
PREMIUM
...SERIES...
SCHOLAR MATE
In every walk in with nature one receives far
more than he seeks. ...
Flowers
KING SIZE
PREMIUM QUALITY NOTEBOOK
* Bright and Fine Quality Paper
* Smooth Writing Paper
* 'A' Grade Paper For Long Lasting

soorajss1729@gmail.com / +91-9400635788

INDEX

(4)

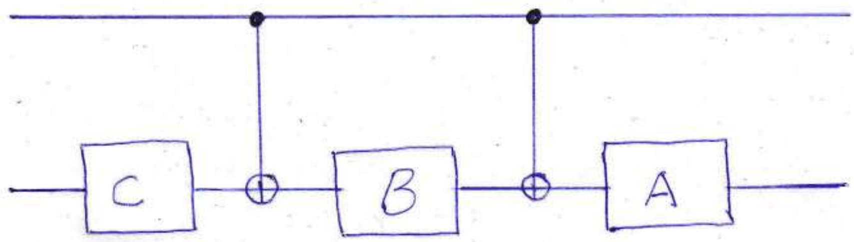
NAME : SOORAJ S.
STD : ....SEC: ....
ROLL No.: ....SUB: ....

S.No.	Date	Title	Page No.	Teacher's Sign/ Comment
		QUANTUM COMPUTATION		
		- Nielsen & Chuang		

Ex: 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 # of single qubit gates needed in the construction from 3 to 2?

Ans: $R_y = AXBXC$ & $ABC = I$



$$AXBXC = R_z(\beta)R_y(\gamma)R_z(\delta)$$

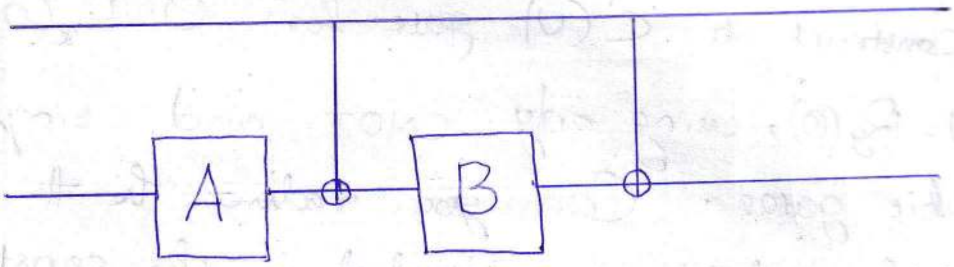
where $A = R_z(\beta)R_y(\gamma/2)$, $B = R_y(-\gamma/2)R_z\left(\frac{-\delta-\beta}{2}\right)$,

$C = R_z\left(\frac{\delta-\beta}{2}\right)$

Take, $\beta = \delta = 0$ gives.

$A = R_y(\gamma/2)$ & $B = R_y(-\gamma/2)$ & $C = I$

such that $R_y = AXBX$

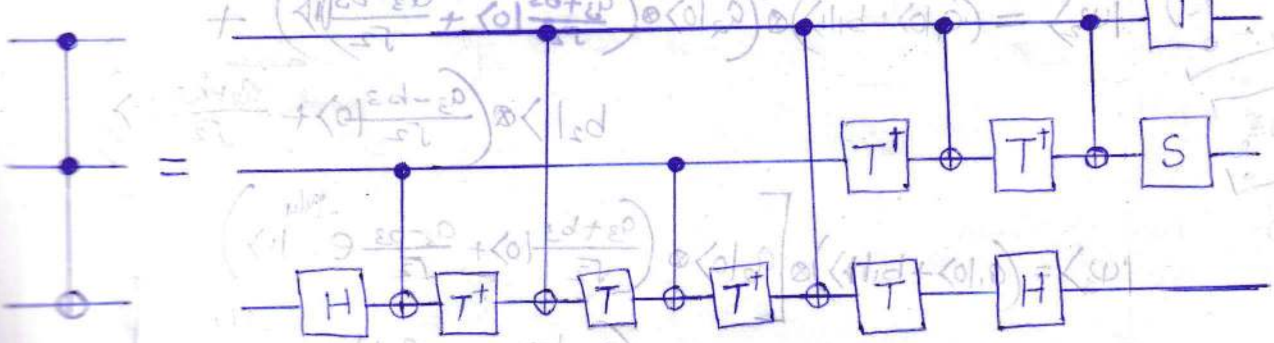

A
B

Ultimately, we will show that any unitary operation can be composed to an arbitrarily good approximation from just the Hadamard, phase, controlled-NOT and $\pi/8$ gates.

$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$, $\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$, $|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$, $\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$

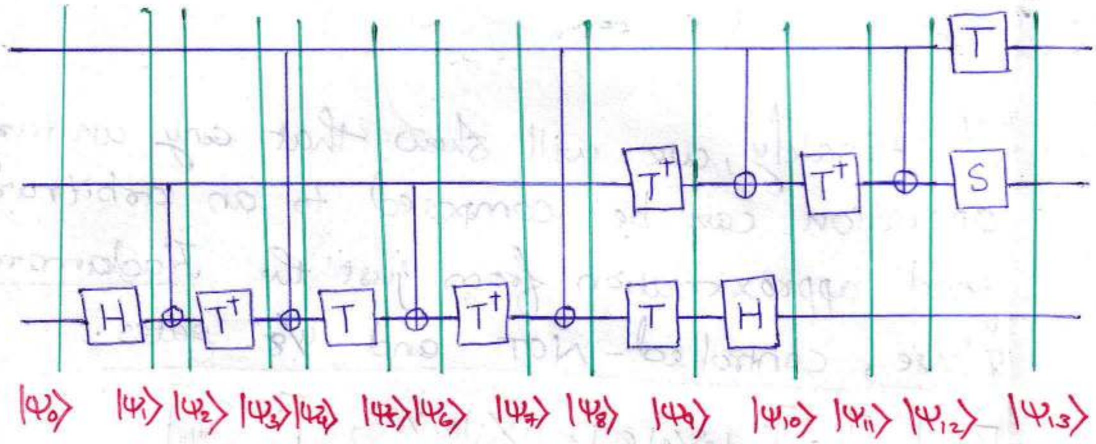
* Implementation of the Toffoli gate using Hadamard, phase, controlled-NOT, and $\pi/8$ gates:

Fig(4.9)



$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}, \quad T^{\dagger} = \begin{bmatrix} 1 & 0 \\ 0 & e^{-i\pi/4} \end{bmatrix}$

$S = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/2} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$



$$|\psi_0\rangle = |\phi_1 \phi_2 \phi_2\rangle = (a_1|0\rangle + b_1|1\rangle) \otimes (a_2|0\rangle + b_2|1\rangle) \otimes (a_3|0\rangle + b_3|1\rangle)$$

$$|\psi_1\rangle = (a_1|0\rangle + b_1|1\rangle) \otimes (a_2|0\rangle + b_2|1\rangle) \otimes \left(\frac{a_3+b_3}{\sqrt{2}}|0\rangle + \frac{a_3-b_3}{\sqrt{2}}|1\rangle\right)$$

$$|\psi_2\rangle = (a_1|0\rangle + b_1|1\rangle) \otimes \left(a_2|0\rangle \otimes \left(\frac{a_3+b_3}{\sqrt{2}}|0\rangle + \frac{a_3-b_3}{\sqrt{2}}|1\rangle\right) + b_2|1\rangle \otimes \left(\frac{a_3-b_3}{\sqrt{2}}|0\rangle + \frac{a_3+b_3}{\sqrt{2}}|1\rangle\right)\right)$$

$$|\psi_3\rangle = (a_1|0\rangle + b_1|1\rangle) \otimes \left[a_2|0\rangle \otimes \left(\frac{a_3+b_3}{\sqrt{2}}|0\rangle + \frac{a_3-b_3}{\sqrt{2}} e^{-i\pi/4}|1\rangle\right) + b_2|1\rangle \otimes \left(\frac{a_3-b_3}{\sqrt{2}}|0\rangle + \frac{a_3+b_3}{\sqrt{2}} e^{-i\pi/4}|1\rangle\right)\right]$$

$$|\psi_4\rangle = a_1|0\rangle \otimes \left[a_2|0\rangle \otimes \left(\frac{a_3+b_3}{\sqrt{2}}|0\rangle + \frac{a_3-b_3}{\sqrt{2}} e^{-i\pi/4}|1\rangle\right) + b_2|1\rangle \otimes \left(\frac{a_3-b_3}{\sqrt{2}}|0\rangle + \frac{a_3+b_3}{\sqrt{2}} e^{-i\pi/4}|1\rangle\right)\right]$$

$$b_1|1\rangle \otimes \left[a_2|0\rangle \otimes \left(\frac{a_3-b_3}{\sqrt{2}} e^{-i\pi/4}|0\rangle + \frac{a_3+b_3}{\sqrt{2}}|1\rangle\right) + b_2|1\rangle \otimes \left(\frac{a_3+b_3}{\sqrt{2}} e^{-i\pi/4}|0\rangle + \frac{a_3-b_3}{\sqrt{2}}|1\rangle\right)\right]$$

$$|\psi_5\rangle = a_1|0\rangle\otimes\left[a_2|0\rangle\otimes\left(\frac{a_3+b_3}{\sqrt{2}}|0\rangle + \frac{a_3-b_3}{\sqrt{2}}|1\rangle\right) + b_2|1\rangle\otimes\left(\frac{a_3-b_3}{\sqrt{2}}|0\rangle + \frac{a_3+b_3}{\sqrt{2}}|1\rangle\right)\right]$$

$$+ b_1|1\rangle\otimes\left[a_2|0\rangle\otimes\left(\frac{a_3-b_3}{\sqrt{2}}e^{-i\pi/4}|0\rangle + \frac{a_3+b_3}{\sqrt{2}}e^{i\pi/4}|1\rangle\right) + b_2|1\rangle\otimes\left(\frac{a_3+b_3}{\sqrt{2}}e^{-i\pi/4}|0\rangle + \frac{a_3-b_3}{\sqrt{2}}e^{i\pi/4}|1\rangle\right)\right]$$

$$|\psi_6\rangle = a_1|0\rangle\otimes\left[a_2|0\rangle\otimes\left(\frac{a_3+b_3}{\sqrt{2}}|0\rangle + \frac{a_3-b_3}{\sqrt{2}}|1\rangle\right) + b_2|1\rangle\otimes\left(\frac{a_3+b_3}{\sqrt{2}}|0\rangle + \frac{a_3-b_3}{\sqrt{2}}|1\rangle\right)\right.$$

$$+ b_1|1\rangle\otimes\left[a_2|0\rangle\otimes\left(\frac{a_3-b_3}{\sqrt{2}}e^{-i\pi/4}|0\rangle + \frac{a_3+b_3}{\sqrt{2}}e^{i\pi/4}|1\rangle\right) + b_2|1\rangle\otimes\left(\frac{a_3-b_3}{\sqrt{2}}e^{i\pi/4}|0\rangle + \frac{a_3+b_3}{\sqrt{2}}e^{-i\pi/4}|1\rangle\right.\right.$$

$$|\psi_7\rangle = a_1|0\rangle\otimes\left[a_2|0\rangle\otimes\left(\frac{a_3+b_3}{\sqrt{2}}|0\rangle + \frac{a_3-b_3}{\sqrt{2}}e^{-i\pi/4}|1\rangle\right) + b_2|1\rangle\otimes\left(\frac{a_3+b_3}{\sqrt{2}}|0\rangle + \frac{a_3-b_3}{\sqrt{2}}e^{-i\pi/4}|1\rangle\right)\right.$$

$$+ b_1|1\rangle\otimes\left[a_2|0\rangle\otimes\left(\frac{a_3-b_3}{\sqrt{2}}e^{-i\pi/4}|0\rangle + \frac{a_3+b_3}{\sqrt{2}}|1\rangle\right) + b_2|1\rangle\otimes\left(\frac{a_3-b_3}{\sqrt{2}}e^{i\pi/4}|0\rangle + \frac{a_3+b_3}{\sqrt{2}}e^{-i\pi/2}|1\rangle\right.\right.$$

$$|\psi_8\rangle = a_1|0\rangle\otimes\left[a_2|0\rangle\otimes\left(\frac{a_3+b_3}{\sqrt{2}}|0\rangle + \frac{a_3-b_3}{\sqrt{2}}e^{-i\pi/4}|1\rangle\right) + b_2|1\rangle\otimes\left(\frac{a_3+b_3}{\sqrt{2}}|0\rangle + \frac{a_3-b_3}{\sqrt{2}}e^{-i\pi/4}|1\rangle\right)\right.$$

$$+ b_1|1\rangle\otimes\left[a_2|0\rangle\otimes\left(\frac{a_3+b_3}{\sqrt{2}}|0\rangle + \frac{a_3-b_3}{\sqrt{2}}e^{-i\pi/4}|1\rangle\right) + b_2|1\rangle\otimes\left(\frac{a_3+b_3}{\sqrt{2}}e^{-i\pi/2}|0\rangle + \frac{a_3-b_3}{\sqrt{2}}e^{i\pi/4}|1\rangle\right)\right]\Bigg]$$

$$|\psi_9\rangle = a_1|0\rangle\otimes\left[a_2|0\rangle\otimes\left(\frac{a_3+b_3}{\sqrt{2}}|0\rangle + \frac{a_3-b_3}{\sqrt{2}}|1\rangle\right) + b_2e^{-i\pi/4}\otimes\left(\frac{a_3+b_3}{\sqrt{2}}|0\rangle + \frac{a_3-b_3}{\sqrt{2}}|1\rangle\right)\right]$$

$$+ b_1|1\rangle\otimes\left[a_2|0\rangle\otimes\left(\frac{a_3+b_3}{\sqrt{2}}|0\rangle + \frac{a_3-b_3}{\sqrt{2}}|1\rangle\right) + b_2e^{-i\pi/4}|1\rangle\otimes\left(\frac{a_3+b_3}{\sqrt{2}}e^{-i\pi/2}|\right.\right.$$

$$|\psi_{10}\rangle = a_1|0\rangle\otimes\left[a_2|0\rangle\otimes\left(a_3|0\rangle + b_3|1\rangle\right) + b_2 e^{-i\pi/4}|1\rangle\otimes\left(a_3|0\rangle + b_3|1\rangle\right)\right]$$

$$+ b_1|1\rangle\otimes\left[b_2 e^{-i\pi/4}|0\rangle\otimes\left(b_3|0\rangle + a_3|1\rangle\right) + a_2|1\rangle\otimes\left(a_3|0\rangle + b_3|1\rangle\right)\right]$$

$$|\psi_{11}\rangle = a_1|0\rangle\otimes\left[a_2|0\rangle\otimes\left(a_3|0\rangle + b_3|1\rangle\right) + b_2 e^{-i\pi/2}|1\rangle\otimes\left(a_3|0\rangle + b_3|1\rangle\right)\right]$$

$$+ b_1|1\rangle\otimes e^{-i3\pi/4}\left[b_2|0\rangle\otimes\left(b_3|0\rangle + a_3|1\rangle\right) + a_2 e^{i\pi/2}|1\rangle\otimes\left(a_3|0\rangle + b_3|1\rangle\right)\right]$$

