Georgia Tech Math, Physics & Computing
Math 4782, Phys 4782, CS4803

Quantum Information & Quantum Computing

Problems Set 1

Due February 9, 2006

Part I :

1. Read carefully Nielsen-Chang, Section 2.1 .
2. Treat as many exercises in Section 2.1 as possible.
3. Turn in exercises (*to be graded*) # 2.17, 2.18, 2.20, 2.21, 2.26, 2.27, 2.33, 2.34, 2.35, 2.39 See Nielsen-Chang Section 2.1 .

Exercises :

– **2.17-** *Show that a normal matrix is Hermitian if and only if it has real eigenvalues.*

By definition, a matrix is normal if it commutes with its adjoint. By the spectral theorem a matrix is normal if and only if admits an orthonormal base of eigenvectors. In such a base this matrix is diagonal and the diagonal elements are its eigenvalues. The adjoint of the matrix is given, in any orthonormal base, by transposing and (complex) conjugating its matrix elements. In particular in the base of eigenvectors the adjoint is obtained simply by (complex) conjugating the diagonal elements. It is selfadjoint if and only if these elements are real. But since the diagonal elements in this base are the eigenvalues the result is proved.

– **2.18-** *Show that the eigenvalues of a unitary matrix have modulus one, that is, can be written in the form $e^{\imath\theta}$ for some real θ.*

A matrix U is unitary if $UU^\dagger = U^\dagger U = I$. In particular it is normal. Using an orthonormal basis of eigenvectors it becomes diagonal and the unitary relation implies that each eigenvalue z satisfies $z\overline{z} = 1$. This proves the result.

– **2.20-** *Suppose A' and $A"$ are matrix representations of a linear operator A on a vector space V with respect to two different orthonormal basis $|v_i\rangle$ and $|w_i\rangle$. Then the elements of A' and $A"$ are $A'_{ij} = \langle v_i|A|v_j\rangle$ and $A"_{ij} = \langle w_i|A|w_j\rangle$. Characterize the relationship between $A', A"$.*

Let S be the matrix with elements $S_{ij} = \langle v_i|w_j\rangle$. Then, since the two basis $|v_i\rangle$ and $|w_i\rangle$ are orthonormal, S is unitary. For indeed $SS^\dagger$ has matrix elements $\left(SS^\dagger\right)_{ij} = \sum_k S_{ik}\overline{S_{jk}} = \sum_k \langle v_i|w_k\rangle\langle w_k|v_j\rangle = \langle v_i|v_j\rangle = \delta_{ij} = (I)_{ij}$ (here the completness relation $\sum_k |w_k\rangle\langle w_k| = I$ has been used). Then, using again the completeness relation twice,

$$\sum_{k,l} S_{ik} A"_{kl}\overline{S_{jl}} = \sum_{kl} \langle v_i|w_k\rangle\langle w_k|A|w_l\rangle\langle w_l|v_j\rangle = \langle v_i|A|v_j\rangle = A'_{ij}$$

In other words $SA"S^\dagger = A'$ and, since S is unitary, $A" = S^\dagger AS$.

– **2.21-** *Repeat the proof of the spectral decomposition in Box 2.2 for the case where M is Hermitian, simplifying th proof whenever possible.*

We want to show that *any Hermitian operator M on a Hilbert space V is diagonal with respect to some orthonormal basis of V with real eigenvalues. Conversely any operator diagonalizable in some orhtonormal basis with real eigenvalues is Hermitian.* While the converse is obvious, let us prove the direct statement by recursion on the dimension d of V. For $d = 1$ the statement is obvious. Let then $d > 1$. Given an eigenvalue λ of M, let P be the orthogonal projection onto the subspace of V of eigenvectors of M for the eigenvalue λ (recall that any orthogonal po[rojection is characterized by $P^2 = P = P^\dagger$). Let then Q be the orthogonal projection on the orthogonal complement of P so that $PQ = QP = 0$ and $P + Q = I$ (and also, $Q = Q^\dagger = Q^2$). Thus $M = (P + Q)M(P + Q) = PMP + PMQ + QMP + QMQ$. By construction, any vector $|\psi\rangle$ in PV satisfies $M|\psi\rangle = \lambda|\psi\rangle$, so that $MP = \lambda P$. Thus $PMP = \lambda P$, because $P^2 = P$. Since M is selfadjoint it follows that $\overline{\lambda}P = (PMP)^\dagger = PMP = \lambda P$ implying $\lambda = \overline{\lambda}$ is real and $PM = (MP)^\dagger = (\lambda P)^\dagger = \overline{\lambda}P = \lambda P = MP$. Hence P commutes to M so that $QMP = QPM = 0$ and $PMQ = MPQ = 0$. Thus $M = \lambda P + QMQ$. Clearly QMQ is selfadjoint and operates on the space QV which as dimension smaller than d. By the recursion hypothesis QMQ can be diagonalized in an orthonormal basis with real eigenvalues and, from the previous decomposition, so can be M.

