Exact synthesis of multiqubit Clifford + T circuits

Brett Giles
Department of Computer Science, University of Calgary, Calgary, Alberta, Canada

Peter Selinger
Department of Mathematics and Statistics, Dalhousie University, Halifax, Nova Scotia, Canada

(Received 4 December 2012; published 26 March 2013)

We prove that a unitary matrix has an exact representation over the Clifford + T gate set with local ancillas if and only if its entries are in the ring $\mathbb{Z}[\frac{1}{\sqrt{2}},i]$. Moreover, we show that one ancilla always suffices. These facts were conjectured by Kliuchnikov, Maslov, and Mosca. We obtain an algorithm for synthesizing a exact Clifford + T circuit from any such n-qubit operator. We also characterize the Clifford + T operators that can be represented without ancillas.

DOI: 10.1103/PhysRevA.87.032332 PACS number(s): 03.67.Lx

I. INTRODUCTION

An important problem in quantum information theory is the decomposition of arbitrary unitary operators into gates from some fixed universal set [1]. Depending on the operator to be decomposed, this may either be done exactly or to within some given accuracy ϵ; the former problem is known as *exact synthesis* and the latter as *approximate synthesis* [2].

Here, we focus on the problem of exact synthesis for n-qubit operators, using the Clifford + T universal gate set. Recall that the Clifford group on n qubits is generated by the Hadamard gate H, the phase gate S, the controlled-NOT gate, and the scalar $\omega = e^{i\pi/4}$ (one may allow arbitrary unit scalars, but it is not convenient for our purposes to do so). It is well known that one obtains a universal gate set by adding the non-Clifford operator T [1],

$$\begin{aligned} \omega &= e^{i\pi/4}, \quad H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \\ CNOT &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}. \end{aligned} \tag{1}$$

In addition to the Clifford + T group on n qubits, as defined above, we also consider the slightly larger group of Clifford + T operators with ancillas. We say that an n-qubit operator U is a *Clifford* + T *operator with ancillas* if there exists $m \geqslant 0$ and a Clifford + T operator U' on $n+m$ qubits, such that $U'(|\phi\rangle \otimes |0\rangle) = (U|\phi\rangle) \otimes |0\rangle$ for all n-qubit states $|\phi\rangle$.

Kliuchnikov, Maslov, and Mosca [2] showed that a single-qubit operator U is in the Clifford + T group if and only if all of its matrix entries belong to the ring $\mathbb{Z}[\frac{1}{\sqrt{2}},i]$. They also showed that the Clifford + T groups with ancillas and without ancillas coincide for $n = 1$, but not for $n \geqslant 2$. Moreover, Kliuchnikov *et al.* conjectured that for all n, an n-qubit operator U is in the Clifford + T group with ancillas if and only if its matrix entries belong to $\mathbb{Z}[\frac{1}{\sqrt{2}},i]$. They also conjectured that a single ancilla qubit is always sufficient in the representation of a Clifford + T operator with ancillas. The purpose of this paper is to prove these conjectures. In particular, this yields an algorithm for exact Clifford + T synthesis of n-qubit operators. We also obtain a characterization of the Clifford + T group on n qubits without ancillas.

It is important to note that, unlike in the single-qubit case, the circuit synthesized here are not in any sense canonical, and very far from optimal. Thus, the question of *efficient* synthesis is not addressed here.

II. STATEMENT OF THE MAIN RESULT

Consider the ring $\mathbb{Z}[\frac{1}{\sqrt{2}},i]$, consisting of complex numbers of the form

$$\frac{1}{2^n}(a + bi + c\sqrt{2} + di\sqrt{2}),$$

where $n \in \mathbb{N}$ and $a,b,c,d \in \mathbb{Z}$. Our goal is to prove the following theorem, which was conjectured by Kliuchnikov *et al.* [2].

Theorem 1. Let U be a unitary $2^n \times 2^n$ matrix. Then the following are equivalent:

(a) U can be exactly represented by a quantum circuit over the Clifford + T gate set, possibly using some finite number of ancillas that are initialized and finalized in state $|0\rangle$.

(b) The entries of U belong to the ring $\mathbb{Z}[\frac{1}{\sqrt{2}},i]$.

Moreover, in (a), a single ancilla is always sufficient.

III. SOME ALGEBRA

We first introduce some notation and terminology, following Ref. [2] where possible. Recall that $\mathbb{N}$ is the set of natural numbers including 0, and $\mathbb{Z}$ is the ring of integers. We write $\mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z}$ for the ring of integers modulo 2. Let $\mathbb{D}$ be the ring of *dyadic fractions*, defined as $\mathbb{D} = \mathbb{Z}[\frac{1}{2}] = \{\frac{a}{2^n} \mid a \in \mathbb{Z}, n \in \mathbb{N}\}$.

Let $\omega = e^{i\pi/4} = (1+i)/\sqrt{2}$. Note that ω is an eighth root of unity satisfying $\omega^2 = i$ and $\omega^4 = -1$. We will consider three different rings related to ω.

Definition 1. Consider the following rings. Note that the first two are subrings of the complex numbers, and the third one is not.

