# Exact synthesis of multiqubit Clifford-cyclotomic circuits

Matthew Amy* Andrew N. Glaudell† Shaun Kelso‡
William Maxwell§ Samuel S. Mendelson¶ Neil J. Ross‖

December 3, 2023

**Abstract**

Let $n \geq 8$ be an integer divisible by 4. The Clifford-cyclotomic gate set $\mathcal{G}_n$ is the universal gate set obtained by extending the Clifford gates with the $z$-rotation $T_n = \text{diag}(1, \zeta_n)$, where $\zeta_n$ is a primitive $n$-th root of unity. In this note, we show that, when $n$ is a power of 2, a multiqubit unitary matrix $U$ can be exactly represented by a circuit over $\mathcal{G}_n$ if and only if the entries of $U$ belong to the ring $\mathbb{Z}[1/2, \zeta_n]$. We moreover show that $\log(n) - 2$ ancillas are always sufficient to construct a circuit for $U$. Our results generalize prior work to an infinite family of gate sets and show that the limitations that apply to single-qubit unitaries, for which the correspondence between Clifford-cyclotomic operators and matrices over $\mathbb{Z}[1/2, \zeta_n]$ fails for all but finitely many values of $n$, can be overcome through the use of ancillas.

# 1 Introduction

## 1.1 Background

Let $n \geq 8$ be an integer divisible by 4. The **single-qubit Clifford-cyclotomic gate set of degree** $n$ was introduced in [7] and consists of the gates

$$H' = \frac{1}{2}\begin{bmatrix} 1+i & 1+i \\ 1+i & -1-i \end{bmatrix} \qquad \text{and} \qquad T_n = \begin{bmatrix} 1 & \cdot \\ \cdot & \zeta_n \end{bmatrix},$$

where $\zeta_n = e^{2\pi i/n}$ is a primitive $n$-th root of unity, $H' = \zeta_8 H$ is equal to the usual **Hadamard gate** $H$ up to a global phase of $\zeta_8$, and $T_n$ is a $z$-rotation gate of order $n$. The gate $S = T_n^{n/4}$ is the usual **phase gate** and the gate $T_8$ is simply known as the $T$ **gate**. The single-qubit Clifford-cyclotomic gate set is a universal extension of the **single-qubit Clifford gate set** $\{H', S\}$; it coincides with the well-studied **single-qubit Clifford+$T$ gate set** when $n = 8$.

The entries of $H'$ and $T_n$ lie in $\mathbb{Z}[1/2, \zeta_n]$, the smallest subring of $\mathbb{C}$ containing $1/2$ and $\zeta_n$. As a consequence, if a 2-dimensional unitary matrix $U$ can be exactly represented by a single-qubit Clifford-cyclotomic circuit of degree $n$, then the entries of $U$ belong to $\mathbb{Z}[1/2, \zeta_n]$. In their seminal 2012 paper [14], Kliuchnikov, Maslov, and Mosca proved that the converse implication holds when $n = 8$: every 2-dimensional unitary matrix with entries in $\mathbb{Z}[1/2, \zeta_8]$ can be exactly represented by a Clifford+$T$ circuit. Thus, single-qubit Clifford+$T$ operators correspond precisely to elements of $\mathrm{U}_2(\mathbb{Z}[1/2, \zeta_8])$, the group of $2 \times 2$ unitary

*Simon Fraser University. meamy@sfu.ca
†Photonic Inc. andrewglaudell@gmail.com
‡NSWC Dahlgren Division. shaun.f.kelso.civ@us.navy.mil
§NSWC Dahlgren Division and Sandia National Laboratories. wjmaxwell@sandia.gov
¶NSWC Dahlgren Division. samuel.mendelson@gmail.com
‖Dalhousie University. neil.jr.ross@dal.ca

matrices over $\mathbb{Z}[1/2, \zeta_8]$. Forest et al. later showed in [7] that such a correspondence holds when $n$ is one of 8, 12, 16, or 24, but, disappointingly, that it fails for almost all other values of $n$. Ingalls et al. put the nail in this coffin in 2019 by proving that 8, 12, 16, and 24 are in fact the only values of $n$ for which such a correspondence holds [10], as had been previously conjectured by Sarnak [18].

