ACADEMIC
PRESS

Available online at www.sciencedirect.com
SCIENCE @ DIRECT®

J. Math. Anal. Appl. 274 (2002) 69–80

Journal of
MATHEMATICAL
ANALYSIS AND
APPLICATIONS

www.academicpress.com

The universality of the quantum Fourier transform in forming the basis of quantum computing algorithms

Charles M. Bowden,[a] Goong Chen,[b,*,1] Zijian Diao,[b] and Andreas Klappenecker[c,2]

[a] *U.S. Army Missile Command, RD&E Center, Redstone Arsenal, AL 35898-5248, USA*
[b] *Department of Mathematics, Texas A&M University, College Station, TX 77843-3368, USA*
[c] *Department of Computer Science, Texas A&M University, College Station, TX 77843-3112, USA*

Received 26 February 2002

Submitted by R.P. Kertz

Abstract

The quantum Fourier transform (QFT) is a powerful tool in quantum computing. The main ingredients of QFT are formed by the Walsh–Hadamard transform H and phase shifts $P(\cdot)$, both of which are 2×2 unitary matrices as operators on the two-dimensional 1-qubit space. In this paper, we show that H and $P(\cdot)$ suffice to generate the unitary group $U(2)$ and, consequently, through controlled-U operations and their concatenations, the entire unitary group $U(2^n)$ on n qubits can be generated. Since any quantum computing algorithm in an n-qubit quantum computer is based on operations by matrices in $U(2^n)$, in this sense we have the universality of the QFT.

[*] Corresponding author.
E-mail addresses: cmbowden@ro.com (C.M. Bowden), gchen@math.tamu.edu (G. Chen), zijian.diao@math.tamu.edu (Z. Diao), klappi@cs.tamu.edu (A. Klappenecker).

[1] Supported in part by Texas A&M University Interdisciplinary Research Initiative IRI 99-22 and TITF, and DARPA QuIST Grant F49620-01-1-0566.

[2] Supported in part by NSF Grant EIA-0218582, and a Texas A&M University TITF initiative.

PII: S0022-247X(02)00227-5

1. Introduction

The quantum Fourier transform (QFT) on the additive group of integers modulo 2^m is defined by

$$\mathcal{F}_{2^m}\big(|a\rangle\big) = \frac{1}{2^{m/2}} \sum_{y=0}^{2^m-1} e^{2\pi i a y/2^m} |y\rangle, \quad \text{for } a \in \{0, 1, 2, \ldots, 2^m - 1\}. \tag{1}$$

QFT plays a significant role in the development of the quantum computer (QC). One may note, for example, that the potentially powerful integer factoring algorithm by Shor relies critically on the QFT for the detection of periodicity springing from the prime factors.

We can further analyze (1) as follows. First, write

$$a = a_1 2^{m-1} + a_2 2^{m-2} + \cdots + a_{m-1} 2^1 + a_m 2^0 = (a_1 a_2 \ldots a_m)$$

and

$$y = y_1 2^{m-1} + y_2 2^{m-2} + \cdots + y_{m-1} 2^1 + y_m 2^0 = (y_1 y_2 \ldots y_m).$$

Then it is well known that

$$\begin{aligned}\text{RHS of (1)} &= \frac{1}{2^{m/2}} \sum_{y=0}^{2^m-1} e^{(2\pi i a y/2^m)} |y_1 \ldots y_m\rangle \\ &= \frac{1}{2^{m/2}} \sum_{y=0}^{2^m-1} e^{2\pi i (0.a_m) y_1} |y_1\rangle e^{2\pi i (0.a_{m-1} a_m) y_2} |y_2\rangle \ldots \\ &\quad \times e^{2\pi i (0.a_1 a_2 \ldots a_m) y_m} |y_m\rangle \\ &= \frac{1}{2^{m/2}} \big(|0\rangle + e^{2\pi i (0.a_m)} |1\rangle\big)\big(|0\rangle + e^{2\pi i (0.a_{m-1} a_m)} |1\rangle\big) \ldots \\ &\quad \times \big(|0\rangle + e^{2\pi i (0.a_1 a_2 \ldots a_m)} |1\rangle\big). \end{aligned} \tag{2}$$