(i) $\mathbb{D}[\omega] = \{a\omega^3 + b\omega^2 + c\omega + d \mid a,b,c,d \in \mathbb{D}\}$.

(ii) $\mathbb{Z}[\omega] = \{a\omega^3 + b\omega^2 + c\omega + d \mid a,b,c,d \in \mathbb{Z}\}$.

(iii) $\mathbb{Z}_2[\omega] = \{p\omega^3 + q\omega^2 + r\omega + s \mid p,q,r,s \in \mathbb{Z}_2\}$.

Note that the ring $\mathbb{Z}_2[\omega]$ only has 16 elements. The laws of addition and multiplication are uniquely determined by the ring axioms and the property $\omega^4 = 1 \pmod 2$. We call the elements of $\mathbb{Z}_2[\omega]$ *residues* (more precisely, residue classes of $\mathbb{Z}[\omega]$ modulo 2).

Remark 1. The ring $\mathbb{D}[\omega]$ is the same as the ring $\mathbb{Z}[\frac{1}{\sqrt{2}},i]$ mentioned in the statement of Theorem 1. However, as already pointed out in Ref. [2], the formulation in terms of ω is far more convenient algebraically.

Remark 2. The ring $\mathbb{Z}[\omega]$ is also called the *ring of algebraic integers* of $\mathbb{D}[\omega]$. It has an intrinsic definition, i.e., one that is independent of the particular presentation of $\mathbb{D}[\omega]$. Namely, a complex number is called an *algebraic integer* if it is the root of some polynomial with integer coefficients and leading coefficient 1. It follows that ω, i, and $\sqrt{2}$ are algebraic integers, whereas, for example, $1/\sqrt{2}$ is not. The ring $\mathbb{Z}[\omega]$ then consists of precisely those elements of $\mathbb{D}[\omega]$ that are algebraic integers.

A. Conjugate and norm

Remark 3 (complex conjugate and norm). Since $\mathbb{D}[\omega]$ and $\mathbb{Z}[\omega]$ are subrings of the complex numbers, they inherit the usual notion of complex conjugation. We note that $\omega^\dagger = -\omega^3$. This yields the following formula:

$$(a\omega^3 + b\omega^2 + c\omega + d)^\dagger = -c\omega^3 - b\omega^2 - a\omega + d. \qquad (2)$$

Similarly, the sets $\mathbb{D}[\omega]$ and $\mathbb{Z}[\omega]$ inherit the usual norm from the complex numbers. It is given by the following explicit formula, for $t = a\omega^3 + b\omega^2 + c\omega + d$:

$$\|t\|^2 = t^\dagger t = (a^2+b^2+c^2+d^2) + (cd+bc+ab-da)\sqrt{2}. \qquad (3)$$

Definition 2 (weight). For $t \in \mathbb{D}[\omega]$ or $t \in \mathbb{Z}[\omega]$, the *weight* of t is denoted $\|t\|_{\text{weight}}$, and is given by

$$\|t\|^2_{\text{weight}} = a^2 + b^2 + c^2 + d^2. \qquad (4)$$

Note that the square of the norm is valued in $\mathbb{D}[\sqrt{2}]$, whereas the square of the weight is valued in $\mathbb{D}$. We also extend the definition of norm and weight to vectors in the obvious way: For $u = (u_j)_j$, we define

$$\|u\|^2 = \sum_j \|u_j\|^2 \quad \text{and} \quad \|u\|^2_{\text{weight}} = \sum_j \|u_j\|^2_{\text{weight}}.$$

Lemma 1. Consider a vector $u \in \mathbb{D}[\omega]^n$. If $\|u\|^2$ is an integer, then $\|u\|^2_{\text{weight}} = \|u\|^2$.

Proof. Any $t \in \mathbb{D}[\sqrt{2}]$ can be uniquely written as $t = a + b\sqrt{2}$, where $a,b \in \mathbb{D}$. We can call a the *dyadic part* of t. Now the claim is obvious, because $\|u\|^2_{\text{weight}}$ is exactly the dyadic part of $\|u\|^2$. ∎

B. Denominator exponents

Definition 3. Let $t \in \mathbb{D}[\omega]$. A natural number $k \in \mathbb{N}$ is called a *denominator exponent* for t if $\sqrt{2}^k t \in \mathbb{Z}[\omega]$. It is obvious that such k always exists. The least such k is called the *least denominator exponent* of t.

More generally, we say that k is a denominator exponent for a vector or matrix if it is a denominator exponent for all of its entries. The least denominator exponent for a vector or matrix is therefore the least k that is a denominator exponent for all of its entries.

Remark 4. Our notion of least denominator exponent is almost the same as the "smallest denominator exponent" of Ref. [2], except that we do not permit $k < 0$.

C. Residues

Remark 5. The ring $\mathbb{Z}_2[\omega]$ is not a subring of the complex numbers; rather, it is a quotient of the ring $\mathbb{Z}[\omega]$. Indeed, consider the *parity function* $\overline{()} : \mathbb{Z} \to \mathbb{Z}_2$, which is the unique ring homomorphism. It satisfies $\overline{a} = 0$ if a is even and $\overline{a} = 1$ if a is odd. The parity map induces a surjective ring homomorphism $\rho : \mathbb{Z}[\omega] \to \mathbb{Z}_2[\omega]$, defined by

$$\rho(a\omega^3 + b\omega^2 + c\omega + d) = \overline{a}\omega^3 + \overline{b}\omega^2 + \overline{c}\omega + \overline{d}.$$

We call ρ the *residue map*, and we call $\rho(t)$ the *residue* of t.

