Exact Synthesis of Multiqutrit Clifford-Cyclotomic Circuits

Andrew N. Glaudell
Photonic Inc.
andrewglaudell@gmail.com

Neil J. Ross
Dalhousie University
neil.jr.ross@dal.ca

John van de Wetering
University of Amsterdam
john@vdwetering.name

Lia Yeh
University of Oxford
lia.yeh@cs.ox.ac.uk

It is known that the matrices that can be exactly represented by a multiqubit circuit over the Toffoli+Hadamard, Clifford+T, or, more generally, Clifford-cyclotomic gate set are precisely the unitary matrices with entries in the ring $\mathbb{Z}[1/2,\zeta_k]$, where k is a positive integer that depends on the gate set and ζ_k is a primitive 2^k-th root of unity. In the present paper, we establish an analogous correspondence for qutrits. We define the multiqutrit Clifford-cyclotomic gate set of degree 3^k by extending the classical qutrit gates X, CX, and CCX with the Hadamard gate H and the T_k gate $T_k = \mathrm{diag}(1,\omega_k,\omega_k^2)$, where ω_k is a primitive 3^k-th root of unity. This gate set is equivalent to the qutrit Toffoli+Hadamard gate set when $k = 1$, and to the qutrit Clifford+T_k gate set when $k > 1$. We then prove that a $3^n \times 3^n$ unitary matrix U can be represented by an n-qutrit circuit over the Clifford-cyclotomic gate set of degree 3^k if and only if the entries of U lie in the ring $\mathbb{Z}[1/3,\omega_k]$.

1 Introduction

1.1 Background

In quantum computing, **synthesis** refers to the process of converting a representation of a unitary into a quantum circuit. In **exact synthesis** the unitary is typically given as a matrix, and the goal is to produce a circuit that implements the matrix exactly. This is in contrast to **approximate synthesis**, where the circuit is only required to implement the given matrix up to some prescribed error budget.

A solution to an exact synthesis problem for a gate set $\mathscr{G}$ sometimes characterizes the unitary matrices that can be exactly represented by a circuit over $\mathscr{G}$. For instance, the matrices with entries in the ring $\mathbb{Z}[1/2]$ of dyadic rationals corresponds precisely to the unitary matrices that can be represented using the Toffoli gate and the tensor product $H \otimes H$ of the Hadamard gate with itself [4]. Similarly, Clifford+T circuits correspond to unitary matrices with entries in $\mathbb{Z}[1/2, e^{2\pi i/8}]$ [12]. More generally, it was recently shown that multiqubit circuits over the Clifford-cyclotomic gate set of degree k, which extends the Clifford gate set with a z-rotation by angle $2\pi/2^k$, correspond to unitary matrices with entries the ring $\mathbb{Z}[1/2, e^{2\pi i/2^k}]$ [2].

In this paper, we consider the exact synthesis problem for qutrits. Like for qubits, fault-tolerant universal quantum computation has been theoretically devised for qutrits through magic state distillation [5, 9, 24] or gauge fixing of colour codes [30]. In recent years, qudit operations have been demonstrated on many experimental platforms [17, 20, 31, 33], with error rates competitive to qubit operations [26, 10]. Qutrit exact synthesis problems, however, have received less attention than their qubit counterparts and only a few results exist: a normal form for single-qutrit Clifford+T unitaries [13, 25], a proof that all classically reversible functions on trits can be implemented using Clifford+T circuits [32], and an exact synthesis result for single-qutrit Clifford+R unitaries [19].

Submitted to:
QPL 2024

Let k be a positive integer and let $\omega_k \in \mathbb{C}$ be the **primitive 3^k-th root of unity** $\omega_k = e^{2\pi i/3^k}$. For simplicity, we write ω for ω_1. The single-qutrit **Pauli** X gate, **Pauli** Z gate, **phase** gate S, and **Hadamard** gate H are defined below.

$$X = \begin{bmatrix} \cdot & \cdot & 1 \\ 1 & \cdot & \cdot \\ \cdot & 1 & \cdot \end{bmatrix} \qquad Z = \begin{bmatrix} 1 & \cdot & \cdot \\ \cdot & \omega & \cdot \\ \cdot & \cdot & \omega^2 \end{bmatrix} \qquad S = \begin{bmatrix} 1 & \cdot & \cdot \\ \cdot & 1 & \cdot \\ \cdot & \cdot & \omega \end{bmatrix} \qquad H = \frac{-\omega^2}{\sqrt{-3}} \begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{bmatrix}$$

The two-qutrit **controlled-X** gate CX is the permutation matrix whose action on the computational basis is defined by $|i\rangle |j\rangle \mapsto |i\rangle |i+j\rangle$, with addition performed modulo 3. The three-qutrit **doubly-controlled-X** gate CCX (or **Toffoli** gate) is similarly defined by $|i\rangle |j\rangle |k\rangle \mapsto |i\rangle |j\rangle |k+ij\rangle$. The gate set $\{H,S,CX\}$ is the **Clifford** gate set. Now define the single-qutrit T_k gate

$$T_k = \begin{bmatrix} 1 & \cdot & \cdot \\ \cdot & \omega_k & \cdot \\ \cdot & \cdot & \omega_k^2 \end{bmatrix}.$$

When $k=2$, T_k is the qutrit T gate [16].

The **Clifford-cyclotomic gate set of degree** 3^k is the gate set $\mathscr{G}_k = \{X, CX, CCX, H, T_k\}$. When $k=1$, we have $T_1 = Z = HXH^\dagger$, so that the Clifford-cyclotomic gate set of degree 3 is equivalent to the qutrit **Toffoli+Hadamard** gate set [27]. As we will show below, when $k \geq 2$, the gate set $\mathscr{G}_k$ is equivalent (up to a single ancillary qutrit) to the **Clifford+T_k** gate set $\{H,S,CX,T_k\}$. In particular, the Clifford-cyclotomic gate set of degree 9 is equivalent to the well-known qutrit **Clifford+T** gate set [13, 14, 25, 32]. Because $T_{k+1}^3 = T_k$, the Clifford-cyclotomic gate sets form a hierarchy of universal gate sets whose first level is given by the Toffoli+Hadamard gate set, whose second level is given by the Clifford+T gate set, and whose subsequent levels are given by finer and finer extensions of the Clifford gate set.

Now consider the ring $\mathbb{Z}[1/3, \omega_k]$, which can be defined as the smallest unital subring of $\mathbb{C}$ containing $1/3$ and ω_k. Since $-\omega^2/\sqrt{-3} = \omega^2(1-\omega)/3$, the entries of X, CX, CCX, H, and T_k lie in $\mathbb{Z}[1/3, \omega_k]$. Hence, any n-qutrit circuit over $\mathscr{G}_k$ must represent a unitary matrix with entries in $\mathbb{Z}[1/3, \omega_k]$. The purpose of this paper is to show that the converse implication is also true.

1.2 Contributions

We show that a $3^n \times 3^n$ unitary matrix U can be exactly represented by an n-qutrit circuit over the Clifford-cyclotomic gate set of degree 3^k if and only if the entries of U belong to the ring $\mathbb{Z}[1/3, \omega_k]$. Furthermore, we show that no more than $k+1$ ancillae are required for this purpose.

We therefore solve the exact synthesis problem for multiqutrit Toffoli+Hadamard circuits, multiqutrit Clifford+T circuits, and, more generally, multiqutrit Clifford-cyclotomic circuits. To the best of our knowledge, this is the first time that a multiqudit exact synthesis result is established for any prime $d > 2$.

A similar hierarchy of Clifford-cyclotomic gate sets exists for qubits, and the correspondence between Clifford-cyclotomic circuits and matrices with entries in rings of algebraic integers also holds in that case [2]. Following [2], we prove our result inductively. We first show that circuits over $\mathscr{G}_1$ correspond to unitary matrices over $\mathbb{Z}[1/3, \omega]$ by reasoning as in [4, 12, 15]. This serves as the base case of our induction. Then, we use properties of the ring extension $\mathbb{Z}[1/3, \omega_k] \subseteq \mathbb{Z}[1/3, \omega_{k+1}]$ and the theory of catalytic embeddings [1] to establish the inductive step.

1.3 Contents

The paper is organized as follows. We discuss the necessary number-theoretic prerequisites in Section 2. In Section 3, we introduce a convenient generating set for the group $\mathrm{U}_n(\mathbb{Z}[1/3,\omega])$ of n-dimensional unitary matrices with entries in the ring $\mathbb{Z}[1/3,\omega]$, and in Section 4 we show that the elements of this generating set can be represented by Clifford-cyclotomic circuits of degree 3 (explicit circuit decompositions are given in Appendix A). We introduce catalytic embeddings in Section 5. We leverage the results of the previous sections in Section 6 to prove our main result. We comment on the complexity of the produced circuits in Section 7 and we conclude in Section 8.

Disclaimer: After the present work was completed, it was brought to our attention that related results were independently established in [18].

2 Rings and Groups

In this section, we discuss the rings and groups which will be important in the rest of the paper. In what follows, when u, u', and v are elements of a ring R, we write $u \equiv_v u'$ if u is congruent to u' modulo v, i.e., if $u - u' = rv$ for some $r \in R$.

2.1 The Ring $\mathbb{Z}[\omega_k]$

Definition 2.1. Let $k \geq 1$. The **primitive 3^k-th root of unity** $\omega_k \in \mathbb{C}$ is defined as $\omega_k = e^{2\pi i/3^k}$.

We have, for $k > 1$, $\omega_k^3 = \omega_{k-1}$, $\omega_k^{3^k} = 1$, $\omega_k^\dagger = \omega_k^{3^k-1}$, and $\omega_k^0 + \omega_k^1 + \ldots + \omega_k^{3^k-1} = 0$. As mentioned in Section 1, we often write ω for ω_1.