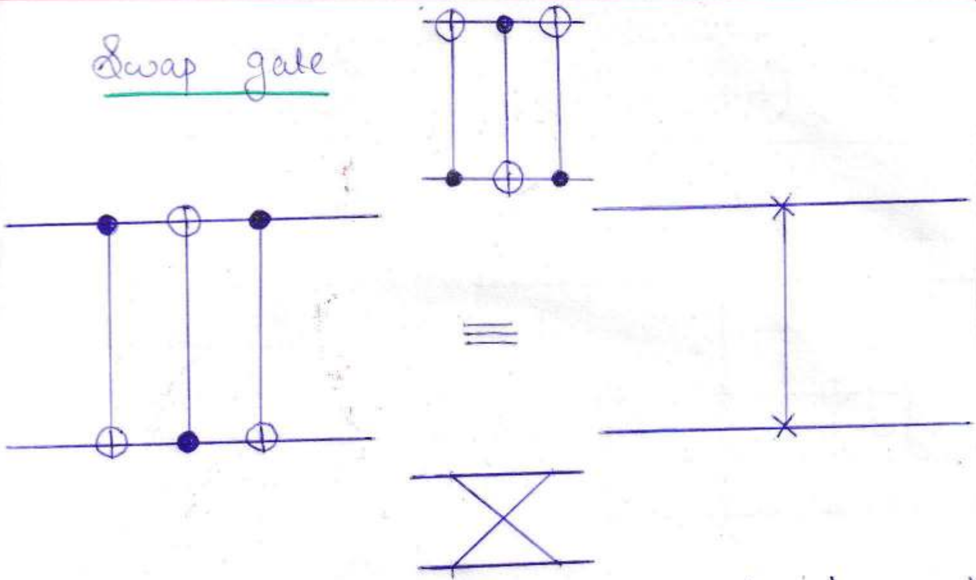
$$|\psi_{12}\rangle = a_1|0\rangle\otimes\left[a_2|0\rangle\otimes\left(a_3|0\rangle + b_3|1\rangle\right) + b_2 e^{-i\pi/2}|1\rangle\otimes\left(a_3|0\rangle + b_3|1\rangle\right)\right]$$

$$+ b_1 e^{-i3\pi/4}|1\rangle\otimes\left[a_2 e^{i\pi/2}|0\rangle\otimes\left(a_3|0\rangle + b_3|1\rangle\right) + b_2|1\rangle\otimes\left(b_3|0\rangle + a_3|1\rangle\right)\right]$$

$$|\psi_{13}\rangle = a_1|0\rangle\otimes\left[a_2|0\rangle\otimes\left(a_3|0\rangle + b_3|1\rangle\right) + b_2|1\rangle\otimes\left(a_3|0\rangle + b_3|1\rangle\right)\right]$$

$$+ b_1|1\rangle\otimes\left[a_2|0\rangle\otimes\left(a_3|0\rangle + b_3|1\rangle\right) + b_2|1\rangle\otimes\left(b_3|0\rangle + a_3|1\rangle\right)\right]$$

Swap gate



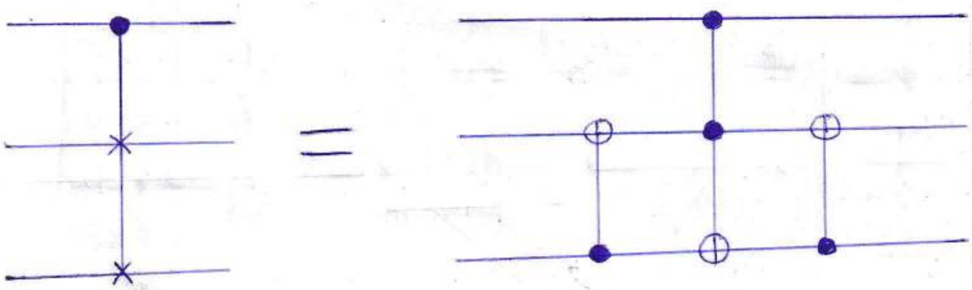
$$|a,b\rangle \rightarrow |a, a\oplus b\rangle \rightarrow |a\oplus(a\oplus b), a\oplus b\rangle = |b, a\oplus b\rangle$$

$$\rightarrow |b, (a\oplus b)\oplus b\rangle = |b, a\rangle$$

$$U_{SWAP} = |00\rangle\langle 00| + |01\rangle\langle 10| + |10\rangle\langle 01| + |11\rangle\langle 11|$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Fredkin (controlled-swap) gate



$$U_{CSWAP} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U_{SWAP}$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Ex: 4.25

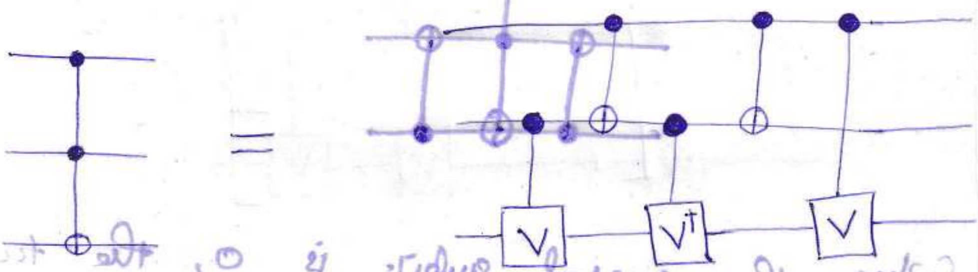
① Given a quantum circuit which uses 3 Toffoli gates to construct the Fredkin gate.

② Show that the 1st and last Toffoli gates can be replaced by CNOT gates.

③ Replace the middle Toffoli gate with the circuit in Fig. 4.8 to obtain a Fredkin gate construction using only 6 two-qubit gates.

④ Can you come up with an even simpler construction, with only 5 two-qubit gates?

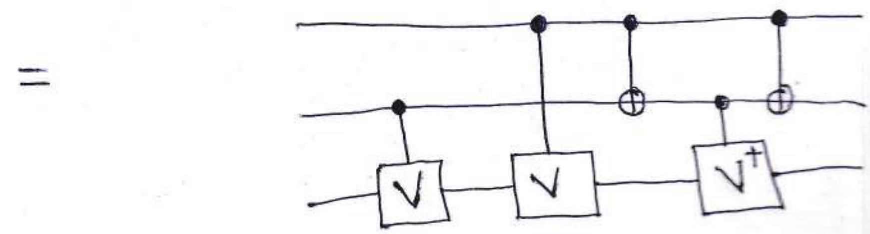
Ans: Toffoli gate.



where, $V = (1-i)(I+iX)/2$ & $V^2 = U$

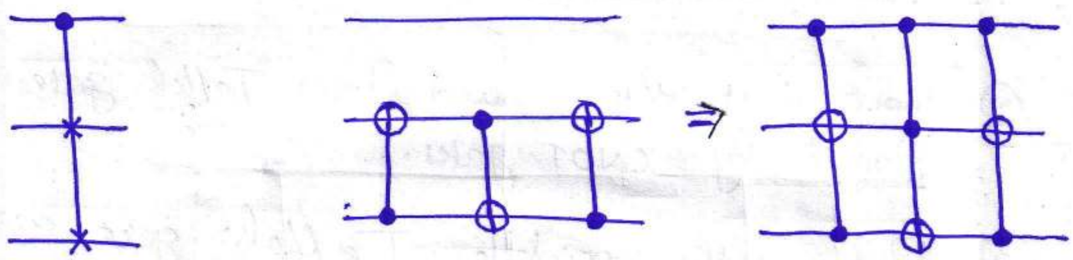
Ex: 4.22

QC3

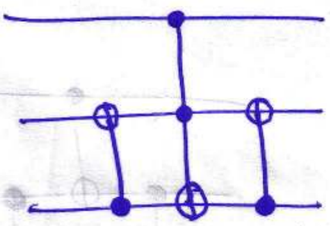


Fredkin gate (Controlled swap gate)

①

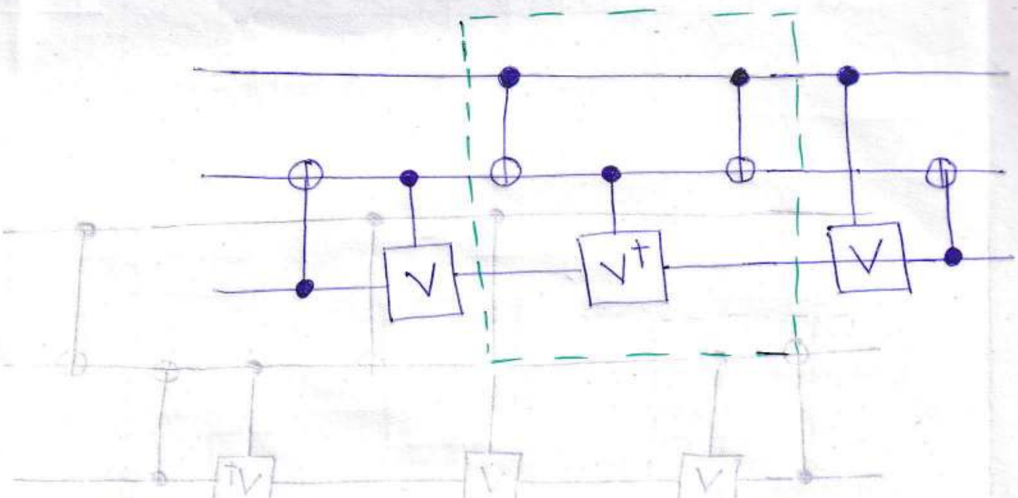


② - The 1st and the last Toffoli gates can be replaced by CNOT gates.



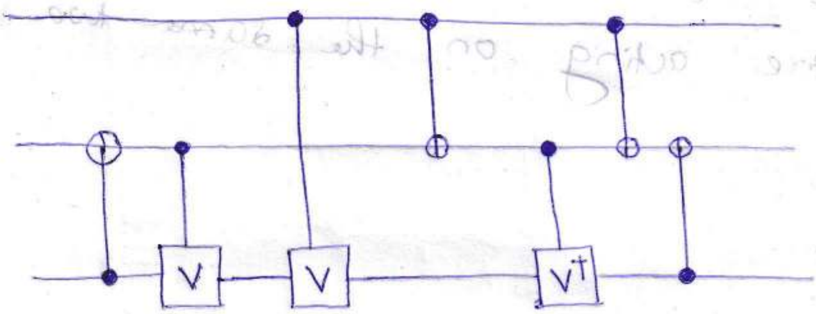
When the control qubit is 0, the two CNOTs cancel each other to identity.

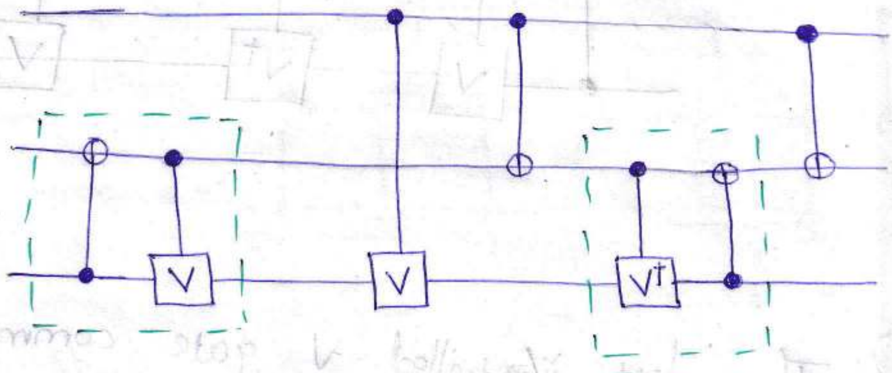
③



④ The last controlled-V gate commutes with the previous 3 gates.