In the above factorization (or “untangling”), each factor is of the form

$$|0\rangle + e^{i\omega} |1\rangle. \tag{3}$$

Such a state can be produced in two steps [2, pp. 340–341]: First, apply the transformation

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \tag{4}$$

where H is known as the Walsh–Hadamard transform, to the state $|0\rangle$:

$$H|0\rangle = \frac{1}{\sqrt{2}} \big(|0\rangle + |1\rangle\big). \tag{5}$$

Next, apply the phase shift operator

$$P(\omega)=\begin{bmatrix}1 & 0\\ 0 & e^{i\omega}\end{bmatrix} \tag{6}$$

to (5), yielding

$$P(\omega)\bigl[H|0\rangle\bigr]=\frac{1}{\sqrt{2}}\bigl(|0\rangle+e^{i\omega}|1\rangle\bigr). \tag{7}$$

The RHS of (7) is (3) (apart from a normalization coefficient). Therefore, we see that the constituents of the QFT are H and $P(\omega)$. From the quantum optics point of view, H is realized by a half-silvered mirror (beam splitter) and $P(\omega)$ represents a phase shifter, as in a standard Mach–Zehnder interferometer [2,4].

First, we wish to emphasize that the QFT strictly by itself is *not universal* in quantum computing; see Remark 2 below. Thus, the question becomes whether the two constituents H an $P(\cdot)$ of QFT are universal or not. The question we want to pose here is the following:

[Q] "Can any QC algorithm be represented as a composition of
Walsh–Hadamard transforms and associated conditional
phase shifts?" (8)

The implication of (8) is that the realization of any QC algorithm translates into a combination of elementary quantum interferometric operations, i.e., single particle beam splitter (Walsh–Hadamard transform) followed by a conditional phase shift. Any QC algorithm can thus be formulated, or reformulated, in terms of elementary multiparticle quantum interferometric operations. The unique universal fundamental properties of QC concerning quantum superposition, entanglement and interference are all explicitly represented in terms of quantum multiparticle interferometry (QMI).

QMI practically is not to be taken as a proposed embodiment of a QC any more than the Turing machine is to be taken as a literal construction in classical computing. Rather, Ekert [3] has suggested its equivalence to QC in the sense of its universality, meaning that QMI could be viewed as the closest QC analogue of the classical Turing machine (through the universality theorem established in this paper). This concept and viewpoint should provide physical insights into the operational aspects and can facilitate efficient design of a universal QC.

2. Mathematical proof of the universality of H and $P(\cdot)$

Our answer to [Q] is affirmative. We now proceed to provide the mathematical justifications below.

As usual, we let $U(n)$ to denote the unitary group on n-dimensional space. By abuse of notation, we regard $U(n)$ the same as the multiplicative group of all

$n \times n$ unitary matrices. $SO(n)$ denotes the orthogonal group on n-dimensional spaces or, equally, the multiplicative group of all $n \times n$ orthogonal matrices. We also define the *maximal torus* $T(n)$ in $U(n)$ as

$$T(n) = \left\{\operatorname{diag}(e^{i\omega_1}, \dots, e^{i\omega_n}) \mid \omega_1, \omega_2, \dots, \omega_n \in \mathbb{R}\right\},$$

i.e., $T(n)$ consists of all $n \times n$ diagonal matrices whose diagonal entries are complex numbers of unit magnitude. $T(n)$ is a subgroup of the multiplicative group $U(n)$.

Let $\mathcal{A}$ be a collection of $n \times n$ unitary matrices. In this paper, we will use $\mathcal{G}_n(\mathcal{A})$ to denote *the unitary subgroup of $U(n)$ generated by $\mathcal{A}$*, i.e.,

$$\mathcal{G}_n(\mathcal{A}) = \bigcap_\alpha \{G_\alpha \mid G_\alpha \text{ is a subgroup of } U(n),\ \mathcal{A} \subseteq G_\alpha\}.$$

We will write $\mathcal{G}_n(\mathcal{A})$ simply as $\mathcal{G}(\mathcal{A})$ if the value of n is clear from the context.