– **2.26-** *Let $|\psi\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$. Write out $|\psi\rangle^{\otimes 2}$ and $|\psi\rangle^{\otimes 3}$ explicitely, both in terms of tensor products of $|0\rangle$'s and $|1\rangle$'s, using the Kronecker product.*

Since the tensor product is multilinear (or distributive with respect to addition) it follows that

$$|\psi\rangle^{\otimes 2} = \frac{|0\rangle \otimes |0\rangle + |0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle}{2} = \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2}$$

Similarly

$$|\psi\rangle^{\otimes 3} = \frac{|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle}{2^{3/2}}$$

More generally, if $x = x_1 2^{n-1} + x_2 2^{n-2} + \cdots + x_{n-1}2 + x_n$

$$|\psi\rangle^{\otimes n} = \frac{1}{2^{n/2}} \sum_{x_1,\cdots,x_n \in \{0,1\}} |x_1\rangle \otimes \cdots \otimes |x_n\rangle = \frac{1}{2^{n/2}} \sum_{x_1,\cdots,x_n \in \{0,1\}} |x_1 \cdots x_n\rangle = \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle$$

– **2.27-** *Calculate the matrix representation of the tensor products of the Pauli operators (a) X and Z ; (b) I and X ; (c) X and I. Is the tensor product commutative ?*

Recall that $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ and $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$. On the other hand, with two binary digits x_1, x_2 is associated the integer $x = 2x_1 + x_2$. Hence the digital basis can be relabelled as $|00\rangle = |0\rangle$, $|01\rangle = |1\rangle$, $|10\rangle = |2\rangle$, $|11\rangle = |3\rangle$. On the other hand, $(A \otimes B)_{xy;x'y'} = A_{xx'}B_{yy'}$ by definition of the Kronecker product. Thus using the labelling by integers this gives

$$X \otimes Z = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix}, \; I \otimes X = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \; X \otimes I = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}.$$

In particular $I \otimes X \neq X \otimes I$ meaning the tensor product is NOT commutative.

– **2.33-** *The Hadamard operator on one qubit maybe written as*

$$H = \frac{1}{\sqrt{2}} \left[(|0\rangle + |1\rangle) \langle 0| + (|0\rangle - |1\rangle) \langle 1| \right].$$

Show explicitly that the Hadamard transform on n-qubits, $H^{\otimes n}$, may be written as

$$H^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x,y} (-1)^{x\dot{y}} |x\rangle\langle y|.$$

Write out an explicit representation for $H^{\otimes 2}$.

For indeed the expression of H given above is equivalent to $H = 1/\sqrt{2} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$. In particular this gives

$$H = \frac{1}{\sqrt{2}} \left[|0\rangle\langle 0| + |1\rangle\langle 0| + |0\rangle\langle 1| - |1\rangle\langle 1| \right] = \frac{1}{\sqrt{2}} \sum_{x,y \in \{0,1\}} (-1)^{xy} |x\rangle\langle y|.$$

Since the tensor product is multilinear it follows that

$$H^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x_i, y_j \in \{0,1\}} (-1)^{x_1 y_1 + \cdots x_n y_n} |x_1\rangle\langle y_1| \otimes \cdots \otimes |x_n\rangle\langle y_n|.$$

