

## A remark on the unitary group of a tensor product of $n$ finite-dimensional Hilbert spaces

K R PARTHASARATHY

Indian Statistical Institute, Delhi Centre, 7, S.J.S. Sansanwal Marg,  
New Delhi 110 016, India  
E-mail: krp@isid.ac.in

MS received 7 September 2001

**Abstract.** Let  $H_i$ ,  $1 \leq i \leq n$  be complex finite-dimensional Hilbert spaces of dimension  $d_i$ ,  $1 \leq i \leq n$  respectively with  $d_i \geq 2$  for every  $i$ . By using the method of quantum circuits in the theory of quantum computing as outlined in Nielsen and Chuang [2] and using a key lemma of Jaikumar [1] we show that every unitary operator on the tensor product  $H = H_1 \otimes H_2 \otimes \dots \otimes H_n$  can be expressed as a composition of a finite number of unitary operators living on pair products  $H_i \otimes H_j$ ,  $1 \leq i, j \leq n$ . An estimate of the number of operators appearing in such a composition is obtained.

**Keywords.**  $n$ -qubit quantum computer; qubits; gates; controlled gates.

### 1. Introduction

From the theory of quantum computing and quantum circuits (as outlined, for example, in [2]) it is now well-known that every unitary operator on the  $n$ -fold tensor product  $(\mathbf{C}^2)^{\otimes n}$  of copies of the two-dimensional Hilbert space  $\mathbf{C}^2$  can be expressed as a composition of a finite number of unitary operators living on pair products  $H_i \otimes H_j$  where  $H_i$  and  $H_j$  denote the  $i$ th and  $j$ th copies of  $\mathbf{C}^2$ . The proof outlined in [2] also yields an upperbound on the number of such ‘pair product’ operators as a function of  $n$ . Following more or less their lines of proof and using a key lemma suggested to me by Jaikumar we present a generalization when copies of  $\mathbf{C}^2$  are replaced by arbitrary finite-dimensional complex Hilbert spaces. Thus the present note is of a pedagogical and expository nature.

### 2. The main theorem

Let  $H_i$ ,  $1 \leq i \leq n$  be complex finite-dimensional Hilbert spaces with  $\dim H_i = d_i \geq 2$  for every  $i$ . Let

$$H = H_1 \otimes H_2 \otimes \dots \otimes H_n. \quad (2.1)$$

We shall identify  $H_i$  with  $L^2(\mathbf{Z}_{d_i})$  where  $\mathbf{Z}_{d_i}$  is the additive Abelian group  $\{0, 1, 2, \dots, d_i - 1\}$  with addition modulo  $d_i$ , denoted by  $\oplus$ . For any  $x \in \mathbf{Z}_{d_i}$  we denote

$$|x\rangle = 1_{\{x\}}$$

---

Dedicated to Prof. A.K. Roy on his 62nd birthday.

where the right-hand side is the indicator function of the singleton set  $\{x\}$  in  $\mathbf{Z}_{d_i}$ . Thus  $|x\rangle$  is a ket vector in  $H_i$  and  $\{|x\rangle, x \in \mathbf{Z}_{d_i}\}$  is an orthonormal basis for  $H_i$ . For  $\underline{x} = (x_1, x_2, \dots, x_n)$ ,  $x_i \in \mathbf{Z}_{d_i}$  we write  $|\underline{x}\rangle = |x_1\rangle|x_2\rangle \dots |x_n\rangle = |x_1\rangle \otimes |x_2\rangle \otimes \dots \otimes |x_n\rangle$  for the product vector in Dirac notation. Then  $\{|\underline{x}\rangle, x_i \in \mathbf{Z}_{d_i}, 1 \leq i \leq n\}$  is an orthonormal basis for  $H$  as defined in (2.1).

A unitary operator  $U$  on  $H$  is called an  $(i, j)$ -gate for some  $1 \leq i < j \leq n$  if it satisfies

$$U|x_1, x_2 \dots zx_n\rangle = \sum_{y \in \mathbf{Z}_{d_i}, z \in \mathbf{Z}_{d_j}} u(x_i, x_j, y, z) |x_1, x_2 \dots x_{i-1}\rangle |y\rangle |x_{i+1}x_{i+2} \dots x_{j-1}\rangle |z\rangle |x_{j+1}x_{j+2} \dots x_n\rangle$$

for some scalars  $u(x_i, x_j, y, z)$  depending on  $x_i, x_j, y, z$ .