We begin with $n = 2$.

Lemma 1 [1, Lemma 4.1]. *We have $U(2) = \mathcal{G}(SO(2), T(2))$, i.e., $U(2)$ is generated by $SO(2)$ and $T(2)$; more precisely, for every $A \in U(2)$, we have*

$$A = \begin{bmatrix} e^{i\delta} & 0 \\ 0 & e^{i\delta} \end{bmatrix} \begin{bmatrix} e^{i\alpha/2} & 0 \\ 0 & e^{-i\alpha/2} \end{bmatrix} \begin{bmatrix} \cos\omega & \sin\omega \\ -\sin\omega & \cos\omega \end{bmatrix} \begin{bmatrix} e^{i\beta/2} & 0 \\ 0 & e^{-i\beta/2} \end{bmatrix},$$

for some $\alpha, \beta, \delta, \omega \in \mathbb{R}$.

Lemma 2. $T(2) \subseteq \mathcal{G}(H, P(\cdot))$.

Proof. We first note that the NOT-gate

$$X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{9}$$

can be obtained as

$$X = HP(-\pi)H. \tag{10}$$

Therefore $X \in \mathcal{G}(H, P(\cdot))$. From this, we have

$$\begin{aligned} XP(\omega_1)XP(\omega_2) &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & e^{i\omega_1} \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & e^{i\omega_2} \end{bmatrix} \\ &= \begin{bmatrix} e^{i\omega_1} & 0 \\ 0 & e^{i\omega_2} \end{bmatrix}, \end{aligned} \tag{11}$$

for any given $\omega_1, \omega_2 \in \mathbb{R}$. Therefore $\mathcal{G}(H, P(\cdot))$ contains the maximal torus $T(2)$. □

Lemma 3. $SO(2) \subseteq \mathcal{G}(H, P(\cdot))$.

Proof. For each rotation matrix

$$R(\omega)=\begin{bmatrix}\cos\omega & \sin\omega\\ -\sin\omega & \cos\omega\end{bmatrix},$$

we easily verify that

$$R(\omega)=P\left(\frac{\pi}{2}\right)HP(\omega)XP(-\omega)HP\left(-\frac{\pi}{2}\right). \qquad \square \tag{12}$$

Theorem 4. $\mathcal{G}(H,P(\cdot))=U(2)$.

Proof. This follows immediately from Lemmas 1–3. □

At this point, it should already be clear from the results in [1] that $U(2^n)$ *can be generated through controlled-*$U(2)$ *gates* for any $n=1,2,\ldots$. To make this paper sufficiently self-contained, however, let us give the following concise, rigorous treatment as to how to construct any $V\in U(2^n)$ from a serial connection of a collection of unitary matrices V_{ij}, where each V_{ij} is a (generalized) controlled-$U(2)$ gate. The precise statement is given below.

Theorem 5. *Let* $V\in U(2^n)$*. Then*

$$V=\prod_{i=1}^{2^n-1}\prod_{j=0}^{i-1}V_{ij} \tag{13}$$

for a collection of matrices $V_{ij}\in U(2^n)$ *such that*

$$\left\{\begin{array}{l} V_{ij}:\mathcal{S}_{ij}\to\mathcal{S}_{ij}\ \text{is the identity transformation},\\ \mathcal{S}_{ij}\equiv\operatorname{span}\{|m\rangle \mid m\in\{0,1,\ldots,2^n-1\},\ m\neq i,\ m\neq j\},\\ \quad 0\leqslant j<i\leqslant 2^n-1\end{array}\right\}. \tag{14}$$

In other words, each $V\in U(2^n)$ *is a product of* (*generalized*) *controlled-*$U(2)$ *unitary matrices* V_{ij}*, which acts nontrivially only on* $\mathcal{S}_{ij}^{\perp}=\operatorname{span}\{|i\rangle,|j\rangle\}$.

