Contributions to the Theory of Clifford-Cyclotomic Circuits

Linh Dinh & Neil J. Ross
Dalhousie University

Let n be a positive integer divisible by 8. The Clifford-cyclotomic gate set $\mathscr{G}_n$ consists of the Clifford gates, together with a z-rotation of order n. It is easy to show that, if a circuit over $\mathscr{G}_n$ represents a unitary matrix U, then the entries of U must lie in $\mathscr{R}_n$, the smallest subring of $\mathbb{C}$ containing $1/2$ and $\exp(2\pi i/n)$. The converse implication, that every unitary U with entries in $\mathscr{R}_n$ can be represented by a circuit over $\mathscr{G}_n$, is harder to show, but it was recently proved to be true when $n = 2^k$. In that case, $k-2$ ancillas suffice to synthesize a circuit for U, which is known to be minimal for $k = 3$, but not for larger values of k. In the present paper, we make two contributions to the theory of Clifford-cyclotomic circuits. Firstly, we improve the existing synthesis algorithm by showing that, when $n = 2^k$ and $k \geq 4$, only $k-3$ ancillas are needed to synthesize a circuit over for U, which is minimal for $k = 4$. Secondly, we extend the existing synthesis algorithm to the case of $n = 3 \cdot 2^k$ with $k \geq 3$.

1 Introduction

1.1 Background

Let n be a positive integer divisible by 8. The **Clifford-cyclotomic gate set of degree** n, which we denote by $\mathscr{G}_n$, consists of the usual **Clifford gates**

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}, \qquad S = \begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}, \qquad \text{and} \qquad CX = \begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix},$$

together with the z-rotation of order n

$$T_n = \begin{bmatrix}1 & 0\\ 0 & \zeta_n\end{bmatrix},$$

where ζ_n is the **primitive n-th root of unity** $\zeta_n = e^{2\pi i/n}$. For any n divisible by 8, $\mathscr{G}_n$ is universal for quantum computation. The gate sets $\mathscr{G}_8$ and $\mathscr{G}_{16}$ are also known as the **Clifford+T** and **Clifford+$\sqrt{T}$** gate sets, respectively. Clifford-cyclotomic circuits are important to the design of quantum algorithms [15], the theory of fault-tolerant quantum computation [5, 10], and the study of quantum complexity [14]. Because of this, they have received significant attention in the literature [2, 3, 7, 8, 9, 11, 13].

An important question in the theory of Clifford-cyclotomic circuits is that of precisely characterizing the matrices that can be exactly represented by a circuit over $\mathscr{G}_n$. Let $\mathscr{R}_n$ be the smallest subring of $\mathbb{C}$ containing $1/2$ and ζ_n. It is easy to see that, if a circuit over $\mathscr{G}_n$ represents a unitary matrix U, then the entries of U must lie in $\mathscr{R}_n$. The converse implication, that every unitary U with entries in $\mathscr{R}_n$ can be represented by a circuit over $\mathscr{G}_n$, is harder to show. Indeed, until recently, it was only known to be true for the Clifford+T gate set $\mathscr{G}_8$, as well as for a handful of adjacent gate sets [3, 8]. Recently, however, it was shown that this converse is true whenever n is a power of 2 [2]. In that case, $\log(n)-2$ ancillas suffice to synthesize a circuit for U, which is known to be minimal for $n = 8$, but not for larger powers of 2.

A. Díaz-Caro, O. Oreshkov, and A.B. Sainz (Eds.):
Quantum Physics and Logic 2025 (QPL 2025)
EPTCS ??, 2025, pp. 1–16, doi:10.4204/EPTCS.??.??

This recent exact synthesis result naturally raises two questions. Firstly, when n is a power of 2, can the number of ancillas needed to synthesize a Clifford-cyclotomic circuit of degree n be made smaller than $\log(n)-2$? Secondly, can one prove an exact synthesis result for Clifford-cyclotomic circuits whose degree is not a power of 2? In the present paper, we contribute to the theory of Clifford-cyclotomic circuits by answering both questions positively.

1.2 Contributions

Let m be a positive integer.

We prove that any 2^m-dimensional unitary U with entries in $\mathscr{R}_{16}$ can be exactly represented by an m-qubit circuit over $\mathscr{G}_{16}$ using at most 1 ancilla, which is minimal. We establish this result through a study of the effect of catalytic embeddings [1] on the determinant which may be of independent interest. We then use this result about circuits over $\mathscr{G}_{16}$ to save an ancilla in synthesizing circuits over $\mathscr{G}_{2^k}$, for $k \geq 4$.

We also prove, inspired by the results of [4], that any 2^m-dimensional unitary U with entries in $\mathscr{R}_{3\cdot 2^k}$ with $k \geq 3$ can be exactly represented by an m-qubit circuit over $\mathscr{G}_{3\cdot 2^k}$, thereby establishing a number-theoretic characterization for Clifford-cyclotomic circuits whose degree is not a power of 2.

2 Rings

We now introduce the rings that will be important in what follows and we discuss some of their properties. For further details, we encourage the reader to consult [6, 17].

We assume that rings have a multiplicative identity. If R is a ring and $u \in R$, we write $R/(u)$ for the **quotient of R by the ideal** (u). Two elements v and v' of the ring R are **congruent modulo** u, if their difference is a multiple of u, that is, if $v - v' \in (u)$. In that case, we write $v \equiv_u v'$, or $v \equiv v' \pmod{u}$. The relation $\equiv_u$ is an equivalence relation on R and the elements of $R/(u)$ are precisely the equivalence classes of elements of R under the relation $\equiv_u$. We sometimes refer to these equivalence classes as **residues**.

2.1 Cyclotomic integers

We write ζ_n for the **primitive n-th root of unity** $\zeta_n = e^{2\pi i/n}$. The **ring of cyclotomic integers** $\mathbb{Z}[\zeta_n]$ is the smallest subring of $\mathbb{C}$ that contains ζ_n. Since $\zeta_n^\dagger = \zeta_n^{n-1}$, the ring $\mathbb{Z}[\zeta_n]$ is closed under complex conjugation.

Let φ denote **Euler's totient function**, so that $\varphi(n)$ counts the integers in $\{1,\ldots,n\}$ that are relatively prime to n. The ring $\mathbb{Z}[\zeta_n]$ can be characterized as

$$\mathbb{Z}[\zeta_n] = \left\{ a_0 + a_1\zeta_n + a_2\zeta_n^2 + \cdots + a_{\varphi(n)-1}\zeta_n^{\varphi(n)-1} \mid a_0,\ldots,a_{\varphi(n)-1} \in \mathbb{Z} \right\}. \tag{1}$$

Every element $u \in \mathbb{Z}[\zeta_n]$ can be uniquely expressed as a $\mathbb{Z}$-linear combination of powers of ζ_n as in Equation (1). That is, we have

$$a_0 + a_1\zeta_n + \cdots + a_{\varphi(n)-1}\zeta_n^{\varphi(n)-1} = a'_0 + a'_1\zeta_n + \cdots + a'_{\varphi(n)-1}\zeta_n^{\varphi(n)-1}$$

if and only if $a_j = a'_j$ for $0 \leq j \leq \varphi(n)-1$.

We will be interested in two families of rings of cyclotomic integers: the one corresponding to $n = 2^k$, and the one corresponding to $n = 3\cdot 2^k$. For $k \leq k'$, we have $\mathbb{Z}[\zeta_{2^k}] \subseteq \mathbb{Z}[\zeta_{2^{k'}}]$ (resp. $\mathbb{Z}[\zeta_{3\cdot 2^k}] \subseteq \mathbb{Z}[\zeta_{3\cdot 2^{k'}}]$).

Moreover, for $k \geq 1$, every element $u \in \mathbb{Z}[\zeta_{2^{k+1}}]$ (resp. $u \in \mathbb{Z}[\zeta_{3\cdot 2^{k+1}}]$) can be uniquely written as $u = a + b\zeta_{2^{k+1}}$ (resp. $u = a + b\zeta_{3\cdot 2^{k+1}}$), with $a, b \in \mathbb{Z}[\zeta_{2^k}]$ (resp. $a, b \in \mathbb{Z}[\zeta_{3\cdot 2^k}]$).