Definition 2.2. Let $k \geq 1$. The ring $\mathbb{Z}[\omega_k]$ of **cyclotomic integers of degree 3^k** is the smallest subring of $\mathbb{C}$ that contains ω_k.

The ring $\mathbb{Z}[\omega_k]$ can be defined in a variety of ways [29]. It will be useful for our purposes to note that $\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$, and that, for $k \geq 2$,

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

Furthermore, the expression of an element of $\mathbb{Z}[\omega_k]$ as a linear combination of elements of $\mathbb{Z}[\omega_{k-1}]$ is unique. The ring $\mathbb{Z}[\omega_k]$ is closed under complex conjugation and, for $k \geq 2$, we have $\mathbb{Z}[\omega_{k-1}] \subseteq \mathbb{Z}[\omega_k]$.

2.2 Properties of $\mathbb{Z}[\omega]$

We now record some useful properties of $\mathbb{Z}[\omega]$. If $u = a + b\omega \in \mathbb{Z}[\omega]$, then

$$u^\dagger u = (a + b\omega)(a + b\omega^2) = a^2 + ab(\omega + \omega^2) + b^2 = a^2 - ab + b^2. \tag{1}$$

In particular, if $u \in \mathbb{Z}[\omega]$, then $u^\dagger u$ is a nonnegative integer, since the Euclidean norm of a complex number is always nonnegative.

Definition 2.3. We define $\lambda \in \mathbb{Z}[\omega]$ as $\lambda = 1 - \omega$.

By Equation (1), we have $\lambda^\dagger \lambda = 3$. Similarly, we have $\lambda^2 = 1 - 2\omega + \omega^2 = -3\omega$, so that $3 = -\lambda^2\omega^2$. Hence, $3 \equiv_\lambda 0$.

Proposition 2.4. *We have*

- $\mathbb{Z}[\omega]/(3) \cong \{0,1,2,\omega,2\omega,1+\omega,1+2\omega,2+\omega,2+2\omega\} \cong \mathbb{Z}/(3)+\omega\mathbb{Z}/(3)$ *and*
- $\mathbb{Z}[\omega]/(\lambda) \cong \{0,1,2\} \cong \mathbb{Z}/(3)$.

Proof. The first item follows from the fact that $3 \equiv_3 0$. The second item follows from the fact that $3 \equiv_\lambda 0$ and the fact that $\omega \equiv_\lambda 1$. □

Proposition 2.5. *If $u \in \mathbb{Z}[\omega]$, then $u^\dagger u \equiv_\lambda 0$ or $u^\dagger u \equiv_\lambda 1$.*

Proof. Let $u = a + b\omega \in \mathbb{Z}[\omega]$. By Proposition 2.4, $\mathbb{Z}[\omega]/(\lambda) \cong \mathbb{Z}/(3)$. By Equation (1),

$$u^\dagger u = a^2 - ab + b^2 \equiv_\lambda a^2 + 2ab + b^2 = (a+b)^2.$$

Hence $u^\dagger u$ is a square modulo λ and therefore cannot be congruent to 2, since 0 and 1 are the only squares in $\mathbb{Z}/(3)$. □

Proposition 2.6. *If $u \in \mathbb{Z}[\omega]$, then $u \not\equiv_\lambda 0$ if and only if $u \equiv_3 \pm\omega^x$ for some $x \in \{0,1,2\}$.*

Proof. The table below lists the elements of $\mathbb{Z}[\omega]/(3)$ as given by Proposition 2.4, together with their residues modulo λ.

$\mathbb{Z}[\omega]/(3)$	$\mathbb{Z}[\omega]/(\lambda)$
0	0
1	1
2	2
ω	1
2ω	2
$1+\omega$	2
$1+2\omega$	0
$2+\omega$	0
$2+2\omega$	1

The statement then follows by inspection of the table, using the fact that $1+\omega = -\omega^2 \equiv_3 -\omega^2$ and $2 \equiv_3 -1$. □

2.3 Denominators

Definition 2.7. Let $k \geq 1$. The ring $\mathbb{Z}[1/3,\omega_k]$ is defined as $\mathbb{Z}[1/3,\omega_k] = \{u/3^\ell \mid u \in \mathbb{Z}[\omega_k] \text{ and } \ell \in \mathbb{N}\}$.

Because the elements of $\mathbb{Z}[\omega_k]$ can be expressed as linear combinations of elements of $\mathbb{Z}[\omega_{k-1}]$, the elements of $\mathbb{Z}[1/3,\omega_k]$ can similarly be expressed as linear combinations of elements of $\mathbb{Z}[1/3,\omega_{k-1}]$. In particular, for $k \geq 2$, every element u of $\mathbb{Z}[1/3,\omega_k]$ can be uniquely written as $u = a + b\omega_k + c\omega_k^2$ with $a,b,c \in \mathbb{Z}[1/3,\omega_{k-1}]$.

The ring $\mathbb{Z}[1/3,\omega_k]$ is the localization of $\mathbb{Z}[\omega_k]$ by the powers of 3. Alternatively, $\mathbb{Z}[1/3,\omega_k]$ can be thought of as the localization of $\mathbb{Z}[\omega_k]$ by the powers of λ. Indeed, since $3 = -\omega^2\lambda^2$, we have $3^{-\ell} = (-\omega^2\lambda^2)^{-\ell} = (-\omega)^\ell(\lambda)^{-2\ell}$. As a result, any element of $\mathbb{Z}[1/3,\omega_k]$ can be written as u/λ^ℓ for some $u \in \mathbb{Z}[\omega_k]$ and some $\ell \in \mathbb{N}$. We leverage this fact to define, in the usual way (see [4, 12, 15]), the notions of **λ-denominator exponent** and **least λ-denominator exponent**.

Definition 2.8. Any nonnegative integer ℓ such that $v \in \mathbb{Z}[1/3, \omega_k]$ can be written as $v = u/\lambda^\ell$ with $u \in \mathbb{Z}[\omega_k]$ is **λ-denominator exponent** of v. The smallest such ℓ is the **least λ-denominator exponent** of v and is denoted $\mathrm{lde}(v)$.

The notions of denominator exponent and least denominator exponent extend to matrices (and therefore to vectors) with entries in $\mathbb{Z}[1/3, \omega_k]$: an integer ℓ is a λ-denominator exponent of a matrix M if it is a λ-denominator exponent of all of the entries of M; the smallest such ℓ is the least λ-denominator exponent of M.

2.4 The Group $\mathrm{U}_n(\mathbb{Z}[1/3, \omega_k])$

Definition 2.9. We write $\mathrm{U}_n(\mathbb{Z}[1/3, \omega_k])$ for the group of n-dimensional unitary matrices with entries in $\mathbb{Z}[1/3, \omega_k]$ and $\mathrm{U}(\mathbb{Z}[1/3, \omega_k])$ for the collection of all unitary matrices with entries in $\mathbb{Z}[1/3, \omega_k]$.

3 Generators for $\mathrm{U}_n(\mathbb{Z}[1/3, \omega])$

Following [4, 12, 15, 23], we use **m-level matrices** to define a subset of $\mathrm{U}_n(\mathbb{Z}[1/3, \omega])$ which we will show to be a generating set.

Definition 3.1. The matrices (-1), (ω), X, and H are defined as follows:

$$(-1) = \begin{bmatrix} -1 \end{bmatrix}, \quad (\omega) = \begin{bmatrix} \omega \end{bmatrix}, \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \text{and} \quad H = \frac{-\omega^2}{\lambda} \begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{bmatrix}.$$

Definition 3.2. Let M be an $m \times m$ matrix, let $m \leq n$, and let $0 \leq x_1 < \ldots < x_m \leq n-1$. The **$m$-level matrix** $M_{[x_1,\ldots,x_m]}$ is the $n \times n$ matrix whose entries are given as follows

$$M_{[x_1,\ldots,x_m]\, i,j} = \begin{cases} M_{i',j'} & \text{if } i = x_{i'} \text{ and } j = x_{j'}, \\ I_{i,j} & \text{otherwise.} \end{cases}$$

For example, for $n = 4$, we have

$$(\omega)_{[1]} = \begin{bmatrix} 1 & \cdot & \cdot & \cdot \\ \cdot & \omega & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & 1 \end{bmatrix} \qquad \text{and} \qquad H_{[0,2,3]} = \frac{-\omega^2}{\lambda} \begin{bmatrix} 1 & \cdot & 1 & 1 \\ \cdot & \lambda/(-\omega^2) & \cdot & \cdot \\ 1 & \cdot & \omega & \omega^2 \\ 1 & \cdot & \omega^2 & \omega \end{bmatrix}.$$

When applied to a vector $|u\rangle$, the matrix $(\omega)_{[1]}$ acts as (ω) on the entry of index 1 and the matrix $H_{[0,2,3]}$ acts as H on the entries of index 0, 2, and 3.

Definition 3.3. We write $\mathscr{S}_n$ for the subset of $\mathrm{U}_n(\mathbb{Z}[1/3, \omega])$ defined as

$$\mathscr{S}_n = \{(-1)_{[x]}, (\omega)_{[x]}, X_{[x,y]}, H_{[x,y,z]} \mid 0 \leq x < y < z \leq n-1\}.$$

Lemma 3.4. *Let $u_0, u_1, u_2 \in \mathbb{Z}[\omega]$ be such that $u_0 \not\equiv_\lambda 0$, $u_1 \not\equiv_\lambda 0$, and $u_2 \not\equiv_\lambda 0$. Then there exists $x_0, x_1, x_2 \in \{0,1,2\}$ and $y_0, y_1, y_2 \in \{0,1\}$ such that*

$$H(\omega)_{[0]}^{x_0}(\omega)_{[1]}^{x_1}(\omega)_{[2]}^{x_2}(-1)_{[0]}^{y_0}(-1)_{[1]}^{y_1}(-1)_{[2]}^{y_2} \begin{bmatrix} u_0 \\ u_1 \\ u_2 \end{bmatrix} = \begin{bmatrix} u_0' \\ u_1' \\ u_2' \end{bmatrix}$$

for some $u_0', u_1', u_2' \in \mathbb{Z}[\omega]$ such that $u_0' \equiv_\lambda 0$, $u_1' \equiv_\lambda 0$, and $u_2' \equiv_\lambda 0$.