By definition, if $x = (x_1, \cdots, x_n) \in \{0,1\}^n$ and $y = (y_1, \cdots, y_n) \in \{0,1\}^n$, then $x\dot{y} = x_1 y_1 + \cdots x_n y_n$. Moreover $|x_1\rangle\langle y_1| \otimes \cdots \otimes |x_n\rangle\langle y_n| = (|x_1\rangle \otimes \cdots \otimes |x_n\rangle) (\langle y_1| \otimes \cdots \otimes \langle y_n|) = |x\rangle\langle y|$. This gives the first result. Using the labelling by integers instead of binary digit we get then

$$H^{\otimes 2} = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix},$$

– **2.34-** *Find the square root and the logarithm of the matrix* $\begin{bmatrix} 4 & 3 \\ 3 & 4 \end{bmatrix}$.

This matrix can be written as $A = 4 + 3X = H(4 + 3Z)H^{-1}$ (recall that $H = H^\dagger = H^{-1}$ is unitary). Since $4 + 3Z$ is diagonal it is easy to get

$$4 + 3Z = \begin{bmatrix} 7 & 0 \\ 0 & 1 \end{bmatrix}, \; \Rightarrow \; (4 + 3Z)^{1/2} = \begin{bmatrix} \sqrt{7} & 0 \\ 0 & 1 \end{bmatrix} = \frac{(\sqrt{7} + 1) + (\sqrt{7} - 1)Z}{2}.$$

In much the same way

$$\ln(4+3Z) = \begin{bmatrix} \ln 7 & 0 \\ 0 & 0 \end{bmatrix} = \ln 7\, \frac{(1+Z)}{2}\,.$$

Applying the Hadamard matrix back this gives

$$A^{1/2} = (4+3X)^{1/2} = \frac{1}{2}\left\{(\sqrt{7}+1) + (\sqrt{7}-1)X\right\}$$

$$\ln A = \ln(4+3X) = \ln 7\, \frac{(1+X)}{2}$$

– **2.35-** *Let $\vec{v}$ be any real three-dimensional unit vector and θ a real number. Prove that*

$$\exp(\imath\vec{v}\cdot\vec{\sigma}) = \cos(\theta)I + \imath\sin(\theta)\,\vec{v}\cdot\vec{\sigma}\,,$$

where $\vec{v}\cdot\vec{\sigma} = v_1\sigma_1 + v_2\sigma_2 + v_3\sigma_3 = v_1X + v_2Y + v_3Z$. This exercise is generalized in Problem 2.1 on page 117.

The commutation rules for Pauli's operators are $XY + YX = 0 = YZ + ZY = ZX + XZ$ and $X^2 = Y^2 = Z^2 = I$. It follows that, if $A = \vec{v}\cdot\vec{\sigma}$, $A^2 = v_1^2 + v_2^2 + v_3^2 = 1$ because $\vec{v}$ is a unit vector. Thus

$$\begin{aligned}
\exp(\imath\theta A) &= I + \imath\theta A - \frac{\theta^2}{2!}I - \imath\frac{\theta^3}{3!}A + \cdots + (-1)^n\frac{\theta^{2n}}{(2n)!}I + \imath(-1)^n\frac{\theta^{2n+1}}{(2n+1)!}A + \cdots \\
&= (1 + \cdots + (-1)^n\frac{\theta^{2n}}{(2n)!} + \cdots)I + \imath(\theta + \cdots + (-1)^n\frac{\theta^{2n+1}}{(2n+1)!} + \cdots)A \\
&= \cos(\theta)I + \imath\sin(\theta)\,A\,,
\end{aligned}$$

proving the result.