**Theorem 1.** *There exists an integer  $D = D(d_1, d_2, \dots, d_n)$  such that every unitary operator  $U$  on  $H$  is a composition of the form*

$$U = U_{i_1 j_1} U_{i_2 j_2} \dots U_{i_k j_k}, \quad k \leq D$$

where  $U_{i_r j_r}$  is an  $(i_r, j_r)$ -gate for each  $r = 1, 2, \dots, k$ .

We divide the proof into several elementary lemmas and finally obtain an upper bound for  $D$ . Our first lemma and its proof are taken from [2] and presented for the reader's convenience. To state it we need a definition.

Let  $\mathcal{H}$  be an  $N$ -dimensional complex Hilbert space with a fixed orthonormal basis  $\{e_1, e_2, \dots, e_N\}$ . A unitary operator  $U$  in  $\mathcal{H}$  is said to be *elementary* with respect to this basis and *rooted* in the pair  $\{e_i, e_j\}$  for some  $1 \leq i < j \leq N$  if there exist scalars  $\alpha, \beta$  satisfying  $|\alpha|^2 + |\beta|^2 = 1$  and

$$\begin{aligned} Ue_i &= \alpha e_i + \beta e_j, \\ Ue_j &= -\bar{\beta} e_i + \bar{\alpha} e_j, \\ Ue_k &= e_k \quad \text{for every } k \notin \{i, j\}. \end{aligned}$$

*Lemma 1.* *Let  $U$  be any unitary operator in a complex Hilbert space  $\mathcal{H}$  with an orthonormal basis  $\{e_1, e_2, \dots, e_N\}$ . Then  $U$  can be expressed as*

$$U = \lambda U_1 U_2 \dots U_k, \quad k \leq \frac{N(N-1)}{2}$$

where  $\lambda$  is a scalar of modulus unity and each  $U_i$  is elementary with respect to the basis  $\{e_1, e_2, \dots, e_N\}$ .

*Proof.* Let the matrix of  $U$  in the basis  $\{e_1, e_2, \dots, e_N\}$ , denoted by  $U$  again, be given by

$$U = \begin{bmatrix} u_{11} & u_{12} & \dots & u_{1N} \\ u_{21} & u_{22} & \dots & u_{2N} \\ \dots & \dots & \dots & \dots \\ u_{N1} & u_{N2} & \dots & u_{NN} \end{bmatrix}.$$

If  $u_{21} = 0$ , do nothing. If  $u_{21} \neq 0$ , left multiply both sides by

$$U_1 = \left[ \begin{array}{cc|c} \alpha & \beta & 0 \\ -\bar{\beta} & \bar{\alpha} & \\ \hline 0 & & I_{N-2} \end{array} \right]$$

where

$$\alpha = \frac{\bar{u}_{11}}{\sqrt{|u_{11}|^2 + |u_{21}|^2}}, \quad \beta = \frac{\bar{u}_{21}}{\sqrt{|u_{11}|^2 + |u_{21}|^2}}.$$

Then the matrix  $U_1U$  assumes the form

$$U_1U = \begin{bmatrix} u'_{11} & u'_{12} & \cdots & u'_{1N} \\ 0 & u'_{22} & \cdots & u'_{2N} \\ u_{31} & u_{32} & \cdots & u_{3N} \\ \cdots & \cdots & \cdots & \cdots \\ u_{N1} & u_{N2} & \cdots & u_{NN} \end{bmatrix}.$$

We now repeat the same procedure with left multiplication by a  $U_2$  which is elementary and rooted in  $\{e_1, e_3\}$  and make the 31 entry in  $U_2U_1U$  vanish. Continuing this  $N - 1$  times we get

$$U_{N-1}U_{N-2} \cdots U_2U_1U = \begin{bmatrix} v_{11} & v_{12} & \cdots & v_{1N} \\ 0 & v_{22} & \cdots & v_{2N} \\ 0 & v_{32} & \cdots & v_{3N} \\ \vdots & \vdots & & \vdots \\ 0 & v_{N2} & \cdots & v_{NN} \end{bmatrix}.$$

The orthonormality of the column vectors on the right-hand side implies  $|v_{11}| = 1, v_{12} = v_{13} = \cdots = v_{1N} = 0$ . Thus