Proof. Let $j \in \{0,1,2\}$. Since $u_j \not\equiv_\lambda 0$, we have, by Proposition 2.6, $u_j \equiv_3 (-1)^{w_j}(\omega)^{z_j}$. Hence, setting $y_j = -w_j$ and $x_j = -z_j$, we get $(\omega)^{x_j}(-1)^{y_j}u_j \equiv_3 1$. Therefore,

$$(\omega)^{x_0}_{[0]}(\omega)^{x_1}_{[1]}(\omega)^{x_2}_{[2]}(-1)^{y_0}_{[0]}(-1)^{y_1}_{[1]}(-1)^{y_2}_{[2]}\begin{bmatrix}u_0\\u_1\\u_2\end{bmatrix} = \begin{bmatrix}v_0\\v_1\\v_2\end{bmatrix}$$

for some $v_0, v_1, v_2 \in \mathbb{Z}[\omega]$ such that $v_0 \equiv_3 v_1 \equiv_3 v_2 \equiv_3 1$. The result then follows by computation, since $v_0 + v_1 + v_2 \equiv_3 v_0 + \omega v_1 + \omega^2 v_2 \equiv_3 v_0 + \omega^2 v_1 + \omega v_2 \equiv_3 0$. □

Lemma 3.5. *Let $|u\rangle \in \mathbb{Z}[1/3,\omega]^n$ be a unit vector. If $\operatorname{lde}|u\rangle = 0$, then $|u\rangle = \pm\omega^x|j\rangle$ for some $0 \le x \le 2$ and some $0 \le j \le n-1$.*

Proof. Let $|u\rangle \in \mathbb{Z}[1/3,\omega]^n$. Since $\operatorname{lde}|u\rangle = 0$, we have $|u\rangle \in \mathbb{Z}[\omega]^n$. Since $|u\rangle$ is a unit vector, we also have

$$1 = \langle u|u\rangle = \sum u_j^\dagger u_j$$

with $u_j \in \mathbb{Z}[\omega]$. Because each $u_j^\dagger u_j$ is a nonnegative integer, there must be exactly one j for which $u_j^\dagger u_j = 1$, while $u_{j'}^\dagger u_{j'} = 0$ for all $j' \neq j$. If $u_j^\dagger u_j = 1$ then $a_j^2 - a_j b_j + b_j^2 = 1$, and this equation can only be true if $a = \pm 1$ and $b = 0$, $a = 0$ and $b = \pm 1$, or $a = b = \pm 1$. In the first case, $|u\rangle = \pm|j\rangle$, in the second case, $|u\rangle = \pm\omega|j\rangle$, and in the third case, $|u\rangle = \pm\omega^2|j\rangle$, □

Lemma 3.6. *Let $|u\rangle \in \mathbb{Z}[1/3,\omega]^n$ be a unit vector. If $\operatorname{lde}|u\rangle > 0$, then there exists $G_0,\ldots,G_q \in \mathscr{S}_n$ such that $\operatorname{lde}(G_q \cdots G_0|u\rangle) < \operatorname{lde}|u\rangle$.*

Proof. Write $|u\rangle$ as $|v\rangle/\lambda^\ell$, with $\ell = \operatorname{lde}|u\rangle$. Since $\langle u|u\rangle = 1$ and $\lambda^\dagger\lambda = 3$, we get $3^\ell = \langle v|v\rangle = \sum v_j^\dagger v_j$. Hence, $\sum v_j^\dagger v_j \equiv_\lambda 0$. By Proposition 2.5, $v_j^\dagger v_j$ is either 0 or 1 modulo λ, and by Proposition 2.4, $\mathbb{Z}[\omega]/(\lambda) \cong \mathbb{Z}/(3)$. Thus, the number of v_j such that $v_j \not\equiv_\lambda 0$ must be a multiple of 3. Hence, we can group the entries of $|v\rangle$ into triples and apply Lemma 3.4 to each such triple. This maps $|u\rangle$ to some $|u\rangle'$ of lower least denominator exponent. □

Lemma 3.7. *Let $|u\rangle \in \mathbb{Z}[1/3,\omega]^n$ be a unit vector and let $0 \le j \le n-1$. Then there exists $G_0,\ldots,G_q \in \mathscr{S}_n$ such that $G_q \cdots G_0|u\rangle = |j\rangle$.*

Proof. By induction on $\operatorname{lde}|u\rangle$. If $\operatorname{lde}(|u\rangle) = 0$, then, by Lemma 3.5, $|u\rangle = \pm\omega^x e_{j'}$ for some $0 \le j' \le n-1$ and some $0 \le x \le 2$. We can therefore reduce $|u\rangle$ to $|j\rangle$ by applying $(-1)_{[j']}$, $(\omega)_{[j']}$, and $X_{[j,j']}$ or $X_{[j',j]}$, as needed. If $\operatorname{lde}|u\rangle > 0$, then, by Lemma 3.6, there exists $G_p,\ldots,G_0 \in \mathscr{S}_n$ such that $\operatorname{lde}(G_p \cdots G_0|u\rangle) < \operatorname{lde}(|u\rangle)$. We can then conclude by applying the induction hypothesis to $G_p \cdots G_0|u\rangle$. □

Proposition 3.8. *Let U be an $n \times n$ matrix. Then $U \in \mathrm{U}_n(\mathbb{Z}[1/3,\omega])$ if and only if U can be written as a product of elements of $\mathscr{S}_n$.*

Proof. The right-to-left direction is immediate. For the left-to-right direction, consider the matrix $U^\dagger \in \mathrm{U}_n(\mathbb{Z}[1/3,\omega])$. Iteratively applying Lemma 3.7 to the columns of $U^\dagger$ yields a sequence $G_0,\ldots,G_q$ of elements of $\mathscr{S}_n$ such that

$$G_0 G_1 \cdots G q U^\dagger = I,$$

and we can therefore write U as $U = G_0 G_1 \cdots G_q$. □

4 Exact Synthesis of Toffoli+Hadamard Circuits

Let $\mathscr{G}$ be a set of quantum gates. A unitary matrix U can be **represented by a circuit over** $\mathscr{G}$ if there exists a circuit C over $\mathscr{G}$ such that, for any state $|u\rangle$, we have $C|u\rangle = U|u\rangle$. The circuit may use ancillary qutrits, but these must start and end the computation in the same state. If that state can be arbitrary, the ancillary qutrits are said to be **borrowed**; if that state is required to be $|0\rangle$, the ancillary qutrits are said to be **fresh**. Unless otherwise specified, ancillae are assumed to be fresh. Note that if a matrix can be represented by a circuit using m borrowed ancillae, then it can also be represented by a circuit using m fresh ancillae.

Recall from Section 1 that the Clifford-cyclotomic gate set $\mathscr{G}_k$ is defined as $\mathscr{G}_k = \{X, CX, CCX, H, T_k\}$. In Appendix A we prove that $\mathscr{G}_1$ is equivalent to the Toffoli+Hadamard gate set, up to two borrowed ancillae and that, when $k \geq 2$, $\mathscr{G}_k$ is equivalent to the Clifford+T_k gate set $\{H, S, CX, T_k\}$, up to a single borrowed ancilla. The next proposition shows that all of the elements of $\mathscr{S}_{3^n}$ can be represented by a circuit over $\mathscr{G}_1$ using no more than 2 borrowed ancillae. The proof of the proposition can be found in Appendix A.

Proposition 4.1. *If $U \in \mathscr{S}_{3^n}$, then U can be represented by a circuit over $\mathscr{G}_1$ using at most 2 borrowed ancillae.*

Using Proposition 4.1 we are now in a position to define an exact synthesis algorithm for multiqutrit Toffoli+Hadamard circuits.

Theorem 4.2. *If $U \in \mathrm{U}_{3^n}(\mathbb{Z}[1/3, \omega_1])$, then U can be represented by an n-qutrit circuit over $\mathscr{G}_1$ using at most 2 ancillae.*

Proof. By Proposition 3.8, $\mathscr{S}_{3^n}$ generates $\mathrm{U}_{3^n}(\mathbb{Z}[1/3, \omega_1])$. Hence, it is sufficient to show that the elements of $\mathscr{S}_{3^n}$ can be represented by an n-qutrit circuit over $\mathscr{G}_1$. This follows from Proposition 4.1, since if 2 borrowed ancillae suffice to construct a circuit for U, then 2 fresh ancillae are also sufficient for this purpose. □

5 Catalytic Embeddings

Definition 5.1. Let $\mathscr{U}$ and $\mathscr{V}$ be collections of unitaries. An m**-dimensional catalytic embedding** of $\mathscr{U}$ into $\mathscr{V}$ is a pair $(\phi, |c\rangle)$ of a function $\phi : \mathscr{U} \to \mathscr{V}$ and a vector $|c\rangle \in \mathbb{C}^m$ such that if $U \in \mathscr{U}$ has dimension n then $\phi(U) \in \mathscr{V}$ has dimension nm and

$$\phi(U)(|u\rangle \otimes |c\rangle) = (U|u\rangle) \otimes |c\rangle$$

for every $|u\rangle \in \mathbb{C}^n$. The vector $|c\rangle$ is the **catalyst** of the catalytic embedding $(\phi, |c\rangle)$. We sometimes express the fact that $(\phi, |c\rangle)$ is a catalytic embedding of $\mathscr{U}$ into $\mathscr{V}$ by writing $(\phi, |c\rangle) : \mathscr{U} \to \mathscr{V}$.