Proof. We first quote the following fact [5,6]: For any $V\in U(2^n)$, there exists a collection of unitary matrices $T_{i,j}$, $0\leqslant j<i\leqslant 2^n-1$, and a $D\in T(2^n)$ such that

$$V=\left(\prod_{i=1}^{2^n-1}\prod_{j=0}^{i-1}T_{i,j}\right)D, \tag{15}$$

where $T_{i,j}\in SO(2^n)\subseteq U(2^n)$ is a rotation involving $|i\rangle$ and $|j\rangle$ and satisfying (14). For the benefit of the reader and for the sake of self-containedness, we include a direct proof of (15) in Appendix A, condensed from [5].

Now we can break up D into

$$D = \begin{pmatrix} d_0 & & & \\ & d_1 & & \\ & & \ddots & \\ & & & d_{2^n-1} \end{pmatrix} = D_1 D_2 \dots D_{2^n-1}, \tag{16}$$

where

$$D_1 = \begin{pmatrix} d_0 & 0 & & & \\ 0 & d_1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix} \tag{17}$$

and

$$D_i = \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & d_i & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix} \tag{18}$$

for $i = 2, 3, \dots, 2^n - 1$. It is easy to see that D_1 acts trivially except on $|0\rangle$ and $|1\rangle$, and the other D_i's act nontrivially only on $|i\rangle$. In addition, D_i's commute with each other, and each D_i commutes with $T_{k,l}$, $\forall 0 \leqslant l < k < i$, as well. Thus,

$$\begin{aligned} V &= T_{2^n-1,2^n-2} \dots T_{2^n-1,0} T_{2^n-2,2^n-3} \dots T_{2^n-2,0} \dots \\ &\quad \times T_{2,1} T_{2,0} T_{1,0} D_1 D_2 \dots D_{2^n-1} \\ &\left.\begin{aligned} &= T_{2^n-1,2^n-2} T_{2^n-2,2^n-3} \dots T_{2^n-1,0} D_{2^n-1} \\ &\quad \times T_{2^n-2,2^n-3} \dots T_{2^n-2,0} D_{2^n-2} \\ &\quad\ \vdots \\ &\quad \times T_{2,1} T_{2,0} D_2 \\ &\quad \times T_{1,0} D_1 \end{aligned}\right\} 2^n-1 \text{ strings of products} \end{aligned} \tag{19}$$

For $0 \leqslant j < i \leqslant 2^n - 1$, define

$$V_{ij} = \begin{cases} T_{i,j} & \text{if } j \neq 0, \\ T_{i,j} D_i = T_{i,0} D_i & \text{if } j = 0. \end{cases}$$

Therefore we have reached

$$V = \prod_{i=1}^{2^n-1} \prod_{j=0}^{i-1} V_{ij},$$

where each V_{ij} is a unitary matrix which acts nontrivially only on the states $|i\rangle$ and $|j\rangle$ satisfying (14). □

Remark 1. (1) In Barenco et al. [1, p. 3465, right column, line 34], the equation there corresponds to our Eq. (15). However, a summation sign $\sum$ is used instead of the product sign $\prod$ (which is actually a double product $\prod_i \prod_j$ in our (15)) which, of course, is a misprint.

(2) The factoring of D in (16) into the product of $D_1, D_2, \ldots$ and D_{2^n-1} in the form of (17) and (18) is peculiar in the sense that D_1 is chosen differently from the other D_i's, $i \neq 1$. It must be done this way (but no further mathematical explanations were given in [1]. The reason for this is that there are $2^n - 1$ strings of products as indicated in (19). Therefore D must be factorized to have $2^n - 1$ factors $D_1, D_2, \ldots, D_{2^n-1}$, in the unique way of (17) and (18) in order to satisfy (14).