We define the ring $\mathscr{R}_n$ as the smallest subring of $\mathbb{C}$ that contains $1/2$ and ζ_n. The ring $\mathscr{R}_n$ can be characterized as in Equation (1). Indeed, we have

$$\mathscr{R}_n = \left\{ a_0 + a_1\zeta_n + a_2\zeta_n^2 + \cdots + a_{\varphi(n)-1}\zeta_n^{\varphi(n)-1} \mid a_0, \ldots, a_{\varphi(n)-1} \in \mathbb{D} \right\}, \tag{2}$$

where $\mathbb{D} = \{a/2^\ell \mid a \in \mathbb{Z} \text{ and } \ell \in \mathbb{N}\}$ is the ring of **dyadic fractions**. Every element $u \in \mathscr{R}_n$ can be uniquely expressed as in Equation (2).

If n is divisible by 8, then $n = 8d$, so that $\zeta_n^{2d} = \zeta_4 = i$, $\zeta_n^d = \zeta_8$, and $\zeta_n^d + \zeta_n^{-d} = \zeta_8 - \zeta_8^\dagger = \sqrt{2}$. Hence, in that case, we have $i \in \mathscr{R}_n$ and $1/\sqrt{2} \in \mathscr{R}_n$, which implies that the entries of the gates H, S, CX, and T_n belong to $\mathscr{R}_n$. Thus, whenever n is divisible by 8, any matrix that can be represented by a circuit over $\mathscr{G}_n$ has entries in $\mathscr{R}_n$.

2.2 The ring $\mathbb{Z}[\zeta_{12}]$

The ring $\mathbb{Z}[\zeta_{12}]$ will play an important role in Section 7. We now record some of its relevant properties. We know from Equation (1) that

$$\mathbb{Z}[\zeta_{12}] = \left\{ a_0 + a_1\zeta_{12} + a_2\zeta_{12}^2 + a_3\zeta_{12}^3 \mid a_0, a_1, a_2, a_3 \in \mathbb{Z} \right\}.$$

We define $\delta \in \mathbb{Z}[\zeta_{12}]$ as $\delta = 1 + \zeta_{12}^3 = 1 + i$. The cyclotomic integer δ is prime in $\mathbb{Z}[\zeta_{12}]$ and the prime factorization of 2 in $\mathbb{Z}[\zeta_{12}]$ is given by

$$2 = (1+i)^2(-i) = \delta^2(-i). \tag{3}$$

Now consider an element $u \in \mathscr{R}_{12}$. By Equations (2) and (3), we can write u as $u = u'/\delta^\ell$, with $u' \in \mathbb{Z}[\zeta_{12}]$ and $\ell \in \mathbb{N}$. The smallest such ℓ is called the **least denominator exponent of** u and is denoted $\operatorname{lde}(u)$. Equivalently, $\operatorname{lde}(u)$ is the smallest $\ell \in \mathbb{N}$ such that $\delta^\ell u \in \mathbb{Z}[\zeta_{12}]$. More generally, if M is a matrix (or a vector) with entries in $\mathscr{R}_{12}$, then $\operatorname{lde}(M)$ is the smallest ℓ such that $\delta^\ell M$ is a matrix (or a vector) over $\mathbb{Z}[\zeta_{12}]$.

Proposition 2.1. *We have:*

- $\mathbb{Z}[\zeta_{12}]/(2) = \{a_0 + a_1\zeta_{12} + a_2\zeta_{12}^2 + a_3\zeta_{12}^3 \mid a_0, a_1, a_2, a_3 \in \{0,1\}\}$, *and*
- $\mathbb{Z}[\zeta_{12}]/(\delta) = \{0, 1, \zeta_{12}, \zeta_{12}^2\}$.

Proof. Let $u = a_0 + a_1\zeta_{12} + a_2\zeta_{12}^2 + a_3\zeta_{12}^3 \in \mathbb{Z}[\zeta_{12}]$. Since $2 \equiv 0 \pmod 2$, the coefficients a_0, a_1, a_2, and a_3 can be chosen in $\{0,1\}$, which establishes the first item in the proposition. For the second item, notice that, since $\delta = 1 + \zeta_{12}^3$, we have $1 + \zeta_{12}^3 \equiv 0 \pmod \delta$ so that $\zeta_{12}^3 \equiv -1 \equiv 1 \pmod \delta$. This, together with the fact that $2 \equiv 0 \pmod \delta$, implies that any $u \in \mathbb{Z}[\zeta_{12}]/(\delta)$ can be written as $u = a_0 + a_1\zeta_{12} + a_2\zeta_{12}^2$ with $a_0, a_1, a_2 \in \{0,1\}$. Since we have the cyclotomic relation $\zeta_{12}^4 - \zeta_{12}^2 + 1 = 0$, we get $\zeta_{12}^2 \equiv \zeta_{12} + 1 \pmod \delta$, from which the second item in the proposition then follows. □

The **quadratic integer ring** $\mathbb{Z}[\sqrt{3}]$ is the smallest subring of $\mathbb{C}$ containing $\mathbb{Z}$ and $\sqrt{3}$. The elements of $\mathbb{Z}[\sqrt{3}]$ can be characterized as $\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\}$ and every element of $\mathbb{Z}[\sqrt{3}]$ can be uniquely written as such a $\mathbb{Z}$-linear combination of 1 and $\sqrt{3}$. Because $\sqrt{3} = \zeta_{12} + \zeta_{12}^\dagger$, we have $\mathbb{Z}[\sqrt{3}] \subseteq$

$u \pmod{\delta}$	$u \pmod 2$	$u^\dagger u \pmod 2$
0	0	0
0	$1+\zeta_{12}^3$	0
0	$1+\zeta_{12}+\zeta_{12}^2$	0
0	$\zeta_{12}+\zeta_{12}^2+\zeta_{12}^3$	0
1	1	1
1	ζ_{12}^3	1
1	$\zeta_{12}+\zeta_{12}^2 \equiv_2 \zeta_{12}(1+\zeta_{12})$	$\sqrt{3}$
1	$1+\zeta_{12}+\zeta_{12}^2+\zeta_{12}^3 \equiv_2 \zeta_{12}^4(1+\zeta_{12})$	$\sqrt{3}$
ζ_{12}	ζ_{12}	1
ζ_{12}	$1+\zeta_{12}^2 \equiv_2 \zeta_{12}^4$	1
ζ_{12}	$\zeta_{12}^2+\zeta_{12}^3 \equiv_2 \zeta_{12}^2(1+\zeta_{12})$	$\sqrt{3}$
ζ_{12}	$1+\zeta_{12}+\zeta_{12}^3 \equiv_2 \zeta_{12}^5(1+\zeta_{12})$	$\sqrt{3}$
ζ_{12}^2	ζ_{12}^2	1
ζ_{12}^2	$1+\zeta_{12}$	$\sqrt{3}$
ζ_{12}^2	$1+\zeta_{12}^2+\zeta_{12}^3 \equiv_2 \zeta_{12}^3(1+\zeta_{12})$	$\sqrt{3}$
ζ_{12}^2	$\zeta_{12}+\zeta_{12}^3 \equiv_2 \zeta_{12}^5$	1

Table 1: The possible residues for $u \in \mathbb{Z}[\zeta_{12}]$ modulo δ and 2, as well as those for $u^\dagger u$ modulo 2.