The **multiqubit Clifford-cyclotomic gate set of degree** $n$, which we denote $\mathcal{G}_n$, is obtained by adding the **controlled-NOT gate**

$$CX = I_2 \oplus \begin{bmatrix} \cdot & 1 \\ 1 & \cdot \end{bmatrix}$$

to the single-qubit Clifford-cyclotomic gate set of degree $n$. In other words, $\mathcal{G}_n$ is the extension of the **multiqubit Clifford gate set** $\{H', S, CX\}$ by the $z$-rotation $T_n$. For convenience, we set $\mathcal{G}_2 = \{X, CX, CCX, H \otimes H\}$ and $\mathcal{G}_4 = \{X, CX, CCX, S, H'\}$, where

$$X = \begin{bmatrix} \cdot & 1 \\ 1 & \cdot \end{bmatrix}, \qquad CCX = I_6 \oplus X, \qquad \text{and} \qquad H \otimes H = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}.$$

The gates $X$ and $CCX$ are the usual **NOT gate** and **doubly-controlled-NOT gate** (or **Toffoli gate**), respectively.

In [8], Giles and Selinger extended Kliuchnikov, Maslov, and Mosca's 2012 result to the multiqubit setting by proving that a unitary matrix $U$ of dimension $2^m$ can be represented by an $m$-qubit circuit over $\mathcal{G}_8$ if and only if the entries of $U$ lie in the ring $\mathbb{Z}[1/2, \zeta_8]$. In [4], some of the present authors showed how to adapt the methods of Giles and Selinger to a handful of other gate sets, including $\mathcal{G}_2$ and $\mathcal{G}_4$. In the multiqubit context, circuits can use ancillary qubits, provided that they are initialized and terminated in the computational basis state $|0\rangle$. It was shown in [4] and [8] that a single ancilla is always sufficient to construct the desired circuits.

Clifford-cyclotomic circuits, and in particular those of degree $2^k$ for some positive integer $k$, are ubiquitous in quantum computation; they appear in Shor's factoring algorithm [19], the study of the Clifford hierarchy [9], and protocols for state distillation [6].

### 1.2 Contributions

Let $k$ and $m$ be positive integers. In the present note, we show that a $2^m$-dimensional unitary matrix $U$ can be exactly represented by an $m$-qubit Clifford-cyclotomic circuit of degree $2^k$ if and only if the entries of $U$ lie in the ring $\mathbb{Z}[1/2, \zeta_{2^k}]$. To construct a circuit for $U$, a single ancilla suffices, when $k \leq 2$, and $k - 2$ ancillas suffice, when $k > 2$.

Our results extend those of [4] and [8] to an infinite family of multiqubit gate sets, but our proof is surprisingly simple. It relies on the fact that the root of unity $\zeta_{2^k}$ can be represented by a 2-dimensional unitary matrix over $\mathbb{Z}[1/2, \zeta_{2^{k-1}}]$, and that this representation can be used to define a well-behaved function $\phi_k : \mathrm{U}(\mathbb{Z}[1/2, \zeta_{2^k}]) \to \mathrm{U}(\mathbb{Z}[1/2, \zeta_{2^{k-1}}])$ mapping unitary matrices over $\mathbb{Z}[1/2, \zeta_{2^k}]$ to unitary matrices over $\mathbb{Z}[1/2, \zeta_{2^{k-1}}]$. The function $\phi_k$ generalizes the standard real representation of complex numbers which was used by Aharonov in [1] to prove the universality of the Toffoli-Hadamard gate set and is an example of a **catalytic embedding** [2]. One can think of our results as circumventing the no-go theorems of [7] and [10] through the use of ancillas: there are elements of $\mathrm{U}_2(\mathbb{Z}[1/2, \zeta_{2^k}])$ that cannot be represented by an ancilla-free single-qubit circuit over $\mathcal{G}_{2^k}$, but every such element becomes representable if sufficiently many additional qubits are available.