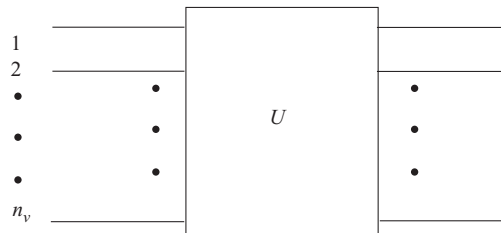
$$\bar{v}_{11}U_{N-1}U_{N-2} \cdots U_2U_1U = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & w_{22} & \cdots & w_{2N} \\ \vdots & \vdots & & \vdots \\ 0 & w_{N2} & \cdots & w_{NN} \end{bmatrix}.$$

Now an induction on the size of the matrix and pooling of the scalars shows the existence of a scalar  $\lambda$  and elementary unitary matrices  $U_1, U_2, \dots, U_k$  such that

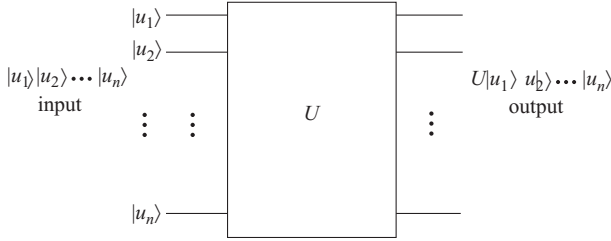
$$\bar{\lambda}U_kU_{k-1} \cdots U_1U = I.$$

Transferring the scalar and the  $U_i$ 's to the right-hand side gives the required composition with  $k \leq (N - 1) + (N - 2) + \cdots + 2 + 1 = N(N - 1)/2$ .  $\square$

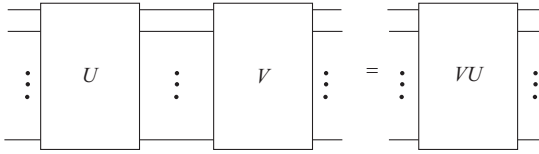
Following the methods of quantum computing we draw a 'circuit diagram' by indicating  $H_i$  by a 'wire' and a unitary operator  $U$  on  $H = H_1 \otimes H_2 \otimes \cdots \otimes H_n$  by



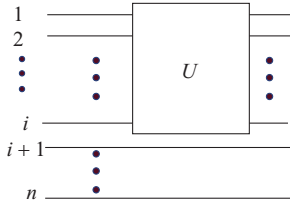
and call  $U$  a *gate*. If  $u_i \in H_i$  and  $|u_1\rangle|u_2\rangle \dots |u_n\rangle \in H$  we say that the gate  $U$  produces the *output*  $U|u_1\rangle|u_2\rangle \dots |u_n\rangle$  for the *input*  $|u_1\rangle|u_2\rangle \dots |u_n\rangle$  and express it as



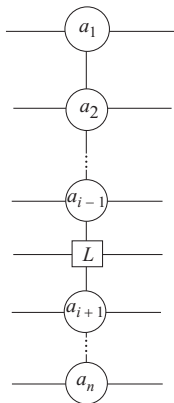
If we have unitary operators  $U, V$  on  $H$  then we have



Here an input goes through the first gate  $U$  and then through the second gate  $V$ . Thus gates must be enumerated from left to right whereas operator multiplication is in the reverse order. If  $U$  is a gate on  $H_1 \otimes H_2 \otimes \dots \otimes H_i$  then  $U \otimes I$ , where  $I$  is the identity on  $H_{i+1} \otimes \dots \otimes H_n$  is represented as



This notation can be adapted to any block of wires. We now introduce the most important and central notion of a quantum gate depicted by



This gate denotes the unique unitary operator  $U$  in  $H$  satisfying for any  $\psi \in H_i, a_j \in \mathbf{Z}_{d_j}, j \neq i$

$$\begin{aligned}
 &U|a_1 a_2 \dots a_{i-1}\rangle|\psi\rangle|a_{i+1} a_{i+2} \dots a_n\rangle \\
 &= |a_1 a_2 \dots a_{i-1}\rangle(L|\psi\rangle)|a_{i+1} a_{i+2} \dots a_n\rangle, \\
 &U|x_1 x_2 \dots x_{i-1}\rangle|\psi\rangle|x_{i+1} x_{i+2} \dots x_n\rangle \\
 &= |x_1 x_2 \dots x_{i-1}\rangle|\psi\rangle|x_{i+1} x_{i+2} \dots x_n\rangle
 \end{aligned}$$

if

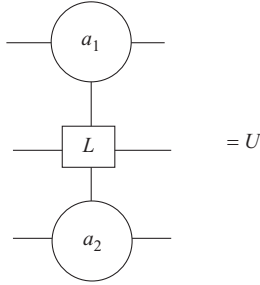
$$(x_1, x_2, \dots, x_{i-1}, x_{i+1}, \dots, x_n) \neq (a_1, a_2, \dots, a_{i-1}, a_{i+1}, \dots, a_n),$$

$L$  being a unitary operator in  $H_i$ . It is called a quantum gate *controlled* at  $a_1, a_2, \dots, a_{i-1}, a_{i+1}, \dots, a_n$  on the wires  $1, 2, \dots, i-1, i+1, \dots, n$  and *targeted* by the unitary operator  $L$  on the  $i$ th wire. Denote the set of all such gates by  $\mathcal{C}_{n-1}$ .