Remark 2. Now it can be readily seen that the QFT itself is not universal in the sense that $U(2^n)$ is not generated by $\mathcal{F}_{2^n}$ (cf. (1), with $m = n$ therein) or (generalized) controlled-$\mathcal{F}_{2^m}$ (where $m < n$) operations. First, check $n = 1$: We see that $\mathcal{F}_{2^n} = \mathcal{F}_2$ is actually the Walsh–Hadamard transform H (apart from the normalization factor $1/\sqrt{2}$). Therefore, the phase shifts $P(\omega)$ in (6) cannot be generated by $\mathcal{F}_2$ because $P(\omega)$ has eigenvalues 1 and $e^{i\omega}$ while H has eigenvalues 1 and -1. For a general positive integer n, the range of $\mathcal{F}_{2^n}$ or of controlled-$\mathcal{F}_{2^m}$, $m < n$, consists at most of linear combinations of states of the form

$$e^{2\pi i[(0.a_n)y_1+(0.a_{n-1}a_n)y_2+\cdots+(0.a_1\ldots a_n)y_n]}|y_1 \ldots y_n\rangle,$$

where $a_j, y_j \in \{0, 1\}$, for $j = 1, 2, \ldots, n$. The phases of such states are *not even dense* with respect to all possible phases $e^{2\pi i\theta}$, $0 \leqslant \theta < 2\pi$.

3. Remarks on circuits

The decomposition (13) is a mathematical rendering of statement [Q] and answers the conjecture affirmatively. In this section, let us further elaborate on the circuit design aspects, based on the work in Barenco et al. [1, Section VIII] and [4].

Each factor V_{ij} in (13) satisfies (14) and thus V_{ij} acts nontrivially only on the states $|i\rangle$ and $|j\rangle$. Denote the restriction of V_{ij} to the 2-dimensional subspace $\mathcal{S}_{ij}^{\perp} = \mathrm{span}\{|i\rangle, |j\rangle\}$ by $\widehat{V}_{ij}$. Then $\widehat{V}_{ij} \in U(2)$. As pointed out in [1, p. 3465], each V_{ij} is not a standard $\Lambda_{n-1}(\widehat{V}_{ij})$ (in the notation of [1, p. 3458]) gate in the sense that the *controls are states rather than bits*.

Nevertheless, using Proposition 6 below, Barenco et al. [1, Section VIII] point out how to rearrange basis states with a "gray code connecting state $|i\rangle$ to state $|j\rangle$" such that V_{ij} becomes unitarily equivalent to $\Lambda_{n-1}(\widehat{V}_{ij})$. In this sense, V_{ij} are *generalized* controlled-$\widehat{V}_{ij}$ gates.

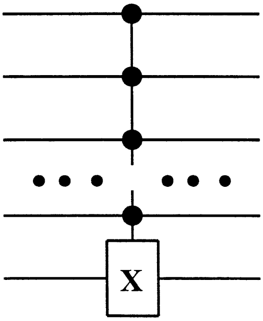

Fig. 1. The n-bit controlled-NOT gate $\Lambda_{n-1}(X)$, where X is given by (9). This gate implements the two cycle $(2^n - 2, 2^n - 1)$ in Proposition 6.

Proposition 6. *The symmetric group* S_{2^n} *of permutations on the symbols* $0, 1, 2, \ldots, 2^n - 1$ *is generated by the 2-cycle* $(2^n - 2, 2^n - 1)$ *and the* 2^n*-cycle* $(0, 1, 2, \ldots, 2^n - 1)$.

Proof. This is a basic fact which can be found in most basic algebra or group theory books.

Incidentally, we note that the 2-cycle $(2^n - 2, 2^n - 1)$ is a permutation between the states

$$|\underbrace{1\,1\ldots1\,0}_{n \text{ bits}}\rangle \quad \text{and} \quad |\underbrace{1\,1\ldots1}_{n \text{ bits}}\rangle$$

and thus can be realized by the controlled-NOT gate with the nth qubit as the *target bit* and the first $(n - 1)$ bits as the *control bits* as shown in Fig. 1.