### 1.3 Contents

The note is organized as follows. In Section 2, we briefly review some important properties of the ring $\mathbb{Z}[1/2, \zeta_{2^k}]$. We introduce catalytic embeddings in Section 3 and define the catalytic embedding $\phi_k$. Section 4 contains the proof of our main result. We discuss future work in Section 5.

## 2 Cyclotomic integers

We start by briefly discussing the rings of **cyclotomic integers** that will be of interest in the rest of the note. For further details, the reader is encouraged to consult [20].

Let $k$ be a positive integer. The ring $\mathbb{Z}[\zeta_{2^k}]$ is the smallest subring of $\mathbb{C}$ containing $\zeta_{2^k}$. Hence, $\mathbb{Z}[\zeta_{2^1}] = \mathbb{Z}$. Moreover, when $k > 1$, we have $\zeta_{2^k}^2 = \zeta_{2^{k-1}}$ and therefore $\mathbb{Z}[\zeta_{2^{k-1}}] \subseteq \mathbb{Z}[\zeta_{2^k}]$. It will be useful for our purposes to further note that, for $k > 1$,

$$\mathbb{Z}[\zeta_{2^k}] = \{a + b\zeta_{2^k} \mid a, b \in \mathbb{Z}[\zeta_{2^{k-1}}]\}. \tag{1}$$

The linear combinations in Equation (1) are unique. That is, every element of $\mathbb{Z}[\zeta_{2^k}]$ can be uniquely written as $a + b\zeta_{2^k}$, for some $a, b \in \mathbb{Z}[\zeta_{2^{k-1}}]$.

We will be interested in an extension of $\mathbb{Z}[\zeta_{2^k}]$ obtained by localizing $\mathbb{Z}[\zeta_{2^k}]$ at 2, i.e., by adding denominators that are powers of 2. The resulting ring is

$$\mathbb{Z}[1/2, \zeta_{2^k}] = \{a/2^\ell \mid a \in \mathbb{Z}[\zeta_{2^k}], \ell \in \mathbb{Z}\}. \tag{2}$$

For brevity, and in keeping with prior work (see, e.g., [4, 8]), we denote $\mathbb{Z}[1/2, \zeta_{2^k}]$ by $\mathbb{D}[\zeta_{2^k}]$ in what follows. This notation emphasizes the fact that $\mathbb{Z}[1/2, \zeta_{2^k}]$ can be seen as the extension by $\zeta_{2^k}$ of the ring $\mathbb{D} = \{a/2^\ell \mid a \in \mathbb{Z}, \ell \in \mathbb{Z}\}$ of **dyadic rationals**.

**Lemma 2.1.** *Let $k \geq 2$. Every element of $\mathbb{D}[\zeta_{2^k}]$ can be uniquely written as $a + b\zeta_{2^k}$ for some $a, b \in \mathbb{D}[\zeta_{2^{k-1}}]$.*

*Proof.* Equations (1) and (2) jointly imply that every element of $\mathbb{D}[\zeta_{2^k}]$ can be written as $a + b\zeta_{2^k}$ for some $a, b \in \mathbb{D}[\zeta_{2^{k-1}}]$. To see that this expression is unique, let $a, b, a', b' \in \mathbb{D}[\zeta_{2^{k-1}}]$ and suppose that $a + b\zeta_{2^k} = a' + b'\zeta_{2^k}$. By choosing $\ell$ large enough, $2^\ell(a + b\zeta_{2^k}) = 2^\ell(a' + b'\zeta_{2^k})$ becomes an equation over $\mathbb{Z}[\zeta_{2^k}]$, from which we get $a = a'$ and $b = b'$. □

## 3 Catalytic embeddings

We now define **catalytic embeddings**. The definition introduced below is a special case of the more general notion of catalytic embedding used in [2], but it suffices for our purposes.