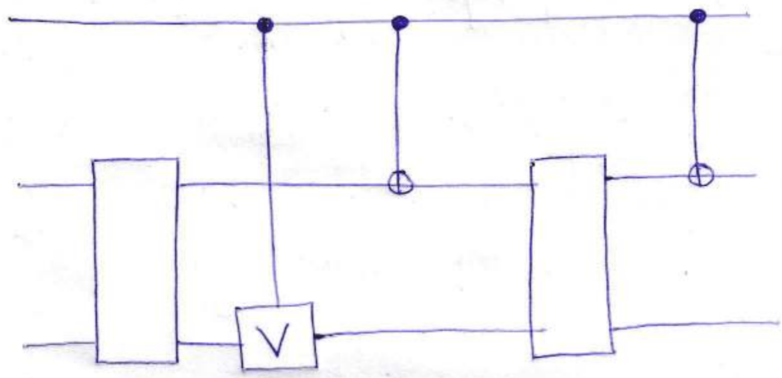
$V = (1-i)(I+iX)/2$ &



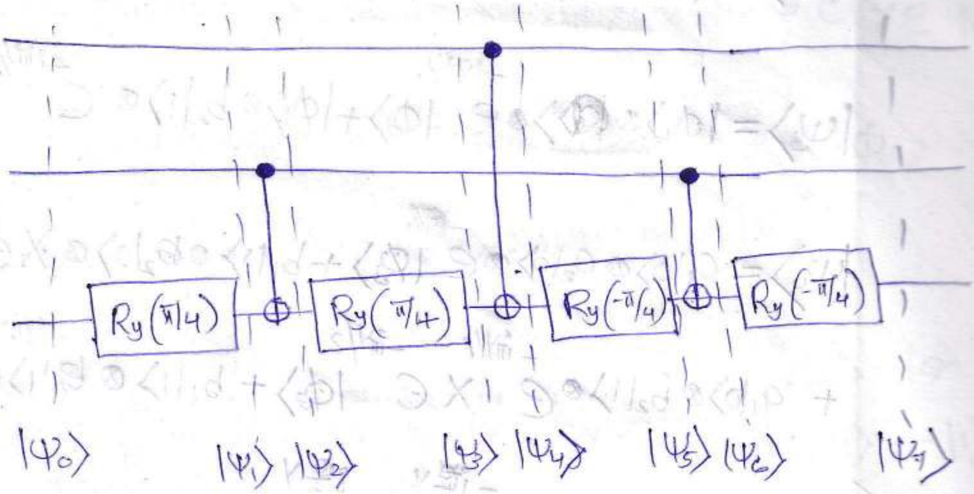


~~The last~~
We can combine controlled-$V^\dagger$ and CNOT gate (the 1st two gates also). since they are acting on the same two qubits.

The Fredkin (controlled-swap) gate with 5 two-qubit gates.



Ex: 4.26 Show that the circuit:



differs from a Toffoli gate only by relative phases. That is, the circuit takes $|c_1, c_2, t\rangle$ to $e^{i\theta(c_1, c_2, t)} |c_1, c_2, t \oplus c_1 \cdot c_2\rangle$ where $e^{i\theta(c_1, c_2, t)}$ is some relative phase factor. Such gates can sometimes be useful in experimental implementations, where it may be much easier to implement a gate that is the same as the Toffoli up to relative phases than it is to do the Toffoli directly.

$$\boxed{|\phi_i\rangle = a_i|0\rangle + b_i|1\rangle}$$

Ans: $|\Psi_0\rangle = |\phi_1 \phi_2 \phi_3\rangle = |\phi_1\rangle \otimes |\phi_2\rangle \otimes |\phi_3\rangle$

$|\Psi_1\rangle = |\phi_1\rangle \otimes |\phi_2\rangle \otimes e^{-i\pi Y/8} |\phi_3\rangle$

$$|\psi_2\rangle = |\phi_1\rangle \otimes a_2|0\rangle \otimes e^{-i\pi Y/8}|\phi_3\rangle + |\phi_1\rangle \otimes b_2|1\rangle \otimes X e^{-i\pi Y/8}|\phi_3\rangle$$

$$|\psi_3\rangle = |\phi_1\rangle \otimes a_2|0\rangle \otimes e^{-i\pi Y/4}|\phi_3\rangle + |\phi_1\rangle \otimes b_2|1\rangle \otimes e^{-i\pi Y/8} X e^{-i\pi Y/8}|\phi_3\rangle$$

$$|\psi_4\rangle = a_1|0\rangle \otimes a_2|0\rangle \otimes e^{-i\pi Y/4}|\phi_3\rangle + b_1|1\rangle \otimes a_2|0\rangle \otimes X e^{-i\pi Y/4}|\phi_3\rangle$$

$$+ a_1|0\rangle \otimes b_2|1\rangle \otimes e^{-i\pi Y/8} X e^{-i\pi Y/8}|\phi_3\rangle + b_1|1\rangle \otimes b_2|1\rangle \otimes X e^{-i\pi Y/8} X e^{-i\pi Y/8}|\phi_3\rangle$$

$$X e^{-i\frac{\theta}{2}Y} = e^{i\frac{\theta}{2}Y} X$$

$$= a_1|0\rangle \otimes a_2|0\rangle \otimes e^{-i\frac{\pi}{4}Y}|\phi_3\rangle + b_1|1\rangle \otimes a_2|0\rangle \otimes X e^{-i\frac{\pi}{4}Y}|\phi_3\rangle$$

$$+ a_1|0\rangle \otimes b_2|1\rangle \otimes X|\phi_3\rangle + b_1|1\rangle \otimes b_2|1\rangle \otimes |\phi_3\rangle$$

$$|\psi_5\rangle = a_1|0\rangle \otimes a_2|0\rangle \otimes e^{-i\frac{\pi}{8}Y}|\phi_3\rangle + b_1|1\rangle \otimes a_2|0\rangle \otimes e^{i\frac{\pi}{8}Y} X e^{-i\frac{\pi}{4}Y}|\phi_3\rangle$$

$$+ a_1|0\rangle \otimes b_2|1\rangle \otimes e^{i\frac{\pi}{8}Y} X|\phi_3\rangle + b_1|1\rangle \otimes b_2|1\rangle \otimes e^{i\frac{\pi}{8}Y}|\phi_3\rangle$$

$$|\psi_6\rangle = a_1|0\rangle \otimes a_2|0\rangle \otimes e^{-i\frac{\pi}{8}Y}|\phi_3\rangle + b_1|1\rangle \otimes a_2|0\rangle \otimes e^{i\frac{\pi}{8}Y} X e^{-i\frac{\pi}{4}Y}|\phi_3\rangle$$

$$+ a_1|0\rangle \otimes b_2|1\rangle \otimes X e^{i\frac{\pi}{8}Y} X|\phi_3\rangle + b_1|1\rangle \otimes b_2|1\rangle \otimes X e^{i\frac{\pi}{8}Y}|\phi_3\rangle$$

$$|\psi_7\rangle = a_1|0\rangle \otimes a_2|0\rangle \otimes |\phi_3\rangle + b_1|1\rangle \otimes a_2|0\rangle \otimes e^{i\frac{\pi}{4}Y} X e^{-i\frac{\pi}{4}Y} |\phi_3\rangle$$

$$+ a_1|0\rangle \otimes b_2|1\rangle \otimes e^{i\frac{\pi}{8}Y} X e^{i\frac{\pi}{8}Y} X |\phi_3\rangle + b_1|1\rangle \otimes b_2|1\rangle \otimes e^{i\frac{\pi}{8}Y} X e^{i\frac{\pi}{8}Y} |\phi_3\rangle$$

$$= a_1|0\rangle \otimes a_2|0\rangle \otimes |\phi_3\rangle + b_1|1\rangle \otimes a_2|0\rangle \otimes e^{i\frac{\pi}{2}Y} X |\phi_3\rangle$$

$$+ a_1|0\rangle \otimes b_2|1\rangle \otimes |\phi_3\rangle + b_1|1\rangle \otimes b_2|1\rangle \otimes X|\phi_3\rangle$$

$$e^{i\frac{\pi}{2}Y} X = \left[\cos\left(\tfrac{\pi}{2}\right) I + i\sin\left(\tfrac{\pi}{2}\right) Y\right] X = iYX$$

$$= -iXY = -i(iZ) = Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$Z|0\rangle = |0\rangle$$

$$Z|1\rangle = -|1\rangle$$

$$= a_1|0\rangle \otimes a_2|0\rangle \otimes |\phi_3\rangle + b_1|1\rangle \otimes a_2|0\rangle \otimes Z|\phi_3\rangle$$

$$+ a_1|0\rangle \otimes b_2|1\rangle \otimes |\phi_3\rangle + b_1|1\rangle \otimes b_2|1\rangle \otimes X|\phi_3\rangle$$

Ex: 4.27. Using just CNOTs and Toffoli gates, construct a quantum circuit to perform the transformation (partial cyclic permutation operator)

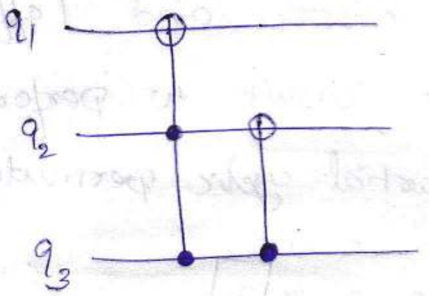
$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Ans: U is 8×8 : 3 qubit operation.

$|000\rangle \rightarrow |000\rangle$
$|001\rangle \rightarrow |010\rangle$
$|010\rangle \rightarrow |011\rangle$
$|011\rangle \rightarrow |100\rangle$
$|100\rangle \rightarrow |101\rangle$
$|101\rangle \rightarrow |110\rangle$
$|110\rangle \rightarrow |111\rangle$
$|111\rangle \rightarrow |001\rangle$

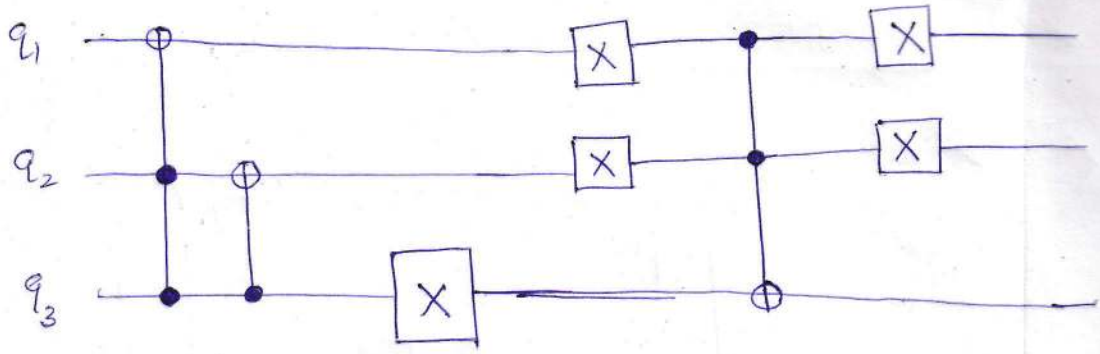
$$\boxed{\begin{array}{l} |q11\rangle \rightarrow |\bar{q}\,x\,x\rangle \\ |q10\rangle \rightarrow |q\,x\,x\rangle \\ |q01\rangle \rightarrow |q\,x\,x\rangle \\ |q00\rangle \rightarrow |q\,x\,x\rangle \end{array}}$$

$$\boxed{\begin{array}{l} |0q1\rangle \rightarrow |*\,\bar{q}\,*\rangle \\ |1q1\rangle \rightarrow |*\,\bar{q}\,*\rangle \\ |1q0\rangle \rightarrow |*\,q\,*\rangle \\ |0q0\rangle \rightarrow |*\,q\,*\rangle \end{array}}$$



$\|000\rangle \rightarrow$	$\|000\rangle \rightarrow$	$\|000\rangle$	NO FLIP
$\|001\rangle \rightarrow$	$\|011\rangle \rightarrow$	$\|010\rangle$	Flip 3^{rd} qubit
$\|010\rangle \rightarrow$	$\|010\rangle \rightarrow$	$\|011\rangle$	"
$\|011\rangle \rightarrow$	$\|101\rangle \rightarrow$	$\|100\rangle$	"
$\|100\rangle \rightarrow$	$\|100\rangle \rightarrow$	$\|101\rangle$	"
$\|101\rangle \rightarrow$	$\|111\rangle \rightarrow$	$\|110\rangle$	"
$\|110\rangle \rightarrow$	$\|110\rangle \rightarrow$	$\|111\rangle$	Flip 3^{rd} qubit
$\|111\rangle \rightarrow$	$\|001\rangle \rightarrow$	$\|001\rangle$	NO FLIP

Instead, we flip all 3^{rd} qubits (X-gate to 3^{rd} qubit) and only flip back when $|q_1 q_2 *\rangle = |00*\rangle$


q1
q2
q3
X
X
X
X
X

$C^n(U)$ operation

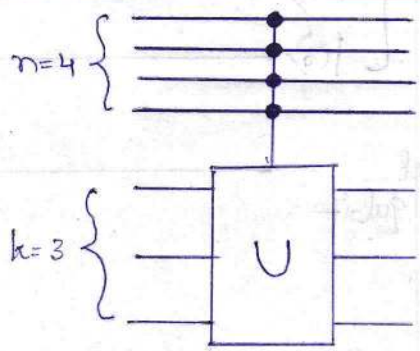
Suppose we have $n+k$ qubits, and U is a k qubit unitary operator. Then we define the controlled operation $C^n(U)$ by the equation,

$$C^n(U)|x_1 x_2 \cdots x_n\rangle|\psi\rangle = |x_1 x_2 \cdots x_n\rangle U^{x_1 x_2 \cdots x_n}|\psi\rangle$$

where,

$x_1 x_2 \cdots x_n$ in the exponent of U means the product of the bits $x_1, x_2, \ldots, x_n$.

ie., the operator U is applied to the last k qubits if the first n qubits are all equal to one, and otherwise, nothing is done.



sample circuit representation for the $C^n(U)$ operation,

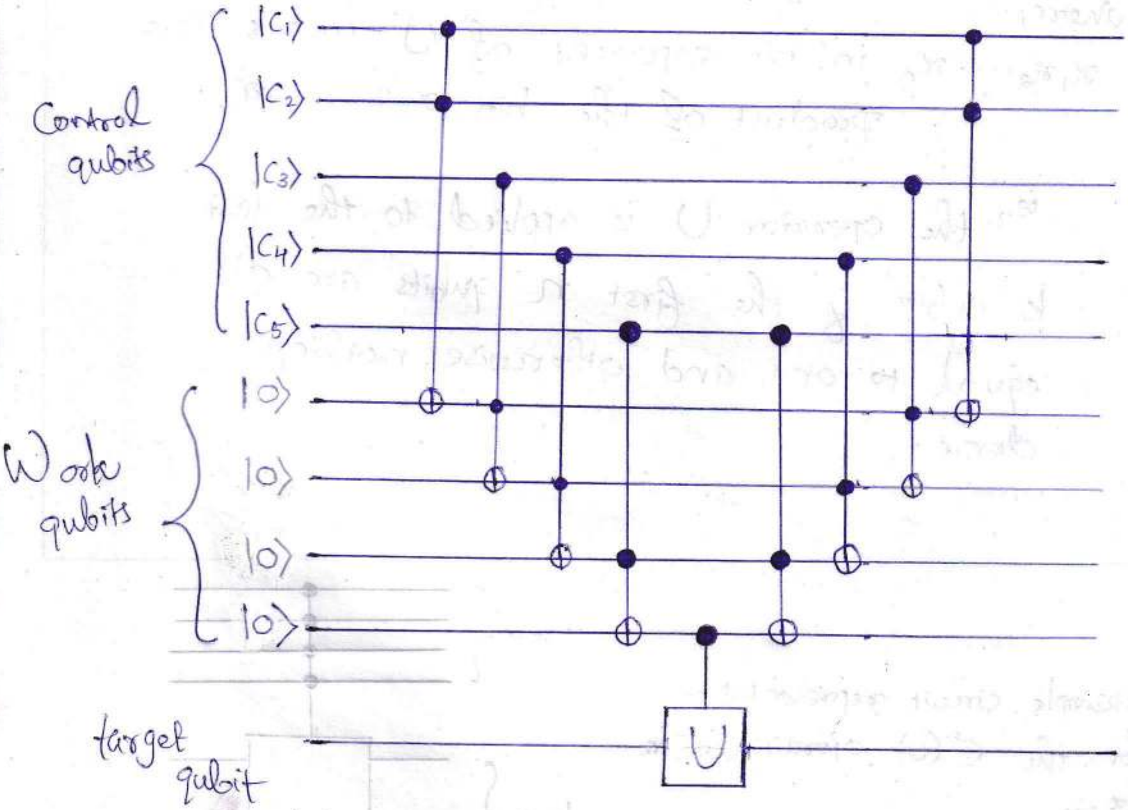
where,

U · unitary operator on k-qubits.