Convention 1. Since residues will be important for the constructions of this paper, we introduce a shortcut notation, writing each residue $p\omega^3 + q\omega^2 + r\omega + s$ as a string of binary digits $pqrs$.

What makes residues useful for our purposes is that many important operations on $\mathbb{Z}[\omega]$ are well defined on residues. Here, we say that an operation $f : \mathbb{Z}[\omega] \to \mathbb{Z}[\omega]$ is *well defined on residues* if for all t,s, $\rho(t) = \rho(s)$ implies $\rho(f(t)) = \rho(f(s))$.

For example, two operations that are obviously well defined on residues are complex conjugation, which takes the form $(pqrs)^\dagger = rqps$ by (2), and multiplication by ω, which is just a cyclic shift $\omega(pqrs) = qrsp$. Table I shows two other important operations on residues, namely multiplication by $\sqrt{2}$ and the squared norm.

Definition 4 (k-residue). Let $t \in \mathbb{D}[\omega]$ and let k be a (not necessarily least) denominator exponent for t. The *k-residue of* t, in symbols $\rho_k(t)$, is defined to be

$$\rho_k(t) = \rho(\sqrt{2}^k t).$$

Definition 5 (reducibility). We say that a residue $x \in \mathbb{Z}_2[\omega]$ is *reducible* if it is of the form $\sqrt{2}\,y$, for some $y \in \mathbb{Z}_2[\omega]$. Moreover, we say that $x \in \mathbb{Z}_2[\omega]$ is *twice reducible* if it is of the form $2y$, for some $y \in \mathbb{Z}_2[\omega]$.

Lemma 2. For a residue x, the following are equivalent:

(1) x is reducible;
(2) $x \in \{0000, 0101, 1010, 1111\}$;
(3) $\sqrt{2}\,x = 0000$;
(4) $x^\dagger x = 0000$.

Moreover, x is twice reducible iff $x = 0000$.

Proof. By inspection of Table I. ∎

Lemma 3. Let $t \in \mathbb{Z}[\omega]$. Then $t/2 \in \mathbb{Z}[\omega]$ if and only if $\rho(t)$ is twice reducible, and $t/\sqrt{2} \in \mathbb{Z}[\omega]$ if and only if $\rho(t)$ is reducible.

Proof. The first claim is trivial, as $\rho(t) = 0000$ if and only if all components of t are even. For the second claim, the left-to-right implication is also trivial: assume $t' = t/\sqrt{2} \in \mathbb{Z}[\omega]$. Then $\rho(t) = \rho(\sqrt{2}\,t')$, which is reducible by definition. Conversely, let $t \in \mathbb{Z}[\omega]$ and assume that $\rho(t)$ is reducible.

TABLE I. Some operations on residues.

$\rho(t)$	$\rho(\sqrt{2}\,t)$	$\rho(t^\dagger t)$	$\rho(t)$	$\rho(\sqrt{2}\,t)$	$\rho(t^\dagger t)$
0000	0000	0000	1000	0101	0001
0001	1010	0001	1001	1111	1010
0010	0101	0001	1010	0000	0000
0011	1111	1010	1011	1010	0001
0100	1010	0001	1100	1111	1010
0101	0000	0000	1101	0101	0001
0110	1111	1010	1110	1010	0001
0111	0101	0001	1111	0000	0000

Then $\rho(t) \in \{0000,0101,1010,1111\}$, and it can be seen from Table I that $\rho(\sqrt{2}\,t) = 0000$. Therefore, $\sqrt{2}\,t$ is twice reducible by the first claim; hence t is reducible. ■

Corollary 1. Let $t \in \mathbb{D}[\omega]$ and let $k > 0$ be a denominator exponent for t. Then k is the least denominator exponent for t if and only if $\rho_k(t)$ is irreducible.

Proof. Since k is a denominator exponent for t, we have $\sqrt{2}^k t \in \mathbb{Z}[\omega]$. Moreover, k is least if and only if $\sqrt{2}^{k-1} t \notin \mathbb{Z}[\omega]$. By Lemma 3, this is the case if and only if $\rho(\sqrt{2}^k t) = \rho_k(t)$ is irreducible. ■

Definition 6. The notions of residue, k-residue, reducibility, and twice reducibility all extend in an obvious componentwise way to vectors and matrices. Thus, the residue $\rho(u)$ of a vector or matrix u is obtained by taking the residue of each of its entries, and similar for k-residues. Also, we say that a vector or matrix is reducible if each of its entries is reducible, and similarly for twice reducibility.