On the other hand, the 2^n-cycle $(0, 1, 2, \ldots, 2^n - 1)$ makes the rotation of the states $|0\rangle \to |1\rangle \to \cdots \to |2^n - 2\rangle \to |2^n - 1\rangle \to |0\rangle$, i.e., the $|x\rangle \to |x + 1 \bmod 2^n\rangle$ operation. This can be implemented by the circuit as shown in Fig. 2. □

Therefore, any permutation of the basis states $|x\rangle$, $x = 0, 1, 2, \ldots, 2^n - 1$, can be realized by finitely many controlled-NOT operations consisting of circuits as shown in Figs. 1 and 2.

Thus, each factor V_{ij} in (13) can be realized by the circuit as shown in Fig. 3.

By concatenating together all the blocks V_{ij} as shown in Fig. 3 according to the factorization (13), we have constructed all $V \in U(2^n)$ with controlled-$\widehat{V}_{ij}$ gates according to (13). Each $\widehat{V}_{ij} \in U(2)$ is then further formed from concatenations of the gates H, $P(\omega) \in U(2)$ by Theorem 4. It is in this sense that we have the universality of the Walsh–Hadamard gate H and the phase shift gate $P(\cdot)$ and, consequently, that of the quantum Fourier transform with the affirmative answer to question [Q] in (10).

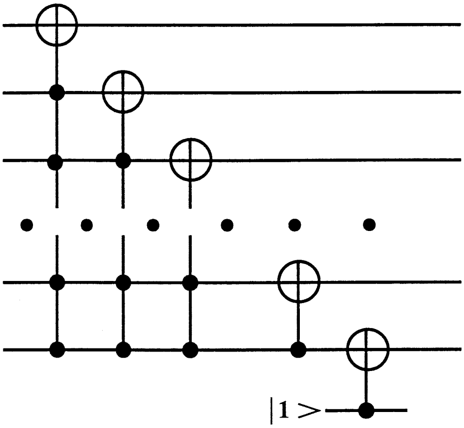

Fig. 2. This circuit implements the operation $|x\rangle \to |x+1 \bmod 2^n\rangle$ or, equivalently, the 2^n-cycle $(0, 1, 2, \ldots, 2^n - 1)$ in Proposition 6. Note that the bit $|1\rangle$ at the bottom of the figure is the "scratch bit" which is sometimes omitted in circuit drawing. All the gates in this circuit are controlled-NOT gates.

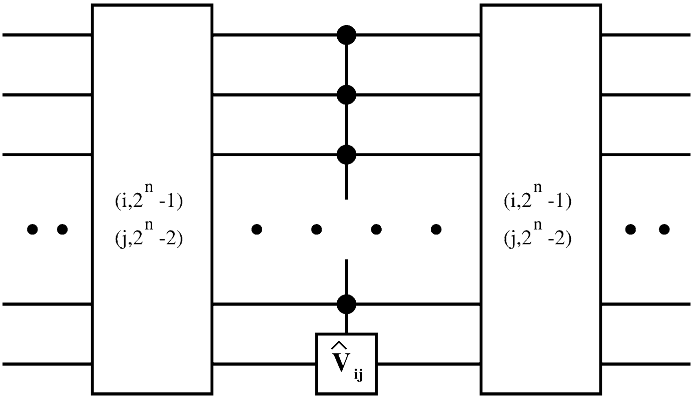

Fig. 3. The unitary matrix V_{ij} in (13) as a controlled-$\widehat{V}_{ij}$ gate where $\widehat{V}_{ij} \in U(2)$. The operations $(i, 2^n - 1)$ and $(j, 2^n - 2)$ in the two boxes are cyclic permutations (which can be realized by concatenations of circuits in Figs. 1 and 2).

