):1476–1489, 2014. DOI: 10.1109/TCAD.2014.2341953. Also available from `arXiv:1303.2042`.

[6] M. Amy, J. Chen, and N. J. Ross. A finite presentation of CNOT-dihedral operators. In *Proceedings of the 14th International Conference on Quantum Physics and Logic*, QPL '17, pages 84–97, 2017. DOI: 10.4204/EPTCS.266.5.

[7] M. Artin. *Algebra*. Prentice Hall, 1991.

[8] M. Backens and A. Kissinger. ZH: A complete graphical calculus for quantum computations involving classical non-linearity. In *Proceedings of the 15th International Conference on Quantum Physics and Logic*, QPL '18, pages 23–42, 2018. DOI: 10.4204/EPTCS.287.2.

[9] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter. Elementary gates for quantum computation. *Physical Review A*, 52: 3457–3467, 1995. DOI: 10.1103/PhysRevA.52.3457. Also available from `arXiv:quant-ph/9503016`.

[10] X. Bian. Private communication, July 2019.

[11] X. Bian and P. Selinger. Relations for the group of 2-qubit Clifford+T operators. Talk given at the Quantum Programming and Circuits Workshop. Slides available from `https://www.mathstat.dal.ca/~xbian/talks/slide_cliffordt2.pdf`, June 2015.

[12] A. Bocharov, Y. Gurevich, and K. M. Svore. Efficient decomposition of single-qubit gates into V basis circuits. *Physical Review A*, 88:012313, 2013. DOI: 10.1103/PhysRevA.88.012313. Also available from `arXiv:1303.1411`.

[13] A. Bocharov, M. Roetteler, and K. M. Svore. Efficient synthesis of probabilistic quantum circuits with fallback. *Physical Review A*, 91:052317, 2015. DOI: 10.1103/PhysRevA.91.052317. Also available from arXiv:1409.3552.

[14] A. Bouland and S. Aaronson. Generation of universal linear optics by any beam splitter. *Physical Review A*, 89:062316, 2014. DOI: 10.1103/PhysRevA.89.062316. Also available from arXiv:1310.6718.

[15] A. De Vos, R. Van Laer, and S. Vandenbrande. The group of dyadic unitary matrices. *Open Systems & Information Dynamics*, 19(01):1250003, 2012. DOI: 10.1142/S1230161212500035.

[16] S. Forest, D. Gosset, V. Kliuchnikov, and D. McKinnon. Exact synthesis of single-qubit unitaries over Clifford-cyclotomic gate sets. *Journal of Mathematical Physics*, 56(8):082201, 2015. DOI: 10.1063/1.4927100. Also available from arXiv:1501.04944.

[17] B. Giles and P. Selinger. Exact synthesis of multiqubit Clifford+T circuits. *Physical Review A*, 87: 032332, 2013. DOI: 10.1103/PhysRevA.87.032332. Also available from arXiv:1212.0506.

[18] B. Giles and P. Selinger. Remarks on Matsumoto and Amano's normal form for single-qubit Clifford+T operators. Preprint available from arXiv:1312.6584, Dec. 2013.

[19] D. Gosset, V. Kliuchnikov, M. Mosca, and V. Russo. An algorithm for the T-count. *Quantum Information & Computation*, 14(15-16):1261–1276, 2014. DOI: 10.26421/QIC14.15-16. Also available from arXiv:1308.4134.

[20] S. Greylyn. Generators and relations for the group $U_4(\mathbb{Z}[1/\sqrt{2}, i])$. Master's thesis. Available from arXiv:1408.6204, 2014.

[21] D. Grier and L. Schaeffer. The classification of stabilizer operations over qubits. Preprint available from arXiv:1603.03999, 2016.

[22] A. K. Hashagen, S. T. Flammia, D. Gross, and J. J. Wallman. Real randomized benchmarking. *Quantum*, 2:85, 2018. DOI: 10.22331/q-2018-08-22-85. Also available from arXiv:1801.06121.

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

[24] E. Jeandel, S. Perdrix, and R. Vilmart. Y-calculus: A language for real matrices derived from the ZX-calculus. In *Proceedings of the 14th International Conference on Quantum Physics and Logic*, QPL '17, pages 23–57, 2017. DOI: 10.4204/EPTCS.266.2.