Example 1. Consider the matrix

$$U = \frac{1}{\sqrt{2}^3}\begin{pmatrix} -\omega^3+\omega-1 & \omega^2+\omega+1 & \omega^2 & -\omega \\ \omega^2+\omega & -\omega^3+\omega^2 & -\omega^2-1 & \omega^3+\omega \\ \omega^3+\omega^2 & -\omega^3-1 & 2\omega^2 & 0 \\ -1 & \omega & 1 & -\omega^3+2\omega \end{pmatrix}.$$

It has least denominator exponent 3. Its 3-, 4-, and 5-residues are:

$$\rho_3(U) = \begin{pmatrix} 1011 & 0111 & 0100 & 0010 \\ 0110 & 1100 & 0101 & 1010 \\ 1100 & 1001 & 0000 & 0000 \\ 0001 & 0010 & 0001 & 1000 \end{pmatrix},$$

$$\rho_4(U) = \begin{pmatrix} 1010 & 0101 & 1010 & 0101 \\ 1111 & 1111 & 0000 & 0000 \\ 1111 & 1111 & 0000 & 0000 \\ 1010 & 0101 & 1010 & 0101 \end{pmatrix}, \quad \rho_5(U) = 0.$$

IV. DECOMPOSITION INTO TWO-LEVEL MATRICES

Recall that a *two-level matrix* is an $n \times n$ matrix that acts nontrivially on at most two vector components [1]. If

$$U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

is a 2×2 matrix and $j \neq \ell$, we write $U_{[j,\ell]}$ for the two-level $n \times n$ matrix defined by

$$U_{[j,\ell]} = \begin{array}{c} \\ \vdots \\ j \\ \vdots \\ \ell \\ \vdots \end{array} \begin{array}{c} \cdots\ \ j\ \ \cdots\ \ \ell\ \ \cdots \\ \left(\begin{array}{c|c|c|c|c} I & & & & \\ \hline & a & & b & \\ \hline & & I & & \\ \hline & c & & d & \\ \hline & & & & I \end{array}\right) \end{array},$$

and we say that $U_{[j,\ell]}$ is a two-level matrix of *type* U. Similarly, if a is a scalar, we write $a_{[j]}$ for the one-level matrix

$$a_{[j]} = \begin{array}{c} \\ \vdots \\ j \\ \vdots \end{array} \begin{array}{c} \cdots\ \ j\ \ \cdots \\ \left(\begin{array}{c|c|c} I & & \\ \hline & a & \\ \hline & & I \end{array}\right) \end{array},$$

and we say that $a_{[j]}$ is a one-level matrix of *type* a.

Lemma 4 (row operation). Let $u = (u_1,u_2)^T \in \mathbb{D}[\omega]^2$ be a vector with denominator exponent $k > 0$ and k-residue $\rho_k(u) = (x_1,x_2)$, such that $x_1^\dagger x_1 = x_2^\dagger x_2$. Then there exists a sequence of matrices $U_1,\ldots,U_h$, each of which is H or T, such that $v = U_1 \cdots U_h u$ has denominator exponent $k-1$, or equivalently, $\rho_k(v)$ is defined and reducible.

Proof. It can be seen from Table I that $x_1^\dagger x_1$ is either 0000, 1010, or 0001.

(i) Case 1: $x_1^\dagger x_1 = x_2^\dagger x_2 = 0000$. In this case, $\rho_k(u)$ is already reducible, and there is nothing to show.

(ii) Case 2: $x_1^\dagger x_1 = x_2^\dagger x_2 = 1010$. In this case, we know from Table I that $x_1,x_2 \in \{0011,0110,1100,1001\}$. In particular, x_1 is a cyclic permutation of x_2, say, $x_1 = \omega^m x_2$. Let $v = HT^m u$. Then

$$\rho_k(\sqrt{2}\,v) = \rho_k\left(\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & \omega^m \end{pmatrix}\begin{pmatrix} u_1 \\ u_2 \end{pmatrix}\right)$$
$$= \rho_k\begin{pmatrix} u_1+\omega^m u_2 \\ u_1-\omega^m u_2 \end{pmatrix} = \begin{pmatrix} x_1+\omega^m x_2 \\ x_1-\omega^m x_2 \end{pmatrix} = \begin{pmatrix} 0000 \\ 0000 \end{pmatrix}.$$

This shows that $\rho_k(\sqrt{2}\,v)$ is twice reducible; therefore, $\rho_k(v)$ is defined and reducible as claimed.

(iii) Case 3: $x_1^\dagger x_1 = x_2^\dagger x_2 = 0001$. In this case, we know from Table I that $x_1,x_2 \in \{0001,0010,0100,1000\} \cup \{0111,1110,1101,1011\}$. If both x_1,x_2 are in the first set, or both are in the second set, then x_1 and x_2 are cyclic permutations of each other, and we proceed as in case 2. The only remaining cases are that x_1 is a cyclic permutation of 0001 and x_2 is a cyclic permutation of 0111, or vice versa. But then there exists some m such that $x_1 + \omega^m x_2 = 1111$. Letting $u' = HT^m u$, we have

$$\rho_k(\sqrt{2}\,u') = \rho_k\left[\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & \omega^m\end{pmatrix}\begin{pmatrix}u_1\\ u_2\end{pmatrix}\right]$$
$$= \rho_k\begin{pmatrix}u_1+\omega^m u_2\\ u_1-\omega^m u_2\end{pmatrix} = \begin{pmatrix}x_1+\omega^m x_2\\ x_1-\omega^m x_2\end{pmatrix} = \begin{pmatrix}1111\\ 1111\end{pmatrix}.$$