$\mathbb{Z}[\zeta_{12}]$. Since $\zeta_{12}^6 = -1$ and $\zeta_{12}^4 - \zeta_{12}^2 + 1 = 0$, we have $\zeta_{12}^\dagger = \zeta_{12} - \zeta_{12}^3$. It can then be verified by direct computation that if $u = a + b\zeta_{12} + c\zeta_{12}^2 + d\zeta_{12}^3 \in \mathbb{Z}[\zeta_{12}]$, then

$$u^\dagger u = ((a^2+c^2+ac)+(b^2+d^2+bd)) + (ab+bc+cd)\sqrt{3}. \tag{4}$$

In particular, the Euclidean norm of $u \in \mathbb{Z}[\zeta_{12}]$ belongs to $\mathbb{Z}[\sqrt{3}]$, i.e., if $u \in \mathbb{Z}[\zeta_{12}]$, then $u^\dagger u \in \mathbb{Z}[\sqrt{3}]$.

Lemma 2.2. *We have:*

- *if $u \in \mathbb{Z}[\zeta_{12}]$ and $u \equiv_\delta 0$, then $u^\dagger u \equiv_2 0$,*
- *if $u \in \mathbb{Z}[\zeta_{12}]$ and $u \not\equiv_\delta 0$, then $u^\dagger u \equiv_2 1$ or $u^\dagger u \equiv_2 \sqrt{3}$, and*
- *if $u, v \in \mathbb{Z}[\zeta_{12}]$ and $u^\dagger u \equiv_2 v^\dagger v$, then $u \equiv_2 \zeta_{12}^m v$ for some integer m.*

Proof. By inspection of Table 1, which lists the possible residues of $u \in \mathbb{Z}[\zeta_{12}]$ modulo δ and 2, as well as the possible residues of $u^\dagger u$ modulo 2. The calculations leading to the construction of Table 1 can be verified using the congruences from the proof of Proposition 2.1, in addition to the following facts: $\delta^\dagger\delta = 2$, $(1+\zeta_{12})^\dagger(1+\zeta_{12}) = 2+\sqrt{3} \equiv_2 \sqrt{3}$, and $\zeta_{12}^4 \equiv_2 \zeta_{12}^2 + 1$. □

3 Matrices and circuits

Let R be a commutative ring. We write $\mathrm{M}(R)$ for the collection of all square matrices with entries in R, and $\mathrm{M}_m(R)$ for the ring of $m \times m$ matrices in R. When R is a subring of $\mathbb{C}$ that is closed under complex conjugation, we write $\mathrm{U}(R)$ for the collection of all unitary matrices with entries in R, and $\mathrm{U}_m(R)$ for the group of $m \times m$ unitary matrices with entries in R.

We now introduce certain matrices which will be useful in Section 7. Let $c \in \mathbb{C}$. For $0 \leq j \leq m-1$, the **one-level operator of type** c is the $m \times m$ matrix $c_{[j]}$ defined as

$$c_{[j]} = \begin{array}{c c} & \begin{array}{ccc} \cdots & j & \cdots \end{array} \\ \begin{array}{c} \vdots \\ j \\ \vdots \end{array} & \begin{bmatrix} I & 0 & 0 \\ 0 & c & 0 \\ 0 & 0 & I \end{bmatrix} \end{array}$$

Similarly, let $M \in \mathrm{M}_2(\mathbb{C})$. For $0 \leq j < j' \leq m-1$, the **two-level operator of type** M is the $m \times m$ matrix $M_{[j,j']}$ defined as

$$M_{[j,j']} = \begin{array}{c c} & \begin{array}{ccccc} \cdots & j & \cdots & j' & \cdots \end{array} \\ \begin{array}{c} \vdots \\ j \\ \vdots \\ j' \\ \vdots \end{array} & \begin{bmatrix} I & 0 & 0 & 0 & 0 \\ 0 & M_{1,1} & 0 & M_{1,2} & 0 \\ 0 & 0 & I & 0 & 0 \\ 0 & M_{2,1} & 0 & M_{2,2} & 0 \\ 0 & 0 & 0 & 0 & I \end{bmatrix} \end{array}$$

The one-level operator $c_{[j]}$ acts on an m-dimensional vector $\mathbf{u}$ by scaling its j-th component by c and leaving the remaining components unchanged. The two-level operator $M_{[j,j']}$ similarly acts as M on the j-th and j'-th components of $\mathbf{u}$ and leaves the remaining components unchanged. Note that if $|c| = 1$ then $c_{[j]}$ is unitary, and that if $M \in \mathrm{U}_2(\mathbb{C})$, then $M_{[j,j']}$ is unitary.

We close this section by recalling the existence of some well-known circuit constructions which will be useful in what follows. As mentioned in Section 1, when n is divisible by 8, the gate set $\mathscr{G}_n$ subsumes the Clifford+T gate set. Hence, any matrix that can be represented by a Clifford+T circuit can also be represented by a circuit over $\mathscr{G}_n$. As a consequence, the one-level operators of type ζ_n and the two-level operators of type X and H can be represented exactly over the gate set $\mathscr{G}_n$ using a single ancilla.

Theorem 3.1 (Giles & Selinger)**.** *The one- and two-level operators of type ζ_n, X, and H can each be exactly represented by a circuit over $\mathscr{G}_n$ using at most one ancilla.*

Proof. Circuit constructions for the one- and two-level operators of type ζ_8, X, and H using a single ancilla can be found in [8, Section 5]. To obtain a circuit for the one-level operator of type ζ_n, it suffices to replace T with T_n where appropriate. □

4 Determinants

The **determinant** is an important function on matrices. We will be interested in the determinant of certain block matrices.

Let R be a commutative ring and let M be an $m \times m$ matrix with entries in R. The **determinant of** M **with respect to** R, denoted by $\det_R(M)$, is defined as

$$\det_R(M) = \sum_{\sigma \in S_m} \operatorname{sgn}(\sigma) \prod_{j=1}^{m} M_{j,\sigma(j)},$$

where S_m is the symmetric group of degree m and $\operatorname{sgn}(\sigma)$ is the sign of the permutation $\sigma \in S_m$. If R is a subring of some ring R' and M is a matrix with entries in R, we have $\det_R(M) = \det_{R'}(M)$. For simplicity, when the ring R in which the determinant is to be computed is clear from context, we sometimes write $\det(M)$ rather than $\det_R(M)$. The determinant is multiplicative, in the sense that for matrices M and M' over R of compatible dimensions, we have $\det_R(MM') = \det_R(M)\det_R(M')$. Moreover, if M is a complex unitary matrix, then $|\det_{\mathbb{C}}(M)| = 1$.

If $\phi : R \to R'$ is a ring homomorphism, then the entrywise application of ϕ is a ring homomorphism $\mathrm{M}_m(R) \to \mathrm{M}_m(R')$. By a slight abuse of notation, we use the symbol ϕ to denote both the homomorphism $R \to R'$ and its entrywise extension $\mathrm{M}(R) \to \mathrm{M}(R')$. Now consider a matrix M over R. Since ϕ is a ring homomorphism and the determinant is a polynomial in the matrix entries, we have

$$\phi(\det_R(M)) = \phi\left(\sum_{\sigma\in S_m} \mathrm{sgn}(\sigma)\prod_{j=1}^{m} M_{j,\sigma(j)}\right) = \sum_{\sigma\in S_m} \mathrm{sgn}(\sigma)\prod_{j=1}^{m} \phi\left(M\right)_{j,\sigma(j)} = \det_{R'}(\phi(M)). \tag{5}$$

Let R be a commutative ring and let R' be a commutative subring of $\mathrm{M}_m(R)$. Now consider a matrix M in $\mathrm{M}_{m'}(R')$. The matrix M is an $m' \times m'$ block matrix whose blocks are $m \times m$ matrices over R. We can therefore compute the determinant of M with respect to R', and then the determinant of the resulting matrix with respect to R. Alternatively, we can "open" the blocks and think of M as an $mm' \times mm'$ matrix over R to directly compute the determinant of M with respect to R. The following theorem, whose proof can be found in [16, Theorem 1], states that these two quantities are equal.

Theorem 4.1 (Silvester)**.** *Let R be a commutative ring, let R' be a commutative subring of* $\mathrm{M}_m(R)$*, and let $M \in \mathrm{M}_{m'}(R')$. Then*

$$\det_R M = \det_R(\det_{R'} M).$$

It will be convenient for us to consider a variant of Theorem 4.1 where R' is not a subring of $\mathrm{M}_m(R)$ but simply related to one.