Let $\mathcal{U}$ and $\mathcal{V}$ be collections of unitaries. An **$\ell$-dimensional catalytic embedding** of $\mathcal{U}$ into $\mathcal{V}$ is a pair $(\phi, |\lambda\rangle)$ consisting of a function $\phi : \mathcal{U} \to \mathcal{V}$ and a quantum state $|\lambda\rangle \in \mathbb{C}^\ell$ such that if $U \in \mathcal{U}$ has dimension $n$ then $\phi(U) \in \mathcal{V}$ has dimension $n\ell$, and

$$\phi(U)(|u\rangle \otimes |\lambda\rangle) = (U|u\rangle) \otimes |\lambda\rangle \tag{3}$$

for every $|u\rangle \in \mathbb{C}^n$. We refer to the state $|\lambda\rangle$ as the **catalyst** and to Equation (3) as the **catalytic condition**. We sometimes write $(\phi, |\lambda\rangle) : \mathcal{U} \to \mathcal{V}$ to indicate that $(\phi, |\lambda\rangle)$ is a catalytic embedding of $\mathcal{U}$ into $\mathcal{V}$. If $(\phi, |\lambda\rangle) : \mathcal{U} \to \mathcal{V}$ and $(\psi, |\omega\rangle) : \mathcal{V} \to \mathcal{W}$ are catalytic embeddings, then $(\psi \circ \phi, |\lambda\rangle \otimes |\omega\rangle)$ is a catalytic embedding of $\mathcal{U}$ into $\mathcal{W}$, since

$$\psi(\phi(U))(|u\rangle \otimes |\lambda\rangle \otimes |\omega\rangle) = (\phi(U)(|u\rangle \otimes |\lambda\rangle)) \otimes |\omega\rangle = (U|u\rangle) \otimes |\lambda\rangle \otimes |\omega\rangle.$$

We refer to this catalytic embedding as the **concatenation** of $(\phi, |\lambda\rangle)$ and $(\psi, |\omega\rangle)$. The concatenation of catalytic embeddings is associative and $(I_{\mathcal{U}}, [1]) : \mathcal{U} \to \mathcal{U}$ acts as the identity for concatenation.

Now let $\mathrm{U}(\mathbb{D}[\zeta_{2^k}])$ denote the collection of all unitary matrices over $\mathbb{D}[\zeta_{2^k}]$. The rest of this section is dedicated to constructing, for every $k \geq 2$, a 2-dimensional catalytic embedding $\mathrm{U}(\mathbb{D}[\zeta_{2^k}]) \to \mathrm{U}(\mathbb{D}[\zeta_{2^{k-1}}])$. To this end, we define the state $|\lambda_k\rangle$ and the matrix $\Lambda_k$ as

$$|\lambda_k\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ \zeta_{2^k} \end{bmatrix} \quad \text{and} \quad \Lambda_k = \begin{bmatrix} 0 & 1 \\ \zeta_{2^{k-1}} & 0 \end{bmatrix},$$

respectively. Note that $\Lambda_k$ is a unitary matrix and $|\lambda_k\rangle$ is an eigenvector of $\Lambda_k$ for eigenvalue $\zeta_{2^k}$. To verify the latter claim, we compute:

$$\Lambda_k |\lambda_k\rangle = \begin{bmatrix} 0 & 1 \\ \zeta_{2^{k-1}} & 0 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ \zeta_{2^k} \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} \zeta_{2^k} \\ \zeta_{2^{k-1}} \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} \zeta_{2^k} \\ \zeta_{2^k}^2 \end{bmatrix} = \zeta_{2^k} |\lambda_k\rangle . \tag{4}$$

Note further that $\zeta_{2^k}^\dagger = \zeta_{2^{k-1}}^\dagger \zeta_{2^k}$ and that $\Lambda_k^\dagger = \zeta_{2^{k-1}}^\dagger \Lambda_k$. In order to define the desired catalytic embedding, we start by showing that the matrix $\Lambda_k$ can be used to define a function $\mathrm{U}(\mathbb{D}[\zeta_{2^k}]) \to \mathrm{U}(\mathbb{D}[\zeta_{2^{k-1}}])$.