[25] V. Kliuchnikov and J. Yard. A framework for exact synthesis. Preprint available from arXiv:1504.04350, April 2015.

[26] V. Kliuchnikov, D. Maslov, and M. Mosca. Fast and efficient exact synthesis of single-qubit unitaries generated by Clifford and T gates. *Quantum Information & Computation*, 13(7-8):607–630, 2013. DOI: 10.26421/QIC13.7-8. Also available from arXiv:1206.5236.

[27] V. Kliuchnikov, A. Bocharov, and K. M. Svore. Asymptotically optimal topological quantum compiling. *Physical Review Letters*, 112:140504, 2014. DOI: 10.1103/PhysRevLett.112.140504. Also available from arXiv:1310.4150.

[28] V. Kliuchnikov, D. Maslov, and M. Mosca. Practical approximation of single-qubit unitaries by single-qubit quantum Clifford and T circuits. *IEEE Transactions on Computers*, 65(1):161–172, 2016. DOI: 10.1109/TC.2015.2409842. Also available from arXiv:1212.6964.

[29] K. Matsumoto and K. Amano. Representation of quantum circuits with Clifford and $\pi/8$ gates. Preprint available from arXiv:0806.3834, June 2008.

[30] G. Meuli, M. Soeken, and G. D. Micheli. SAT-based {CNOT, T} quantum circuit synthesis. In *Proceedings of the 10th International Conference on Reversible Computation*, RC '17, pages 175–188, 2018. DOI: 10.1007/978-3-319-99498-7˙12.

[31] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge Series on Information and the Natural Sciences. Cambridge University Press, 2000. ISBN 9780521635035. DOI: 10.1017/CBO9780511976667.

[32] O. Parzanchevski and P. Sarnak. Super-Golden-Gates for PU(2). *Advances in Mathematics*, 327: 869 – 901, 2018. DOI: https://doi.org/10.1016/j.aim.2017.06.022. Special volume honoring David Kazhdan. Also available from arXiv:1704.02106.

[33] N. J. Ross. Optimal ancilla-free Clifford+V approximation of z-rotations. *Quantum Information & Computation*, 15(11–12):932–950, 2015. DOI: 10.26421/QIC15.11-12. Also available from arXiv:1409.4355.

[34] N. J. Ross and P. Selinger. Optimal ancilla-free Clifford+T approximation of z-rotations. *Quantum Information & Computation*, 16(11-12):901–953, 2016. DOI: 10.26421/QIC16.11-12. Also available from `arXiv:1403.2975`.
[35] T. Rudolph and L. Grover. A 2 rebit gate universal for quantum computing. Preprint available from `arXiv:quant-ph/0210187`, Nov. 2002.
[36] P. Selinger. Generators and relations for n-qubit Clifford operators. *Logical Methods in Computer Science*, 11(10):1–17, 2015. DOI: 10.2168/LMCS-11(2:10)2015. Also available from `arXiv:1310.6813`.
[37] Y. Shi. Both Toffoli and controlled-NOT need little help to do universal quantum computing. *Quantum Information & Computation*, 3(1):84–92, 2003. DOI: 10.26421/QIC3.1. Also available from `arXiv:quant-ph/0205115`.
[38] R. Vilmart. A ZX-calculus with triangles for Toffoli-Hadamard, Clifford+T, and beyond. In *Proceedings of the 15th International Conference on Quantum Physics and Logic*, QPL '18, pages 313–344, 2018. DOI: 10.4204/EPTCS.287.18.
[39] J. Welch, A. Bocharov, and K. M. Svore. Efficient approximation of diagonal unitaries over the Clifford+T basis. *Quantum Information & Computation*, 16(1-2):87–104, 2016. DOI: 10.26421/QIC16.1-2. Also available from `arXiv:1412.5608`.

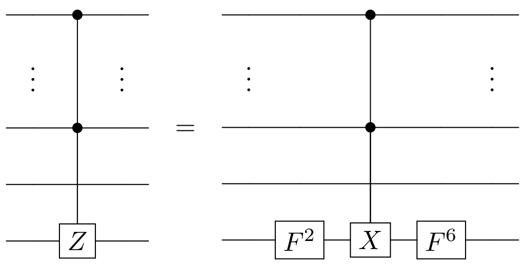
A Ancilla-Free Circuit Constructions

A.1 The $\mathbb{D}\left[i\sqrt{2}\right]$ case

In this appendix, we give ancilla-free constructions of the two-level operators XZ, $ZX = (XZ)^\dagger$, FZ, and ZF over $\{X, CX, CCX, F\}$. We progressively build up to the necessary operators.