– **2.39-** *The set L_V of linear operators on a Hilbert space V is obviously a (complex) vector space - the sum of two linear operators is a linear operator, zA is a linear operator if A is a linear operator and z a complex number, and there is a zero element 0. An important additional result is that the vector space L_V can be given a natural inner product structure turning it into a Hilbert space.*

1. *Show that the function $(\cdot,\cdot)$ on $L_V \times L_V$ defined by*

$$(A,B) = \mathrm{tr}\,(A^\dagger B)$$

   is an inner product function. This inner product is known as the Hilbert-Schmidt *or* trace *inner product.*

2. *If V has d dimensions show that L_V has dimension d^2.*

3. *Find an orthonormal basis of Hermitian matrices for the Hilbert space L_V.*

1.- Clearly, since the trace is linear, $(\cdot,\cdot)$ is linear on the right and antilinear on the left. Moreover, $\overline{(A,B)} = \mathrm{tr}\,\left((A^\dagger B)^\dagger\right) = \mathrm{tr}\,(B^\dagger A) = (B,A)$. Also, if $A = (a_{ij})_{i,j=1}^d$ is the matrix of A is some orthonormal basis, then $(A,A) = \mathrm{tr}\,(A^\dagger A) = \sum_{i,j=1}^d |a_{ij}|^2 > 0$ unless $A = 0$.

2.- Since an operator acting on V admits d^2 matrix elements in any orthonormal basis of V, it follows that $\dim L_V = d^2$. Actually let $\{|v_i\rangle\,;\, 1 \le i \le d\}$ be an orthonormal

basis of V. Then the operators $E_{ij} = |v_i\rangle\langle v_j|$ define an orthonormal basis of L_V because (i) any operator A can be written as $A = \sum_{ij} a_{ij}|v_i\rangle\langle v_j|$, showing that the E_{ij}'s are generating, (ii) $(E_{ij}, E_{i'j'}) = \mathrm{tr}\,(E_{ij}^\dagger E_{i'j'}) = \mathrm{tr}\,(|v_j\rangle\langle v_i|v_{i'}\rangle\langle v_{j'}|) = \langle v_i|v_{i'}\rangle\langle v_j|v_{j'}\rangle = \delta_{ii'}\delta_{jj'}$ so that the family is orthonormal and thus, linearly independent. Therefore this family is an orthonormal basis of L_V. Since it contains d^2 element so is the dimension of L_V.

3.- The previous orthonormal basis is not made of Hermitian matrices unless for $i = j$. However, $E_{ij}^\dagger = E_{ji}$. Thus, setting, for $i < j$, $R_{ij} = (E_{ij} + E_{ji})/\sqrt{2}$ and $S_{ij} = (E_{ij} - E_{ji})/\imath\sqrt{2}$ gives self adjoint elements such that $(R_{ij}, R_{kl}) = (R_{ij}, S_{kl}) = (S_{ij}, R_{kl}) = (S_{ij}, S_{kl}) = 0$ if one of the indices i, j differs from one of k, l. Similarly $(R_{ij}, E_{kk}) = 0 = (S_{ij}, E_{kk})$ for $i < j$ and all k's. Moreover $(R_{ij}, S_{ij}) = 0$ while $(R_{ij}, R_{ij}) = 1 = (S_{ij}, S_{ij})$ as can be checked immediately. Hence $\{E_{ii}\,,\, R_{ij}\,,\, S_{ij}\,;\, 1 \le i < j \le d\}$ defines an orthonormal basis of L_V made of d^2 selfadjoint operators.

Part II :

1. Read carefully Nielsen-Chang, Section 4.2 & 4.3 .
2. Treat as many exercises in Section 4.3 as possible.
3. Turn in exercises (*to be graded*) # 4.21, 4.23, 4.24, 4.25, 4.35 .

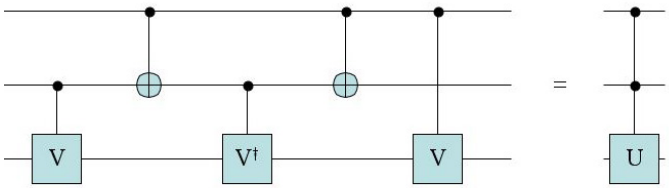


Fig 4.8 - Circuit for C²(U)-gate. Here V²=U

Exercises :