Definition 5.2. Let $(\phi, |c\rangle) : \mathscr{U} \to \mathscr{V}$ and $(\phi', |c\rangle') : \mathscr{V} \to \mathscr{W}$ be catalytic embeddings of dimension m and m', respectively. The **concatenation** of $(\phi, |c\rangle)$ and $(\phi', |c\rangle')$ is the $m'm$-dimensional catalytic embedding $(\phi', |c\rangle') \circ (\phi, |c\rangle)$ defined by $(\phi', |c\rangle') \circ (\phi, |c\rangle) = (\phi' \circ \phi, |c\rangle \otimes |c\rangle')$.

The concatenation of catalytic embeddings is associative and the catalytic embedding $(1_{\mathscr{U}}, [1]) : \mathscr{U} \to \mathscr{U}$ acts as an identity for concatenation.

Definition 5.3. Let $k \geq 2$. We define Ω_k and $|c_k\rangle$ as

$$\Omega_k = \begin{bmatrix} \cdot & \cdot & \omega_{k-1} \\ 1 & \cdot & \cdot \\ \cdot & 1 & \cdot \end{bmatrix} \qquad \text{and} \qquad |c_k\rangle = \frac{1}{\lambda} \begin{bmatrix} 1 \\ \omega_k^{-1} \\ \omega_k^{-2} \end{bmatrix}.$$

The matrix Ω_k is unitary and the vector $|c_k\rangle$ is an eigenvector of Ω_k for eigenvalue ω_k. Indeed, since $\omega_{k-1} = \omega_k^3$, we have

$$\Omega_k |c_k\rangle = \frac{1}{\lambda}\begin{bmatrix} \cdot & \cdot & \omega_{k-1} \\ 1 & \cdot & \cdot \\ \cdot & 1 & \cdot \end{bmatrix}\begin{bmatrix} 1 \\ \omega_k^{-1} \\ \omega_k^{-2} \end{bmatrix} = \frac{1}{\lambda}\begin{bmatrix} \omega_k \\ 1 \\ \omega_k^{-1} \end{bmatrix} = \frac{\omega_k}{\lambda}\begin{bmatrix} 1 \\ \omega_k^{-1} \\ \omega_k^{-2} \end{bmatrix} = \omega_k |c_k\rangle . \tag{2}$$

Now recall from Section 2.3 that, for $k \geq 2$, every $u \in \mathbb{Z}[1/3, \omega_k]$ can be written uniquely as a linear combination of the form $u = a + b\omega_k + c\omega_k^2$, where $a, b, c \in \mathbb{Z}[1/3, \omega_{k-1}]$. Therefore, every matrix U over $\mathbb{Z}[1/3, \omega_k]$ can be uniquely written as $U = A + B\omega_k + C\omega_k^2$, where A, B, and C are matrices over $\mathbb{Z}[1/3, \omega_{k-1}]$. We use this fact below to define a function $\mathrm{U}(\mathbb{Z}[1/3, \omega_k]) \to \mathrm{U}(\mathbb{Z}[1/3, \omega_{k-1}])$.

Proposition 5.4. *Let $k \geq 2$. The assignment*

$$A + B\omega_k + C\omega_k^2 \longmapsto A \otimes I + B \otimes \Omega_k + C \otimes \Omega_k^2$$

defines a function $\phi_k : \mathrm{U}(\mathbb{Z}[1/3, \omega_k]) \to \mathrm{U}(\mathbb{Z}[1/3, \omega_{k-1}])$.

Proof. Let $U \in \mathrm{U}(\mathbb{Z}[1/3, \omega_k])$ and write U as $U = A + B\omega_k + C\omega_k^2$ for some matrices A, B, and C over $\mathbb{Z}[1/3, \omega_{k-1}]$. Now let $U' = A \otimes I + B \otimes \Omega_k + C \otimes \Omega_k^2$. It is clear that U' is a matrix with entries in $\mathbb{Z}[1/3, \omega_{k-1}]$. We now show that U' is unitary. Since U is unitary and since $U = A + B\omega_k + C\omega_k^2$, we can express the equation $U^\dagger U = I$ in terms of A, B, and C. Using $\omega_k^\dagger = \omega_{k-1}^\dagger \omega_k^2$, this yields

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

Hence, $A^\dagger A + B^\dagger B + C^\dagger C = I$ and $A^\dagger B + B^\dagger C + C^\dagger A\omega_{k-1}^\dagger = A^\dagger C + B^\dagger A\omega_{k-1}^\dagger + C^\dagger B\omega_{k-1}^\dagger = 0$. Now note that $\Omega_k^\dagger = \omega_{k-1}^\dagger \Omega_k^2$, so that $U'^\dagger U'$ is equal to

$$(A^\dagger A + B^\dagger B + C^\dagger C) \otimes I + (A^\dagger B + B^\dagger C + C^\dagger A\omega_{k-1}^\dagger) \otimes \Omega_k + (A^\dagger C + B^\dagger A\omega_{k-1}^\dagger + C^\dagger B\omega_{k-1}^\dagger) \otimes \Omega_k^2.$$

Hence, $U'^\dagger U' = I$. Reasoning analogously shows that $U' U'^\dagger = I$, so that U' is indeed unitary. □

Proposition 5.5. *Let $k \geq 2$. The pair $(\phi_k, |c_k\rangle)$ is a 3-dimensional catalytic embedding of* $\mathrm{U}(\mathbb{Z}[1/3, \omega_k])$ *into* $\mathrm{U}(\mathbb{Z}[1/3, \omega_{k-1}])$.

Proof. By Proposition 5.4, $\phi_k : \mathrm{U}(\mathbb{Z}[1/3, \omega_k]) \to \mathrm{U}(\mathbb{Z}[1/3, \omega_{k-1}])$ is a function and, by construction, if $U \in \mathrm{U}(\mathbb{Z}[1/3, \omega_k])$ has dimension n, then $\phi_k(U)$ has dimension $3n$. Moreover, if $|u\rangle \in \mathbb{C}^n$, then

$$\begin{aligned}
\phi_k(U)(|u\rangle \otimes |c_k\rangle) &= (A \otimes I + B \otimes \Omega_k + C \otimes \Omega_k^2)(|u\rangle \otimes |c_k\rangle) \\
&= A \otimes I(|u\rangle \otimes |c_k\rangle) + B \otimes \Omega_k(|u\rangle \otimes |c_k\rangle) + C \otimes \Omega_k^2(|u\rangle \otimes |c_k\rangle) \\
&= A|u\rangle \otimes I|c_k\rangle + B|u\rangle \otimes \Omega_k|c_k\rangle + C|u\rangle \otimes \Omega_k^2|c_k\rangle \\
&= A|u\rangle \otimes |c_k\rangle + B|u\rangle \otimes \omega_k|c_k\rangle + C|u\rangle \otimes \omega_k^2|c_k\rangle \\
&= A|u\rangle \otimes |c_k\rangle + \omega_k B|u\rangle \otimes |c_k\rangle + \omega_k^2 C|u\rangle \otimes |c_k\rangle \\
&= (A|u\rangle + \omega_k B|u\rangle + \omega_k^2 C|u\rangle) \otimes |c_k\rangle \\
&= (U|u\rangle) \otimes |c_k\rangle .
\end{aligned}$$

Hence, $(\phi_k, |c_k\rangle)$ is a catalytic embedding. □

Remark 5.6. The catalytic embedding constructed in Proposition 5.4 and Proposition 5.5 takes advantage of the fact that the matrix Ω_k and the algebraic number ω_k have many properties in common. Importantly, the polynomial $x^3 - \omega_{k-1}$ is both the characteristic polynomial of Ω_k and the minimal polynomial of ω_k over the ring $\mathbb{Z}[1/3, \omega_{k-1}]$. This construction generalizes to many other rings of interest (see [1]).

Corollary 5.7. *Let $k \geq 2$. There is a 3^{k-1}-dimensional catalytic embedding $(\phi, |c\rangle) : \mathrm{U}(\mathbb{Z}[1/3, \omega_k]) \to \mathrm{U}(\mathbb{Z}[1/3, \omega])$.*

Proof. Applying Proposition 5.5 repeatedly yields a sequence of catalytic embeddings

$$\mathrm{U}(\mathbb{Z}[1/3, \omega_k]) \xrightarrow{(\phi_k, |c_k\rangle)} \cdots \xrightarrow{(\phi_3, |c_3\rangle)} \mathrm{U}(\mathbb{Z}[1/3, \omega_2]) \xrightarrow{(\phi_2, |c_2\rangle)} \mathrm{U}(\mathbb{Z}[1/3, \omega]).$$

Concatenating the catalytic embeddings in this sequence yields the desired result. □

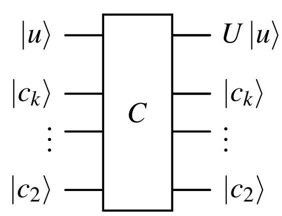
Note that the catalyst $|c\rangle$ in the catalytic embedding $(\phi, |c\rangle)$ of Corollary 5.7 is the product state $|c\rangle = |c_2\rangle \otimes \cdots \otimes |c_k\rangle$.

6 Exact Synthesis of Clifford-Cyclotomic Circuits

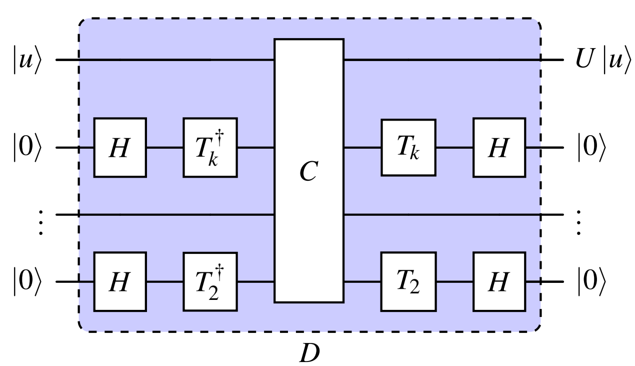
We can now prove our main result, which will follow straightforwardly from the results of Sections 3, 4 and 5.