Since this is reducible, u' has denominator exponent k. Let $\rho_k(u') = (y_1, y_2)$. Because $\sqrt{2}\,y_1 = \sqrt{2}\,y_2 = 1111$, we see from Table I that $y_1, y_2 \in \{0011, 0110, 1100, 1001\}$ and $y_1^\dagger y_1 = y_2^\dagger y_2 = 1010$. Therefore, u' satisfies the condition of case 2 above. Proceeding as in case 2, we find m' such that $v = HT^{m'}u' = HT^{m'}HT^m u$ has denominator exponent $k-1$. This finishes the proof. ■

Lemma 5 (column lemma). Consider a unit vector $u \in \mathbb{D}[\omega]^n$, i.e., an n-dimensional column vector of norm 1 with entries from the ring $\mathbb{D}[\omega]$. Then there exists a sequence $U_1, \ldots, U_h$ of one- and two-level unitary matrices of types X, H, T, and ω such that $U_1 \cdots U_h u = e_1$, the first standard basis vector.

Proof. The proof is by induction on k, the least denominator exponent of u. Let $u = (u_1, \ldots, u_n)^T$.

(i) Base case. Suppose $k = 0$. Then $u \in \mathbb{Z}[\omega]^n$. Since by assumption $\|u\|^2 = 1$, it follows by Lemma 1 that $\|u\|^2_{\mathrm{weight}} = 1$. Since $u_1, \ldots, u_n$ are elements of $\mathbb{Z}[\omega]$, their weights are non-negative integers. It follows that there is precisely one j with $\|u_j\|_{\mathrm{weight}} = 1$, and $\|u_\ell\|_{\mathrm{weight}} = 0$ for all $\ell \neq j$. Let $u' = X_{[1,j]}u$ if $j \neq 1$, and $u' = u$ otherwise. Now u'_1 is of the form ω^{-m}, for some $m \in \{0, \ldots, 7\}$, and $u'_\ell = 0$ for all $\ell \neq 1$. We have $\omega^m_{[1]}u' = e_1$, as desired.

(ii) Induction step. Suppose $k > 0$. Let $v = \sqrt{2}^k u \in \mathbb{Z}[\omega]^n$, and let $x = \rho_k(u) = \rho(v)$. From $\|u\|^2 = 1$, it follows that $\|v\|^2 = v_1^\dagger v_1 + \cdots + v_n^\dagger v_n = 2^k$. Taking residues of the last equation, we have

$$x_1^\dagger x_1 + \cdots + x_n^\dagger x_n = 0000. \qquad (5)$$

It can be seen from Table I that each summand $x_j^\dagger x_j$ is either 0000, 0001, or 1010. Since their sum is 0000, it follows that there is an even number of j such that $x_j^\dagger x_j = 0001$, and an even number of j such that $x_j^\dagger x_j = 1010$.

We do an inner induction on the number of irreducible components of x. If x is reducible, then u has denominator exponent $k-1$ by Corollary 1, and we can apply the outer induction hypothesis. Now suppose there is some j such that x_j is irreducible; then $x_j^\dagger x_j \neq 0000$ by Lemma 2. Because of the evenness property noted above, there must exist some $\ell \neq j$ such that $x_j^\dagger x_j = x_\ell^\dagger x_\ell$. Applying Lemma 4 to $u' = (u_j, u_\ell)^T$, we find a sequence $\vec{U}$ of row operations of types H and T, making $\rho_k(\vec{U}u')$ reducible. We can lift this to a two-level operation $\vec{U}_{[j,\ell]}$ acting on u; thus $\rho_k(\vec{U}_{[j,\ell]}u)$ has fewer irreducible components than $x = \rho_k(u)$, and the inner induction hypothesis applies. ■

Lemma 6 (matrix decomposition). Let U be a unitary $n \times n$ matrix with entries in $\mathbb{D}[\omega]$. Then there exists a sequence $U_1, \ldots, U_h$ of one- and two-level unitary matrices of types X, H, T, and ω such that $U = U_1 \cdots U_h$.

Proof. Equivalently, it suffices to show that there exist one- and two-level unitary matrices $V_1, \ldots, V_h$ of types X, H, T, and ω such that $V_h \cdots V_1 U = I$. This is an easy consequence of the column lemma, exactly as in, e.g., Sec. 4.5.1 of Ref. [1]. Specifically, first use the column lemma to find suitable one- and two-level row operations $V_1, \ldots, V_{h_1}$ such that the leftmost column of $V_{h_1} \cdots V_1 U$ is e_1. Because $V_{h_1} \cdots V_1 U$ is unitary, it is of the form

$$\left(\begin{array}{c|c}1 & 0\\ \hline 0 & U'\end{array}\right).$$

Now recursively find row operations to reduce U' to the identity matrix. ■

Example 2. We will decompose the matrix U from Example 1. We start with the first column u of U

$$u = \frac{1}{\sqrt{2}^3}\begin{pmatrix}-\omega^3+\omega-1\\ \omega^2+\omega\\ \omega^3+\omega^2\\ -1\end{pmatrix},$$

$$\rho_3(u) = \begin{pmatrix}1011\\ 0110\\ 1100\\ 0001\end{pmatrix}, \quad \rho_3(u_j^\dagger u_j) = \begin{pmatrix}0001\\ 1010\\ 1010\\ 0001\end{pmatrix}.$$