$n=4, \ k=3$

How may we implement $C^n(U)$ gates using our existing repertoire of gates, where U is an arbitrary single qubit unitary operation ?

Fig 4.10



3 stages & $(n-1)$ working qubits which all start and end in the state $|0\rangle$.

Suppose

The control qubits are in the computational basis state $|c_1, c_2, \ldots, c_n\rangle$.

Step 1: Reversibly AND all the control bits $c_1, \ldots, c_n$ together to produce the product $c_1 \cdot c_2 \cdot \ldots \cdot c_n$.

AND gate

i/p		o/p
0	0	0
0	1	0
1	0	0
1	1	1

To do this,

the 1st gate in the circuit ANDs c_1 and c_2 together, using a Toffoli gate, changing the state of the 1st work qubit to $|c_1 \cdot c_2\rangle$.

The next Toffoli gate ANDs c_3 with the product $c_1 \cdot c_2$ changing the state of the 2nd work qubit to $|c_1 \cdot c_2 \cdot c_3\rangle$. We continue applying Toffoli gates in this fashion, until the final work qubit is in the state $|c_1 \cdot c_2 \cdot \ldots \cdot c_n\rangle$.

Step 2: a U operation on the target qubit is performed, conditional on the final work qubit being set to one.

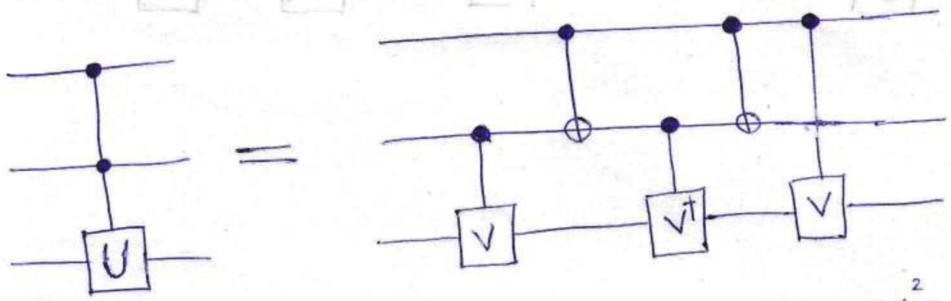
i.e., U is applied iff all of c_1 thro' c_n are set. ~~Hammer~~

Step 3: The last part of the circuit just reverses the steps of the 1st stage, returning all the work qubits to their initial state $|0\rangle$.

Combine result $\Rightarrow$ Apply the unitary operator U to the target qubit, iff all the control Bits c_1 thro' c_n are set, as desired.

Ex: ~~4~~.28 For $U = V^2$ with V unitary, construct a $C^5(U)$ gate analogous to that in Fig. 4.10 but using no work qubits. You may use controlled-V and controlled-$V^\dagger$ gates.

Ans: $C^2(U)$ gate



$V^2 = U$.

$$|00\rangle|\phi\rangle \longrightarrow |00\rangle|\phi\rangle$$

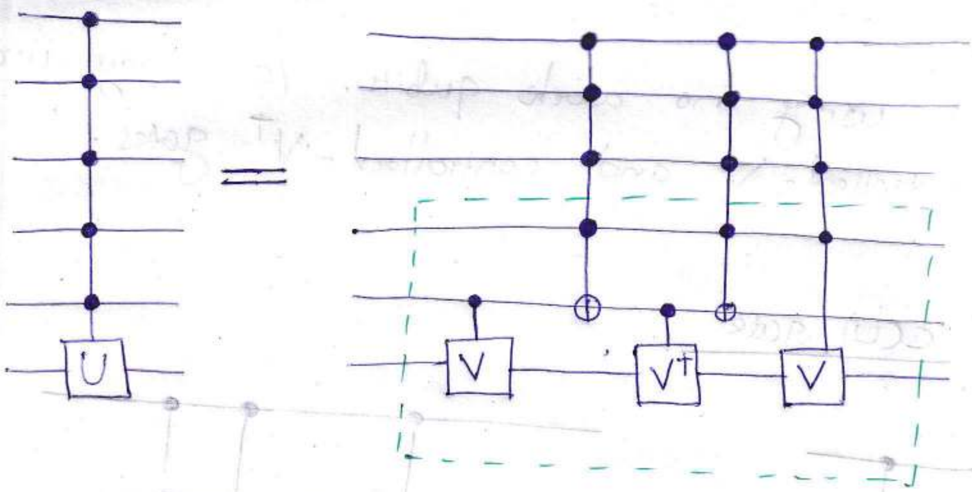
$$|01\rangle|\phi\rangle \longrightarrow |01\rangle V^\dagger V|\phi\rangle \Longrightarrow |01\rangle|\phi\rangle$$

$$|10\rangle|\phi\rangle \longrightarrow |10\rangle V^\dagger V|\phi\rangle \longrightarrow |10\rangle|\phi\rangle$$

$$|11\rangle|\phi\rangle \longrightarrow |11\rangle V^2|\phi\rangle \longrightarrow |11\rangle U|\phi\rangle$$

$C^5(U)$ operation

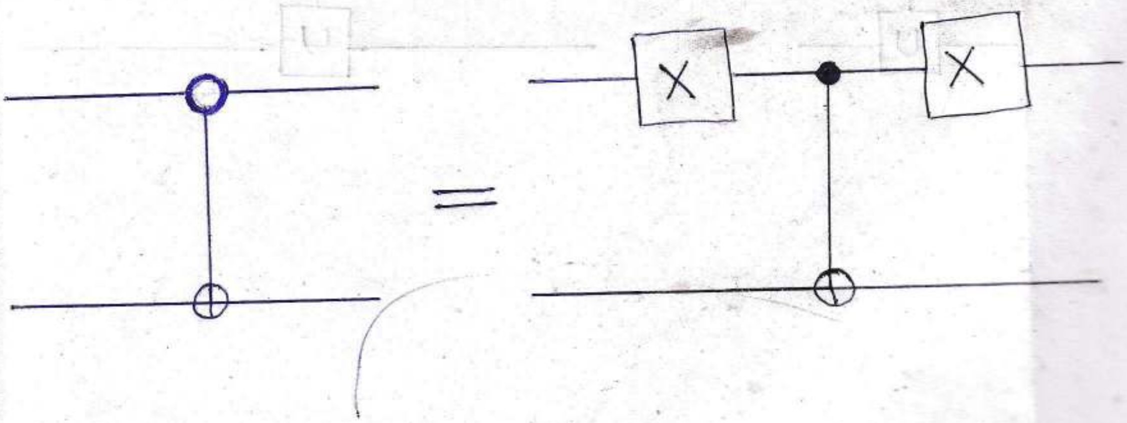
$U = V^2$



In the controlled gates we have been considering conditional dynamics on the target qubit occurs if the control bits are set to one.

There is nothing special about one, and it is often useful to consider dynamics which occur conditional on the control bit being set to zero.

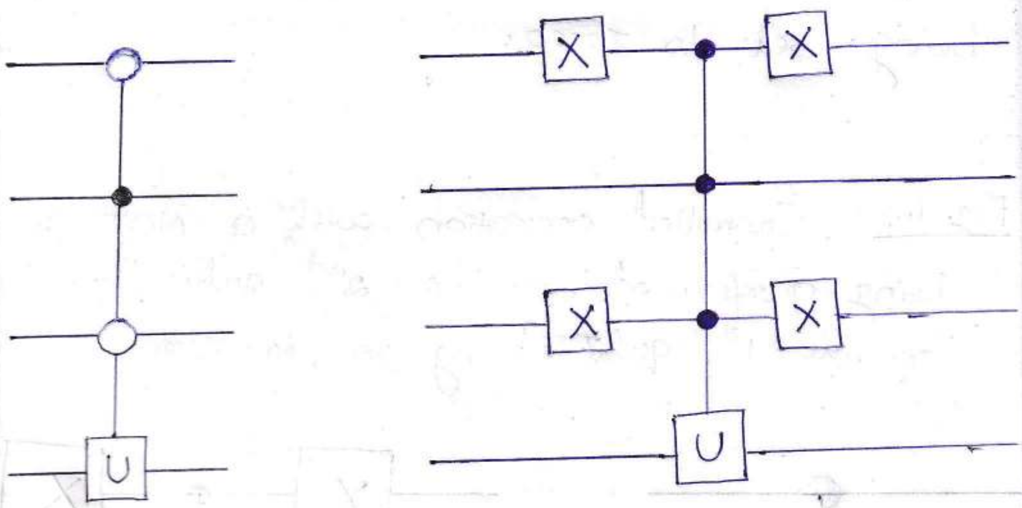
* Fig. 4.11 : Controlled operation with a NOT gate being performed on the 2nd qubit, conditional on the 1st qubit being set to zero.



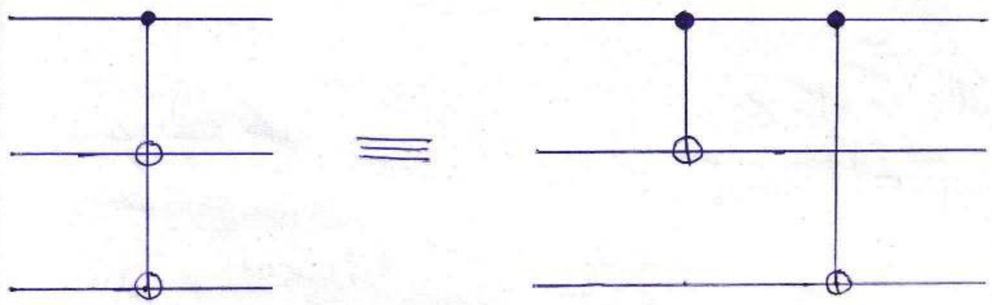
- The open circle notation indicates conditioning on the qubit being set to zero, while a closed circle indicates conditioning on the qubit being set to one.

* Fig 4.12 : Controlled-U operation and its equivalent in terms of circuit elements we already know how to implement.

The 4^{th} qubit has U applied if the 1^{st} and 3^{rd} qubits are set to zero, and the 2^{nd} qubit is set to one.



* Fig. 4.13 : Controlled-NOT gate with multiple targets.



→ When the control qubit is 1, then all the qubits marked with a ⊕ are flipped, and otherwise nothing happens.

Ex: 4.31

Let subscripts denote which qubit an operator acts on, and let C be a CNOT with qubit 1 the control qubit and qubit 2 the target qubit. Prove

① $CX_1C = X_1X_2$ $\quad X = |0\rangle\langle 1| + |1\rangle\langle 0| = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

Ans: $C = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$

$$CX_1C = \left(|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X\right) X_1 \left(|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X\right)$$

$$= \left(|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X\right)\left(|1\rangle\langle 0| \otimes I + |0\rangle\langle 1| \otimes X\right)$$

$$= \left(|0\rangle\langle 1| + |1\rangle\langle 0|\right) \otimes X = X \otimes X = (X \otimes I)(I \otimes X) = X_1X_2$$

② $CY_1C = Y_1X_2$ $\quad Y = -i|0\rangle\langle 1| + i|1\rangle\langle 0| = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$

Ans: $CY_1C = \left(|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X\right) Y_1 \left(|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X\right)$

$$= \left(|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X\right) i \left(|1\rangle\langle 0| \otimes I - |0\rangle\langle 1| \otimes X\right)$$

$$= i\left(-|0\rangle\langle 1| + |1\rangle\langle 0|\right) \otimes X = Y \otimes X = (Y \otimes I)(I \otimes X)$$

$$= Y_1X_2$$

③ $CZ_1C = Z_1$

$$\underline{\underline{Z = |0\rangle\langle 0| - |1\rangle\langle 1|}} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Ans:

$$CZ_1C = \left(|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X\right) Z_1 \left(|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X\right)$$

$$= \left(|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X\right)\left(|0\rangle\langle 0| \otimes I - |1\rangle\langle 1| \otimes X\right)$$

$$= \left(|0\rangle\langle 0| - |1\rangle\langle 1|\right) \otimes I = Z \otimes I = Z_1$$

④ $CX_2C = X_2$

Ans: $X = |0\rangle\langle 1| + |1\rangle\langle 0| = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

$$Y = -i|0\rangle\langle 1| + i|1\rangle\langle 0| = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

$$Z = |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$CX_2C = \left(|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X\right)(X_2)\left(|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X\right)$$

$$= \left(|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X\right)\left(|0\rangle\langle 0| \otimes X + |1\rangle\langle 1| \otimes I\right) \quad (X^2 = I$$

$$= \left(|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X\right) = \left(|0\rangle\langle 0| + |1\rangle\langle 1|\right) \otimes X$$

$$= I \otimes X = X_2$$

⑤ $CY_2C = Z_1Y_2$

Ans: $CY_2C = (|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X)\, Y_2\, (|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X)$

$= (|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X)(|0\rangle\langle 0| \otimes Y + |1\rangle\langle 1| \otimes YX)$.