Appendix A. Decomposition procedure of general finite-dimensional unitary transformations into a product of plane unitary transformations

First, we define a special type of unitary transformations $T_{pq}(\phi, \sigma) \in U(n)$ by

$$T_{pq}(\phi, \sigma) = [t_{ij}]_{n\times n}, \quad 1 \leqslant p, q \leqslant n, \ p \neq q,$$

where

$$t_{ij} = \begin{cases} 1, & i = j,\ i \neq p,\ i \neq q, \\ \cos\phi, & i = j = p \text{ or } i = j = q, \\ 0, & i \neq j,\ i \neq p,\ j \neq q \text{ and } i \neq q,\ j \neq p, \\ -e^{-i\sigma}\sin\phi, & i = p \text{ and } j = q, \\ e^{i\sigma}\sin\phi, & i = q \text{ and } j = p; \end{cases}$$

i.e.,

$$T_{pq}(\phi,\sigma) = (\,p \quad q\,)\begin{pmatrix} p \\ q \end{pmatrix}$$

$$\times \begin{bmatrix} 1 & 0 & 0 & & & & & & 0 \\ 0 & 1 & & & & & & & \\ & & 1 & & & & & & \\ & & & \ddots & & & & & \\ & & & & \cos\phi & -e^{-i\sigma}\sin\phi & & & \\ & & & & e^{i\sigma}\sin\phi & \cos\phi & & & \\ & & & & & & 1 & & 0 \\ 0 & 0 & & & & & & \ddots & \\ & & & & & & & 0 & 1 \end{bmatrix}.$$

$T_{pq}(\phi,\sigma)$ is just a plane unitary transformation acting nontrivially only on states p and q.

Let $V \in U(n)$. We want to find some $T_{n,n-1}(\phi,\sigma)$ such that $T^*_{n,n-1}V = V' = [v'_{ij}]_{n\times n}$, where $v'_{n-1,n} = 0$:

$$T^*_{n,n-1}V = \begin{bmatrix} 1 & 0 & 0 & & & \\ 0 & 1 & 0 & & & \\ 0 & 0 & 1 & & \bigcirc & \\ & & & \ddots & & \\ & & & & \cos\phi & e^{-i\sigma}\sin\phi \\ & & \bigcirc & & -e^{i\sigma}\sin\phi & \cos\phi \end{bmatrix}$$

$$\times \begin{bmatrix} v_{11} & \cdots & v_{1,n-1} & v_{1n} \\ \vdots & & \vdots & \vdots \\ v_{n-1,1} & \cdots & v_{n-1,n-1} & v_{n-1,n} \\ v_{n1} & \cdots & v_{n,n-1} & v_{nn} \end{bmatrix},$$

so

$$v'_{n-1,n} = v_{n-1,n}\cos\phi + v_{nn}e^{-i\sigma}\sin\phi.$$

We consider all possibilites:

Case 1: $v_{n-1,n} = 0$. Then we choose $\phi = 0$, $\sigma = 0$, i.e., $T_{n-1,n}(\phi,\sigma) = I_n$, and we obtain $v'_{n-1,n} = v_{n-1,n} = 0$.

Case 2: $v_{n-1,n} \neq 0$, $v_{nn} = 0$. Then choose $\phi = \pi/2$, $\sigma = 0$. Obtain $v'_{n-1,n} = 0$.

Case 3: $v_{n-1,n} \neq 0$, $v_{nn} \neq 0$. Write $v_{n-1,n} = r_{n-1,n}e^{i\theta_{n-1,n}}$, $v_{nn} = r_{nn}e^{i\theta_{nn}}$. Choose $\sigma = -\theta_{n-1,n} + \theta_{nn}$ and $\phi = \tan^{-1}(-r_{n-1,n}/r_{nn})$. Obtain

$$\begin{aligned} v'_{n-1,n} &= \cos\phi \cdot r_{n-1,n}e^{i\theta_{n-1,n}} + \sin\phi \cdot r_{nn}e^{i(-\sigma+\theta_{nn})} \\ &= \left(\frac{r_{n-1,n}}{r_{nn}} + \tan\phi\right) r_{nn}\cos\phi e^{i\theta_{n-1,n}} = 0. \end{aligned}$$

Therefore, we have found $T_{n,n-1} \in U(n)$ such that

$$T^*_{n,n-1}V = \left[\begin{array}{ccc|c} * & \dots & * & v'_{1n} \\ \vdots & & \vdots & \vdots \\ \vdots & & \vdots & v'_{n-2,n} \\ * & \dots & * & 0 \\ \cline{1-3} v'_{n1} & \dots & v'_{n,n-1} & v'_{nn} \end{array}\right].$$