**Lemma 3.1.** *Let $k \geq 2$, let $A$ and $B$ be matrices over $\mathbb{D}[\zeta_{2^{k-1}}]$, and assume that $A + B\zeta_{2^k} \in \mathrm{U}(\mathbb{D}[\zeta_{2^k}])$. Then $A \otimes I + B \otimes \Lambda_k \in \mathrm{U}(\mathbb{D}[\zeta_{2^{k-1}}])$.*

*Proof.* Let $k$, $A$, and $B$ be as stated. Since $A + B\zeta_{2^k}$ is unitary and $\zeta_{2^k}^\dagger = \zeta_{2^{k-1}}^\dagger \zeta_{2^k}$, we have

$$I = (A + B\zeta_{2^k})^\dagger (A + B\zeta_{2^k}) = A^\dagger A + A^\dagger B \zeta_{2^k} + B^\dagger A \zeta_{2^k}^\dagger + B^\dagger B = (A^\dagger A + B^\dagger B) + (A^\dagger B + B^\dagger A \zeta_{2^{k-1}}^\dagger)\zeta_{2^k}.$$

This implies that $A^\dagger A + B^\dagger B = I$ and that $A^\dagger B + B^\dagger A \zeta_{2^{k-1}}^\dagger = 0$. Now consider $A \otimes I + B \otimes \Lambda_k$. Since $\Lambda_k$ is unitary and $\Lambda_k^\dagger = \zeta_{2^{k-1}}^\dagger \Lambda_k$ , we have

$$\begin{aligned} (A \otimes I + B \otimes \Lambda_k)^\dagger (A \otimes I + B \otimes \Lambda_k) &= A^\dagger A \otimes I + A^\dagger B \otimes \Lambda_k + B^\dagger A \otimes \Lambda_k^\dagger + B^\dagger B \otimes I \\ &= (A^\dagger A + B^\dagger B) \otimes I + (A^\dagger B + B^\dagger A \zeta_{2^{k-1}}^\dagger) \otimes \Lambda_k \\ &= I. \end{aligned}$$

By reasoning analogously, one can also show that $(A \otimes I + B \otimes \Lambda_k)(A \otimes I + B \otimes \Lambda_k)^\dagger = I$, which proves that $A \otimes I + B \otimes \Lambda_k$ is indeed unitary. □

**Proposition 3.2.** *Let $k \geq 2$ and let $\phi_k : \mathrm{U}(\mathbb{D}[\zeta_{2^k}]) \to \mathrm{U}(\mathbb{D}[\zeta_{2^{k-1}}])$ be the function defined by*

$$\phi_k : A + B\zeta_{2^k} \mapsto A \otimes I + B \otimes \Lambda_k.$$

*Then the pair $(\phi_k, |\lambda_k\rangle)$ is a 2-dimensional catalytic embedding of $\mathrm{U}(\mathbb{D}[\zeta_{2^k}])$ into $\mathrm{U}(\mathbb{D}[\zeta_{2^{k-1}}])$.*

*Proof.* Every element $U$ of $\mathrm{U}(\mathbb{D}[\zeta_{2^k}])$ can be uniquely written $U = A + \zeta_{2^k} B$, where $A$ and $B$ are matrices over $\mathbb{D}[\zeta_{2^{k-1}}]$. Hence, Lemma 3.1 implies that $\phi_k : \mathrm{U}(\mathbb{D}[\zeta_{2^k}]) \to \mathrm{U}(\mathbb{D}[\zeta_{2^{k-1}}])$ is indeed a function. Moreover, by construction, $\phi_k(U) \in \mathrm{U}(\mathbb{D}[\zeta_{2^{k-1}}])$ has dimension $2n$, if $U \in \mathrm{U}(\mathbb{D}[\zeta_{2^k}])$ has dimension $n$. Now let $|u\rangle \in \mathbb{C}^n$. Then

$$\begin{aligned} \phi_k(U)(|u\rangle \otimes |\lambda_k\rangle) &= (A \otimes I + B \otimes \Lambda_k)(|u\rangle \otimes |\lambda_k\rangle) \\ &= (A \otimes I)(|u\rangle \otimes |\lambda_k\rangle) + (B \otimes \Lambda_k)(|u\rangle \otimes |\lambda_k\rangle) \\ &= A|u\rangle \otimes I|\lambda_k\rangle + B|u\rangle \otimes \Lambda_k |\lambda_k\rangle \\ &= A|u\rangle \otimes |\lambda_k\rangle + B|u\rangle \otimes \zeta_{2^k} |\lambda_k\rangle \\ &= A|u\rangle \otimes |\lambda_k\rangle + B\zeta_{2^k} |u\rangle \otimes |\lambda_k\rangle \\ &= (A|u\rangle + B\zeta_{2^k}|u\rangle) \otimes |\lambda_k\rangle \\ &= (U|u\rangle) \otimes |\lambda_k\rangle . \end{aligned}$$