– **4.21-** *Verify that Fig 4.8 implements the $C^2(U)$ operation.*

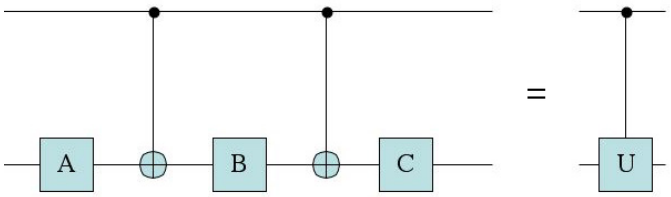
To verify this claim, because each quantum circuit represents a unitary operator on the qubit-space, it is sufficient to check that the result on both sides are identical when applied to any basis vector of the computer basis. So let $|\psi_0\rangle = |x\rangle \otimes |y\langle\otimes|z\langle$ be the input vector (where the labeling x, y, z goes from the rop to the bottom lines). After the first gate V the input becomes $|\psi_1\rangle = |x\rangle \otimes |y\rangle \otimes V^y|z\rangle$. After the CNOT-gate it becomes $|\psi_2\rangle = |x\rangle \otimes |x \oplus y\rangle \otimes V^y|z\rangle$. After the $V^\dagger$-gate it gives $|\psi_3\rangle = |x\rangle \otimes |x \oplus y\rangle \otimes (V^\dagger)^{x\oplus y}V^y|z\rangle$. After the next CNOT-gate, it gives $|\psi_4\rangle = |x\rangle \otimes |y\rangle \otimes (V^\dagger)^{x\oplus y}V^y|z\rangle$ so that the output is $|\psi_5\rangle = |x\rangle \otimes |y\rangle \otimes V^x(V^\dagger)^{x\oplus y}V^y|z\rangle$. If $x = y = 0$ then $V^x(V^\dagger)^{x\oplus y}V^y = I$ and nothing happens. For $x \neq y$ then either $x = 0, y = 1$ or $x = 1, y = 0$, so that in both cases $x \oplus y = 1$ and $V^x(V^\dagger)^{x\oplus y}V^y$ becomes either $V^\dagger V = I$ or $VV^\dagger = I$, so that nothing happens as well. For $x = y = 1$, then $x \oplus y = 0$ so that $V^x(V^\dagger)^{x\oplus y}V^y = V^2 = U$. Hence only if $x = y = 1$ is this gate acting and it acts as U on the third line of the circuit, namely this is exactly how the $C^2(U)$ gate acts.

– **4.23-** *Construct a $C^1(U)$-gate for $U = R_x(\theta)$ and $U = R_y(\theta)$, using only* CNOT *and single qubit gates. Can you reduce the number of single qubit gates needed in the construction from three to two ?*

The circuit designed in the next Figure below gives an output $|x\rangle \otimes CX^xBX^xA|y\rangle$ for an

input $|x, y\rangle$. Thus finding matrices A, B, C such that $CBA = I$ and $CXBXA = U$ solves the problem. For $U = R_y(\theta) = e^{\imath\theta Y}$ a solution is given by $A = I, B = C^{-1}$ and $C = e^{\imath\theta/2Y}$, simply because $XYX = -Y$. In this latter case, two one-qubit gates are sufficient. For $U = R_x(\theta)$, a possible solution is $A = e^{\imath\theta/2Z}H$, $B = e^{-\imath\theta/2Z}$ and $C = H$.

In the case of $U = R_x(\theta)$, reducing the number of one-qubit gates from three to two would mean to find a unitary matrix B such that $BXB^{-1}X = R_x(\theta)$. Writing B as $B = e^{\imath\alpha\vec{v}\cdot\vec{\sigma}} = \cos(\alpha) + \imath\sin(\alpha)\vec{\sigma}\cdot\vec{v}$ with $\vec{v} = (a, b, c)$ a real three-dimensional unit vector, gives $BXB^{-1}X = \cos^2\alpha + \sin^2\alpha(a^2 - b^2 - c^2) + \imath 2a(cY - bZ) + \imath\sin(2\alpha)(bY + cZ)$. Such a matrix cannot commute to X unless if a multiple of the identity. Hence it cannot equal $R_x(\theta)$ for $\theta \neq 0 \bmod 2\pi$. So three one-qubit gates at least are necessary.