Corollary 4.2. *Let R and R' be two commutative rings, let $\phi : R' \to \mathrm{M}_m(R)$ be a ring homomorphism, and let $M \in \mathrm{M}_{m'}(R')$. Then*

$$\det_R(\phi(M)) = \det_R(\phi(\det_{R'}(M))).$$

Proof. Let $Q = \phi[R']$ be the direct image of R' under ϕ. Then Q is a commutative subring of $\mathrm{M}_m(R)$, since R' is commutative. Hence, by Theorem 4.1 and Equation (5),

$$\det_R(\phi(M)) = \det_R(\det_Q(\phi(M))) = \det_R(\phi(\det_{R'}(M))),$$

as desired. □

5 Catalytic embeddings

We now introduce **catalytic embeddings** [1, 2, 9]. Let $\mathscr{U}$ and $\mathscr{V}$ be two sets of unitary matrices. An m-**dimensional catalytic embedding** from $\mathscr{U}$ into $\mathscr{V}$ is a pair $(\phi, \mathbf{c})$ where $\phi : \mathscr{U} \to \mathscr{V}$ is a function and $\mathbf{c} \in \mathbb{C}^m$ is a unit vector such that

1. If $U \in \mathscr{U}$ has dimension d, then $\phi(U) \in \mathscr{V}$ has dimension md, and
2. For any $\mathbf{u} \in \mathbb{C}^d$, $\phi(U)(\mathbf{u}\otimes\mathbf{c}) = (U\mathbf{u})\otimes\mathbf{c}$.

We often write $(\phi, \mathbf{c}) : \mathscr{U} \to \mathscr{V}$ to indicate that $(\phi, \mathbf{c})$ is a catalytic embedding from $\mathscr{U}$ to $\mathscr{V}$. The composition of an m-dimensional catalytic embedding $(\phi, \mathbf{c}) : \mathscr{U} \to \mathscr{V}$ and an m'-dimensional catalytic embedding $(\phi', \mathbf{c}') : \mathscr{V} \to \mathscr{W}$ is the mm'-dimensional catalytic embedding $(\phi' \circ \phi, \mathbf{c} \otimes \mathbf{c}') : \mathscr{U} \to \mathscr{W}$. The catalytic embedding $(\mathrm{id}_{\mathscr{U}}, 1) : \mathscr{U} \to \mathscr{U}$ acts as the identity for this notion of composition.

We now discuss two specific catalytic embeddings which will be important in the rest of this paper. Let $k \geq 2$ and define the matrix Λ_k and the vector $\mathbf{c}_k$ by

$$\Lambda_k = \begin{bmatrix} 0 & 1 \\ \zeta_{2^{k-1}} & 0 \end{bmatrix} \qquad \text{and} \qquad \mathbf{c}_k = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ \zeta_{2^k} \end{bmatrix}.$$

We can use Λ_k and $\mathbf{c}_k$ to define a catalytic embedding, following [1, 2]. Consider a matrix $M \in \mathrm{M}(\mathscr{R}_{2^k})$. Then M can be uniquely written as $M = A + B\zeta_{2^k}$, for some $A, B \in \mathrm{M}(\mathscr{R}_{2^{k-1}})$, so that we can construct the matrix $A \otimes I_2 + B \otimes \Lambda_k \in \mathrm{M}(\mathscr{R}_{2^{k-1}})$. It can be shown that the assignment

$$A + B\zeta_{2^k} \longmapsto A \otimes I_2 + B \otimes \Lambda_k \tag{6}$$

defines, for every m, a ring homomorphism $\phi_k : \mathrm{M}_m(\mathscr{R}_{2^k}) \to \mathrm{M}_{2m}(\mathscr{R}_{2^{k-1}})$. Moreover, we have $\phi_k(M^\dagger) = \phi_k(M)^\dagger$ for every M, so that ϕ_k restricts to a group homomorphism $\mathrm{U}_m(\mathscr{R}_{2^k}) \to \mathrm{U}_{2m}(\mathscr{R}_{2^{k-1}})$. Now let $\mathbf{u}$ be an arbitrary vector. Then

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

The pair $(\phi_k, \mathbf{c}_k)$ is therefore a catalytic embedding. For future reference, we record this fact in the proposition below.

Proposition 5.1. *Let $k \geq 2$. Then $(\phi_k, \mathbf{c}_k)$ is a 2-dimensional catalytic embedding from $\mathrm{U}(\mathscr{R}_{2^k})$ to $\mathrm{U}(\mathscr{R}_{2^{k-1}})$.*

By identifying $\mathrm{M}_1(\mathscr{R}_{2^k})$ with $\mathscr{R}_{2^k}$, we can think of the function ϕ_k, when restricted to $\mathscr{R}_{2^k}$ as a ring homomorphism $\mathscr{R}_{2^k} \to \mathrm{M}_2(\mathscr{R}_{2^{k-1}})$. The function ϕ_k as defined by Equation (6) is then the entrywise extension of ϕ_k from $\mathscr{R}_{2^k}$ to $\mathrm{M}(\mathscr{R}_{2^k})$. We can therefore use Corollary 4.2 to get, for $U \in \mathrm{U}(\mathscr{R}_{2^k})$, an expression for the determinant of $\phi_k(U)$.

Corollary 5.2. *Let $k \geq 2$ and let $U \in \mathrm{U}_n(\mathscr{R}_{2^k})$. Then we have*

$$\det_{\mathscr{R}_{2^{k-1}}}(\phi_k(U)) = \det_{\mathscr{R}_{2^{k-1}}}(\phi_k(\det_{\mathscr{R}_{2^k}}(U))).$$

In other words, Corollary 5.2 states that, for $U \in \mathrm{U}(\mathscr{R}_{2^k})$, to compute the determinant of $\phi_k(U)$ over $\mathscr{R}_{2^{k-1}}$, one can first compute the determinant u of U over $\mathscr{R}_{2^k}$, and then compute the determinant of $\phi_k(u)$ over $\mathscr{R}_{2^{k-1}}$.

Remark 5.3. The function $\det_{\mathscr{R}_{2^{k-1}}} \circ \phi_k : \mathscr{R}_{2^k} \to \mathscr{R}_{2^{k-1}}$ is known in number theory as the **relative norm** of the field extension $\mathbb{Q}(\zeta_{2^k})/\mathbb{Q}(\zeta_{2^{k-1}})$, and is often denoted by $\mathrm{N}_{\mathbb{Q}(\zeta_{2^k})/\mathbb{Q}(\zeta_{2^{k-1}})}$. Corollary 5.2 therefore states that the determinant (over $\mathscr{R}_{2^{k-1}}$) of $\phi_k(U)$ is the relative norm of the determinant (over $\mathscr{R}_{2^k}$) of U, i.e., $\det_{\mathscr{R}_{2^{k-1}}} \circ \phi_k = \mathrm{N}_{\mathbb{Q}(\zeta_{2^k})/\mathbb{Q}(\zeta_{2^{k-1}})} \circ \det_{\mathscr{R}_{2^k}}$.

We close this section by introducing a second catalytic embedding. The construction is essentially the same as in the definition of $(\phi_k, \mathbf{c}_k)$. We define the matrix Γ_k and the vector $\mathbf{d}_k$ by

$$\Gamma_k = \begin{bmatrix} 0 & 1 \\ \zeta_{3\cdot 2^{k-1}} & 0 \end{bmatrix} \qquad \text{and} \qquad \mathbf{d}_k = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ \zeta_{3\cdot 2^k} \end{bmatrix}.$$

We then define the function $\psi_k : \mathrm{M}(\mathscr{R}_{3\cdot 2^k}) \to \mathrm{M}(\mathscr{R}_{3\cdot 2^{k-1}})$ by

$$\psi_k(A + B\zeta_{2^k}) = A \otimes I_2 + B \otimes \Gamma_k.$$

Reasoning as above, we obtain the proposition below.