Proposition 6.1. *Let $k \geq 2$. If $U \in \mathrm{U}_{3^n}(\mathbb{Z}[1/3, \omega_k])$, then U can be represented by an n-qutrit circuit over $\mathscr{G}_k$ using at most $k+1$ ancillae.*

Proof. Let $U \in \mathrm{U}_{3^n}(\mathbb{Z}[1/3, \omega_k])$ and let $(\phi, |c\rangle)$ be the catalytic embedding constructed in Corollary 5.7, with $|c\rangle = |c_2\rangle \otimes \cdots \otimes |c_k\rangle$. We then have $\phi(U) \in \mathrm{U}_{3^{n+k-1}}(\mathbb{Z}[1/3, \omega])$, so that, by Theorem 4.2, $\phi(U)$ can be represented by an $(n+k-1)$-qutrit circuit C over $\mathscr{G}_1$ using at most 2 fresh ancillae. By Definition 5.1, the action of $\phi(U)$ on an input of the form $|u\rangle \otimes |c_2\rangle \otimes \cdots \otimes |c_k\rangle$ can be depicted as below (where the ancillary qutrits used in C, if any, are omitted).



But, for $2 \leq \ell \leq k$, we have $|c_\ell\rangle = T_\ell^\dagger H |0\rangle$ and $T_\ell^\dagger = (T_k^\dagger)^{3^{k-\ell}}$. Hence, we can construct the following circuit over $\mathscr{G}_k$.



Since all of the ancillae in D (including the ancillae potentially present in C) start and end the computation in the $|0\rangle$ state, then D is a circuit over $\mathcal{G}_k$ which represents U and uses at most $k+1$ (fresh) ancillae, as desired. □

Remark 6.2. The circuit constructed in Proposition 6.1 actually use $k-1$ fresh ancillae and no more than 2 borrowed ancillae. For brevity, we simply stated the proposition in terms of fresh ancillae. One can amend the constructions in Appendix A to reduce the total ancilla-count from $k+1$ to k, at the cost of requiring all ancillae to be fresh.

Theorem 6.3. *Let $k \geq 1$ and let U be a $3^n \times 3^n$ unitary matrix. Then U can be represented by an n-qutrit circuit over $\mathcal{G}_k$ if and only if $U \in \mathrm{U}_{3^n}(\mathbb{Z}[1/3, \omega_k])$. Moreover, $k+1$ ancillae are always sufficient to construct a circuit for U.*

Proof. The left-to-right direction is a consequence of the fact that the entries of the elements of $\mathcal{G}_k$ lie in the ring $\mathbb{Z}[1/3, \omega_k]$. The right-to-left direction is given by Theorem 4.2 and Proposition 6.1. □

7 Circuit Complexity

The proof of Theorem 6.3 is constructive: it provides an algorithm to construct a circuit for a given matrix. In this section, we briefly discuss the complexity of the resulting circuit, reasoning as in [3, 12]. We start by considering Proposition 3.8 before turning to Theorem 6.3.

Lemma 7.1. *Let $U \in \mathrm{U}_m(\mathbb{Z}[1/3, \omega])$ and let $\ell = \mathrm{lde}(U)$. The algorithm of Proposition 3.8 expresses U as a product of $O(2^m \ell)$ elements of $\mathcal{S}_m$ in the worst case.*

Proof. Consider the first column of U. In the worst case, its least denominator exponent is ℓ. To reduce this least denominator exponent by one requires $O(m)$ operations. Hence, reducing the first column of U completely requires $O(\ell m)$ operations in the worst case. The reduction of the first column may increase the least denominator exponent of the second column from ℓ to 2ℓ, since each entry of the second column may be affected by up to ℓ 3-level matrices in the course of this first reduction. Once the first column has been reduced, the second column may still have $m-1$ nonzero entries. Reducing the second column will hence require $O(2\ell(m-1))$ operations in the worst case. In general, reducing the j-th column will require $O(2^{j-1}\ell(m-j))$ operations in the worst case so that the overall reduction of U requires at most

$$O\left(\sum_{i=0}^{n-1} 2^i \ell(m-i)\right)$$

operations. Simplifying the resulting sum yields a total of $O(2^m \ell)$ operations. □

Theorem 7.2. *Let $U \in \mathrm{U}_{3^n}(\mathbb{Z}[1/3, \omega_k])$ and let $\ell = \mathrm{lde}(U)$. The algorithm of Theorem 6.3 represents U as a circuit of $O((n+k)2^{3^{n+k-1}} \ell)$ gates in the worst case.*

Proof. The algorithm of Theorem 6.3 uses the catalytic embedding $(\phi, |c\rangle)$ of Corollary 5.7 to construct a matrix $\phi(U)$ over $\mathbb{Z}[1/3, \omega]$. The dimension of $\phi(U)$ is 3^{n+k-1} and its least denominator exponent is no more than ℓ. Hence, by Lemma 7.1, the algorithm of Proposition 3.8 will express $\phi(U)$ as a product of no more than $O(2^{3^{n+k-1}} \ell)$ elements of $\mathcal{S}_{3^{n+k-1}}$. It follows from the circuit constructions given in Appendix A, that each element of $\mathcal{S}_{3^{n+k-1}}$ can be represented by a circuit consisting of $O(n+k)$ gates. Hence, the circuit produced by Theorem 6.3 consists of no more than $O((n+k)2^{3^{n+k-1}} \ell)$ gates. □

8 Conclusion

We showed that the matrices that can be exactly represented by an n-qutrit circuit over the Clifford-cyclotomic gate set of degree 3^k are precisely the elements of $\mathrm{U}_{3^n}(\mathbb{Z}[1/3,\omega_k])$. Moreover, we showed that no more than $k+1$ ancillae are required to construct a circuit for an element of $\mathrm{U}_{3^n}(\mathbb{Z}[1/3,\omega_k])$.

Our proof contains an algorithm for synthesizing a circuit over $\mathscr{G}_k$, given a matrix in $\mathrm{U}_{3^n}(\mathbb{Z}[1/3,\omega_k])$. However, the circuits constructed in this way are very large and their optimization is a promising direction for future research. It would be interesting to reduce the gate-complexity of the circuits produced by Theorem 6.3. The techniques employed in [3, 22] for the synthesis of multiqubit Toffoli+Hadamard and Clifford+T circuits are likely to apply in the qutrit context as well. Similarly, it would also be interesting to reduce the number of ancillae used by the algorithm. As Appendix A shows, some of the ancillae can be removed by choosing a slightly different gate set, but the bulk of the ancillae come from the use of catalytic embeddings, so a different synthesis technique may be required for more significant savings. Along this line of inquiry, it would be interesting to characterize the matrices that can be represented by ancilla-free circuits. Such characterizations exist for qubit matrices [4, 12], but are likely to be different for qutrits [32].

Finally, a natural generalization of this work would be to consider higher-dimensional qudits. However, preliminary research suggests that the techniques used here and in [2] might not adapt straightforwardly to primes larger than 3. While it stands to reason that some version of our results should continue to hold for larger prime dimensions, proving this to be the case might require new ideas.

Acknowledgements

The authors would like to thank Sarah Meng Li, Ewan Murphy, and the anonymous reviewers of 21st International Conference on Quantum Physics and Logic (QPL 2024) for insightful comments on an earlier version of this paper. LY is funded by a Google PhD Fellowship. The circuit diagrams in the proof of Proposition 6.1 were typeset using Quantikz [21].

References

[1] Matthew Amy, Matthew Crawford, Andrew N. Glaudell, Melissa L. Macasieb, Samuel S. Mendelson & Neil J. Ross (2023): *Catalytic embeddings of quantum circuits*. Preprint available from `arXiv:2305.07720`.

[2] Matthew Amy, Andrew N. Glaudell, Shaun Kelso, William Maxwell, Samuel S. Mendelson & Neil J. Ross (2023): *Exact Synthesis of Multiqubit Clifford-Cyclotomic Circuits*. Preprint available from `arXiv:2311.07741`.

[3] Matthew Amy, Andrew N. Glaudell, Sarah Meng Li & Neil J. Ross (2023): *Improved Synthesis of Toffoli-Hadamard Circuits*. In Martin Kutrib & Uwe Meyer, editors: *Reversible Computation*, Springer Nature Switzerland, Cham, pp. 169–209, doi:10.1007/978-3-031-38100-3_12. Also available from `arXiv:2305.11305`.

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

[5] Hussain Anwar, Earl T Campbell & Dan E Browne (2012): *Qutrit magic state distillation*. *New Journal of Physics* 14(6), p. 063006, doi:10.1088/1367-2630/14/6/063006. Also available from `arXiv:1202.2326`.

[6] Alex Bocharov (2016): *A Note on Optimality of Quantum Circuits over Metaplectic Basis*. *Quantum Information and Computation* 18, doi:10.26421/QIC18.1-2-1. Also available from `arXiv:1606.02315`.

[7] Alex Bocharov, Shawn Cui, Martin Roetteler & Krysta Svore (2016): *Improved Quantum Ternary Arithmetics*. Quantum Information and Computation 16, pp. 862–884, doi:10.26421/QIC16.9-10-8. Also available from arXiv:1512.03824.

[8] Alex Bocharov, Martin Roetteler & Krysta M. Svore (2017): *Factoring with qutrits: Shor's algorithm on ternary and metaplectic quantum architectures*. Phys. Rev. A 96, p. 012306, doi:10.1103/PhysRevA.96.012306. Also available from arXiv:1605.02756.

[9] Earl T. Campbell, Hussain Anwar & Dan E. Browne (2012): *Magic-State Distillation in All Prime Dimensions Using Quantum Reed-Muller Codes*. Phys. Rev. X 2, p. 041021, doi:10.1103/PhysRevX.2.041021. Also available from arXiv:1205.3104.