$XY = -YX$

$= |0\rangle\langle 0| \otimes Y + |1\rangle\langle 1| \otimes XYX$

$XY = iZ$

$XYX = iZX$
$= i \cdot iY$
$= -Y$

$= |0\rangle\langle 0| \otimes Y - |1\rangle\langle 1| \otimes Y$

$= (|0\rangle\langle 0| - |1\rangle\langle 1|) \otimes Y$

$= Z \otimes Y = (Z \otimes I)(I \otimes Y)$

$= Z_1Y_2$

⑥ $CZ_2C = Z_1Z_2$

Ans: $CZ_2C = (|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X)\, Z_2\, (|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X)$

$= (|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X)(|0\rangle\langle 0| \otimes Z + |1\rangle\langle 1| \otimes ZX)$

$= |0\rangle\langle 0| \otimes Z + |1\rangle\langle 1| \otimes XZX$

$ZX = iY$
$XZX = iXY$
$= i \cdot iZ$
$= -Z$

$= |0\rangle\langle 0| \otimes Z - |1\rangle\langle 1| \otimes Z$

$= (|0\rangle\langle 0| - |1\rangle\langle 1|) \otimes Z$

$= Z \otimes Z = (Z \otimes I)(I \otimes Z)$

$= Z_1Z_2$ //

⑦ $R_{z,1}(\theta)C = C R_{z,1}(\theta)$

Ans:

$$R_{z,1}(\theta)\,C = \left(e^{-i\frac{\theta}{2}Z} \otimes I\right)\left(|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X\right)$$

$$R_z = e^{-i\frac{\theta}{2}Z} = \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2} Z$$

where, $Z = |0\rangle\langle 0| - |1\rangle\langle 1| \longrightarrow Z|0\rangle\langle 0| = |0\rangle\langle 0|$

$Z|1\rangle\langle 1| = |1\rangle\langle 1|.$

$ZX = -XZ$

$|0\rangle\langle 0|Z = |0\rangle\langle 0|$

$|1\rangle\langle 1|Z = |1\rangle\langle 1|$

$$[Z, |0\rangle\langle 0|] = 0 \quad \& \quad [Z, |1\rangle\langle 1|] = 0$$

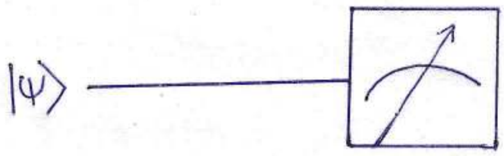
$$= \left(|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X\right)\left(e^{-i\theta/2 Z} \otimes I\right) = C R_{z,1}(\theta)$$

⑧ $R_{x,2}(\theta)C = C R_{x,2}(\theta)$

Measurement

(A final element used in quantum circuits, almost implicitly sometimes, is measurement.

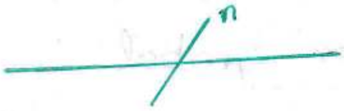
In our circuits, we shall denote a projective measurement in the computational basis using a 'meter' symbol. — projection onto $|0\rangle$ and $|1\rangle$



* Fig 4.14

Symbol for projective measurement on a single qubit.

In this circuit nothing further is done with the measurement result, but in more general quantum circuits it is possible to change later parts of the quantum circuit, conditional on measurement outcomes in earlier parts of the circuit.

qubit		wire carrying a single qubit (time goes left to right)
Classical bit		wire carrying a single classical bit
n qubits		wire carrying n qubits

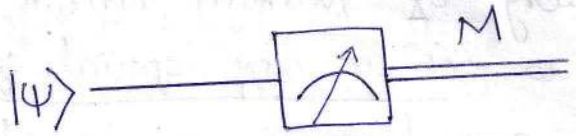


Fig. 1.10 → Quantum circuit symbol for measurement

- this operation converts a single qubit state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ into a probabilistic classical bit M (distinguished from a qubit by drawing it as a double-line wire), which is 0 with probability $|\alpha|^2$, or 1 with probability $|\beta|^2$.

* In the theory of quantum circuits it is conventional to not use any special symbols to denote more general measurements, because, they can always be represented by unitary transforms with ancilla qubits followed by projective measurements.

Quantum teleportation

- a technique for moving quantum states around even in the absence of a quantum communications channel linking the sender of the quantum state to the recipient.

Alice and Bob met long ago but now live far apart. While together they generated an EPR pair, each taking one qubit of the EPR pair when they separated. Many years later, Bob is in hiding, and Alice's mission, should she choose to accept it, is to deliver a qubit $|\psi\rangle$ to Bob. She does not know the state of the qubit, and moreover can only send classical information to Bob. Should Alice accept the mission ?

Alice doesn't know the state $|\psi\rangle$ of the qubit she has to send to Bob, and the laws of QM prevent her from determining the state when she only has a single copy of $|\psi\rangle$ in her possession.

Even if she did know the state $|\psi\rangle$, describing it precisely takes an infinite amount of classical information since $|\psi\rangle$ takes values in a continuous space. So even if she did know $|\psi\rangle$, it would take forever for Alice to describe the state to Bob.

Not looking good!

Quantum teleportation is a way of utilizing the entangled EPR pair in order to send $|\psi\rangle$ to Bob, with only a small overhead of classical communication.

Quantum teleportation in short : Alice interacts the qubit $|\psi\rangle$ with her half of the EPR pair, and then measures the 2 qubits in her possession, obtaining one of the 4 possible classical results 00, 01, 10, and 11. She sends this information to Bob. Depending on Alice's classical message, Bob performs one of 4 operations on his half of the EPR pair. By doing this, he can recover the original state $|\psi\rangle$.

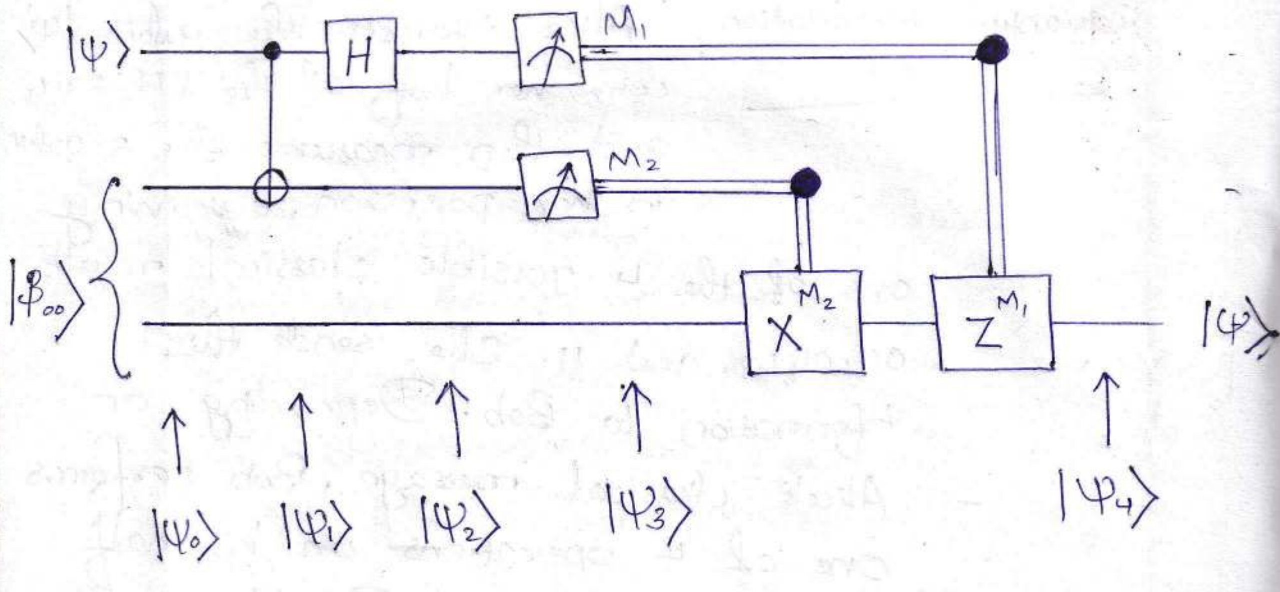


Fig 1.13 Quantum circuit for teleporting a qubit.

The two top lines represent Alice's system, while the bottom line is Bob's system. The meters represent measurement, and the double lines coming out of them carry classical bits. (single lines denote qubits)

The state to be teleported is $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where α, β are unknown amplitudes.

The state i/p into the circuit $|\psi_0\rangle$ is,

$$|\psi_0\rangle = |\psi\rangle \otimes |\beta_{00}\rangle = |\psi\rangle|\beta_{00}\rangle$$

$$= \frac{1}{\sqrt{2}}\left[\left(\alpha|0\rangle + \beta|1\rangle\right) \otimes \left(|00\rangle + |11\rangle\right)\right]$$

QC (2) / H2

where, $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$ is the 1st Bell state.

$$= \frac{1}{\sqrt{2}}\left(|0\rangle\otimes|0\rangle + |1\rangle\otimes|1\rangle\right)$$

$$= \frac{1}{\sqrt{2}}\left[\alpha|0\rangle\left(|00\rangle + |11\rangle\right) + \beta|1\rangle\left(|00\rangle + |11\rangle\right)\right]$$

1st two qubits on the left belong to Alice, and the 3rd qubit to Bob.

Alice's 2^{nd} qubit and Bob's qubits start out in an EPR state.

Alice sends her qubits through a CNOT gate, obtaining,

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\Big[\alpha|0\rangle\big(|00\rangle+|11\rangle\big)+\beta|1\rangle\big(|10\rangle+|01\rangle\big)\Big]$$

She then sends the 1^{st} qubit through a Hadamard gate, obtaining

$$|\psi_2\rangle = \frac{1}{2}\Big[\alpha\big(|0\rangle+|1\rangle\big)\big(|00\rangle+|11\rangle\big)+\beta\big(|0\rangle-|1\rangle\big)\big(|10\rangle+|01\rangle\big)\Big]$$

Regrouping the terms,

$$|\psi_2\rangle = \frac{1}{2}\Big[|00\rangle(\alpha|0\rangle+\beta|1\rangle) + |01\rangle(\alpha|1\rangle+\beta|0\rangle)$$
$$+ |10\rangle(\alpha|0\rangle-\beta|1\rangle) + |11\rangle(\alpha|1\rangle-\beta|0\rangle)\Big]$$

Since,

$$|x\rangle|y,z\rangle = |x\rangle\otimes(|y\rangle\otimes|z\rangle) = (|x\rangle\otimes|y\rangle)\otimes|z\rangle = |x,y\rangle\otimes|z\rangle$$
$$= |x,y\rangle|z\rangle$$

The expression for the state $|\psi_2\rangle$ breaks down into 4 terms. The 1st term has Alice's qubits in the state $|00\rangle$, and Bob's qubit in the state $\alpha|0\rangle+\beta|1\rangle$. Similarly, we can read off Bob's post measurement state, given the result of Alice's measurement :

$$00 \longrightarrow |\psi_3(00)\rangle \equiv \alpha|0\rangle+\beta|1\rangle$$
$$01 \longrightarrow |\psi_3(01)\rangle \equiv \alpha|1\rangle+\beta|0\rangle$$
$$10 \longrightarrow |\psi_3(10)\rangle \equiv \alpha|0\rangle-\beta|1\rangle$$
$$11 \longrightarrow |\psi_3(11)\rangle \equiv \alpha|1\rangle-\beta|0\rangle$$

Depending on Alice's measurement outcome, Bob's qubit will end up in one of these 4 possible states. To know which state it is in, Bob must be told the result of Alice's measurement - it is this fact which prevents teleportation from being used to transmit information faster than light.

Once Bob has learned the measurement outcome, Bob can fix up his state, recovering $|\psi\rangle$, by applying the appropriate quantum gate.

Ex:-

In the case where the measurement yields 00, Bob doesn't need to do anything.

If the measurement is 01 then Bob can fix up his state by applying the X gate.

If the measurement is 10 then Bob can fix up his state by applying the Z gate

If the measurement is 11 then Bob can fix up his state by applying 1st an X and then a Z gate.

$$00 : |\psi_4\rangle = |\psi_3(00)\rangle \equiv \alpha|0\rangle + \beta|1\rangle = |\psi\rangle$$

$$01 : |\psi_4\rangle = X|\psi_3(01)\rangle \equiv X(\alpha|1\rangle + \beta|0\rangle) = \alpha|0\rangle + \beta|1\rangle = |\psi\rangle$$

$$10 : |\psi_4\rangle = Z|\psi_3(10)\rangle \equiv Z(\alpha|0\rangle - \beta|1\rangle) = \alpha|0\rangle + \beta|1\rangle = |\psi\rangle$$

$$11 : |\psi_4\rangle = ZX|\psi_3(11)\rangle \equiv ZX(\alpha|1\rangle - \beta|0\rangle) = Z(\alpha|0\rangle - \beta|1\rangle)$$
$$= \alpha|0\rangle + \beta|1\rangle = |\psi\rangle$$

$\Longrightarrow$ Bob needs to apply the transformation $Z^{M_1} X^{M_2}$ to his qubit, and he will recover the state $|\psi\rangle$.

1* Doesn't teleportation allow one to transmit quantum states faster than light ?

The theory of relativity implies that faster than light information transfer could be used to send information backwards in time.

Quantum teleportation does not enable faster than light communication, because to complete the teleportation Alice must transmit her measurement result to Bob over a classical channel. Without this classical communication, teleportation does not convey any information at all (proof follows).

The classical channel is limited by the speed of light, so it follows that quantum teleportation cannot be accomplished faster than the speed of light.