Rows 2 and 3 satisfy case 2 of Lemma 4. As they are not aligned, first apply $T^3_{[2,3]}$ and then $H_{[2,3]}$. Rows 1 and 4 satisfy case 3. Applying $H_{[1,4]}T^2_{[1,4]}$, the residues become $\rho_3(u'_1) = 0011$ and $\rho_3(u'_4) = 1001$, which requires applying $H_{[1,4]}T_{[1,4]}$. We now have

$$H_{[1,4]}T_{[1,4]}H_{[1,4]}T^2_{[1,4]}H_{[2,3]}T^3_{[2,3]}u = v = \frac{1}{\sqrt{2}^2}\begin{pmatrix}0\\ 0\\ \omega^2+\omega\\ -\omega+1\end{pmatrix},$$

$$\rho_2(v) = \begin{pmatrix}0000\\ 0000\\ 0110\\ 0011\end{pmatrix}, \quad \rho_2(v_j^\dagger v_j) = \begin{pmatrix}0000\\ 0000\\ 1010\\ 1010\end{pmatrix}.$$

Rows 3 and 4 satisfy case 2, while rows 1 and 2 are already reduced. We reduce rows 3 and 4 by applying $H_{[3,4]}T_{[3,4]}$. Continuing, the first column is completely reduced to e_1 by further applying $\omega^7_{[1]}X_{[1,4]}H_{[3,4]}T^3_{[3,4]}$. The complete decomposition of u is therefore given by

$$W_1 = \omega^7_{[1]}X_{[1,4]}H_{[3,4]}T^3_{[3,4]}H_{[3,4]}T_{[3,4]}$$
$$H_{[1,4]}T_{[1,4]}H_{[1,4]}T^2_{[1,4]}H_{[2,3]}T^3_{[2,3]}.$$

Applying this to the original matrix U, we have $W_1 U =$

$$\frac{1}{\sqrt{2}^3}\begin{pmatrix}\sqrt{2}^3 & 0 & 0 & 0\\ 0 & \omega^3-\omega^2+\omega+1 & -\omega^2-\omega-1 & \omega^2\\ 0 & 0 & \omega^3+\omega^2-\omega+1 & \omega^3+\omega^2-\omega-1\\ 0 & \omega^3+\omega^2+\omega+1 & \omega^2 & \omega^3-\omega^2+1\end{pmatrix}.$$

Continuing with the rest of the columns, we find $W_2 = \omega^6_{[2]} H_{[2,4]} T^3_{[2,4]} H_{[2,4]} T_{[2,4]}$, $W_3 = \omega^4_{[3]} H_{[3,4]} T^3_{[3,4]} H_{[3,4]}$, and $W_4 = \omega^5_{[4]}$. We then have $U = W_1^\dagger W_2^\dagger W_3^\dagger W_4^\dagger$, or explicitly,

$$
\begin{aligned}
U = {} & T^5_{[2,3]} H_{[2,3]} T^6_{[1,4]} H_{[1,4]} T^7_{[1,4]} H_{[1,4]} \\
& T^7_{[3,4]} H_{[3,4]} T^5_{[3,4]} H_{[3,4]} X_{[1,4]} \omega_{[1]} \\
& T^7_{[2,4]} H_{[2,4]} T^5_{[2,4]} H_{[2,4]} \omega^2_{[2]} H_{[3,4]} T^5_{[3,4]} H_{[3,4]} \omega^4_{[3]} \omega^3_{[4]}.
\end{aligned}
$$

V. PROOF OF THEOREM 1

A. Equivalence of (a) and (b)

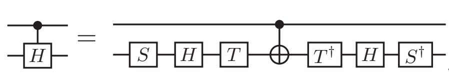
First note that, since all the elementary Clifford + T gates, as shown in (1), take their matrix entries in $\mathbb{D}[\omega] = \mathbb{Z}[\frac{1}{\sqrt{2}}, i]$, the implication (a) $\Rightarrow$ (b) is trivial. For the converse, let U be a unitary $2^n \times 2^n$ matrix with entries from $\mathbb{D}[\omega]$. By Lemma 6, U can be decomposed into one- and two-level matrices of types X, H, T, and ω. It is well known that each such matrix can be further decomposed into controlled-NOT gates and multiply controlled X, H, T, and ω-gates, for example using Gray codes (Sec. 4.5.2 of Ref. [1]). But all of these gates have well-known exact representations in Clifford + T with ancillas (see, e.g., Figs. 4(a) and 9 in Ref. [3]) (and noting that a controlled-ω gate is the same as a T gate). This finishes the proof of (b) $\Rightarrow$ (a).