[10] Yulin Chi, Jieshan Huang, Zhanchuan Zhang, Jun Mao, Zinan Zhou, Xiaojiong Chen, Chonghao Zhai, Jueming Bao, Tianxiang Dai, Huihong Yuan, Ming Zhang, Daoxin Dai, Bo Tang, Yan Yang, Zhihua Li, Yunhong Ding, Leif K. Oxenløwe, Mark G. Thompson, Jeremy L. O'Brien, Yan Li, Qihuang Gong & Jianwei Wang (2022): *A programmable qudit-based quantum processor*. Nature Communications 13(1), p. 1166, doi:10.1038/s41467-022-28767-x.

[11] Shawn X. Cui & Zhenghan Wang (2015): *Universal quantum computation with metaplectic anyons*. Journal of Mathematical Physics 56(3), p. 032202, doi:10.1063/1.4914941. Also available from arXiv:1405.7778.

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

[13] Andrew N. Glaudell, Neil J. Ross & Jacob M. Taylor (2019): *Canonical forms for single-qutrit Clifford+T operators*. Annals of Physics 406, pp. 54–70, doi:10.1016/j.aop.2019.04.001. Also available from arXiv:1803.05047.

[14] Andrew N. Glaudell, Neil J. Ross, John van de Wetering & Lia Yeh (2022): *Qutrit Metaplectic Gates Are a Subset of Clifford+T*. In François Le Gall & Tomoyuki Morimae, editors: 17th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2022), Leibniz International Proceedings in Informatics (LIPIcs) 232, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl, Germany, pp. 12:1–12:15, doi:10.4230/LIPIcs.TQC.2022.12. Also available from arXiv:2202.09235.

[15] Seth Evenson Murray Greylyn (2014): *Generators and relations for the group* $\mathrm{U}_4(\mathbb{Z}[1/\sqrt{2},i])$. Master's thesis, Dalhousie University. Available from arXiv:1408.6204.

[16] Mark Howard & Jiri Vala (2012): *Qudit versions of the qubit* $\pi/8$ *gate*. Phys. Rev. A 86, p. 022316, doi:10.1103/PhysRevA.86.022316. Also available from arXiv:1206.1598.

[17] Pavel Hrmo, Benjamin Wilhelm, Lukas Gerster, Martin W. van Mourik, Marcus Huber, Rainer Blatt, Philipp Schindler, Thomas Monz & Martin Ringbauer (2023): *Native qudit entanglement in a trapped ion quantum processor*. Nature Communications 14(1), p. 2242, doi:10.1038/s41467-023-37375-2. Also available from arXiv:2206.04104.

[18] Amolak Ratan Kalra, Manimugdha Saikia, Dinesh Valluri, Sam Winnick & Jon Yard (2024): *Multi-qutrit exact synthesis*. Preprint available from arXiv:2405.08147.

[19] Amolak Ratan Kalra, Dinesh Valluri & Michele Mosca (2024): *Synthesis and Arithmetic of Single Qutrit Circuits*. Preprint available from arXiv:2311.08696.

[20] Valentin Kasper, Daniel González-Cuadra, Apoorva Hegde, Andy Xia, Alexandre Dauphin, Felix Huber, Eberhard Tiemann, Maciej Lewenstein, Fred Jendrzejewski & Philipp Hauke (2021): *Universal quantum computation and quantum error correction with ultracold atomic mixtures*. Quantum Science and Technology 7(1), p. 015008, doi:10.1088/2058-9565/ac2d39. Also available from arXiv:2010.15923.

[21] Alastair Kay (2018): *Tutorial on the quantikz package*. Preprint available from arXiv:1809.03842.

[22] Vadym Kliuchnikov (2013): *Synthesis of unitaries with Clifford+T circuits*. Preprint available from arXiv:1306.3200.

[23] Michael A. Nielsen & Isaac L. Chuang (2000): *Quantum Computation and Quantum Information*. Cambridge Series on Information and the Natural Sciences, Cambridge University Press, doi:10.1017/CBO9780511976667.

[24] Shiroman Prakash (2020): *Magic state distillation with the ternary Golay code*. Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences 476(2241), p. 20200187, doi:10.1098/rspa.2020.0187. Also available from arXiv:2003.02717.

[25] Shiroman Prakash, Akalank Jain, Bhakti Kapur & Shubangi Seth (2018): *Normal form for single-qutrit Clifford+T operators and synthesis of single-qutrit gates*. Physical Review A 98, p. 032304, doi:10.1103/PhysRevA.98.032304. Available from arXiv:1803.05047.

[26] Martin Ringbauer, Thomas R. Bromley, Marco Cianciaruso, Ludovico Lami, W. Y. Sarah Lau, Gerardo Adesso, Andrew G. White, Alessandro Fedrizzi & Marco Piani (2018): *Certification and Quantification of Multilevel Quantum Coherence*. Phys. Rev. X 8, p. 041007, doi:10.1103/PhysRevX.8.041007. Also available from arXiv:1707.05282.

[27] Patrick Roy, John van de Wetering & Lia Yeh (2023): *The Qudit ZH-Calculus: Generalised Toffoli+Hadamard and Universality*. Electronic Proceedings in Theoretical Computer Science 384, pp. 142–170, doi:10.4204/eptcs.384.9. Also available from arXiv:2307.10095.

[28] Peter Selinger (2016): *Reversible k-valued logic circuits are finitely generated for odd k*. Available from arXiv:1604.01646.

[29] L. C. Washington (1982): *Introduction to Cyclotomic Fields*. Springer New York, NY, doi:10.1007/978-1-4612-1934-7.

[30] Fern H. E. Watson, Earl T. Campbell, Hussain Anwar & Dan E. Browne (2015): *Qudit color codes and gauge color codes in all spatial dimensions*. Phys. Rev. A 92, p. 022312, doi:10.1103/PhysRevA.92.022312. Also available from arXiv:1503.08800.

[31] Jordi R. Weggemans, Alexander Urech, Alexander Rausch, Robert Spreeuw, Richard Boucherie, Florian Schreck, Kareljan Schoutens, Jiří Minář & Florian Speelman (2022): *Solving correlation clustering with QAOA and a Rydberg qudit system: a full-stack approach*. Quantum 6, p. 687, doi:10.22331/q-2022-04-13-687. Also available from arXiv:2106.11672v3.

[32] Lia Yeh & John van de Wetering (2022): *Constructing all qutrit controlled Clifford+T gates in Clifford+T*. In Claudio Antares Mezzina & Krzysztof Podlaski, editors: Reversible Computation, Springer International Publishing, Cham, pp. 28–50, doi:10.1007/978-3-031-09005-9_3. Also available from arXiv:2204.00552.

[33] M. A. Yurtalan, J. Shi, M. Kononenko, A. Lupascu & S. Ashhab (2020): *Implementation of a Walsh-Hadamard Gate in a Superconducting Qutrit*. Phys. Rev. Lett. 125, p. 180504, doi:10.1103/PhysRevLett.125.180504. Also available from arXiv:2003.04879.

[34] Wei Zi, Qian Li & Xiaoming Sun (2023): *Optimal Synthesis of Multi-Controlled Qudit Gates*. In: 2023 60th ACM/IEEE Design Automation Conference (DAC), pp. 1–6, doi:10.1109/DAC56929.2023.10247925. Also available from arXiv:2303.12979.

A Circuit Constructions

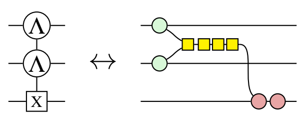
In this appendix, we show that the Clifford-cyclotomic gate set $\mathscr{G}_k$ is equivalent to the Clifford+T_k gate set when $k \geq 2$, we give a construction of the CX gate over the $\{X, CCX, H\}$ gate set, and we provide a proof of Proposition 4.1. In addition, we show that the matrices $(-1)_{[x]}$, $(\omega_k)_{[x]}$, $X_{[x_1,x_2]}$, and $H_{[x_1,x_2,x_3]}$ can be represented by circuits over the $\mathscr{G}_k$ gate set using at most k borrowed ancillae. The constructions in this appendix are exact (i.e., not up to a global or relative phase). Implementations of our constructions, for a fixed number of controls, are available at https://github.com/lia-approves/qutrit-Clifford-cyclotomic.

A.1 Gate Set Equivalences

Recall from Section 1 that the qutrit Toffoli (or CCX) gate acts on computational basis states as

$$|x,y,z\rangle \mapsto |x,y,z+xy\rangle,$$

where the arithmetic operations are performed modulo 3. In higher prime dimension d, the Toffoli gate is defined similarly, except that the arithmetic operations are performed modulo d. The Toffoli gate can be represented in the qupit ZH-calculus [27] as below.



(3)

In Equation (3), Λ denotes the following type of control: if U is a unitary and $|c\rangle$ and $|t\rangle$ are computational basis states, then $\Lambda(U)|c\rangle|t\rangle = |c\rangle \otimes (U^c|t\rangle)$. In particular, $\Lambda(X)$ is the CX gate and $\Lambda(\Lambda(X)) = \Lambda(CX)$ is the CCX gate.

We now recall the definition of the $|0\rangle$**-controlled** X gate, which applies an X gate to its target if and only if its control is in the state $|0\rangle$ [27].

Definition A.1. Let d be a prime. The qudit $|0\rangle$**-controlled** X gate acts on computational basis states as

$$|c,t\rangle \mapsto \begin{cases} |c,t+1\rangle & \text{if } c = 0, \text{ and} \\ |c,t\rangle & \text{otherwise,} \end{cases}$$

where arithmetic is performed modulo d.

Remarkably, when d is a prime greater than 2, the X gate and the $|0\rangle$-controlled X gate suffices to generate all of the d-ary classical reversible gates [27]. Moreover, as was shown in [28, 32], when $d = 3$, no ancillary qutrits are needed for this purpose. In contrast, there is no collection of reversible one and two-qubit gates that suffices to generate all of the binary reversible gates.