Immediately before Alice makes her measurement the quantum state of the 3 qubits is,

$$|\psi_2\rangle = \frac{1}{2}\Big[|00\rangle(\alpha|0\rangle+\beta|1\rangle) + |01\rangle(\alpha|1\rangle+\beta|0\rangle) + |10\rangle(\alpha|0\rangle-\beta|1\rangle) + |11\rangle(\alpha|1\rangle-\beta|0\rangle)\Big]$$

Measuring in Alice's computational basis, the state of the system after the measurement is,

$|\varphi_1\rangle = |00\rangle[\alpha|0\rangle+\beta|1\rangle]$ with probability $\frac{1}{4}$

$|\varphi_2\rangle = |01\rangle[\alpha|1\rangle+\beta|0\rangle]$ "

$|\varphi_3\rangle = |10\rangle[\alpha|0\rangle-\beta|1\rangle]$ with probability $\frac{1}{4}$

$|\varphi_4\rangle = |11\rangle[\alpha|1\rangle-\beta|0\rangle]$ "

$\Longrightarrow$ The quantum system after the measurement is in one of the 4 states from above, with probabilities $1/4$. $\Longrightarrow$ Mixed state

$$|\varphi_1\rangle = |00\rangle\left[\alpha|0\rangle + \beta|1\rangle\right] = |00\rangle \otimes \left[\alpha|0\rangle + \beta|1\rangle\right]$$

$$(A\otimes B)^\dagger = A^\dagger \otimes B^\dagger$$

$$\langle\varphi_1| = \left(|00\rangle\left[\alpha|0\rangle + \beta|1\rangle\right]\right)^\dagger = \left(|00\rangle \otimes \left[\alpha|0\rangle + \beta|1\rangle\right]\right)^\dagger$$

$$= \langle 00| \otimes \left[\alpha^*\langle 0| + \beta^*\langle 1|\right] = \langle 00|\left[\alpha^*\langle 0| + \beta^*\langle 1|\right]$$

$\therefore$

$$|\varphi_1\rangle\langle\varphi_1| = \left(|00\rangle\left[\alpha|0\rangle + \beta|1\rangle\right]\right)\left(|00\rangle\left[\alpha|0\rangle + \beta|1\rangle\right]\right)^\dagger =$$

$$= \left(|00\rangle\left[\alpha|0\rangle + \beta|1\rangle\right]\right)\left(\langle 00|\left[\alpha^*\langle 0| + \beta^*\langle 1|\right]\right)$$

$$= \left(|00\rangle \otimes \left[\alpha|0\rangle + \beta|1\rangle\right]\right)\left(\langle 00| \otimes \left[\alpha^*\langle 0| + \beta^*\langle 1|\right]\right)$$

$$(A\otimes B)(C\otimes D) = (AC)\otimes(BD)$$

$$= |00\rangle\langle 00| \otimes \left(\alpha|0\rangle + \beta|1\rangle\right)\left(\alpha^*\langle 0| + \beta^*\langle 1|\right)$$

$$= |00\rangle\langle 00|\left(\alpha|0\rangle + \beta|1\rangle\right)\left(\alpha^*\langle 0| + \beta^*\langle 1|\right)$$

The density operator of the system (after the measurement in the Alice's computational basis) is,

$$\rho = \sum_{i=1}^{4} p_i |\varphi_i\rangle\langle\varphi_i| = \frac{1}{4}\Big[|\varphi_1\rangle\langle\varphi_1| + |\varphi_2\rangle\langle\varphi_2| + |\varphi_3\rangle\langle\varphi_3| + |\varphi_4\rangle\langle\varphi_4|\Big]$$

$$= \frac{1}{4}\Big[|00\rangle\langle 00|(\alpha|0\rangle+\beta|1\rangle)(\alpha^*\langle 0|+\beta^*\langle 1|) + |01\rangle\langle 01|(\alpha|1\rangle+\beta|0\rangle)(\alpha^*\langle 1|+\beta^*\langle 0|) + |10\rangle\langle 10|(\alpha|0\rangle-\beta|1\rangle)(\alpha^*\langle 0|-\beta^*\langle 1|) + |11\rangle\langle 11|(\alpha|1\rangle-\beta|0\rangle)(\alpha^*\langle 1|-\beta^*\langle 0|)\Big]$$

Q(3)

$$Tr_B\left((|\psi_1\rangle \otimes |\psi_2\rangle)(\langle\psi_1| \otimes \langle\psi_2|)\right) = Tr_B\left(|\psi_1\rangle\langle\psi_1| \otimes |\psi_2\rangle\langle\psi_2|\right)$$

Q(3)

$$= \sum_{i=1}^{d} (I \otimes \langle i|)\, |\psi_1\rangle\langle\psi_1| \otimes |\psi_2\rangle\langle\psi_2| \,(I \otimes |i\rangle)$$

$$= \sum_{i=1}^{d} |\psi_1\rangle\langle\psi_1| \cdot \langle i|\psi_2\rangle\langle\psi_2|i\rangle$$

$$= |\psi_1\rangle\langle\psi_1| \cdot \sum_{i=1}^{d} \langle i|\psi_2\rangle\langle\psi_2|i\rangle$$

$$= |\psi_1\rangle\langle\psi_1| \cdot Tr\left(|\psi_2\rangle\langle\psi_2|\right)$$

$$= |\psi_1\rangle\langle\psi_1|$$

$$Tr_B(\rho) = Tr_B(\rho_1 \otimes \rho_2) = \rho_1 \cdot Tr(\rho_2)$$

$$Tr_A(\rho) = Tr_A(\rho_1 \otimes \rho_2) = Tr(\rho_1) \cdot \rho_2$$

Tracing out Alice's system, the reduced density operator of Bob's system is:

$$\rho^B = \frac{1}{4}\Big[(\alpha|0\rangle+\beta|1\rangle)(\alpha^*\langle 0|+\beta^*\langle 1|)+(\alpha|1\rangle+\beta|0\rangle)(\alpha^*\langle 1|+\beta^*\langle 0|)$$
$$+(\alpha|0\rangle-\beta|1\rangle)(\alpha^*\langle 0|-\beta^*\langle 1|)+(\alpha|1\rangle-\beta|0\rangle)(\alpha^*\langle 1|-\beta^*\langle 0|)\Big]$$

$$= \frac{2(|\alpha|^2+|\beta|^2)|0\rangle\langle 0|+2(|\alpha|^2+|\beta|^2)|1\rangle\langle 1|}{4}$$

$$= \frac{|0\rangle\langle 0|+|1\rangle\langle 1|}{2} = I/2$$

⇒ The state of Bob's system after Alice has performed the measurement but before Bob has learned the measurement result is $I/2$. This state is the maximally mixed state which represents the case where we know nothing about ~~our~~ system, which has no dependence upon the state $|\psi\rangle$ being teleported.

Thus any measurements performed by Bob will contain no information about $|\psi\rangle$, therefore preventing Alice from using teleportation to transmit information to Bob faster than light.

(2*) It appears to create a copy of the quantum state being teleported, in apparent violation of the no-cloning theorem.

SC(3) H2 This violation is only illusory since after the teleportation process only the target qubit is left in the state $|\psi\rangle$, and the original data qubit ends up in one of the computational basis states $|0\rangle$ or $|1\rangle$, depending upon the measurement result on the 1st qubit.

$\Rightarrow$ Quantum teleportation emphasizes the interchangeability of different resources in QM, showing that one shared EPR pair together with two classical bits of communication is a resource at least the equal of one qubit of communication.

Measurement = Continue . . . . . .

There two important principles about quantum circuits bearing it mind.

The 1^{st} principle is that classically conditioned operations can be replaced by quantum conditioned operations :

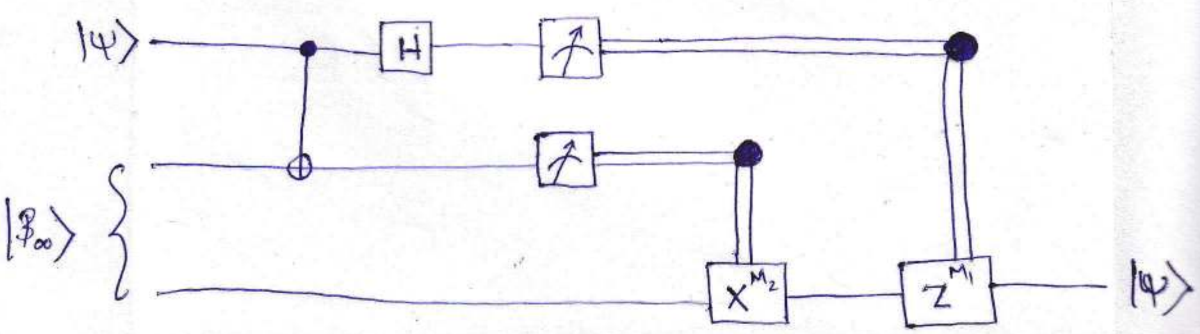
A Principle of deferred measurement

Measurements can always be moved from an intermediate stage of a quantum circuit to the end of the circuit;

If the measurement results are used at any stage of the circuit then the classically controlled operations can be replaced by conditional quantum operations.

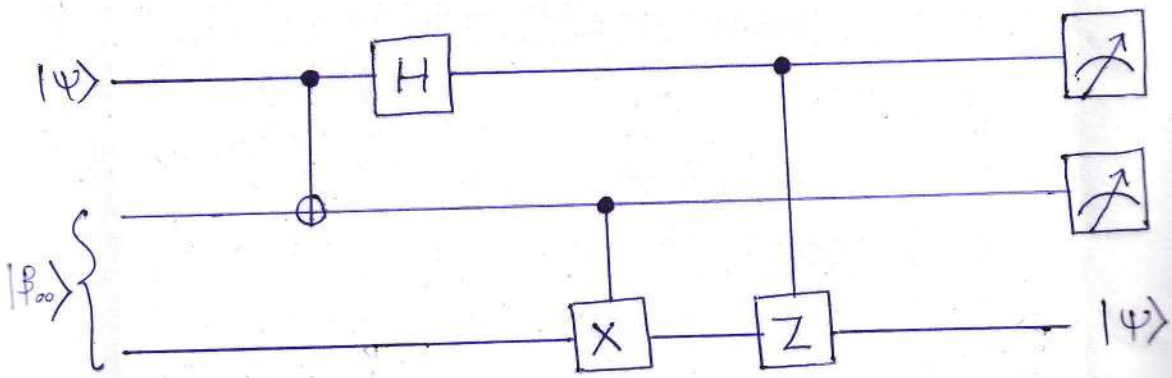
Often, quantum measurements are performed as an intermediate step in a quantum circuit, and the measurement results are used to conditionally control subsequent quantum gates.

Ex:- In the teleportation circuit



However, such measurements can always be moved to the end of the circuit. This may be done by replacing all the classical conditional operations by corresponding quantum conditional operations.

Fig 4.15 Quantum teleportation circuit in which measurements are done at the end, instead of in the middle of the circuit.



Of course, some of the interpretation of this circuit as performing 'teleportation' is lost, because no classical information is transmitted from Alice to Bob, but it is clear that the overall action of the two quantum circuits is the same, which is the key point.

B Principle of implicit measurement

Without loss of generality, any undetermined quantum wires (qubits which are not measured) at the end of a quantum circuit may be assumed to be measured.

Imagine you have a quantum circuit containing just 2 qubits, and only the first qubit is measured at the end of the circuit. Then the measurement statistics observed at this time are completely determined by the reduced density matrix of the 1st qubit.

However,

If a measurement had also been performed on the 2nd qubit, then that measurement could not change the statistics of measurement on the 1st qubit. This can be proved by showing that the reduced density matrix of the 1st qubit is not affected by performing a measurement on the second.

Proof

Ex: 4.32 Suppose ρ is the density matrix describing a 2 qubit system. Suppose we perform a projective measurement in the computational basis of the 2nd qubit. Let $P_0 = |0\rangle\langle 0|$ and $P_1 = |1\rangle\langle 1|$ be the projectors onto the $|0\rangle$ and $|1\rangle$ states of the 2nd qubit, respectively. Let ρ' be the density matrix which would be assigned to the system after the measurement by an observer who did not learn the measurement result. Show that

$$\boxed{\rho' = P_0 \rho P_0 + P_1 \rho P_1}$$

Also show that the reduced density matrix for the 1st qubit is not affected by the measurement, i.e., $tr_2(\rho) = tr_2(\rho')$

Ans:

G.C ② H1

ρ

wh

Ans: $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$

$$p(m|i) = \langle\psi_i| M_m^\dagger M_m |\psi_i\rangle = \mathrm{tr}\left(M_m^\dagger M_m |\psi_i\rangle\langle\psi_i|\right)$$

$$p(m) = \sum_i p(m|i)\, p_i = \sum_i p_i\, \mathrm{tr}\left(M_m^\dagger M_m |\psi_i\rangle\langle\psi_i|\right)$$

$$= \mathrm{tr}\left[M_m^\dagger M_m \sum_i p_i |\psi_i\rangle\langle\psi_i|\right] = \mathrm{tr}\left(M_m^\dagger M_m \rho\right)$$

$$= \mathrm{tr}\left(M_m \rho M_m^\dagger\right)$$

5.c (2)
H1

$$\rho_m = \sum_i p(i|m)\, |\psi_i^m\rangle\langle\psi_i^m|$$

$$= \sum_i p(i|m) \frac{M_m|\psi_i\rangle\langle\psi_i|M_m^\dagger}{\langle\psi_i|M_m^\dagger M_m|\psi_i\rangle} = \sum_i p(i|m) \frac{M_m|\psi_i\rangle\langle\psi_i|M_m^\dagger}{\mathrm{tr}\left(M_m^\dagger M_m |\psi_i\rangle\langle\psi_i|\right)}$$

where, $p(i|m) = \dfrac{p(m,i)\, p_i}{p(m)} = \dfrac{p(m|i)\, p_i}{p(m)}$

$$\rho_m = \sum_i p(i|m) \frac{M_m|\psi_i\rangle\langle\psi_i|M_m^\dagger}{p(m|i)}$$

$$= \sum_i \frac{p_i}{p(m)} M_m|\psi_i\rangle\langle\psi_i|M_m^\dagger$$

$$= \frac{M_m\left(\sum_i p_i|\psi_i\rangle\langle\psi_i|\right)M_m^\dagger}{\mathrm{tr}\left(M_m^\dagger M_m \rho\right)}$$

$$= \frac{M_m \rho M_m^\dagger}{\mathrm{tr}\left(M_m^\dagger M_m \rho\right)}$$

$$\boxed{\rho' = \sum_m p(m)\, \rho_m}$$

$$= \sum_m \mathrm{tr}\left(P_m \rho P_m\right) \times \frac{P_m \rho P_m}{\mathrm{tr}\left(P_m \rho P_m\right)}$$

$$= \sum_m P_m \rho P_m$$

$$= P_0 \rho P_0 + P_1 \rho P_1$$

$$\left.\begin{array}{l} P_0|0\rangle = |0\rangle \;\; \& \;\; P_0|1\rangle = 0 \\ P_1|1\rangle = |1\rangle \;\; \& \;\; P_1|1\rangle = 0 \end{array}\right\} \text{acts on the } 2^{nd} \text{ qubit}$$