B. One ancilla is sufficient

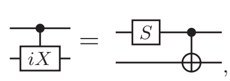
The final claim that needs to be proved is that a circuit for U can always be found using at most one ancilla. It is already known that for $n > 1$, an ancilla is sometimes necessary [2]. To show that a single ancilla is sufficient, in light of the above decomposition, it is enough to show that the following can be implemented with one ancilla:

(1) a multiply controlled X gate;
(2) a multiply controlled H gate;
(3) a multiply controlled T gate.

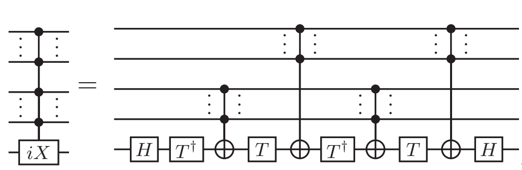
We first recall from Fig. 4(a) of Ref. [3] that a singly controlled Hadamard gate can be decomposed into Clifford + T gates with no ancillas,



We also recall that an n-fold controlled iX gate can be represented using $O(n)$ Clifford + T gates with no ancillas. Namely, for $n = 1$, we have

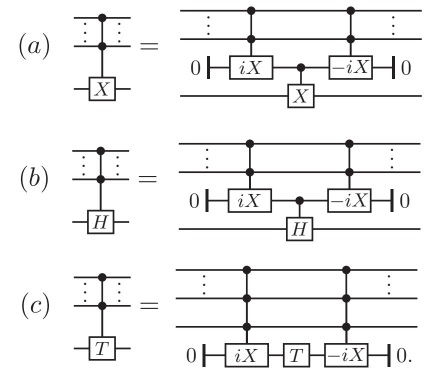


and for $n \geqslant 2$, we can use



with further decompositions of the multiply controlled NOT gates as in Lemma 7.2 of Ref. [4] and Fig. 4.9 of Ref. [1].

We then obtain the following representations for (a)–(c), using only one ancilla:



Remark 6. The fact that one ancilla is always sufficient in Theorem 1 is primarily of theoretical interest. In practice, one may assume that on most quantum computing architectures, ancillas are relatively cheap. Moreover, the use of additional ancillas can significantly reduce the size and depth of the generated circuits (see, e.g., Ref. [5]).

VI. THE NO-ANCILLA CASE

Lemma 7. Under the hypotheses of Theorem 1, assume that $\det U = 1$. Then U can be exactly represented by a Clifford + T circuit with no ancillas.

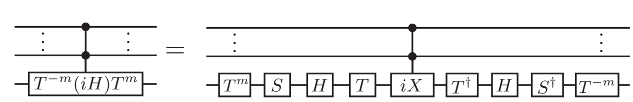
Proof. This requires only minor modifications to the proof of Theorem 1. First observe that whenever an operator of the form HT^m was used in the proof of Lemma 4, we can instead use $T^{-m}(iH)T^m$ without altering the rest of the argument. In the base case of Lemma 5, the operator $X_{[1,j]}$ can be replaced by $iX_{[1,j]}$. Also, in the base case of Lemma 5, whenever $n \geqslant 2$, the operator $\omega_{[1]}$ can be replaced by $W_{[1,2]}$, where

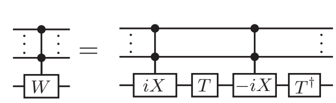
$$
W = \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}.
$$

Therefore, the decomposition of Lemma 6 can be performed so as to yield only two-level matrices of types

$$
iX, \quad T^{-m}(iH)T^m, \quad \text{and } W, \tag{6}
$$

plus at most one one-level matrix of type ω^m. But since all two-level matrices of types (6), as well as U itself, have determinant 1, it follows that $\omega^m = 1$. We finish the proof by observing that the multiply controlled operators of types (6) possess ancilla-free Clifford + T representations, with the latter two given by





■

As a corollary, we obtain a characterization of the n-qubit Clifford + T group (with no ancillas) for all n.

Corollary 2. Let U be a unitary $2^n \times 2^n$ matrix. Then the following are equivalent:

(a) U can be exactly represented by a quantum circuit over the Clifford + T gate set on n qubits with no ancillas.

(b) The entries of U belong to the ring $\mathbb{Z}[\frac{1}{\sqrt{2}},i]$, and:

(i) $\det U = 1$, if $n \geqslant 4$;

(ii) $\det U \in \{-1,1\}$, if $n = 3$;

(iii) $\det U \in \{i,-1,-i,1\}$, if $n = 2$;

(iv) $\det U \in \{\omega,i,\omega^3,-1,\omega^5,-i,\omega^7,1\}$, if $n \leqslant 1$.

Proof. For (a) $\Rightarrow$ (b), it suffices to note that each of the generators of the Clifford + T group, regarded as an operation on n qubits, satisfies the conditions in (b). For (b) $\Rightarrow$ (a), let us define for convenience $d_0 = d_1 = \omega$, $d_2 = i$, $d_3 = -1$, and $d_n = 1$ for $n \geqslant 4$. First note that for all n, the Clifford + T group on n qubits (without ancillas) contains an element D_n whose determinant is d_n, namely $D_n = I$ for $n \geqslant 4$, $D_3 = T \otimes I \otimes I$, $D_2 = T \otimes I$, $D_1 = T$, and $D_0 = \omega$. Now consider some U satisfying (b). By assumption, $\det U = d_n^m$ for some m. Let $U' = U D_n^{-m}$, then $\det U' = 1$. By Lemma 7, U', and therefore U, is in the Clifford + T group with no ancillas. ■

Remark 7. Note that the last condition in Corollary 2, namely that $\det U$ is a power of ω for $n \leqslant 1$, is of course redundant, as this already follows from $\det U \in \mathbb{Z}[\frac{1}{\sqrt{2}},i]$ and $|\det U| = 1$. We stated the condition for consistency with the case $n \geqslant 2$.