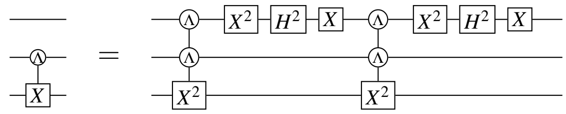
Theorem A.2 ([32], Theorem 2)**.** *Any ternary classical reversible function $f : \{0,1,2\}^n \to \{0,1,2\}^n$ can be represented by an ancilla-free circuit of X and $|0\rangle$-controlled X gates.*

Here, we only need multiply-controlled Toffoli gates, which can be built with a gate count linear in the number of controls, as in [27, 34]. The constructions of [27, 34] use no more borrowed ancillae than there are controls. They can be made into ancilla-free constructions by building Toffoli gates with $n/2$ controls using at most $n/2$ borrowed ancillae. Following [32], one can then combine six of these Toffoli gates with $n/2$ controls to construct a Toffoli gate with $n-1$ controls, and then combine 3 of these Toffoli gates with $n-1$ controls to add the final control.

We now show that the CX gate can be represented by a circuit over $\{X, CCX, H\}$.

Lemma A.3. *The gate sets $\{X, CX, CCX, H\}$ and $\{X, CCX, H\}$ are equivalent up to a single borrowed ancilla.*

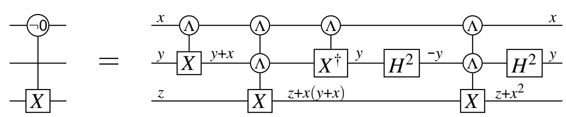
Proof. The circuit below represents the CX gate using a single borrowed ancilla.



□

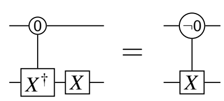
Proposition A.4. *Let $C_{|0\rangle}X$ denote the qutrit $|0\rangle$-controlled X gate. Then the gate sets $\{X, CCX, H\}$ and $\{X, C_{|0\rangle}X, H\}$ are equivalent up to a single borrowed ancilla.*

Proof. The gates X and CCX are ternary classical reversible functions. Hence, by Theorem A.2, they can both be represented by a circuit over $\{X, C_{|0\rangle}X, H\}$. Thus, every matrix that can be represented by a circuit over $\{X, CCX, H\}$ can be represented by a circuit over $\{X, C_{|0\rangle}X, H\}$. Conversely, we have



(4)

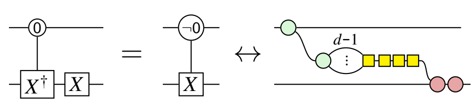
where $x, y, z \in \{0, 1, 2\}$ are input qutrit computational basis states and the basis state on a wire is updated whenever it is changed by the circuit. The $\neg 0$ on the left-hand side of Equation (4) indicates that the X gate is applied when the control is not in the state $|0\rangle$. To see that Equation (4) holds, note that $x^2 = 1$ for $x \neq 0$ so that $z + x^2$ is indeed the desired state. Moreover, we have



(5)

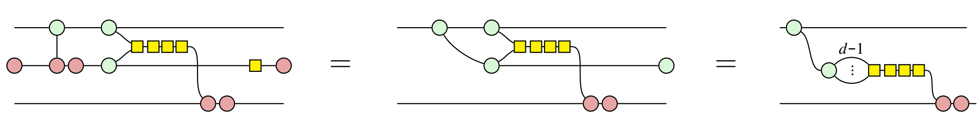
Therefore, multiplying the inverse of the circuit on the right-hand side of Equation (4) by an X gate yields a representation of the $C_{|0\rangle}X$ over the gate $\{X, CCX, H\}$ by Lemma A.3. Hence, every matrix that can be represented by a circuit over $\{X, C_{|0\rangle}X, H\}$ can be represented by a circuit over $\{X, CCX, H\}$ using a single borrowed ancilla. □

Remark A.5. The construction in Proposition A.4 can be explained (and, in fact, was found) using the qupit ZH-calculus [27]. In the qupit ZH-calculus, we have



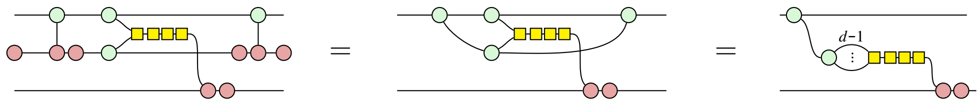
(6)

where the $d-1$ label indicates there are $d-1$ number of wires in parallel. We then get the following construction of the $|\neg 0\rangle$-controlled X gate:



(7)

The post-selected circuit in Equation (7) can be made deterministic by adding a $CX^\dagger$ gate for uncomputation, which yields a construction requiring a fresh ancilla:



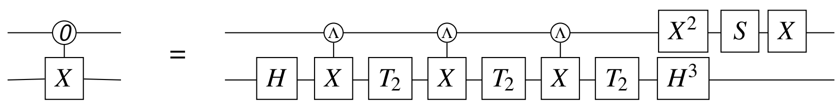
(8)

The construction is then modified in order to work with a borrowed ancilla, which yields the circuit in Equation (4).

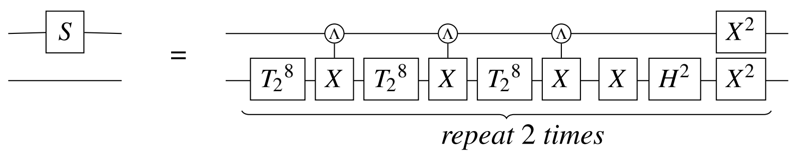
By Lemma A.3 and Proposition A.4, the gate set $\mathscr{G}_1$ is equivalent (up to a borrowed ancilla) to the gate set consisting of the X gate, the $|0\rangle$-controlled X gate, and the Hadamard gate. Hence, by Theorem A.2, any ternary classical reversible function can be represented by a circuit over $\mathscr{G}_1$ using at most one borrowed ancilla.

We now show that, when $k \geq 2$, the Clifford-cyclotomic gate set of degree 3^k is equivalent, up to a borrowed ancilla, to the Clifford+T_k gate set. We take advantage of some constructions from [8] (see, in particular, Figure 6 in [8]).

Lemma A.6. *We have:*



Lemma A.7. *We have:*



Proposition A.8. *When $k \geq 2$, the Clifford-cyclotomic gate set $\mathscr{G}_k$ is equivalent to the Clifford+T_k gate set up to a single borrowed ancilla.*

Proof. Recall that $\mathscr{G}_k = \{X, CX, CCX, H, T_k\}$ and that Clifford+$T_k = \{H, S, CX, T_k\}$. To prove the proposition, we therefore need to show that the S gate can be represented by a circuit over $\mathscr{G}_k$ and that the X and CCX gates can be represented by Clifford+T_k circuits. That the S gate can be represented by a circuit over $\mathscr{G}_k$ follows from Lemma A.7 and the fact that $T_2 = T_k^{3^{k-2}}$. That the X can be represented by a Clifford+T_k circuit simply follows from the fact that $X = H^\dagger T_2^3 H$. That the CCX gate can be represented by a Clifford+T_k circuit follows from Lemma A.6 and Theorem A.2. □

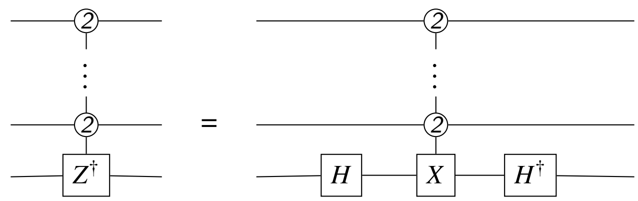
The propositions above show that there is some flexibility in the definition of Clifford-cyclotomic gate sets and, in particular, that the gate set $\{X, CX, CCX, H, T_k\}$ is by no means minimal.

A.2 Circuit Representations for the Elements of $\mathscr{S}_{3^n}$

We now provide explicit constructions for the elements of $\mathscr{S}_{3^n}$. We focus on the matrices in $\mathscr{S}_{3^n}$ where, writing each computational basis state on n qutrits as n trits, the levels are chosen to be those with the greatest value (taking the last qutrit to have the least significant trit). Indeed, these constructions can then be adapted to arbitrary levels by conjugating them by ternary classical reversible circuits using Theorem A.2 and Proposition A.4.

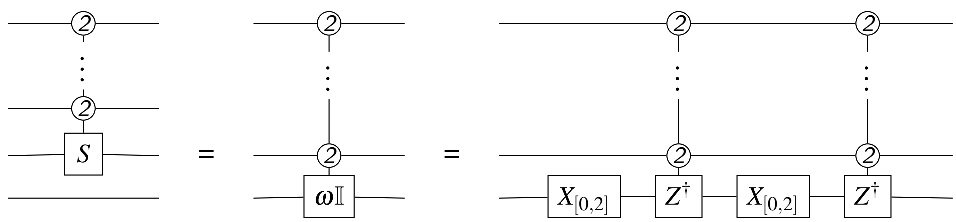
By Theorem A.2 and Proposition A.4, the multiply-controlled X gate can be expressed as a circuit over $\mathscr{G}_1$ using a single borrowed ancilla. We can therefore express the multiply-controlled Z gate as well, since $Z^\dagger = HXH^\dagger$.

Lemma A.9. *We have:*



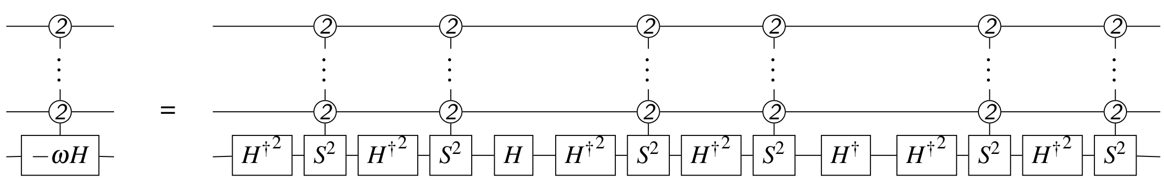
From this and the fact that $(\omega)_{[2]} = S$ when acting on a single qutrit, we can construct the 1-level matrix $(\omega)_{[x]}$ using a single borrowed ancilla.