Constructing $C^1(U)$: here CXBXA= U and CBA=I

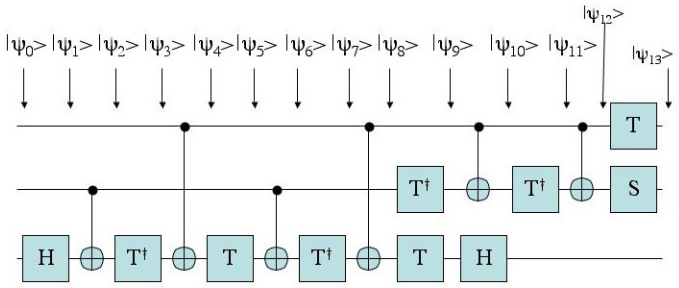


Fig 4.9 - Implementing the Toffoli gate

– **4.24-** *Check that Figure 4.9 implements the Toffoli gate.*

The right hand side in Figure 4.9 can be seen as a product of 13 unitary operators, so that if $|\psi_j\rangle$ denotes the state in the 3-qubit space after the operator #j, with input for $j = 0$, the output will be $|\psi_{13}\rangle$. As usual, it is sufficient to assume that the input is $|\psi_0\rangle = |xyz\rangle$ where x, y, z are the binary digit labeling the upper, middle and lower line of the quantum circuit respectively. This gives

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\left(|xy0\rangle + (-1)^z|xy1\rangle\right)$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}\left(|xyy\rangle + (-1)^z|xy\overline{y}\rangle\right)$$

$$|\psi_3\rangle = \frac{1}{\sqrt{2}}\left(e^{-\imath y\pi/4}|xyy\rangle + (-1)^z e^{-\imath(1-y)\pi/4}|xy\overline{y}\rangle\right)$$

$$|\psi_4\rangle = \frac{1}{\sqrt{2}}\left(e^{-\imath y\pi/4}|xy(x\oplus y)\rangle + (-1)^z e^{-\imath(1-y)\pi/4}|xy(x\oplus\overline{y})\rangle\right)$$

$$|\psi_5\rangle = \frac{1}{\sqrt{2}}\left(e^{\imath\{(x\oplus y)-y\}\pi/4}|xy(x\oplus y)\rangle + (-1)^z e^{\imath\{(x\oplus(1-y))-1+y\}\pi/4}|xy(x\oplus\overline{y})\rangle\right)$$

$$|\psi_6\rangle = \frac{1}{\sqrt{2}}\left(e^{\imath\{(x\oplus y)-y\}\pi/4}|xyx\rangle + (-1)^z e^{\imath\{(x\oplus(1-y))-1+y\}\pi/4}|xy\overline{x})\rangle\right)$$

$$|\psi_7\rangle = \frac{1}{\sqrt{2}}\left(e^{\imath\{(x\oplus y)-x-y\}\pi/4}|xyx\rangle + (-1)^z e^{\imath\{(x\oplus(1-y))-2+x+y\}\pi/4}|xy\overline{x})\rangle\right)$$

$$|\psi_8\rangle = \frac{1}{\sqrt{2}}\left(e^{\imath\{(x\oplus y)-x-y\}\pi/4}|xy0\rangle + (-1)^z e^{\imath\{(x\oplus(1-y))-2+x+y\}\pi/4}|xy1)\rangle\right)$$

$$|\psi_9\rangle = \frac{1}{\sqrt{2}}\left(e^{\imath\{(x\oplus y)-x-2y\}\pi/4}|xy0\rangle + (-1)^z e^{\imath\{(x\oplus(1-y))-1+x\}\pi/4}|xy1)\rangle\right)$$

$$\begin{aligned}|\psi_{10}\rangle &= \frac{1}{2}\left(e^{\imath\{(x\oplus y)-x-2y\}\pi/4} + (-1)^z e^{\imath\{(x\oplus(1-y))-1+x\}\pi/4}\right)|x(x\oplus y)0\rangle \\ &\quad + \frac{1}{2}\left(e^{\imath\{(x\oplus y)-x-2y\}\pi/4} - (-1)^z e^{\imath\{(x\oplus(1-y))-1+x\}\pi/4}\right)|x(x\oplus y)1)\rangle\end{aligned}$$