Remark 8. The situation of Theorem 1 and Corollary 2 is analogous to the case of classical reversible circuits. It is well known that the NOT gate, controlled-NOT gate, and Toffoli gate generate all classical reversible functions on $n \leqslant 3$ bits. For $n \geqslant 4$ bits, they generate exactly those reversible boolean functions that define an *even permutation* of their inputs (or equivalently, those that have determinant 1 when viewed in matrix form) [6]; the addition of a single ancilla suffices to recover all boolean functions.

VII. COMPLEXITY

The proof of Theorem 1 immediately yields an algorithm, albeit not a very efficient one, for synthesizing a Clifford + T circuit with ancillas from a given operator U. We estimate the size of the generated circuits.

We first estimate the number of (one- and two-level) operations generated by the matrix decomposition of Lemma 6. The row operation from Lemma 4 requires only a constant number of operations. Reducing a single n-dimensional column from denominator exponent k to $k-1$, as in the induction step of Lemma 5, requires $O(n)$ operations; therefore, the number of operations required to reduce the column completely is $O(nk)$.

Now consider applying Lemma 6 to an $n \times n$ matrix with least denominator exponent k. Reducing the first column requires $O(nk)$ operations, but unfortunately, it may increase the least denominator exponent of the rest of the matrix, in the worst case, to $3k$. Namely, each row operation of Lemma 4 potentially increases the denominator exponent by 2, and any given row may be subject to up to k row operations, resulting in a worst-case increase of its denominator exponent from k to $3k$ during the reduction of the first column. It follows that reducing the second column requires up to $O(3(n-1)k)$ operations, reducing the third column requires up to $O(9(n-2)k)$ operations, and so on. Using the identity $\sum_{j=0}^{n-1} 3^j(n-j) = (3^{n+1}-2n-3)/4$, this results in a total of $O(3^n k)$ one- and two-level operations for Lemma 6.

In the context of Theorem 1, we are dealing with n qubits, i.e., a $2^n \times 2^n$ operator, which therefore decomposes into $O(3^{2^n}k)$ two-level operations. Using one ancilla, each two-level operation can be decomposed into $O(n)$ Clifford + T gates, resulting in a total gate count of $O(3^{2^n}nk)$ elementary Clifford + T gates.

VIII. FUTURE WORK

As mentioned in the introduction, the algorithm arising out of the proof of Theorem 1 produces circuits that are very far from optimal. This can be seen heuristically by taking any simple Clifford + T circuit, calculating the corresponding operator, and then running the algorithm to resynthesize a circuit.

Moreover, it is unlikely that the algorithm is optimal even in the asymptotic sense. The algorithm's worst case gate count of $O(3^{2^n}nk)$ is separated from information-theoretic lower bounds by an exponential gap. Specifically, the number of different unitary n-qubit operators with denominator exponent k can be bounded: for $n \geqslant 1$, it is between $2^{2^{n-1}k}$ and $2^{4^n(4+2k)}$. Therefore, such an operator carries between $\Omega(2^n k)$ and $O(4^n k)$ bits of information. Regardless of where the true number falls within this spectrum, the resulting information-theoretic lower bound for the number of elementary gates required to represent such an operator is exponential, not superexponential, in n.

While the information-theoretic analysis does not, of course, imply the existence of an asymptotically better synthesis algorithm, it nevertheless suggests that it may be worthwhile to look for one.

Given that the gate count estimate is dominated by the term 3^{2^n}, the most obvious target for improvement is the part of the algorithm that causes this superexponential blowup. As noted above, this blowup is caused by the fact that row reductions that reduce the denominator exponent of one column might simultaneously increase the denominator exponent of the remaining columns.

ACKNOWLEDGMENTS

This research was supported by the Natural Sciences and Engineering Research Council of Canada (NSERC). This research was also supported by the Intelligence Advanced Research Projects Activity (IARPA) via Department of Interior National Business Center, Contract No. D11PC20168. The US Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright annotation thereon. Disclaimer: The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of IARPA, DoI/NBC, or the US Government.

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2002).

[2] V. Kliuchnikov, D. Maslov, and M. Mosca, arXiv:1206.5236v3.

[3] M. Amy, D. Maslov, M. Mosca, and M. Roetteler, arXiv:1206.0758v3.

[4] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, Phys. Rev. A **52**, 3457 (1995).

[5] P. Selinger, arXiv:1210.0974 [Phys. Rev. A (to be published)].

[6] J. Musset, Technical Report 97-32, Institut de Mathématiques de Luminy, 1997. Available from http://iml.univ-mrs.fr/editions/.