$P_0 = I \otimes |0\rangle\langle 0|$ and $P_1 = I \otimes |1\rangle\langle 1|$

$$tr_2(\rho') = tr_2(P_0\rho P_0) + tr_2(P_1\rho P_1) \qquad \left[tr(AB) = tr(BA) \right.$$

$$= tr_2\Big[a_{00,00}|00\rangle\langle 00| + a_{00,10}|00\rangle\langle 10| + a_{10,00}|10\rangle\langle 00| + a_{10,10}|10\rangle\langle 10|\Big]$$

$$+ tr_2\Big[a_{01,01}|01\rangle\langle 01| + a_{01,11}|01\rangle\langle 11| + a_{11,01}|11\rangle\langle 01| + a_{11,11}|11\rangle\langle 11|\Big]$$

For a product state, $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$

$$\rho = \big(|\psi_1\rangle \otimes |\psi_2\rangle\big)\big(\langle\psi_1| \otimes \langle\psi_2|\big)$$

$$= |\psi_1\rangle\langle\psi_1| \otimes |\psi_2\rangle\langle\psi_2|$$

$$tr_B(\rho) = |\psi_1\rangle\langle\psi_1| \cdot tr\big(|\psi_2\rangle\langle\psi_2|\big).$$

$$= |\psi_1\rangle\langle\psi_1|$$

$$tr_2(\rho') = (a_{00,00} + a_{01,01})|0\rangle\langle 0| + (a_{00,10} + a_{01,11})|0\rangle\langle 1|$$

$$+ (a_{10,00} + a_{11,01})|1\rangle\langle 0| + (a_{10,10} + a_{11,11})|1\rangle\langle 1|$$

$$= tr_2(\rho)$$

$P_0 = I \otimes |0\rangle\langle 0|$ and $P_1 = I \otimes |1\rangle\langle 1|$

Note

ρ can be expanded in the 16 dimensional basis $|i,j\rangle\langle k,l|$ with $i,j,k,l = 0,1$

$P_0 \rho P_0 = 0$ if $j=1$ (or) $l=1$

$P_1 \rho P_1 = 0$ if $j=0$ (or) $l=0$.

$$P_0 \rho P_0 = a_{00,00}|00\rangle\langle 00| + a_{00,10}|00\rangle\langle 10| + a_{10,00}|10\rangle\langle 00| + a_{10,10}|10\rangle\langle 10|$$

$$P_1 \rho P_1 = a_{01,01}|01\rangle\langle 01| + a_{01,11}|01\rangle\langle 11| + a_{11,01}|11\rangle\langle 01| + a_{11,11}|11\rangle\langle 11|$$

* In its role as an interface b/w the quantum and classical worlds, measurement is generally considered to be an irreversible operation, destroying quantum information and replacing it with classical information.

Note: In certain carefully designed cases, however, this need not be true, as is vividly illustrated by teleportation and quantum error-correction.

What teleportation and quantum error-correction have in common is that in neither instance does the measurement result reveal any information about the identity of the quantum state being measured.

In order for a measurement to be reversible, it must reveal no information about the quantum state being measured.

Ex: 4.33 Measurement in the Bell Basis.

* For any orthonormal bases $B_1 = \{|\psi_i\rangle\}_{i=1}^{d} \in \mathbb{C}^d$ and $B_2 = \{|\phi_i\rangle\}_{i=1}^{d} \in \mathbb{C}^d$, there exists a unitary U mapping B_1 to B_2, given by

$$U = \sum_{i=1}^{d} |\phi_i\rangle\langle\psi_i| \quad \text{such that} \quad U|\psi_i\rangle = |\phi_i\rangle.$$

* Simulating a measurement in an arbitrary basis $B = \{|\psi_1\rangle, |\psi_2\rangle\}$ on $\mathbb{C}^2$ with standard basis measurements.

There exists a unitary mapping $U = \sum_{i=1}^{2} |i\rangle\langle\psi_i|$ from B to the standard basis,

i.e., $U|\psi_1\rangle = |0\rangle$ and $U|\psi_2\rangle = |1\rangle$.

$$Pr(\text{outcome } |\psi_i\rangle) = tr\left(\Pi_i |\psi\rangle\langle\psi|\right) = \langle\psi|\Pi_i|\psi\rangle$$

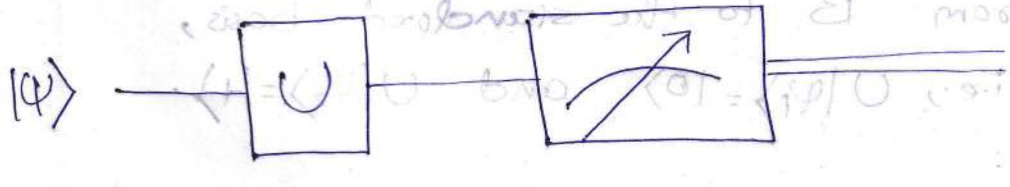
where $\Pi_i = |\psi_i\rangle\langle\psi_i|$ & $U|\psi_i\rangle = |i\rangle$ & $U^{\dagger}|i\rangle = |\psi_i\rangle$

$$= tr\left(|\psi_i\rangle\langle\psi_i| \psi\rangle\langle\psi|\right)$$

$$= tr\left(\left(U^{\dagger}|i\rangle\langle i|U\right)|\psi\rangle\langle\psi|\right)$$

$$= tr\left(|i\rangle\langle i| \left(U|\psi\rangle\langle\psi|U^{\dagger}\right)\right)$$

$\Longrightarrow$ Inorder to make measurement with operator $\Pi_i = |\psi_i\rangle\langle\psi_i|$ for the state $|\psi\rangle$, one might as well measure state $U|\psi\rangle$ against operator $|i\rangle\langle i|$.



where, $U = \sum_{i=1}^{2} |i\rangle\langle\psi_i|$

Bell states

$$|\Phi^+\rangle = |\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

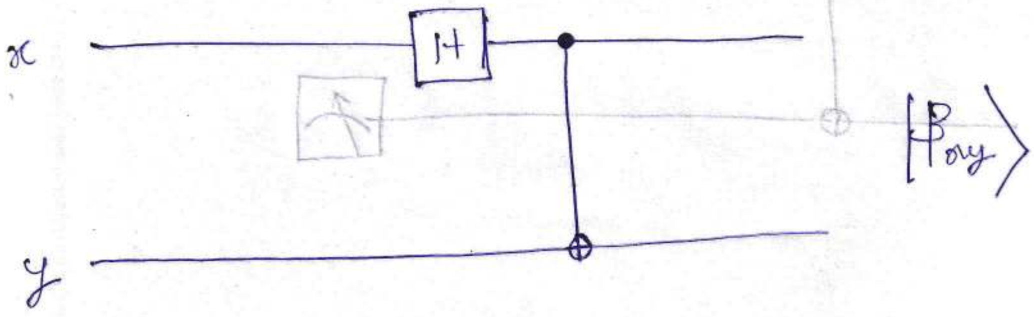
$$|\Psi^+\rangle = |\beta_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$

$$|\Phi^-\rangle = |\beta_{10}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$

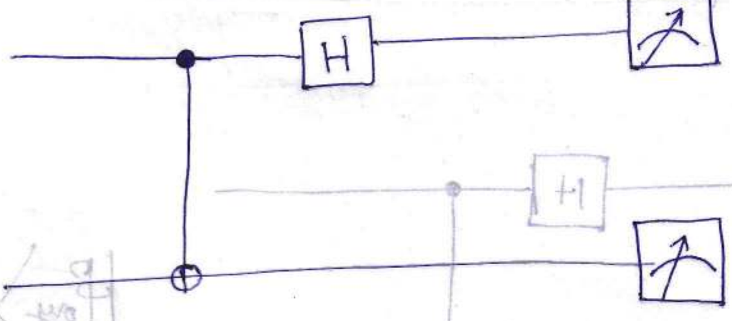
$$|\Psi^-\rangle = |\beta_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

$$|\beta_{xy}\rangle = \frac{|0,y\rangle + (-1)^x |1,\bar{y}\rangle}{\sqrt{2}}$$

⇒ * The quantum circuit to create Bell states is :



* Circuit to perform a measurement in the basis of the Bell states.



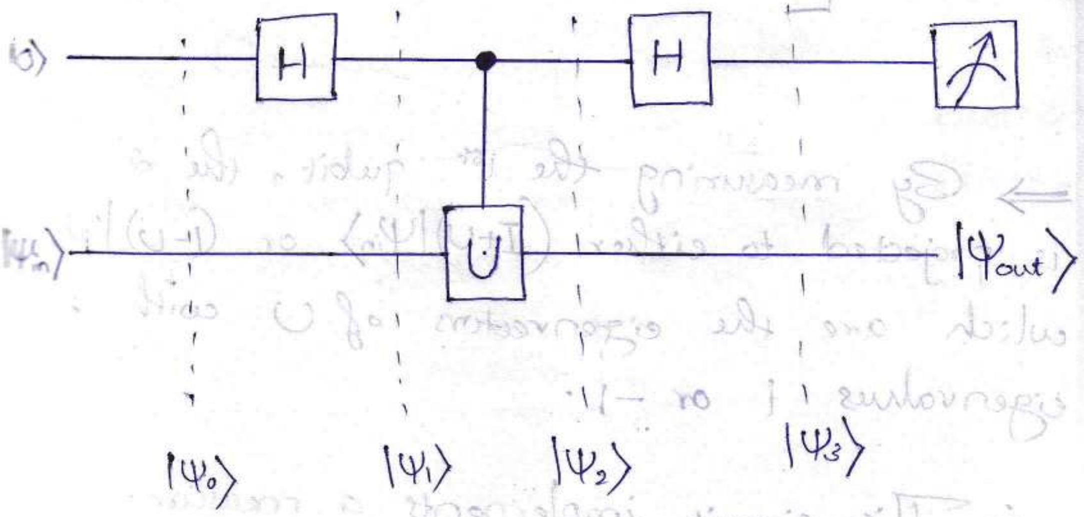
Ex.: 4.34 Measuring an operator

Back 1/10/21 G.C.

Suppose we have a single qubit operator U with eigenvalues ± 1, so that U is both Hermitian and unitary, so it can be regarded both as an observable and a quantum gate.

Suppose we wish to measure the observable U. i.e., we desire to obtain a measurement result indicating one of the two eigenvalues, and leaving a post-measurement state which is the corresp. eigenvector. How can this be implemented by a quantum circuit?

Ans:



$$|\psi_0\rangle = |0\rangle \otimes |\psi_{in}\rangle$$

$$|\psi_1\rangle = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes |\psi_{in}\rangle$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle \otimes |\psi_{in}\rangle + |1\rangle \otimes U|\psi_{in}\rangle\right)$$

$$|\psi_3\rangle = \frac{1}{\sqrt{2}}\left(\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes |\psi_{in}\rangle + \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \otimes U|\psi_{in}\rangle\right)$$

$$= \frac{1}{2}\left[|0\rangle \otimes (I+U)|\psi_{in}\rangle + |1\rangle \otimes (I-U)|\psi_{in}\rangle\right]$$

$\Rightarrow$ By measuring the 1st qubit, the 2nd qubit is projected to either $(I+U)|\psi_{in}\rangle$ or $(I-U)|\psi_{in}\rangle$ which are the eigenvectors of U with the eigenvalues 1 or -1.

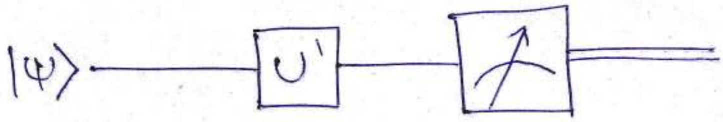
$\therefore$ This circuit implements a measurement of U.

$$U(I+U)|\psi\rangle = (U+U^2)|\psi\rangle = (I+U)|\psi\rangle$$

$$U(I-U)|\psi\rangle = (U-U^2)|\psi\rangle = -(I-U)|\psi\rangle$$

Stack 2

What about the circuit ?



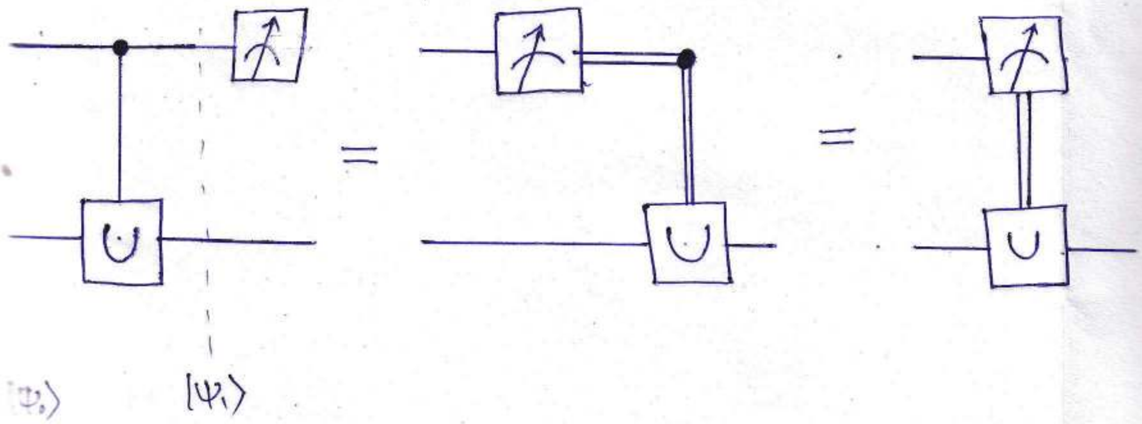
where, $U' = \sum |m\rangle\langle\psi_m|$

$|\psi_m\rangle$: eigenvectors of U.