Hence, $(\phi_k, |\lambda_k\rangle)$ is a 2-dimensional catalytic embedding of $\mathrm{U}(\mathbb{D}[\zeta_{2^k}])$ into $\mathrm{U}(\mathbb{D}[\zeta_{2^{k-1}}])$. □

*Remark* 3.3. The catalytic embedding of Proposition 3.2 is an example of what is called a **standard catalytic embedding** in [2]. At the heart of this construction lies the fact that $\zeta_{2^k}$ can be represented by the matrix $\Lambda_k$, whose characteristic polynomial is also the minimal polynomial of $\zeta_k$ over $\mathbb{Q}[\zeta_{2^{k-1}}]$. A more general description of this construction can be found in [2].

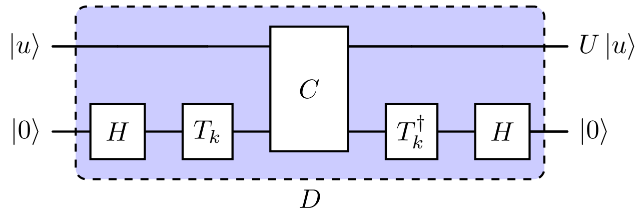


Figure 1: The circuit constructed in the proof of Theorem 4.1.

# 4 Exact synthesis

We now prove our main result. While it is clear that if a unitary $U$ can be represented by a circuit over $\mathcal{G}_{2^k}$ then it is an element of $\mathrm{U}(\mathbb{D}[\zeta_{2^k}])$, the challenge is to show that the converse implication is also true. The main idea behind the proof is to use Proposition 3.2 to inductively reduce the problem for $\mathrm{U}(\mathbb{D}[\zeta_{2^k}])$ to the problem for $\mathrm{U}(\mathbb{D}[\zeta_{2^{k-1}}])$, and so on until one reaches a case for which the result is known, such as $\mathrm{U}(\mathbb{D}[\zeta_{2^3}])$, $\mathrm{U}(\mathbb{D}[\zeta_{2^2}])$, or $\mathrm{U}(\mathbb{D}[\zeta_{2^1}])$. We formalize this intuition in the proposition below.

**Theorem 4.1.** *Let $k$ and $m$ be positive integers. A $2^m \times 2^m$ unitary matrix $U$ can be exactly represented by an $m$-qubit circuit over $\mathcal{G}_{2^k}$ if and only if $U \in \mathrm{U}_{2^m}(\mathbb{D}[\zeta_{2^k}])$. Moreover, to construct a circuit for $U$, a single ancilla suffices, when $k \leq 2$, and $k-2$ ancillas suffice, when $k > 2$.*

*Proof.* The left-to-right direction is an immediate consequence of the fact that the elements of $\mathcal{G}_{2^k}$ have entries in $\mathbb{D}[\zeta_{2^k}]$. For the right-to-left direction, we proceed by induction on $k$. The cases of $k = 1, 2, 3$ follow from [4, Corollary 5.6], [4, Corollary 5.27], and [8, Theorem 1], respectively. Now suppose that $k > 3$, let $U \in \mathrm{U}_{2^m}(\mathbb{D}[\zeta_{2^k}])$, and let $(\phi_k, |\lambda_k\rangle) : \mathrm{U}(\mathbb{D}[\zeta_{2^k}]) \to \mathrm{U}(\mathbb{D}[\zeta_{2^{k-1}}])$ be the catalytic embedding of Proposition 3.2. Then

$$\phi_k(U) \in \mathrm{U}_{2^{m+1}}(\mathbb{D}[\zeta_{2^{k-1}}]).$$

Thus, by the induction hypothesis, there exists an $(m+1)$-qubit circuit $C$ for $\phi_k(U)$ over $\mathcal{G}_{2^{k-1}}$ that uses no more than $k-3$ ancillas. For every state $|u\rangle$, we then have

$$C(|u\rangle \otimes |\lambda_k\rangle) = \phi_k(U)(|u\rangle \otimes |\lambda_k\rangle) = (U|u\rangle) \otimes |\lambda_k\rangle\,. \tag{5}$$