For any of the groups  $\mathbf{Z}_{d_i}$  we write for any  $x \in \mathbf{Z}_{d_i}$

$$\alpha(x) = \begin{cases} 1 & \text{if } x = 0, \\ 0 & \text{otherwise.} \end{cases}$$

Then we have, for example,

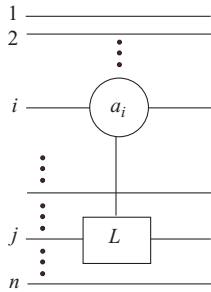


where  $U$  is the unique unitary operator in  $H_1 \otimes H_2 \otimes H_3$  satisfying

$$U|x_1\rangle|\psi\rangle|x_3\rangle = |x_1\rangle(L^{\alpha(x_1-a_1)\alpha(x_3-a_3)}|\psi\rangle)|x_3\rangle$$

for all  $x_1 \in \mathbf{Z}_{d_1}, x_3 \in \mathbf{Z}_{d_3}, \psi \in H_2, a_1 \in \mathbf{Z}_{d_1}, a_2 \in \mathbf{Z}_{d_2}$  and  $L$  a unitary operator in  $H_2$ .

We denote by  $\mathcal{C}_k$  the set of all gates which are controlled on  $k$  wires and targeted by some unitary operator on a wire different from these  $k$  wires. For example

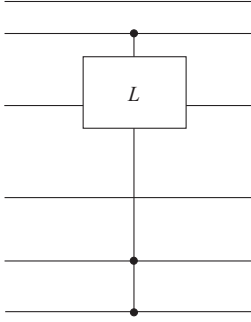


is a  $\mathcal{C}_1$  gate satisfying

$$U|x_1 x_2 \dots x_n\rangle = |x_1 x_2 \dots x_{j-1}\rangle(L^{\alpha(x_i-a_i)}|x_j\rangle)|x_{j+1} x_{j+2} \dots x_n\rangle$$

for all  $x_r \in \mathbf{Z}_{d_r}$ ,  $1 \leq r \leq n$ .

Whenever the controls are at the null elements of the groups  $\mathbf{Z}_{d_i}$  we indicate them by dots on the appropriate wires. For example

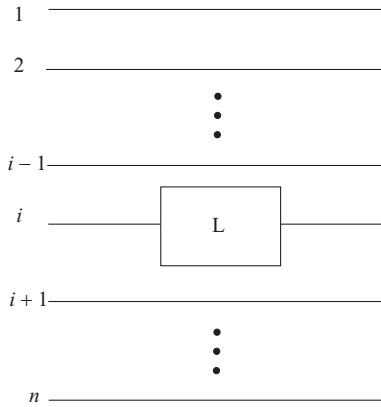


is a gate in  $H_1 \otimes H_2 \otimes \cdots \otimes H_6$  satisfying

$$U|x_1x_2 \dots x_6\rangle = |x_1x_2\rangle(L^{\alpha(x_2)\alpha(x_5)\alpha(x_6)}|x_3\rangle)|x_4x_5x_6\rangle$$

for all  $x_i \in \mathbf{Z}_{d_i}$ ,  $1 \leq i \leq 6$ . This is an example of a  $\mathcal{C}_3$  gate which is controlled at 0 on wires 2, 5, 6 and targeted by  $L$  on wire 3.

We denote by  $\mathcal{C}_k^0 \subset \mathcal{C}_k$  the subset of those gates where all the controls are at 0.  $\mathcal{C}_0$  denotes the set of all gates in  $H_1 \otimes H_2 \otimes \cdots \otimes H_n$  which are targeted on one wire but without any control on other wires. For example

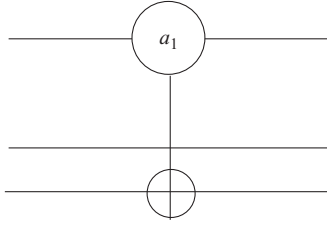


is a  $\mathcal{C}_0$  gate satisfying

$$U|x_1x_2 \dots x_n\rangle = |x_1 \dots x_{i-1}\rangle(L|x_i\rangle)|x_{i+1} \dots x_n\rangle$$

for all  $x_i \in \mathbf{Z}_{d_i}$ ,  $1 \leq i \leq n$ .