Lemma A.1. *For any n, the n-qubit two-level X and Z gates can be represented over the gate set $\{X, CX, CCX, F\}$ with a single dirty ancilla.*

Proof. Recall that the two-level X gate is representable over $\{X, CX, CCX\}$ with a single dirty ancilla [9]. The two-level Z gate can then be constructed as follows.



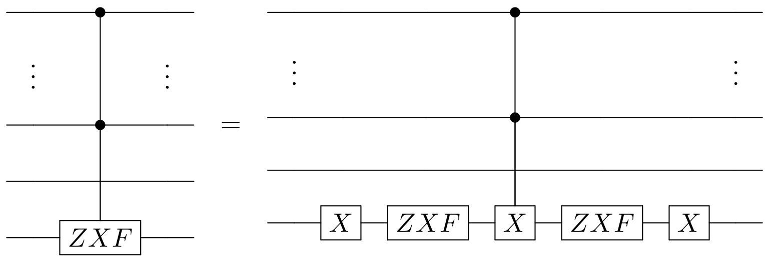
□

Lemma A.2. *For any n, the n-qubit two-level ZXF gate can be represented over $\{X, CX, CCX, F\}$ with a single dirty ancilla.*

Proof. Recall that

$$(ZXF)^2 = I$$
$$X(ZXF)X(ZXF)X = ZXF.$$

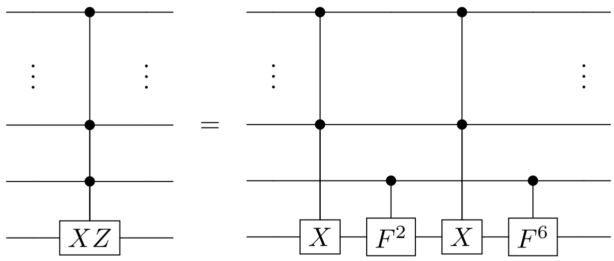
Hence it follows that the two-level ZXF gate can be implemented over $\{X, CX, CCX, F\}$ with a single dirty ancilla as follows.



∎

Proposition A.3. *For any n, the n-qubit two-level XZ gates can be represented without ancillas over $\{X, CX, CCX, F\}$.*

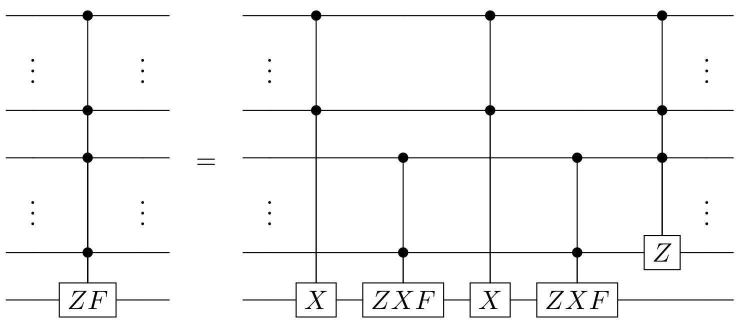
Proof. Recall that the controlled-F gate is representable with a single dirty ancilla. The two-level XZ gate is then constructible without ancillas using the following circuit.



∎

Proposition A.4. *For any n, the n-qubit two-level FZ and ZF gates can be represented without ancillas over $\{X, CX, CCX, F\}$.*