Proposition 5.4. *Let $k \geq 2$. Then $(\psi_k, \boldsymbol{d}_k)$ is a 2-dimensional catalytic embedding from $\mathrm{U}(\mathscr{R}_{3\cdot 2^k})$ to $\mathrm{U}(\mathscr{R}_{3\cdot 2^{k-1}})$.*

An analogue of Corollary 5.2 holds for $(\psi_k, \mathbf{d}_k)$, but we omit it here, since it will not be useful for our purposes.

6 Clifford-cyclotomic circuits of degree 2^k

We now turn to the exact synthesis of circuits for matrices with entries in the ring $\mathscr{R}_{2^k}$. We will take advantage of the following result, which was established in [8, Lemma 7].

Theorem 6.1 (Giles & Selinger)**.** *If U is a $2^m \times 2^m$ matrix with entries in $\mathscr{R}_8$ and $\det(U) = 1$, then U can be exactly represented by an ancilla-free m-qubit circuit over $\mathscr{G}_8$.*

Let U be a unitary matrix with entries in $\mathscr{R}_{16}$. Then the determinant of U over $\mathscr{R}_{16}$ is an element of $\mathscr{R}_{16}$ of norm 1. The next lemma shows that this determinant must be a power of ζ_{16}. The proof is relegated to Appendix A.

Lemma 6.2. *Let $u \in \mathscr{R}_{16}$ be such that $|u| = 1$. Then $u = \zeta_{16}^\ell$ for some $0 \leq \ell \leq 15$.*

In order to save an ancilla in synthesizing circuits over $\mathscr{G}_{16}$ our strategy is the following. Consider an m-qubit unitary U with entries in $\mathscr{R}_{16}$. By Lemma 6.2, the determinant of U is a power of ζ_{16}. Hence, multiplying U by an appropriate power of the one-level operator of type ζ_{16} if needed, we can assume without loss of generality that U has determinant 1. By Corollary 5.2, $\phi_4(U)$ is then an $(m+1)$-qubit unitary of determinant 1 with entries in $\mathscr{R}_8$ and it can thus be represented by an $(m+1)$-qubit circuit by Theorem 6.1.

Theorem 6.3. *A $2^m \times 2^m$ matrix U can be exactly represented by an m-qubit circuit over $\mathscr{G}_{16}$ if and only if $U \in \mathrm{U}_{2^m}(\mathscr{R}_{16})$. Furthermore, a single ancilla suffices to synthesize a circuit for U.*

Proof. The left-to-right implication follows immediately from the fact that all the elements of $\mathscr{G}_{16}$ belong to $\mathrm{U}(\mathscr{R}_{16})$. For the right-to-left implication, let $U \in \mathrm{U}_{2^m}(\mathscr{R}_{16})$. Since U is unitary, $\det_{\mathscr{R}_{16}}(U)$ is an element of $\mathscr{R}_{16}$ of norm 1. Thus, by Lemma 6.2, we have that $\det_{\mathscr{R}_{16}}(U) = \zeta_{16}^\ell$ for some $0 \leq \ell \leq 15$. Now let P be the fully-controlled phase gate

$$P = \mathrm{diag}(1, 1, ..., 1, \zeta_{16}^\ell),$$

and let $V = P^\dagger U$. Note that $\det_{\mathscr{R}_{16}}(V) = \det_{\mathscr{R}_{16}}(P^\dagger)\det_{\mathscr{R}_{16}}(U) = 1$. Now consider the catalytic embedding $(\phi_4, \mathbf{c}_4)$ defined in Section 5. By Corollary 5.2, we have

$$\det_{\mathscr{R}_8}(\phi_4(V)) = \det_{\mathscr{R}_8}(\phi_4(\det_{\mathscr{R}_{16}}(V))) = \det_{\mathscr{R}_8}(I_2) = 1.$$

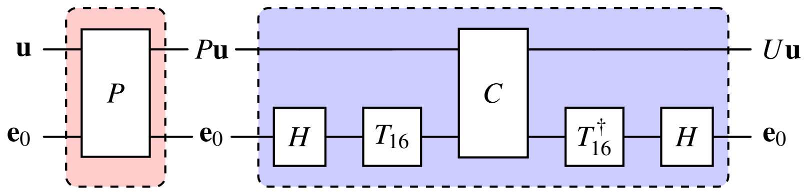

Figure 1: The circuit constructed in the proof of Theorem 6.3.

Hence, $\phi_4(V) \in \mathrm{U}_{2^{m+1}}(\mathscr{R}_8)$ and $\det_{\mathscr{R}_8}(\phi_4(V)) = 1$ so that, by Theorem 6.1, $\phi_4(V)$ can be represented by an ancilla-free circuit C over $\mathscr{G}_8$. Now let D be the circuit $D = (I_m \otimes (T_{16}H))^\dagger \circ C \circ (I_m \otimes (T_{16}H))$ over $\mathscr{G}_{16}$. Then $T_{16}H\mathbf{e}_0 = \mathbf{c}_4$, so that, for an arbitrary $\mathbf{u}$, we have:

$$\begin{aligned} D(\mathbf{u}\otimes\mathbf{e}_0) &= (I_m \otimes (T_{16}H))^\dagger \circ C \circ (I_m \otimes (T_{16}H))(\mathbf{u}\otimes\mathbf{e}_0) \\ &= (I_m \otimes (T_{16}H))^\dagger \circ C(\mathbf{u}\otimes\mathbf{c}_4) \\ &= (I_m \otimes (T_{16}H))^\dagger \circ \phi_4(V)(\mathbf{u}\otimes\mathbf{c}_4) \\ &= (I_m \otimes (T_{16}H))^\dagger ((V\mathbf{u})\otimes\mathbf{c}_4) \\ &= (V\mathbf{u})\otimes\mathbf{e}_0. \end{aligned}$$

Hence D exactly represents V over $\mathscr{G}_{16}$ using a single ancilla. Moreover, P can also be represented by a circuit over $\mathscr{G}_{16}$ using a single ancilla. Indeed, this follows from Theorem 3.1, since P is (a power of) a one-level operator of type ζ_{16}. Thus, the unitary U can be represented using a single ancilla as well. □

The circuit constructed in the proof of Theorem 6.3 is depicted in Figure 1. We note that, if U is a unitary with entries in $\mathscr{R}_{16}$ and the dimension of U is larger than 4, then an ancilla is necessary to synthesize a matrix for a U. As a result, the construction of Theorem 6.3 uses the minimal number of ancillas (in the worst case).

Corollary 6.4. *Let $k \geq 4$. A $2^m \times 2^m$ matrix U can be exactly represented by an m-qubit circuit over $\mathscr{G}_{2^k}$ if and only if $U \in \mathrm{U}_{2^m}(\mathscr{R}_{2^k})$. Furthermore, $k-3$ ancillas suffice to synthesize a circuit for U.*

Proof. By induction, using Theorem 6.3 as the base case, and a construction similar to the one given in Figure 1 in the inductive step. □

7 Clifford-cyclotomic circuits of degree $3 \cdot 2^k$

We now turn to the exact synthesis of circuits for matrices with entries in the ring $\mathscr{R}_{3\cdot 2^k}$. Our strategy is to first prove that every matrix with entries in $\mathscr{R}_{24}$ can be represented by a circuit over $\mathscr{G}_{24}$, and to then use an inductive argument like the one used in proving Corollary 6.4. In order to establish the result for $n = 24$, we start by showing that every unitary matrix with entries in $\mathscr{R}_{12}$ can be factored as a product of convenient generators.

7.1 Generating $\mathrm{U}_n(\mathscr{R}_{12})$

To generate $\mathrm{U}_n(\mathscr{R}_{12})$, we use one-level operators of type ζ_{12} and two-level operators of type X and H', where

$$H' = \zeta_8 H = \frac{\delta}{2}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

Note that $H' \in \mathrm{U}(\mathscr{R}_{12})$. We follow [3, 8] and first show that a unit vector with entries in $\mathscr{R}_{12}$ can be mapped to a standard basis vector using one- and two-level operators of type ζ_{12}, X, and H'. To this end, we proceed by induction on the least denominator exponent of the vector.