When the targeted operator  $L$  on the  $i$ th wire is the cyclic permutation of the basis in  $\mathbf{Z}_{d_i}$ , i.e.,  $L|x\rangle = |x \oplus 1\rangle$  we indicate it on the  $i$ th wire by  $\oplus$ . For example,

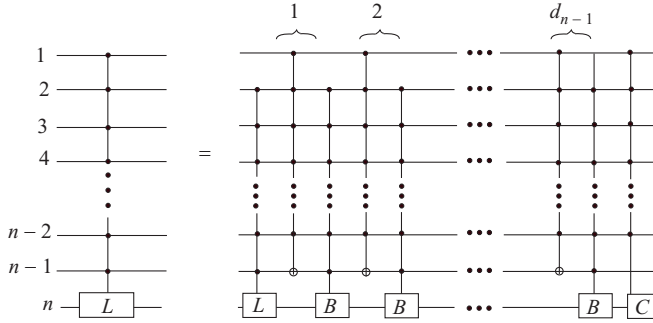


means the gate satisfying

$$U|x_1x_2x_3\rangle = |x_1x_2\rangle|x_3 \oplus \alpha(x_1 - a_1)\rangle.$$

With these conventions adapted to our situation from the theory of quantum computing (as outlined for example in [2,3]) we are ready to formulate and prove a lemma due to Jaikumar [1].

*Lemma 2.* [1] *Let  $L$  be any unitary operator in  $H_n$ . Then*



where  $B = C^{-1}$ ,  $C = L^{1/d_{n-1}}$  is a fixed  $d_{n-1}$ th root of  $L$ . The right-hand side is a composition of  $2(d_{n-1} + 1)$  gates from  $\mathcal{C}_{n-2}^0$ .

*Proof.* Consider an input  $|x_1x_2 \dots x_{n-1}\rangle|\psi\rangle$ . The left-hand side produces the output

$$|x_1x_2 \dots x_{n-1}\rangle L^{\alpha(x_1)\alpha(x_2)\dots\alpha(x_{n-1})}|\psi\rangle. \tag{2.2}$$

We now examine the output produced by the ‘quantum circuit’ on the right-hand side. After passage through the first  $\mathcal{C}_{n-2}^0$  gate we get

$$|x_1x_2 \dots x_{n-1}\rangle L^{\alpha(x_2)\dots\alpha(x_{n-1})}|\psi\rangle.$$

When this passes through the next  $j$  pairs of gates with  $j \leq d_{n-1}$  we get the output

$$|x_1x_2 \dots x_{n-2}\rangle|x_{n-1} \oplus j\alpha(x_1) \dots \alpha(x_{n-2})\rangle B^{r_j\alpha(x_2)\dots\alpha(x_{n-2})} L^{\alpha(x_2)\dots\alpha(x_{n-1})}|\psi\rangle$$

where

$$r_j = \sum_{s=1}^j \alpha(x_{n-1} \oplus s\alpha(x_1) \dots \alpha(x_{n-2})).$$

Since  $d_{n-1}$  and 0 are to be identified in the group  $\mathbf{Z}_{d_{n-1}}$  we see that the passage through the  $d_{n-1}$ th pair and then the last gate yields the final output

$$|x_1 x_2 \dots x_{n-1}\rangle C^{\alpha(x_1)\dots\alpha(x_{n-2})} B^{r\alpha(x_2)\dots\alpha(x_{n-2})} L^{\alpha(x_2)\dots\alpha(x_{n-1})} |\psi\rangle \quad (2.3)$$

where

$$r = \sum_{s=0}^{d_{n-1}-1} \alpha(x_{n-1} \oplus s\alpha(x_1)\alpha(x_2) \dots \alpha(x_{n-2})). \quad (2.4)$$

Suppose  $x_j \neq 0$  for some  $2 \leq j \leq n-2$ . Then the expression (2.3) reduces to  $|x_1 x_2 \dots x_{n-1}\rangle |\psi\rangle$  and coincides with (2.2). Thus it suffices to examine the case when  $x_j = 0$  for  $2 \leq j \leq n-2$ . Then (2.3) and (2.4) reduce respectively to

$$|x_1 0, 0 \dots 0 x_{n-1}\rangle C^{\alpha(x_1)} B^r L^{\alpha(x_{n-1})} |\psi\rangle \quad (2.5)$$

and

$$r = \sum_{s=0}^{d_{n-1}-1} \alpha(x_{n-1} \oplus s\alpha(x_1)). \quad (2.6)$$

Now we examine four cases.