→ Upon measuring we destroy the state in the sense that we get the outcome m but we don't obtain a state left in the eigenvector of U.

Ex: 4.35 . Measurement commutes with controls.

Principle of deferred measurement } Measurements commute with quantum gates when the qubit being measured is a control qubit.



$$|\psi_0\rangle = (a_1|0\rangle + b_1|1\rangle)\otimes(a_2|0\rangle + b_2|1\rangle)$$

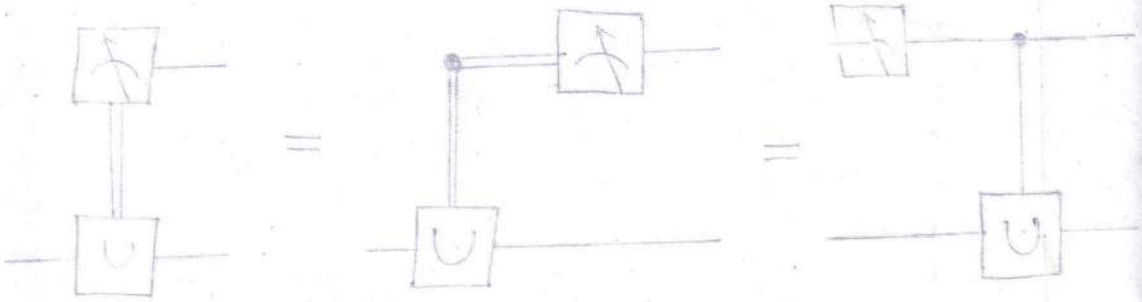
$$|\psi_1\rangle = a_1a_2|0\rangle\otimes|0\rangle + a_1b_2|0\rangle\otimes|1\rangle + a_2b_1|1\rangle\otimes U|0\rangle + a_2b_2|1\rangle\otimes U|1\rangle$$

$$= |0\rangle\otimes(a_1a_2|0\rangle + a_2b_2|1\rangle) + |1\rangle\otimes(a_2b_1U|0\rangle + a_2b_2U|1\rangle)$$

$\longrightarrow$ After the measurement, the 2^{nd} qubit becomes either $\alpha_1|0\rangle + \beta_1|1\rangle$ for classical 0 or $\alpha_2|0\rangle + \beta_2|1\rangle$ for classical 1.

Middle circuit :

At the end,
the 2^{nd} qubit is either $a_2|0\rangle + b_2|1\rangle$ or $a_2 U|0\rangle + b_2 U|1\rangle$.



Universal Quantum Gates.

A small set of gates (e.g. AND, OR, NOT) can be used to compute an arbitrary classical function, we say that such a set of gates is universal for classical computation.

Since the Toffoli gate is universal for classical computation, quantum circuits subsume classical circuits. A similar universality result is true for quantum computation, where a set of gates is said to be universal for quantum computation if any unitary operation may be approximated ~~to~~ arbitrary accuracy by a quantum circuit involving only those gates.

3 universality constructions for quantum computation } Any unitary operation can be approximated to arbitrary accuracy using Hadamard, phase, CNOT, and $\pi/8$ gates.

Q.C③

Hadamard $-\boxed{H}-$ $H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{X+Z}{\sqrt{2}}$

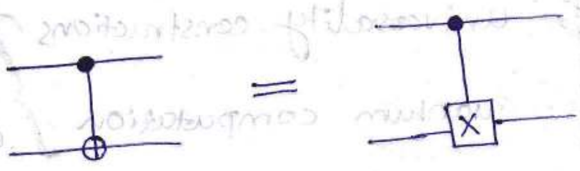
$$H|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$$

$$H|1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$

Phase gate $-\boxed{S}-$ $S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$

$\pi/8$ gate $-\boxed{T}-$ $T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$

CNOT gate



$$U_{CN} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

(*) Phase gate can be constructed from two $\pi/8$ gates; Still it is included in the list because of its natural role in the fault-tolerant constructions (Chapter 10).

Ex: 4.36 Construct a quantum circuit to add two two-bit numbers x and y modulo 4. That is, the circuit should perform the transformation $|x, y\rangle \longrightarrow |x, x+y \bmod 4\rangle$.

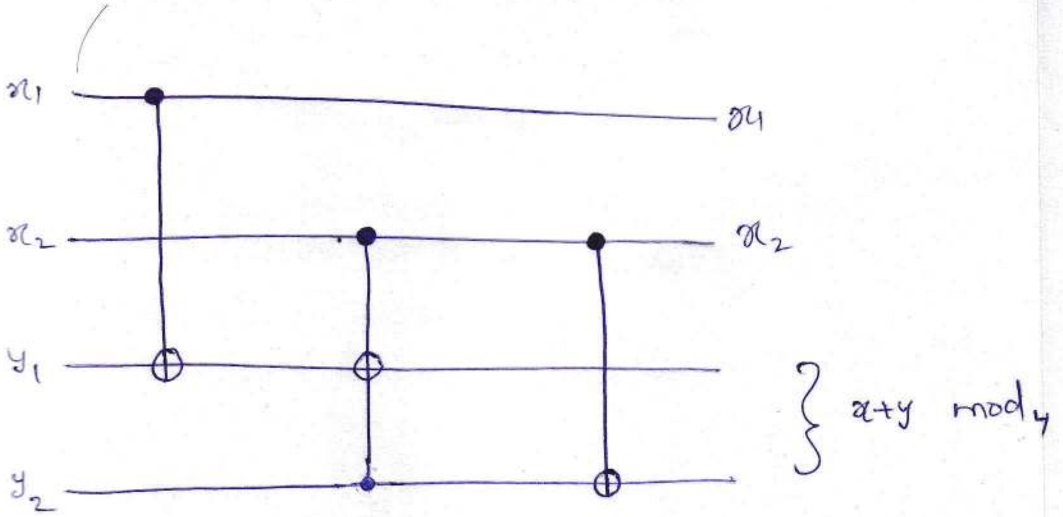
Ans:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

+	00	01	10	11
00	00	01	10	11
01	01	10	11	00
10	10	11	00	01
11	11	00	01	10

$x = x_1 x_2$ and $y = y_1 y_2$

x_1 flips



- y_2 is flipped when $x_2 = 1$

- y_1 is flipped : $x_2 y_2 = 1,1$ & $x_1 = 0$

  do not when $x_2 y_2 = 1,1$ & $x_1 = 1$

- y_1 is flipped : $x_2 y_2 = 00, 01, 10$ & $x_1 = 1$

  do not : $x_2 y_2 = 00, 01, 10$ & $x_1 = 0$.

Ⓐ Two-level unitary gates are universal.

Consider a unitary matrix U which acts on a d-dimensional Hilbert space. i.e., $U \in \mathcal{L}(\mathbb{C}^d)$ and $U^\dagger = U^{-1}$

- A unitary matrix $U \in \mathcal{L}(\mathbb{C}^d)$ may be decomposed into a product of two-level unitary matrices; i.e., unitary matrices which act non-trivially only on two-or-fewer vector components.

ie.,

A is a two-level matrix if it can be written as $A = \tilde{A} \oplus I$ for some 2×2 matrix $\tilde{A}$ (up to a rearrangement of the matrix components).

When U is 3×3,

$$U = \begin{bmatrix} a & d & g \\ b & e & h \\ c & f & j \end{bmatrix}$$

We will find two-level unitary matrices $U_1, \ldots, U_3$ such that

$$U_3 U_2 U_1 U = I$$

$$\Longrightarrow U = U_1^\dagger U_2^\dagger U_3^\dagger$$

U_1, U_2, U_3 are all two-level unitary matrices. & their inverses $U_1^\dagger, U_2^\dagger, U_3^\dagger$ are also two-level unitary matrices.

If $b=0$, then set $U_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

If $b \neq 0$ then set

$$U_1 = \begin{bmatrix} \frac{a^*}{\sqrt{|a|^2+|b|^2}} & \frac{b^*}{\sqrt{|a|^2+|b|^2}} & 0 \\ \frac{b}{\sqrt{|a|^2+|b|^2}} & \frac{-a}{\sqrt{|a|^2+|b|^2}} & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Note: U_1 is a two-level unitary matrix, since.

$$U_1 \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} * \\ * \\ z \end{bmatrix}$$

$$U_1 U = \begin{bmatrix} a' & d' & g' \\ 0 & e' & h' \\ c' & f' & j' \end{bmatrix}$$

Note: the middle entry in the left hand column is zero.

Derive U_1

ILA ⑥ Givens Rotations

& QM ㉓ SU(2) group

$$U_1 = \begin{bmatrix} \varphi_1 & -\varphi_2 & 0 \\ +\varphi_2^* & \varphi_1^* & 0 \\ 0 & 0 & 1 \end{bmatrix}$$ such that $(2,1)^{th}$ entry of $U_1 U$ is 0.

$$U_1 U = \begin{bmatrix} \varphi_1 & -\varphi_2 & 0 \\ +\varphi_2^* & \varphi_1^* & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} a & d & g \\ b & e & h \\ c & f & j \end{bmatrix}$$

$$= \begin{bmatrix} * & * & * \\ +\varphi_2^* a + \varphi_1^* b & * & * \\ * & * & * \end{bmatrix} = \begin{bmatrix} * & * & * \\ 0 & * & * \\ * & * & * \end{bmatrix}$$

$$+\varphi_2^* a + \varphi_1^* b = 0 \implies \frac{a}{b} = \frac{-\varphi_1^*}{\varphi_2^*}$$

$$|\varphi_1|^2 + |\varphi_2|^2 = |\varphi_2|^2 \frac{|a|^2}{|b|^2} + |\varphi_2|^2 = |\varphi_2|^2 \left[\frac{|a|^2+|b|^2}{|b|^2}\right] = 1$$

$$\Longrightarrow \quad |\varphi_2| = \frac{|b|}{\sqrt{|a|^2+|b|^2}} \quad \& \quad |\varphi_1| = \frac{|a|}{\sqrt{|a|^2+|b|^2}}$$

We can take,

$$\varphi_1 = \frac{a^*}{\sqrt{|a|^2+|b|^2}} \quad \& \quad \varphi_2 = \frac{-b^*}{\sqrt{|a|^2+|b|^2}}$$

$$U_1 = \begin{bmatrix} \frac{a^*}{\sqrt{|a|^2+|b|^2}} & \frac{+b^*}{\sqrt{|a|^2+|b|^2}} & 0 \\ \frac{+b}{\sqrt{|a|^2+|b|^2}} & \frac{-a}{\sqrt{|a|^2+|b|^2}} & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Apply a similar procedure to find a two-level matrix U_2 such that U_2U_1U has no entry in the bottom left corner.

If $c' = 0$, we set $U_2 = \begin{bmatrix} a'^* & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

$b' = 0, c' = 0 \Rightarrow |a'|^2 = 1$

If $c' \neq 0$, then we set

$$U = \begin{bmatrix} \frac{a'^*}{\sqrt{|a'|^2 + |c'|^2}} & 0 & \frac{c'^*}{\sqrt{|a'|^2 + |c'|^2}} \\ 0 & 1 & 0 \\ \frac{c'}{\sqrt{|a'|^2 + |c'|^2}} & 0 & \frac{-a'}{\sqrt{|a'|^2 + |c'|^2}} \end{bmatrix}$$

U_2U_1U is unitary

$\therefore$ 1st row & 1st column must have norm 1.

$$U_2U_1U = \begin{bmatrix} 1 & d'' & g'' \\ 0 & e'' & h'' \\ 0 & f'' & j'' \end{bmatrix}$$

U, U_1, U_2 are unitary $\Longrightarrow$ $U_2 U_1 U$ is unitary

$\therefore \quad d'' = g'' = 0.$ [since the 1st row of $U_2 U_1 U$ must have norm 1.

$$U_2 U_1 U = \begin{bmatrix} 1 & 0 & 0 \\ 0 & e'' & h'' \\ 0 & f'' & j'' \end{bmatrix} \quad \& \quad |e''|^2 + |h''|^2 = 1$$
$$|f''|^2 + |j''|^2 = 1$$

Set $U_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & e''^* & f''^* \\ 0 & h''^* & j''^* \end{bmatrix} \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & e'' & h'' \\ 0 & f'' & j'' \end{bmatrix}$

Such that, $U_3 U_2 U_1 U = I$

$$\Longrightarrow \quad U = U_1^{\dagger} U_2^{\dagger} U_3^{\dagger}$$

which is a decomposition of U into two-level unitaries.

More generally,

Procedure

Suppose the unitary matrix U acts on a d-dimensional space. We can find two-level unitary matrices $U_1, \cdots, U_{d-1}$ such that the matrix $U_{d-1}U_{d-2}\cdots U_1U$ has a one in the top left corner, and all zeros elsewhere in the 1st row and column (1st column).

We then repeat this procedure for the $(d-1)\times(d-1)$ unitary submatrix in the lower right hand corner of $U_{d-1}U_{d-2}\cdots U_1U$, and so on, with the end result that an arbitrary $d\times d$ unitary matrix may be written:

$$U = V_1 \cdots V_k$$

where the matrices V_i are two-level unitary matrices, and $k \le (d-1)+(d-2)+\cdots+1 = \frac{d(d-1)}{2}$.

$\Rightarrow$ An arbitrary unitary matrix on an n qubit system may be written as a product of at most $2^{n-1}(2^n-1)$ two-level unitary matrices.

$$d = 2^n \Rightarrow \frac{d(d-1)}{2} = \frac{2^n(2^n-1)}{2} = 2^{n-1}(2^n-1)$$

* There exists a $d \times d$ unitary matrix U which cannot be decomposed as a product of fewer than $(d-1)$ two-level unitary matrices.