Lemma 7.1. *Let a and b be integers, at least one of which is nonzero. Then $a^2+b^2+ab \geq 1$, and equality is achieved exactly when (a,b) is one of $(\pm 1,0)$, $(0,\pm 1)$, or $(\pm 1,\mp 1)$.*

Proof. First notice that if $a \neq 0$ and $b=0$, then $a^2+b^2+ab = a^2 \geq 1$, since $a \in \mathbb{Z}$. A similar argument applies when $a=0$ and $b\neq 0$. Equality in the first of these cases happens exactly when $a=\pm 1$ and $b=0$, while equality in the second of these cases happens exactly when $a=0$ and $b=\pm 1$. Now suppose that a and b are both nonzero, and assume, without loss of generality, that $|a| \geq |b|$. We then have $a^2 \geq |ab|$, so that $a^2+ab \geq 0$. Hence,

$$a^2+ab+b^2 \geq b^2 \geq 1,$$

since $b \in \mathbb{Z}$. Equality in this case happens exactly when $b^2=1$ and $a^2+ab=0$ which, in turn, happens exactly when $b=\pm 1$ and $a=\mp 1$. □

Lemma 7.2. *If $\boldsymbol{u}$ is an m-dimensional unit vector with entries in $\mathscr{R}_{12}$ and $\mathrm{lde}(\boldsymbol{u})=0$, then, for any $0 \leq j \leq m-1$, there exists a sequence $G_1,\ldots,G_q$ of one- and two-level operators of type ζ_{12}, X, and H' such that $G_1 \cdots G_q \boldsymbol{u} = \boldsymbol{e}_j$.*

Proof. It suffices to show that $\mathbf{u} = \zeta_{12}^{\ell}\mathbf{e}_{j'}$ for some integers j' and ℓ, since, if $\mathbf{u}$ is of that form, then it can be mapped to $\mathbf{e}_j$ by applying the appropriate operators of type ζ_{12} and X. Because $\mathbf{u}$ is a unit vector, we have $\mathbf{u}^\dagger\mathbf{u}=1$. Hence, using Equation (4), we get

$$1 = \mathbf{u}^\dagger\mathbf{u} = \sum_j u_j^\dagger u_j = \sum_j ((a_j^2+c_j^2+a_jc_j)+(b_j^2+d_j^2+b_jd_j)) + (a_jb_j+b_jc_j+c_jd_j)\sqrt{3}.$$

Since every element $\mathbb{Z}[\sqrt{3}]$ can be uniquely expressed as an integer linear combination of 1 and $\sqrt{3}$, the equation above implies the equations below.

$$\sum_j ((a_j^2+c_j^2+a_jc_j)+(b_j^2+d_j^2+b_jd_j)) = 1 \tag{7}$$

$$\sum_j (a_jb_j+b_jc_j+c_jd_j) = 0 \tag{8}$$

It follows from Lemma 7.1 that Equation (7) can only be satisfied if there is exactly one index j such that either $a_j^2+c_j^2+a_jc_j=1$ or $b_j^2+d_j^2+b_jd_j=1$, but not both. By Lemma 7.1, this happens precisely when (a_j,c_j) is one of $(\pm 1,0)$, $(0,\pm 1)$, or $(\pm 1,\mp 1)$, and (b_j,d_j) is $(0,0)$, or when (b_j,d_j) is one of $(\pm 1,0)$, $(0,\pm 1)$, or $(\pm 1,\mp 1)$, and (a_j,c_j) is $(0,0)$. These 12 solutions all satisfy Equation (8) and correspond exactly to the possible powers of ζ_{12}. □

Lemma 7.3. *If $u,v \in \mathbb{Z}[\zeta_{12}]$ are such that $u^\dagger u \equiv_2 v^\dagger v$, then there exists ℓ such that*

$$H'T_{12}^{\ell}\begin{bmatrix} u \\ v \end{bmatrix} = \begin{bmatrix} u' \\ v' \end{bmatrix}$$

for some $u',v' \in \mathbb{Z}[\zeta_{12}]$ such that $u' \equiv v' \equiv 0 \pmod{\delta}$.

Proof. Let u and v be as stated. Then, by Lemma 2.2, we have $u \equiv_2 \zeta_{12}^{\ell} v$ for some ℓ. Equivalently, $u \pm \zeta_{12}^{\ell} v \equiv 0 \pmod 2$, so that $u + \zeta_{12}^{\ell} v = 2w$ and $u - \zeta_{12}^{\ell} v = 2w'$ for some $w, w' \in \mathbb{Z}[\zeta_{12}]$. We then get

$$H' T_{12}^{\ell} \begin{bmatrix} u \\ v \end{bmatrix} = H' \begin{bmatrix} u \\ \zeta_{12}^{\ell} v \end{bmatrix} = \frac{\delta}{2} \begin{bmatrix} u + \zeta_{12}^{\ell} v \\ u - \zeta_{12}^{\ell} v \end{bmatrix} = \frac{\delta}{2} \begin{bmatrix} 2w \\ 2w' \end{bmatrix} = \delta \begin{bmatrix} w \\ w' \end{bmatrix},$$

which completes the proof. □

Lemma 7.4. *If $\boldsymbol{u}$ is an m-dimensional unit vector with entries in $\mathscr{R}_{12}$ and $\operatorname{lde}(\boldsymbol{u}) \geq 1$, then there exists a sequence $G_1, \ldots G_q$ of one- and two-level operators of type ζ_{12}, X, and H' such that* $\operatorname{lde}(G_1 \cdots G_q \boldsymbol{u}) < \operatorname{lde}(\boldsymbol{u})$.

Proof. Let $k = \operatorname{lde}(\mathbf{u})$ and let $\mathbf{v} = \delta^k \mathbf{u} \in \mathbb{Z}[\zeta_{12}]$. We know from Lemma 2.2 that, for $v \in \mathbb{Z}[\zeta_{12}]$, if $v \not\equiv_{\delta} 0$, then $v^{\dagger} v \equiv_2 1$ or $v^{\dagger} v \equiv_2 \sqrt{3}$. We can therefore write $\mathbf{v}^{\dagger}\mathbf{v}$ as

$$\mathbf{v}^{\dagger}\mathbf{v} = \sum_j v_j^{\dagger} v_j = \sum_{v_j \equiv_{\delta} 0} v_j^{\dagger} v_j + \sum_{v_j \not\equiv_{\delta} 0} v_j^{\dagger} v_j = \sum_{v_j \equiv_{\delta} 0} v_j^{\dagger} v_j + \sum_{v_j^{\dagger} v_j \equiv_2 1} v_j^{\dagger} v_j + \sum_{v_j^{\dagger} v_j \equiv_2 \sqrt{3}} v_j^{\dagger} v_j. \tag{9}$$

Since $\mathbf{u}$ is a unit vector and $\delta^{\dagger}\delta = 2$, we have $\mathbf{v}^{\dagger}\mathbf{v} = \mathbf{u}^{\dagger}\mathbf{u}(\delta^{\dagger}\delta)^k = 2^k$. Because $k \geq 1$, this implies that $\mathbf{v}^{\dagger}\mathbf{v} \equiv_2 0$. Hence, by Lemma 2.2, taking Equation (9) modulo 2 yields

$$0 \equiv_2 \mathbf{v}^{\dagger}\mathbf{v} \equiv_2 a + b\sqrt{3},$$

where a is the number of v_j such that $v_j^{\dagger} v_j \equiv_2 1$, and b be the number of v_j such that $v_j^{\dagger} v_j \equiv_2 \sqrt{3}$. It then follows that we must have $a \equiv_2 b \equiv_2 0$. That is, both a and b are even integers. We can therefore group the entries of $\mathbf{v}$ that are not congruent to 0 modulo δ into pairs $(v_j, v_{j'})$ such that $v_j^{\dagger} v_j \equiv_2 v_{j'}^{\dagger} v_{j'}$. Applying Lemma 7.3 to every such pair reduces the least denominator exponent of $\mathbf{u}$. □