*Case 1.*  $x_1 \neq 0, x_{n-1} \neq 0$ .

We have  $\alpha(x_1) = \alpha(x_{n-1}) = r = 0$  and (2.5) reduces to  $|x_1 00 \dots 0 x_{n-1}\rangle |\psi\rangle$ .

*Case 2.*  $x_1 \neq 0, x_{n-1} = 0$ .

We have  $\alpha(x_1) = 0, \alpha(x_{n-1}) = 1, r = d_{n-1}$  and (2.5) reduces to

$$|x_1 00 \dots 0\rangle B^{d_{n-1}} L |\psi\rangle = |x_1 0 \dots 0\rangle |\psi\rangle,$$

owing to the definition of  $B$  and  $C$  in the lemma.

*Case 3.*  $x_1 = 0, x_{n-1} \neq 0$ .

Now  $\alpha(x_1) = 1, \alpha(x_{n-1}) = 0$  and  $r = \sum_{s=0}^{d_{n-1}-1} \alpha(x_{n-1} \oplus s)$ . As  $s$  varies from 0 to  $d_{n-1} - 1$  exactly one of the elements  $x_{n-1} \oplus s$  is 0 and hence  $r = 1$ . Thus (2.5) reduces to  $|00 \dots 0 x_{n-1}\rangle C B |\psi\rangle = |00 \dots 0 x_{n-1}\rangle |\psi\rangle$ .

*Case 4.*  $x_1 = 0, x_{n-1} = 0$ .

Now  $\alpha(x_1) = 1, \alpha(x_{n-1}) = 1$  and  $r = \sum_{s=0}^{d_{n-1}-1} \alpha(s) = 1$ . Thus (2.5) reduces to  $|00 \dots 0\rangle C B L |\psi\rangle = |00 \dots 0\rangle L |\psi\rangle$ .

In other words, in all the cases, the two circuits on both sides of the lemma produce the same output. The last part of the lemma is obvious.  $\square$

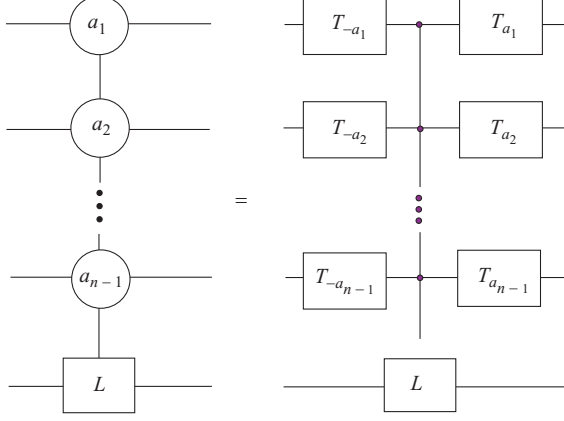
#### COROLLARY 1

Let  $d = \max_i d_i$ . Then any gate in  $C_{n-1}^0$  is a composition of at most  $[2(d+1)]^{n-2}$  gates in  $C_1^0$ .

*Proof.* By the last part of Lemma 3 and a shuffle of the wires it follows that any  $C_{n-1}^0$  gate is a composition of at most  $2(d+1)$  gates from  $C_{n-2}^0$ . Rest follows from induction.  $\square$



**Lemma 3.** In  $H_i = L^2(\mathbf{Z}_{d_i})$  denote by  $T_a, a \in \mathbf{Z}_{d_i}$  the unitary operator satisfying  $T_a|x\rangle = |x + a\rangle$  for every  $x \in \mathbf{Z}_{d_i}$ . Then for any  $a_i \in \mathbf{Z}_{d_i}, i = 1, 2, \dots, n-1$  and any unitary operator  $L$  in  $H_n$  the following holds:



*Proof.* Apply both sides to the input  $|x_1 x_2 \dots x_{n-1}\rangle|\psi\rangle$  for any  $x_i \in \mathbf{Z}_{d_i}, i = 1, 2, \dots, n-1$  and  $\psi \in H_n$ . A straightforward check by inspection completes the proof.  $\square$

**Lemma 4.** Any  $C_{n-1}$  gate can be expressed as a composition of at most  $2(n-1)$  gates from  $C_0$  and  $[2(d+1)]^{n-2}$  gates from  $C_1^0$ .