Similarly, we can find $T_{n,n-2}, T_{n,n-3}, \dots, T_{n,1}$ such that

$$T^*_{n,n-2}T^*_{n,n-1}V = \begin{bmatrix} * & \dots & * & v''_{1n} \\ \vdots & & \vdots & \vdots \\ \vdots & & \vdots & v''_{n-3,n} \\ \vdots & & \vdots & 0 \\ * & \dots & * & 0 \\ v''_{n1} & \dots & v''_{n,n-1} & v''_{nn} \end{bmatrix},$$

$$\vdots$$

$$T^*_{n1}T^*_{n2}\cdots T^*_{n,n-2}T^*_{n,n-1}V = \begin{bmatrix} * & \dots & * & 0 \\ \vdots & & \vdots & 0 \\ \vdots & & \vdots & \vdots \\ * & \dots & * & 0 \\ \tilde{v}_{n1} & \dots & \tilde{v}_{n,n-1} & \tilde{v}_{nn} \end{bmatrix} \equiv W.$$

Since W is unitary, we conclude $\tilde{v}_{n1} = \tilde{v}_{n2} = \cdots = \tilde{v}_{n,n-1} = 0$ and $\tilde{v}_{nn} = e^{i\alpha_n} \equiv d_n$ for some $\alpha_n \in \mathbb{R}$. Thus

$$T^*_{n1}T^*_{n2}\cdots T^*_{n,n-2}T^*_{n,n-1}V = \left[\begin{array}{ccc|c} & & & 0 \\ & ** & & \vdots \\ & & & 0 \\ \cline{1-3} 0 & \dots & 0 & d_n \end{array}\right].$$

Now, applying the same technique to the remaining $(n-1) \times (n-1)$ undiagonalized matrix block $(**)$ above, together with a simple induction argument, we obtain plane unitary transformation $T_{n1}, \ldots, T_{n,n-1}, T_{n-1,1}, \ldots, T_{n-1,n-2}, \ldots, T_{31}$, T_{32} and T_{21} such that

$$\begin{aligned} &T_{21}^*T_{31}^*T_{32}^*T_{41}^* \ldots T_{n-1,1}^* \ldots T_{n-1,n-2}^*T_{n1}^* \ldots T_{n,n-1}^*V \\ &\quad = \begin{bmatrix} d_1 & & \\ & d_2 & & 0 \\ & & \ddots & \\ & 0 & & d_n \end{bmatrix} = D, \end{aligned}$$

where $d_j = e^{i\alpha_j}$ for $j = 1, 2, \ldots, n$.

Therefore

$$\begin{aligned} V &= T_{n,n-1}T_{n,n-2} \ldots T_{n1}T_{n-1,n-2} \ldots T_{n-1,1} \ldots T_{32}T_{31}T_{21}D \\ &= \left(\prod_{i=1}^{n}\prod_{j=1}^{i-1} T_{i,j}\right)D \end{aligned}$$

and (15) is proved.

References

[1] A. Barenco, C.H. Bennett, R. Cleve, D.P. Divincenzo, N. Margolus, P. Shor, T. Sleator, J.A. Smolin, H. Weinfurter, Elementary gates for quantum computation, Phys. Rev. A 52 (1995) 3457–3467.

[2] R. Cleve, A. Ekert, C. Macchiavello, M. Mosca, Quantum algorithms revisited, Proc. Roy. Soc. London Ser. A 454 (1998) 339–354.

[3] A. Ekert, Quantum interferometers as quantum computers, Phys. Scripta T 76 (1998) 218–222.

[4] A. Klappenecker, Computing with a quantum flavor, manuscript (2000).

[5] F.D. Murnaghan, The Unitary and Rotation Groups, Spartan, Washington, DC, 1962.

[6] M. Reck, A. Zeilinger, H.J. Bernstein, P. Bertani, Experimental realization of any discrete unitary operator, Phys. Rev. Lett. 73 (1994) 58–61.