Lemma 7.5. *If $\boldsymbol{u}$ is an m-dimensional unit vector with entries in $\mathscr{R}_{12}$, then, for any $0 \leq j \leq m-1$, there exists a sequence $G_1, \ldots, G_q$ of one- and two-level operators of type ζ_{12}, X, and H' such that $G_1 \cdots G_q \boldsymbol{u} = \boldsymbol{e}_j$.*

Proof. By induction on $\operatorname{lde}(\mathbf{u})$. If $\operatorname{lde}(\mathbf{u}) = 0$, then the result follows from Lemma 7.2. If $\operatorname{lde}(\mathbf{u}) \geq 1$, then, by Lemma 7.4, there exists a sequence $G_1, \ldots G_q$ of two-level operators of type ζ_{12}, X, and H' such that $\operatorname{lde}(G_1 \cdots G_q \mathbf{u}) < \operatorname{lde}(\mathbf{u})$. Now let $\mathbf{u}' = G_1 \cdots G_q \mathbf{u}$. By the induction hypothesis, there exists a sequence $G'_1, \ldots, G'_{q'}$ of one- and two-level operators of type ζ_{12}, X, and H such that $G'_1 \cdots G'_{\ell'} \mathbf{u}' = \mathbf{e}_j$. We therefore have

$$\mathbf{e}_j = G'_1 \cdots G'_{q'} \mathbf{u}' = G'_1 \cdots G'_{q'} \cdot G_1 \cdots G_q \mathbf{u},$$

which completes the proof. □

Theorem 7.6. *A matrix U belongs to $\mathrm{U}(\mathscr{R}_{12})$ if and only if U can be expressed as a product of one- and two-level operators of type ζ_{12}, X, and H'.*

Proof. The right-to-left direction follows immediately from the fact that one- and two-level operators of type ζ_{12}, X, and H' are unitaries with entries in $\mathscr{R}_{12}$. We now prove the left-to-right direction. Let $U \in \mathrm{U}(\mathscr{R}_{12})$ and let $\mathbf{u}$ be the first column of U. Then $\mathbf{u}$ is a unit vector with entries in $\mathscr{R}_{12}$. Hence, by

Lemma 7.5, there exists a sequence $G_1,\ldots,G_q$ of one- and two-level operators of type ζ_{12}, X, and H' such that $G_1\cdots G_q\mathbf{u}=\mathbf{e}_1$. Since U and $G_1,\ldots,G_q$ are unitaries with entries in $\mathscr{R}_{12}$, we have

$$G_1\cdots G_qU=\left[\begin{array}{c|ccc} 1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & U' & \\ 0 & & & \end{array}\right],$$

for some smaller $U'\in\mathrm{U}(\mathscr{R}_{12})$. Repeating this process inductively, we ultimately obtain a sequence $F_1,\ldots,F_{q'}$ of one- and two-level operators of type ζ_{12}, X and H' such that $F_1\cdots F_{q'}U=I$. Multiplying by $(F_1\cdots F_{q'})^{-1}$ on both sides then yields the desired decomposition. □

7.2 Exact synthesis

Theorem 7.7. *A $2^m\times 2^m$ matrix U can be exactly represented by an m-qubit circuit over $\mathscr{G}_{24}$ if and only if $U\in\mathrm{U}_{2^m}(\mathscr{R}_{24})$. Furthermore, 2 ancillas suffice to synthesize a circuit for U.*

Proof. The left-to-right follows immediately from the fact that elements of $\mathscr{G}_{24}$ belong to $\mathrm{U}(\mathscr{R}_{24})$. Now let $U\in\mathrm{U}_{2^m}(\mathscr{R}_{24})$ and let $(\psi_3,\mathbf{d}_3):\mathrm{U}(\mathscr{R}_{24})\to\mathrm{U}(\mathscr{R}_{12})$ be the catalytic embedding defined in Section 5. Then $\psi_3(U)\in\mathrm{U}_{2^{m+1}}(\mathscr{R}_{12})$ and can be represented as a product of one- and two-level operators of type ζ_{12}, X, and H'. By Theorem 3.1, these 1- and 2-level operators can each be represented by a circuit over $\mathscr{G}_{24}$ using a single ancilla. Hence, there is a circuit C over $\mathscr{G}_{24}$ that represents $\psi_3(U)$. Using an additional ancilla and reasoning as in Theorem 6.3, we obtain a circuit over $\mathscr{G}_{24}$ for U that uses 2 ancillas. □

We can now use Theorem 7.7 to obtain an exact synthesis result for Clifford-cyclotomic gate sets of degree $3\cdot 2^k$, with $k\geq 3$. The proof is very similar to that of Corollary 6.4, so we omit it here.

Corollary 7.8. *Let $k\geq 3$. A $2^m\times 2^m$ matrix U can be exactly represented by an m-qubit circuit over $\mathscr{G}_{3\cdot 2^k}$ if and only if $U\in U_{2^m}(\mathscr{R}_{3\cdot 2^k})$. Furthermore, $k-1$ ancillas suffice to synthesize a circuit for U.*

8 Conclusion

We now know that, for $n=2^k$ and $n=3\cdot 2^k$, m-qubit circuits with ancillas over $\mathscr{G}_n$ correspond precisely to matrices in $\mathrm{U}_{2^m}(\mathscr{R}_n)$. Yet, many questions in the theory of Clifford-cyclotomic circuits remain unanswered. Two natural open problems are the following.

1. For which values of n does the correspondence between circuits over $\mathscr{G}_n$ and matrices in $\mathrm{U}(\mathscr{R}_n)$ hold?

2. For the values of n for which the correspondence holds, what is the smallest number of ancillas required to synthesize circuits in the worst case?

A natural initial step in addressing the first of these open problems is to consider values of n of the form $p\cdot 2^k$, for p a prime. While it stands to reason that our results might generalize to such cases, it gets progressively harder to analyze the relevant residues; this indicates that a novel approach may be needed for such generalizations.

Acknowledgements

We thank the QPL reviewers for their very thoughtful comments. This work was supported by the Natural Sciences and Engineering Research Council of Canada (NSERC). The circuit in Section 6 was drawn using the Quantikz package [12].

References

[1] Matthew Amy, Matthew Crawford, Andrew N. Glaudell, Melissa L. Macasieb, Samuel S. Mendelson & Neil J. Ross (2023): *Catalytic embeddings of quantum circuits*, doi:10.48550/arXiv.2305.07720. Preprint. Available from arXiv:2305.07720.

[2] Matthew Amy, Andrew N. Glaudell, Shaun Kelso, William Maxwell, Samuel S. Mendelson & Neil J. Ross (2024): *Exact synthesis of multiqubit Clifford-cyclotomic circuits*. In Torben Ægidius Mogensen & Łukasz Mikulski, editors: *Proceedings of the Reversible Computation, RC 2024, Torún, Poland*, Springer Nature Switzerland, Cham, pp. 238–245, doi:10.1007/978-3-031-62076-8_15. Available from arXiv:2311.07741.

[3] 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. Available from arXiv:1908.06076.

[4] Alex Bocharov, Martin Roetteler & Krysta M. Svore (2015): *Efficient synthesis of probabilistic quantum circuits with fallback*. *Physical Review A* 91, p. 052317, doi:10.1103/PhysRevA.91.052317. Available from arXiv:1409.3552.

[5] Guillaume Duclos-Cianci & David Poulin (2015): *Reducing the quantum-computing overhead with complex gate distillation*. *Physical Review A* 91(4), p. 042315, doi:10.1103/PhysRevA.91.042315. Available from arXiv:1403.5280.

[6] David S. Dummit & Richard M. Foote (2004): *Abstract Algebra*, 3 ed. edition. Wiley, New Delhi.