*Proof.* By Lemma 3 any  $C_{n-1}$  gate is a composition of  $2(n-1)$  gates from  $C_0$  and a  $C_{n-1}^0$  gate. The required result follows from Corollary 1.  $\square$

To state our next lemma we introduce a definition.

For any  $a \neq b, a, b \in \mathbf{Z}_{d_i}$  we define the swap operator  $S(a, b)$  in  $L^2(\mathbf{Z}_{d_i})$  as the unique unitary operator satisfying

$$\begin{aligned} S(a, b)|x\rangle &= |x\rangle \text{ if } x \notin \{a, b\}, \\ &= |b\rangle \text{ if } x = a, \\ &= |a\rangle \text{ if } x = b. \end{aligned}$$

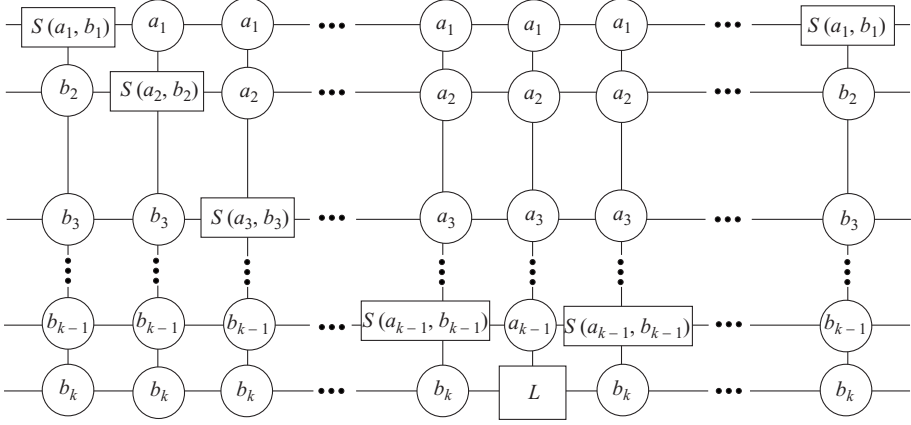
**Lemma 5.** Let  $a_i, b_i \in \mathbf{Z}_{d_i}, i = 1, 2, \dots, k, a_i \neq b_i$  for every  $i$ . Consider the unitary operator  $U$  in  $H_1 \otimes H_2 \otimes \dots \otimes H_k$  determined by

$$\begin{aligned} U|a_1 a_2 \dots a_k\rangle &= \alpha|a_1 a_2 \dots a_k\rangle + \beta|b_1 b_2 \dots b_k\rangle, \\ U|b_1 b_2 \dots b_k\rangle &= -\bar{\beta}|a_1 a_2 \dots a_k\rangle + \bar{\alpha}|b_1 b_2 \dots b_k\rangle, \\ U|x_1 x_2 \dots x_k\rangle &= |x_1 x_2 \dots x_k\rangle \quad \text{if } (x_1, x_2, \dots, x_k) \notin \{(a_1, a_2, \dots, a_k), \\ &\quad (b_1, b_2, \dots, b_k)\} \end{aligned}$$

where  $\alpha, \beta$  are scalars satisfying  $|\alpha|^2 + |\beta|^2 = 1$ . Define the unitary operator  $L$  in  $H_k$  by the equations

$$\begin{aligned} L|a_k\rangle &= \alpha|a_k\rangle + \beta|b_k\rangle, \\ L|b_k\rangle &= -\bar{\beta}|a_k\rangle + \bar{\alpha}|b_k\rangle, \\ L|x\rangle &= |x\rangle \quad \text{if } x \notin \{a_k, b_k\}. \end{aligned}$$

Then  $U$  can be expressed as



where the circuit has  $2k - 1$  gates from  $\mathcal{C}_{k-1}$  and the last  $(k - 1)$  gates are also the first  $(k - 1)$  gates in reverse order.