To simplify the expression for $|\psi_{11}\rangle$, it is worth remarking that $x\oplus(1-y)-x\oplus y$ can be computed as follows : (i) if $y=0$ then it gives $1-2x$, (ii) if $y=1$ it gives $2x-1$. So that $x\oplus(1-y)-x\oplus y=(-1)^y(1-2x)=(-1)^{x+y}$. Hence :

$$\begin{aligned}|\psi_{11}\rangle &= \frac{1}{2}\left(e^{-\imath\{x+2y\}\pi/4} + (-1)^z e^{\imath\{(-1)^{x+y}-1+x\}\pi/4}\right)|x(x\oplus y)0\rangle \\ &\quad + \frac{1}{2}\left(e^{-\imath\{x+2y\}\pi/4} - (-1)^z e^{\imath\{(-1)^{x+y}-1+x\}\pi/4}\right)|x(x\oplus y)1)\rangle\end{aligned}$$

$$\begin{aligned}|\psi_{12}\rangle &= \frac{1}{2}\left(e^{-\imath\{x+2y\}\pi/4} + (-1)^z e^{\imath\{(-1)^{x+y}-1+x\}\pi/4}\right)|xy0\rangle \\ &\quad + \frac{1}{2}\left(e^{-\imath\{x+2y\}\pi/4} - (-1)^z e^{\imath\{(-1)^{x+y}-1+x\}\pi/4}\right)|xy1)\rangle\end{aligned}$$

The last gates multiplies the state by $e^{(x+2y)\pi/4}$ thus the first term, in the phase factor of each basis vector, becomes 1, while the phase in the second one becomes $((1-2x)(1-2y)+x+2y-1+x)\pi/4=xy\pi$ (since $1-2x=(-1)^x$). Thus

$$|\psi_{13}\rangle = \frac{1}{2}\left(1+(-1)^{z+xy}\right)|xy0\rangle + \frac{1}{2}\left(1-(-1)^{z+xy}\right)|xy1)\rangle$$

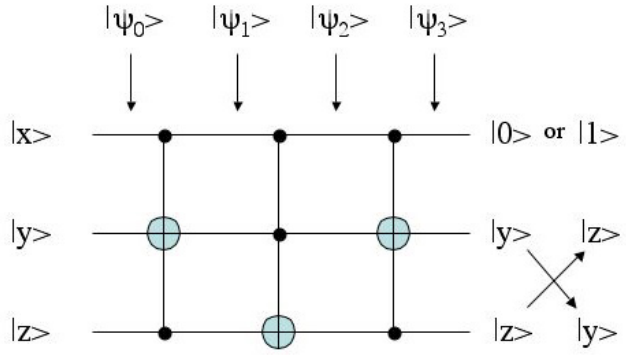
Then if $(x,y)\neq(1,1)$ it follows that $xy=0$ so that the right hand side is nothing but $|xyz\rangle$. If $x=y=1$, then the right hand side is $|xy\overline{z}\rangle$. Hence the circuit acts as the Toffoli gate.

– **4.25-** *Recall that the Fredkin (controlled-swap) gate performs the transform (where "·" means 0)*

$$\begin{bmatrix} 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 \end{bmatrix}$$

.

1. *Give a quantum circuit which used three Toffoli gates to construct the Fredkin gate (*Hint : *think of the* SWAP*-gate construction-you can control each gate, one at a time).*
2. *Show that the first and the last Toffoli gates can be replaced by* CNOT*-gates.*
3. *Now replace the middle Toffoli gate by the circuit in Figure 4.8 to obtain a Fredkin gate construction using only six two-qubits gates.*
4. *Can you come up with an even simpler construction, with only five two-qubit gates ?*



Circuit for the Fredkin gate

1.- The circuit "Constructing the Fredkin gate" gives the solution. For indeed if $|\psi_0\rangle = |xyz\rangle$ is the input, then after the first Toffoli gate it gives