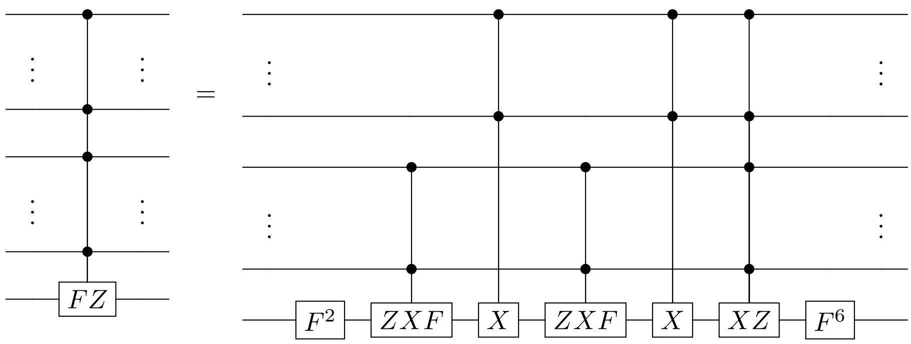
Proof. In the $n = 1$ and $n = 2$ cases, this is trivially true, as the controlled F and controlled Z are both implementable without ancillas. For $n \geq 3$, note that $XZ = -ZX$, and so $(ZXF)X(ZXF)X = X(ZXF) = -ZF$. Hence, we have the equality below.



Finally for FZ, we can note that

$$\begin{aligned} F^6(XZ)X(ZXF)X(ZXF)F^2 &= F^6(XZ)(ZXF)XF^2 \\ &= FF^6XF^2 \\ &= FZ, \end{aligned}$$

giving the following circuit identity



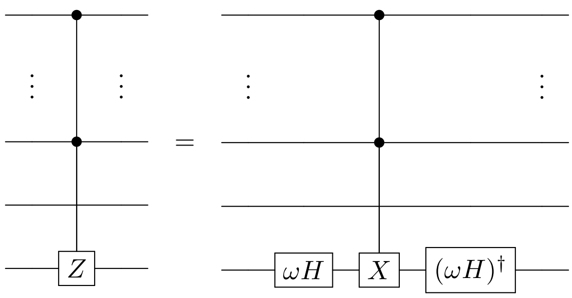
where no ancillas are needed. ☐

A.2 The $\mathbb{D}[i]$ case

In this appendix we give ancilla-free constructions of the two-level operators iX, iZ, ωSH, and ωHS over $\{X, CX, CCX, \omega H, S\}$. We progressively build up to the necessary operators.

Lemma A.5. *For any n, the n-qubit two-level X and Z gates can be represented over the gate set $\{X, CX, CCX, \omega H, S\}$ with a single dirty ancilla.*

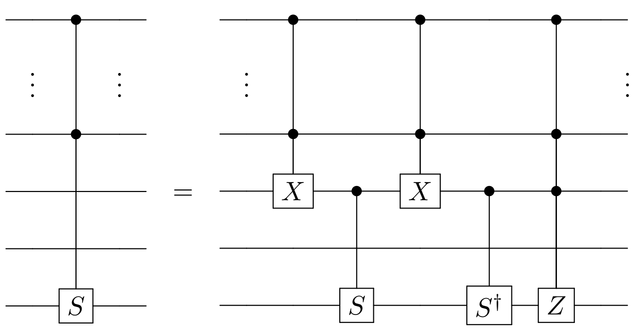
Proof. Recall that the two-level X gate is representable over $\{X, CX, CCX\}$ with a single dirty ancilla [9]. The two-level Z gate can then be constructed as follows.



☐

Lemma A.6. *For any n, the n-qubit two-level S operators can be represented over $\{X, CX, CCX, \omega H, S\}$ with two dirty ancillas.*

Proof. Observe that the two-level S operator can be constructed as follows.



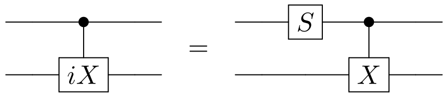
☐

Proposition A.7. *For any n, the n-qubit two-level iX operators can be represented without ancillas over $\{X, CX, CCX, \omega H, S\}$.*