[7] Simon Forest, David Gosset, Vadym Kliuchnikov & David McKinnon (2015): *Exact synthesis of single-qubit unitaries over Clifford-cyclotomic gate sets*. *Journal of Mathematical Physics* 56(8), p. 082201, doi:10.1063/1.4927100. Available from arXiv:1501.04944.

[8] 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.

[9] Andrew N. Glaudell, Neil J. Ross, John van de Wetering & Lia Yeh (2024): *Exact synthesis of multiqutrit Clifford-cyclotomic circuits*. In Alejandro Díaz-Caro & Vladimir Zamdzhiev, editors: *Proceedings of the 21st International Conference on Quantum Physics and Logic, QPL 2024, Buenos Aires, Argentina*, *EPTCS* 406, pp. 44–62, doi:10.4204/EPTCS.406.2. Available from arXiv:2405.08136.

[10] Daniel Gottesman & Isaac L. Chuang (1999): *Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations*. *Nature* 402(6760), pp. 390–393, doi:10.1038/46503.

[11] Colin Ingalls, Bruce W. Jordan, Allan Keeton, Adam Logan & Yevgeny Zaytman (2021): *The Clifford-cyclotomic group and Euler–Poincaré characteristics*. *Canadian Mathematical Bulletin* 64(3), pp. 651–666, doi:10.4153/S0008439520000727. Available from arXiv:1903.09497.

[12] Alastair Kay (2018): *Tutorial on the Quantikz package*, doi:10.48550/arXiv.1809.03842. Preprint. Available from arXiv:1809.03842.

[13] Vadym Kliuchnikov, Dmitri Maslov & Michele Mosca (2013): *Fast and efficient exact synthesis of single-qubit unitaries generated by Clifford and T gates*. *Quantum Information & Computation* 13(7-8), pp. 607–630, doi:10.26421/QIC13.7-8-4. Available from arXiv:1206.5236.

[14] Dorian Rudolph (2024): *Towards a universal gate set for* QMA_1, doi:10.48550/arXiv.2411.02681. Preprint. Available from arXiv:2411.02681.

[15] Peter W. Shor (1997): *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*. SIAM Journal on Computing 26(5), pp. 1484–1509, doi:10.1137/S0097539795293172. Available from `arXiv:quant-ph/9508027`.

[16] John R. Silvester (2000): *Determinants of block matrices*. The Mathematical Gazette 84(501), pp. 460–467, doi:10.2307/3620776.

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

A A Proof of Lemma 6.2

Let R be a ring. A **unit** of R is an element of R that admits a multiplicative inverse. A ring R is an **integral domain** if $uv \neq 0$, for all nonzero elements $u,v \in R$. An element $u \in R$ is an **associate** of an element $v \in R$ if there exists a unit $w \in R$ such that $v = wu$. A nonunit, nonzero element $u \in R$ is called **prime** if u divides v or u divides w, whenever u divides vw. An ideal $I \subsetneq R$ is called **prime** if $uv \in I$ implies $u \in I$ or $v \in I$.

We start by recalling two well known facts, before establishing a property of roots of unity.

Proposition A.1. *Let R be a commutative ring with identity and let $u,v \in R$. Then u and v are associates if and only if $u \mid v$ and $v \mid u$.*

Proposition A.2. *Let R be a commutative ring with identity and let $u \in R$. Then u is prime if and only if the ideal generated by u is prime.*

Lemma A.3. *Let $a,b \in \mathbb{N}$ be such that $\gcd(a,b) = 1$. Then $1-\zeta_a^b$ and $1-\zeta_a$ are associates.*

Proof. We have
$$1-\zeta_a^b = (1-\zeta_a)(1+\zeta_a+\zeta_a^2+\ldots+\zeta_a^{b-1}).$$
Hence, $1-\zeta_a \mid 1-\zeta_a^b$. Now since $\gcd(a,b) = 1$, there exist $c,d \in \mathbb{Z}$ such that $ac+bd = 1$. Then $1-\zeta_a = 1-\zeta_a^{ac+bd} = 1-(\zeta_a^b)^d$, and thus
$$1-\zeta_a = 1-(\zeta_a^b)^d = (1-\zeta_a^b)(1+\zeta_a^b+(\zeta_a^b)^2+\ldots+(\zeta_a^b)^{d-1}).$$
Hence, $1-\zeta_a^b \mid 1-\zeta_a$. Thus, $1-\zeta_a$ and $1-\zeta_a^b$ are associates by Proposition A.1. □

We are now in a position to prove Lemma 6.2, whose statement we reproduce below.

Lemma. *Let $u \in \mathscr{R}_{16}$ be such that $|u| = 1$. Then $u = \zeta_{16}^\ell$ for some $0 \leq \ell \leq 15$.*

Proof. Let $\chi = 1-\zeta_{16} \in \mathscr{R}_{16}$. Then χ is a prime element in $\mathbb{Z}[\zeta_{16}]$ and, by Proposition A.2, $\langle\chi\rangle$ is a prime ideal of $\mathscr{R}_{16}$. By Lemma A.3, we can decompose 2 in $\mathbb{Z}[\zeta_{16}]$ as
$$\begin{aligned}
2 &= (1+i)(1-i) \\
&= (1-i)^2 u_1 \\
&= (1-\zeta_8)^2(1+\zeta_8)^2 u_1 \\
&= (1-\zeta_8)^4 u_2 u_1 \\
&= (1-\zeta_{16})^4(1+\zeta_{16})^4 u_2 u_1 \\
&= (1-\zeta_{16})^8 u_3 u_2 u_1 \\
&= \chi^8 u_3 u_2 u_1,
\end{aligned}$$
where u_1, u_2, and u_3 are units in $\mathbb{Z}[i]$, $\mathbb{Z}[\zeta_8]$, and $\mathbb{Z}[\zeta_{16}]$, respectively. Hence, any $u \in \mathscr{R}_{16}$, can be written as $u = v/\chi^\ell$ with $\ell \in \mathbb{N}$ and $v \in \mathbb{Z}[\zeta_{16}]$. Now let $u \in \mathscr{R}_{16}$ be such that $|u| = 1$ and write u as $u = v/\chi^\ell$ with ℓ minimal. Observe that $\chi^\dagger = 1-\zeta_{16}^\dagger = -\zeta_{16}^\dagger\chi$. We hence have
$$1 = |u|^2 = u^\dagger u = \frac{v^\dagger v}{(-\zeta_{16}^\dagger)^\ell \chi^{2\ell}},$$

so that $v^\dagger v = \chi^{2\ell} \cdot (-\zeta_{16}^\dagger)^\ell$. If $\ell > 0$, we have $v^\dagger v \in \langle \chi \rangle$. Since χ is prime, this implies that we must have either $v \in \langle \chi \rangle$ or $v^\dagger \in \langle \chi \rangle$. But $v^\dagger \in \langle \chi \rangle$ would imply $v \in \langle \chi \rangle$ since χ and $\chi^\dagger$ are associates. Hence, if $\ell > 0$, then $v \in \langle \chi \rangle$, which contradicts the minimality of ℓ. It must thus be the case that $\ell = 0$, so that u is in fact an element of $\mathbb{Z}[\zeta_{16}]$. Writing u as $u = \sum_{j=0}^{7} a_j \zeta_{16}^j$, with $a_j \in \mathbb{Z}$, we then get

$$\begin{aligned} 1 &= u^\dagger u \\ &= \sum_{j=0}^{7} a_j^2 + 2Re(\zeta_{16})((\sum_{j=0}^{6} a_j a_{j+1}) - a_0 a_7) + 2Re(\zeta_{16}^2)((\sum_{j=0}^{5} a_j a_{j+2}) - a_0 a_6 - a_1 a_7) \\ &+ 2Re(\zeta_{16}^3)((\sum_{j=0}^{4} a_j a_{j+3}) - a_0 a_5 - a_1 a_6 - a_2 a_7). \end{aligned}$$

The above equation holds when exactly one $a_j = \pm 1$ and the rest are zero. Hence $u = \zeta_{16}^\ell$ for some $0 \le \ell \le 15$, as desired. $\square$