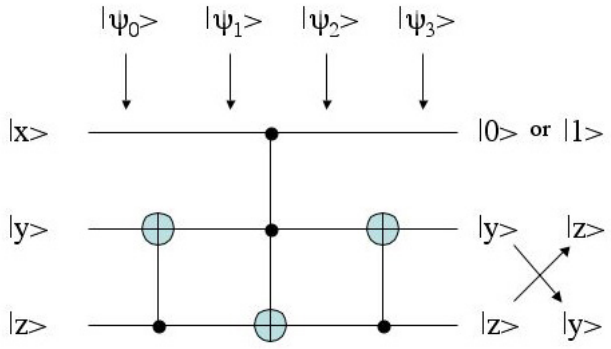
$$|\psi_1\rangle = |x(xz \oplus y)z\rangle$$
$$|\psi_2\rangle = |x(xz \oplus y)(xz \oplus xy \oplus z\rangle = |x(xz \oplus y)(xy \oplus \overline{x}z)\rangle$$
$$|\psi_3\rangle = |x(\overline{x}y \oplus xz)(xy \oplus \overline{x}z)\rangle$$

In particular if $x = 0$ then $|\psi_3\rangle = |0yz\rangle$ whereas if $x = 1$ then $|\psi_3\rangle = |1yz\rangle$, which is what the Fredkin gate is doing.

2.- The circuit 2 for the Fredkin gate, indeed gives also the Fredkin gate by replacing the left and right Toffoli gates by two CNOT gates each. Again, if $|\psi_0\rangle = |xyz\rangle$ is the input, it gives

$$|\psi_1\rangle = |x(y \oplus z)z\rangle$$
$$|\psi_2\rangle = |x(y \oplus z)(xy \oplus xz \oplus z)\rangle = |x(y \oplus z)(xy \oplus \overline{x}z)\rangle$$
$$|\psi_3\rangle = |x(\overline{x}y \oplus xz)(xy \oplus \overline{x}z)\rangle$$

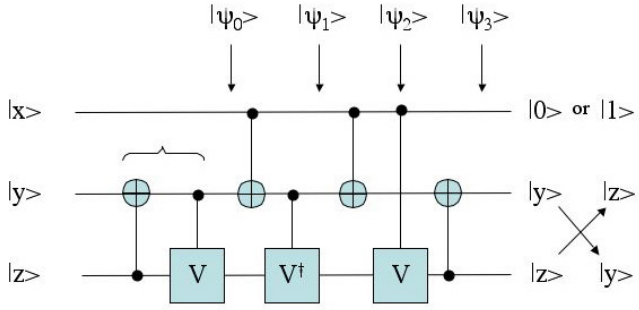
namely the same result as in the previous question.



Circuit for the Fredkin gate

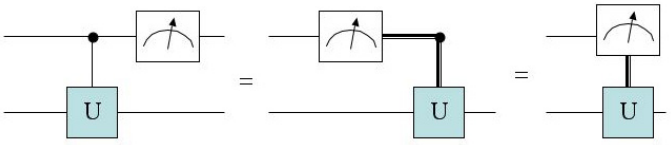
3.- Thanks to Figure 4.8, with $V = e^{\imath(X-1)\pi/4}$, then $U = V^2 = X$ giving a Toffoli gate. This produce a circuit with $5+2 = 7$ two-qubit gates. However the first two gates (a CNOT and a $C^1(V)$) combine to give one two-qubit gate, leading to a circuit with 6 two-qubit gates.

4.- It does not seems possible to decrease the number of two-qubit gates.



Circuit 3 for the Fredkin gate with V= $e^{i(X-I)\pi/4}$

– **4.35- (Measurement commutes with controls** *A consequence of the principle of deferred measurement is that measurements commute with quantum gates when the qubit being measured is a control qubit, that is :*



Measurement commutes with control

(Recall that double lines represent classical bits in this diagram). Prove the first equality. The rightmost circuit is simply a convenient notation to depict the use of a measurement result to classically control a quantum gate.

Looking at the Figure *Measurement commutes with control* the left hand side give $|x\rangle \otimes U^x|y\rangle$. If a measurement is applied to the qubit $|x\rangle$ and gives the outcome $m \in \{0,1\}$ then the second qubit is given by $U^m|y\rangle$. But this is exactly what the right hand side is giving.