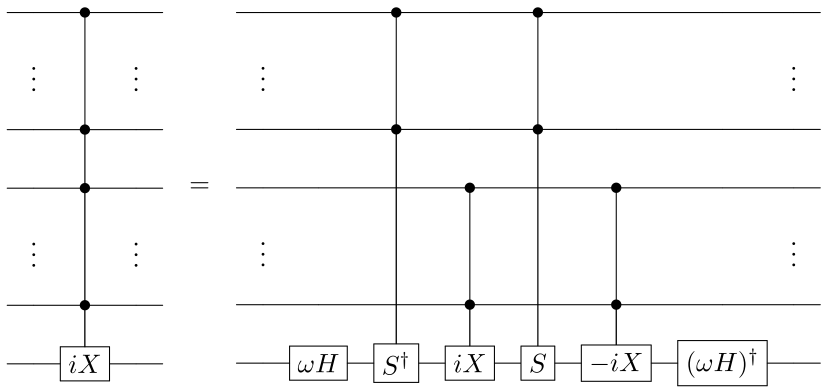
Proof. For $n = 1$, we have

$$iX = (\omega H)S^2(\omega H).$$

For $n = 2$, we have



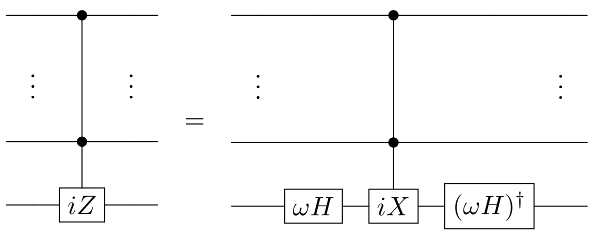
and for $n \geq 3$, we have the circuit below.



□

Proposition A.8. *For any n, the n-qubit two-level iZ operator can be represented without ancillas over $\{X, CX, CCX, \omega H, S\}$.*

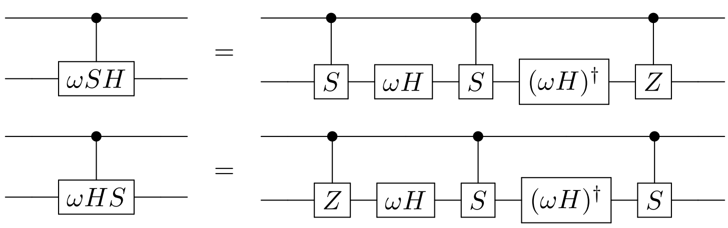
Proof. Using the n-qubit iX operator as follows.



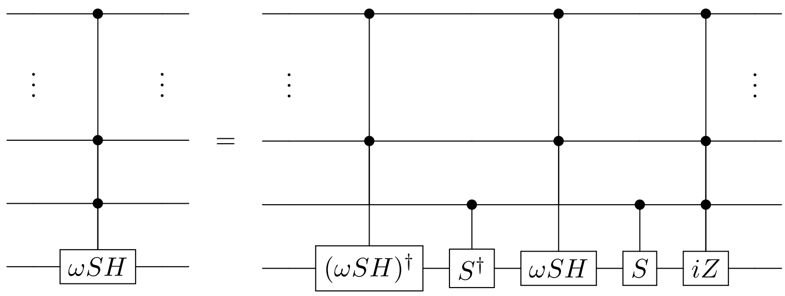
□

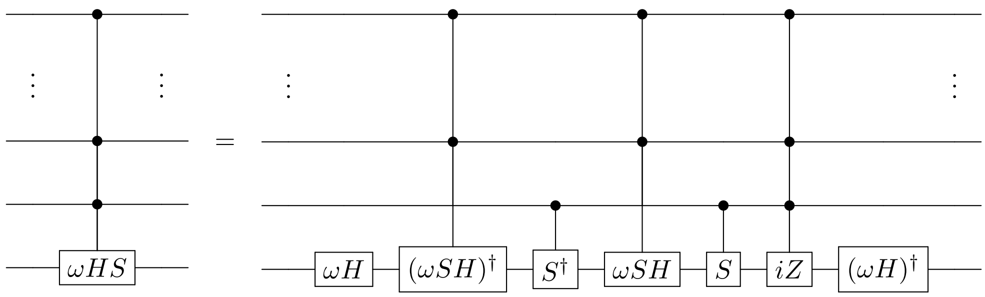
Proposition A.9. *For any $n \neq 2$, the n-qubit two-level ωSH and ωHS operators are can be represented without ancillas over $\{X, CX, CCX, \omega H, S\}$. For $n = 2$, the 2-qubit two-level ωSH and ωHS operators can be represented if CS is appended to the gate list.*

Proof. The $n = 1$ case is trivially true. For $n = 2$, if we do not use ancillas, we are left with the Clifford group generators and are unable to implement non-Clifford operators. However, appending CS to our list of operators gives us the following circuits.



Note moreover that the 2-qubit circuits can also be represented over $\{X, CX, CCX, \omega H, S\}$ with a single dirty ancilla, which we use in the identities for $n \geq 3$ below.





$\square$