Now let $D$ be the circuit defined by $D = (I \otimes (T_{2^k} H))^\dagger \circ C \circ (I \otimes (T_{2^k} H))$. This is a circuit over $\mathcal{G}_{2^k}$, since $H$ can be expressed as

$$H = H' S^2 H' T_{2^k}^{2^{k-3}} H' S^2 H' T_{2^k}^{2^{k-3}} H'$$

when $k \geq 3$. By Equation (5), and since $|\lambda_k\rangle = T_{2^k} H |0\rangle$, we then have

$$\begin{aligned} D(|u\rangle \otimes |0\rangle) &= (I \otimes (T_{2^k} H))^\dagger \circ C \circ (I \otimes (T_{2^k} H))(|u\rangle \otimes |0\rangle) \\ &= (I \otimes (T_{2^k} H))^\dagger \circ C(|u\rangle \otimes |\lambda_k\rangle) \\ &= (I \otimes (T_{2^k} H))^\dagger((U|u\rangle) \otimes |\lambda_k\rangle) \\ &= (U|u\rangle) \otimes |0\rangle\,. \end{aligned}$$

That is, $D$ represents $U$ exactly and uses no more than $k-2$ ancillas, which completes the proof. □

The circuit constructed in the inductive step of Theorem 4.1 is depicted in Figure 1. The ancillary qubits used by $C$ are not represented in Figure 1 (just as they are kept implicit in the proof of the theorem).

The construction of Theorem 4.1 can be used to give an alternative proof of [4, Corollary 5.27] and [8, Theorem 1], albeit one that uses more ancillas than is necessary. In the proof of Theorem 4.1, the cases of $k = 1$, $k = 2$, and $k = 3$ are all treated as base cases. Instead, one could use only the case of $k = 1$ as the base case and establish the cases of $k = 2$ and $k = 3$ inductively. The resulting circuit would then use $k$ ancillas to represent an element of $\mathrm{U}(\mathbb{D}[\zeta_{2^k}])$ for all $k$, rather than $k-2$ ancillas when $k > 2$, as in the current proof.

## 5 Conclusion

We showed that a unitary matrix can be represented by a Clifford-cyclotomic circuit of degree $2^k$ if and only if its entries belong to the ring $\mathbb{D}[\zeta_{2^k}]$. We also showed that $k-2$ ancillas are always sufficient for this purpose.

Several questions arise from this work. Firstly, can the proof Theorem 4.1 be modified so as to produce smaller circuits? The size of the circuits produced by Theorem 4.1 depends on the exact synthesis algorithm applied in the base case, but the produced circuits remain large, even if improved synthesis methods such as [3, 12, 15, 17] are used. Indeed, representing an element of $\mathrm{U}_{2^m}(\mathbb{D}[\zeta_{2^k}])$ using the algorithm of [12] in the base case of Theorem 4.1 currently yields a circuit containing $O(4^{m+k}(m+k))$ gates and using $k-2$ ancillas. Lowering this cost is an important avenue for future work. Secondly, can Theorem 4.1 be generalized to Clifford-cyclotomic gate sets of degree $n \neq 2^k$ or can such an extension be shown to be impossible? Preliminary research indicates that arbitrary roots of unity can be represented using circuits over $\{X, CX, CCX, H \otimes H\}$ in the presence of appropriate catalysts, but the construction is more intricate than the one presented here. Finally, and further afield, can Theorem 4.1 be used to develop algorithms for the approximation of unitaries using Clifford-cyclotomic circuits, following prior work such as [5, Appendix A], [13], or [16]?