Lemma A.10. *We have:*

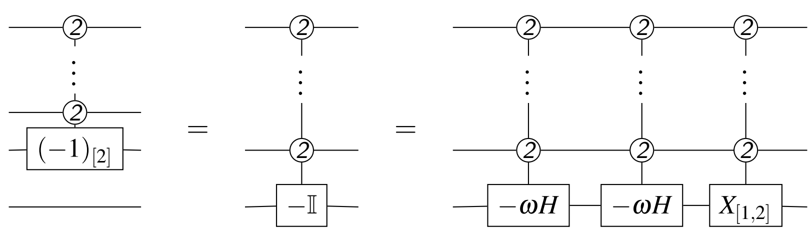


The next two lemmas let us construct the 1-level matrix $(-1)_{[x]}$. When acting on a single qutrit, this is the $(-1)_{[2]} = \mathrm{diag}(1,1,-1)$ gate. This gate is also known as the **metaplectic** gate [6, 8, 11] and in earlier work, we referred to this gate as the R gate [14].

Lemma A.11. *We have:*

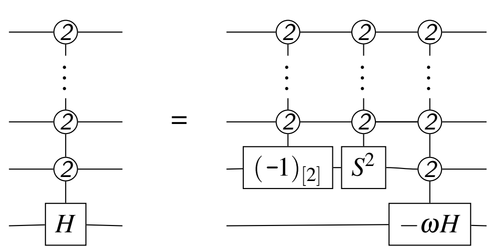


Lemma A.12. *We have:*



We can now synthesize the 3-level matrix $H_{[x_1,x_2,x_3]}$ matrix over $\mathscr{G}_1$. To do this, apply Lemma A.11 as well as the appropriate controlled global phase correction: a product of 1-level $\omega_{[x]}$ matrices and $(-1)_{[x]}$ matrices.

Lemma A.13. *We have:*



We have now constructed all of the required 1-, 2-, and 3-level matrices (up to a permutation). We can therefore prove Proposition 4.1, which we restate below, making the ancilla requirements explicit.

Proposition. *If $U \in \mathscr{S}_{3^n}$, then U can be represented by a circuit over $\mathscr{G}_1$ using at most 2 borrowed ancillae. Explicitly,*

- $(-1)_{[x]}$ *requires 2 borrowed ancillae,*
- $(\omega)_{[x]}$ *requires 1 borrowed ancillae,*
- $X_{[x_1,x_2]}$ *requires 1 borrowed ancilla, and*
- $H_{[x_1,x_2,x_3]}$ *requires 1 borrowed ancillae.*

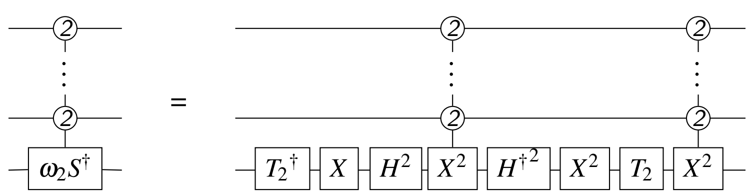
Proof. This follows from Lemmas A.3, A.10, A.12 and A.13, Proposition A.4, and Theorem A.2. □

The number of ancillae required to represent the elements of $\mathscr{S}_{3^n}$ is, to a certain extent, an artifact of the choice of gate set. For example, including the $|0\rangle$-controlled X gate to the gate set would lower the ancilla-count for some of the elements of $\mathscr{S}_{3^n}$.

The proposition above shows that the matrices that can be represented by a multiqutrit circuit over the Clifford+$(-1)_{[2]}$ gate set (also known as the **Clifford+R** or the **metaplectic** gate set) are a subset of those representable by a circuit over $\mathscr{G}_1$. At the time of writing, we do not know whether this inclusion is strict, although the conjecture in [7] that not all ternary classical reversible gates can be exactly represented over the Clifford+$(-1)_{[2]}$ gate set lends credence to this idea.

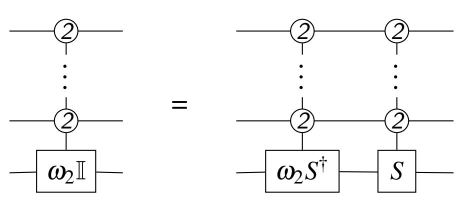
If a matrix can be represented by a circuit over $\mathscr{G}_k$, it can also be represented by a circuit over $\mathscr{G}_{k+1}$. It therefore follows from the proposition above that all of the elements of $\mathscr{S}_{3^n}$ can be represented by a circuit over $\mathscr{G}_2$. We close this appendix by showing that the 1-level matrix $(\omega_2)_{[x]}$ can be represented by a circuit over $\mathscr{G}_2$ and by providing further generalizations of the above constructions. This paves the way for a direct proof of exact synthesis for Clifford+T circuits (rather than the more indirect one using catalytic embeddings, as in Theorem 6.3). Over $\mathscr{G}_2$, the ancilla requirements are lowered, since the $|0\rangle$-controlled X gate can be represented by an ancilla-free circuit by Lemma A.6. To construct $(\omega_2)_{[x]}$, we first build a modification of $(\omega)_{[x]}$ which differs by a controlled global phase of ω_2.

Lemma A.14. *We have:*



We note that unlike the construction in Lemma A.10 which required one (additional) borrowed ancilla, this construction requires no (additional) borrowed ancillae. By combining the construction of Lemma A.14 and that of Lemma A.13, we can therefore represent $H_{[x_1,x_2,x_3]}$ without ancillae. Similarly, by combining the construction of Lemma A.14 and that of Lemma A.12, we can represent $(-1)_{[x]}$ using a single borrowed ancillae. Finally, $(\omega_2)_{[x]}$ can be constructed as in the next lemma using 2 borrowed ancillae.

Lemma A.15. *We have:*



Proposition A.16. *The 1-, 2-, and 3-level matrices $(-1)_{[x]}$, $(\omega_2)_{[x]}$, $X_{[x_1,x_2]}$, and $H_{[x_1,x_2,x_3]}$ can be represented by a circuit over $\mathscr{G}_2$ using at most 2 borrowed ancillae. Explicitly,*

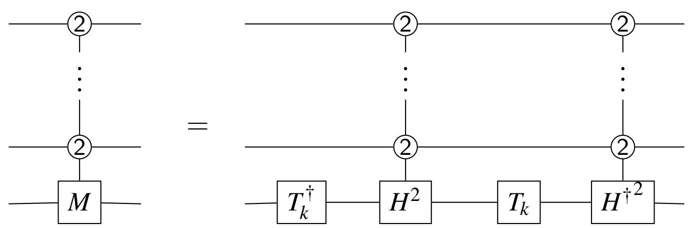
- $(-1)_{[x]}$ *requires 1 borrowed ancilla,*
- $(\omega_2)_{[x]}$ *requires 2 borrowed ancillae,*
- $X_{[x_1,x_2]}$ *requires 0 borrowed ancillae, and*
- $H_{[x_1,x_2,x_3]}$ *requires 0 borrowed ancillae.*

Proof. This follows from Lemmas A.6, A.12, A.13, A.14 and A.15 and Theorem A.2. □

We can generalize the above construction to Clifford-cyclotomic gate sets of higher degree.

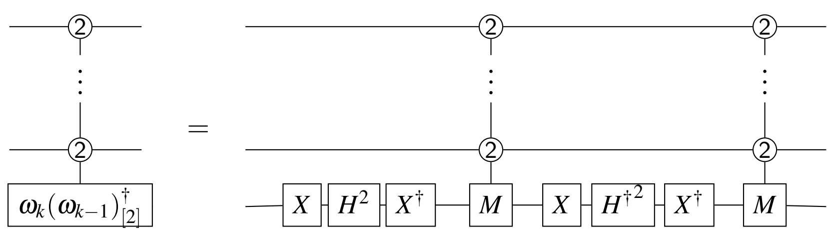
Proposition A.17. *Let $k \geq 1$. The 1-level matrix $(\omega_k)_{[x]}$ can be represented by a circuit over $\mathscr{G}_k$ using k borrowed ancillae.*

Proof. First, we build the multiply-controlled M gate, where $M = \mathrm{diag}(1, \omega_k, \omega_k^\dagger)$.



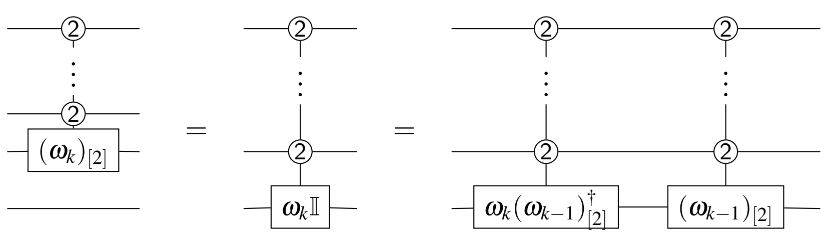
(9)

Then, we can build the multiply-controlled one-qutrit gate $\omega_k(\omega_{k-1})^\dagger_{[2]} = \omega_k \mathrm{diag}(1, 1, \omega^\dagger_{k-1})$.



(10)

Finally, we can combine this with the multiply-controlled one-qutrit gate $(\omega_{k-1})_{[2]} = \mathrm{diag}(1, 1, \omega_{k-1})$ to get $(\omega_k)_{[2\ldots 2]}$.



(11)

Since a single borrowed ancilla suffices to build (ω) and 2 borrowed ancillae suffice to build (ω_2), the above equation shows that k ancillae suffice to build (ω_k). □