*Proof.* By the definition of  $L$ , the  $k$ th gate in the circuit is an elementary operator with respect to the basis  $\{|x_1 x_2 \dots x_k\rangle, x_i \in \mathbf{Z}_{d_i}, 1 \leq i \leq k\}$  rooted in the pair  $\{|a_1 a_2 \dots a_k\rangle, |a_1, a_2 \dots a_{k-1}, b_k\rangle\}$  and all other gates are unitary operators whose squares are equal to identity. Since the composition of the last  $(k - 1)$  gates is the inverse of the composition of the first  $(k - 1)$  gates it follows that the circuit in the lemma yields a gate which is conjugate to an elementary operator. Now consider the two inputs  $|a_1 a_2 \dots a_k\rangle$  and  $|b_1 b_2 \dots b_k\rangle$  for the circuit in the lemma. By the definition of  $L$  it follows that the respective outputs are, indeed,  $U|a_1 a_2 \dots a_k\rangle$  and  $U|b_1 b_2 \dots b_k\rangle$ . Thus  $U$  is represented by the circuit in the lemma.  $\square$

*Proof of Theorem 1.* Let  $N = d_1 d_2 \dots d_n$  denote the dimension of  $H = H_1 \otimes H_2 \otimes \dots \otimes H_n$  and let  $d = \max_i d_i$ . Now let  $U$  be an arbitrary unitary operator in  $H$ . By Lemma 1,  $U$  can be expressed as a product of a scalar  $\lambda$  of modulus unity and at most  $N(N - 1)/2$  unitary operators, each of which is elementary with respect to the basis  $\{|x_1 x_2 \dots x_n\rangle, x_i \in \mathbf{Z}_{d_i}, 1 \leq i \leq n\}$ .

Now consider a pair of product vectors of the form

$$|x_1 x_2 \dots x_n\rangle, |y_1 y_2 \dots y_n\rangle \quad \text{where } \#\{i | x_i = y_i\} = r.$$

After an appropriate permutation of  $\{1, 2, \dots, n\}$  (or equivalently, a shuffling of the wires) we may assume, without loss of generality, that

$$\begin{aligned} (x_1, x_2, \dots, x_n) &= (c_1, c_2, \dots, c_r, a_1, a_2, \dots, a_k), \\ (y_1, y_2, \dots, y_n) &= (c_1, c_2, \dots, c_r, b_1, b_2, \dots, b_k) \end{aligned}$$

where  $k + r = n$  and  $a_i \neq b_i$  for every  $1 \leq i \leq k$ . By adding  $r$  more wires to the circuit in Lemma 5 and putting controls at  $c_1, c_2, \dots, c_r$  on these wires above each of the gates we observe that a gate which is elementary with respect to our fixed coordinate system and rooted in the pair  $\{|c_1 c_2 \dots c_r a_1 a_2 \dots a_k\rangle, |c_1 c_2 \dots c_r b_1 b_2 \dots b_k\rangle\}$  can be expressed as a composition of  $(2k - 1)$  gates from  $\mathcal{C}_{n-1}$ . Now an application of Lemma 4 shows that this

same elementary operator can be expressed as a composition of at most  $(2k-1)\{2(n-1) + [2(d+1)]^{n-2}\}$  gates from  $\mathcal{C}_0 \cup \mathcal{C}_1^0$ . Thus  $U$  can be expressed as a composition of at most

$$\frac{N(N-1)}{2}(2n-1)\{2(n-1) + [2(d+1)]^{n-2}\} \quad (2.7)$$

gates from  $\mathcal{C}_0 \cup \mathcal{C}_1^0$ . Any gate in  $\mathcal{C}_0 \cup \mathcal{C}_1^0$ , is, indeed, an  $(i, j)$  gate. Choosing  $D$  equal to the expression in (2.7) the proof becomes complete.  $\square$

*Remark 1.* When  $d_i = d$  for every  $i$  and  $n$  increases to  $\infty$  the number  $D$  in Theorem 1 is  $O(n[2d^2(d+1)]^n)$ .

### Acknowledgements

I thank the Indian National Science Academy for its financial support for the period 2000–June 2001 during which this work was done at the Delhi Centre of the Indian Statistical Institute. I thank Amitava Bhattacharya and Jaikumar of the Tata Institute, Mumbai for several fruitful discussions on quantum computing. I acknowledge the hospitality of the Volterra Centre of The University of Rome ‘Tor Vergata’ where I wrote this note in July 2001.

### References

- [1] Jaikumar Radhakrishnan: Private communication, April 2001
- [2] Nielsen M A and Chuang I L, Quantum Computation and Quantum Information (Cambridge: Cambridge University Press) (2000)
- [3] Parthasarathy K R, Lectures on quantum computation and quantum error correcting codes, Notes by Amitava Bhattacharya, Tata Institute of Fundamental Research, Mumbai (2001)