## Acknowledgements

The authors would like to thank Vadym Kliuchnikov, Kira Scheibelhut, and Peter Selinger for insightful comments on an earlier version of this note. The circuit diagram in this note was typeset using Quantikz [11]. MA acknowledges support from the Canada Research Chairs program. MA and NJR acknowledge support from the Natural Sciences and Engineering Research Council of Canada (NSERC). SK gratefully acknowledges support from ONR, whose sponsorship and continuing guidance of the ILIR program has made this research possible. These efforts were funded under ONR award N0001423WX00070. SK, SSM, and WM were supported in part by Naval Innovative Science and Engineering funding. WM acknowledges support from the U.S. Department of Energy, Office of Science, National Quantum Information Science Research Centers, Quantum Systems Accelerator.

## References

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

[2] M. Amy, M. Crawford, A. N. Glaudell, M. L. Macasieb, S. S. Mendelson, and N. J. Ross. Catalytic embeddings of quantum circuits. Preprint. Available from arXiv:2305.07720, 2023.

[3] M. Amy, A. N. Glaudell, S. M. Li, and N. J. Ross. Improved synthesis of Toffoli-Hadamard circuits. In *Reversible Computation: 15th International Conference, RC 2023, Proceedings*, pages 169–209, 2023. Available from arXiv:2305.11305.

[4] M. Amy, A. N. Glaudell, and N. J. Ross. Number-theoretic characterizations of some restricted Clifford+$T$ circuits. *Quantum*, 4:252, 2020. Available from arXiv:1908.06076.

[5] M. Beverland, E. T. Campbell, M. Howard, and V. Kliuchnikov. Lower bounds on the non-Clifford resources for quantum computations. *Quantum Science & Technology*, 5, 2019. Available from arXiv:1904.01124.

[6] G. Duclos-Cianci and D. Poulin. Reducing the quantum-computing overhead with complex gate distillation. *Physical Review A*, 91(4):042315, 2015. Available from arXiv:1403.5280.

[7] 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. Available from arXiv:1501.04944.

[8] B. Giles and P. Selinger. Exact synthesis of multiqubit Clifford+$T$ circuits. *Physical Review A*, 87(3):032332, 2013. Available from arXiv:1212.0506.

[9] D. Gottesman and I. L. Chuang. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature*, 402(6760):390–393, 1999. Available from https://doi.org/10.1038/46503.

[10] C. Ingalls, B. W. Jordan, A. Keeton, A. Logan, and Y. Zaytman. The Clifford-cyclotomic group and Euler–Poincaré characteristics. *Canadian Mathematical Bulletin*, 64(3):651–666, 2021. Available from arXiv:1903.09497.

[11] A. Kay. Tutorial on the Quantikz package. Preprint. Available from arXiv:1809.03842, 2018.

[12] V. Kliuchnikov. Synthesis of unitaries with Clifford+$T$ circuits. Preprint. Available from arXiv:1306.3200, 2013.

[13] V. Kliuchnikov, K. Lauter, R. Minko, A. Paetznick, and C. Petit. Shorter quantum circuits. Preprint. Available from arXiv:2203.10064, 2022.

[14] 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. Available from arXiv:1206.5236.

[15] P. Niemann, R. Wille, and R. Drechsler. Improved synthesis of Clifford+$T$ quantum functionality. In *2018 Design, Automation & Test in Europe Conference & Exhibition, DATE 2018, Proceedings*, pages 597–600, 2018.

[16] N. J. Ross and P. Selinger. Optimal ancilla-free Clifford+$T$ approximation of $z$-rotations. *Quantum Information & Computation*, 16(11–12):901–953, 2016. Available from arXiv:1403.2975.

[17] T. Russell. The exact synthesis of 1- and 2-qubit Clifford+$T$ circuits. Preprint. Available from arXiv:14086202, 2014.

[18] P. Sarnak. Letter to Scott Aaronson and Andy Pollington on the Solavay-Kitaev theorem. Available from https://publications.ias.edu/sarnak/paper/2637, 2015.

[19] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997. Available from arXiv:quant-ph/9508027.

[20] L. C. Washington. *Introduction to Cyclotomic Fields*. Springer New York, NY, 1982.