Georgia Tech

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

Quantum Information & Quantum Computing

Homework # 2

Due September 18, 2007

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*) # 4.2, 4.4, 4.5, 4.7, 4.8, 4.9, 4.13, 4.17, 4.18, 4.21, 4.23, 4.24, 4.25, 4.35 .

Exercises :

– **4.2-** *Let $x \in \mathbb{R}$ and A be a matrix such that $A^2 = 1$ then show that $e^{\imath x A} = \cos x I + \imath \sin x A$.* □

By definition

$$\begin{aligned} e^{\imath x A} &= \sum_{n=0}^{\infty} \frac{(\imath x A)^n}{n!} \\ &= \sum_{n=0}^{\infty} \frac{(\imath x A)^{2n}}{(2n)!} + \sum_{n=0}^{\infty} \frac{(\imath x A)^{2n+1}}{(2n+1)!} \\ &= \sum_{n=0}^{\infty} \frac{(-1)^n x^{2n}}{(2n)!}\, I + \imath \sum_{n=0}^{\infty} \frac{(-1)^n x^{2n+1}}{(2n+1)!}\, A \\ &= \cos x\, I + \imath \sin x\, A \end{aligned}$$

– **4.4-** *Express the Hadamard gate as a product of R_x and R_y rotation and a phase.* □

By definition the matrix of the Hadamard gate in the computer basis is given by

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

Thanks to (**4.2**), $e^{\imath \pi X/4} = (I + \imath X)/\sqrt{2}$ and $e^{\imath \pi Z/4} = (I + \imath Z)/\sqrt{2}$ are the R_x, R_z rotations of angle $\pi/4$. Hence

$$\begin{aligned} \frac{(I+\imath X)}{\sqrt{2}} \frac{(I+\imath Z)}{\sqrt{2}} \frac{(I+\imath X)}{\sqrt{2}} &= \frac{1}{2\sqrt{2}} \left(I + \imath (X+Z) - XZ\right)(I + \imath X) \\ &= \frac{1}{2\sqrt{2}} \left(I + \imath(X+Z) - XZ + \imath X - I - ZX - \imath XZX\right) \\ &= \frac{\imath}{\sqrt{2}} (X+Z) = \imath\, H \end{aligned}$$

where $XZ + ZX = 0 \Rightarrow XZX = -Z$ have been used. Thus $H = e^{-\imath\pi/2} e^{\imath\pi X/4} e^{\imath\pi Z/4} e^{\imath\pi X/4}$.
□

Here $\hat{n} = (n_x, n_y, n_z) \in \mathbb{R}^3$ is a vector of length one. Thus

$$\begin{aligned}(\hat{n}\cdot\vec{\sigma})^2 &= (n_x X + n_y Y + n_z Z)^2 \\ &= (n_x^2 + n_y^2 + n_z^2)\, I + n_x n_y (XY + YX) + n_y n_z (YZ + ZY) + n_z n_x (ZX + XZ) \\ &= I\end{aligned}$$

since $XY + YX = 0 = YZ + ZY = ZX + XZ$.

– **4.7-** *Show that $XYX = -Y$ and use it to prove that $XR_y(\theta)X = R_y(-\theta)$.* □

By definition $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ and $Y = \begin{bmatrix} 0 & -\imath \\ \imath & 0 \end{bmatrix}$. Therefore a direct calculation gives

$$XY = \begin{bmatrix} \imath & 0 \\ 0 & -\imath \end{bmatrix}, \qquad YX = \begin{bmatrix} -\imath & 0 \\ 0 & \imath \end{bmatrix} = -XY\,.$$

Hence $XYX = -YX^2 = -Y$. Moreover, thanks to (**4.2**), $R_y(\theta) = \cos\theta\, I + \imath \sin\theta\, Y$ so that indeed

$$XR_y(\theta)X = \cos\theta\, X^2 + \imath\sin\theta\, XYX = \cos\theta\, I - \imath\sin\theta\, Y = R_y(-\theta)\,.$$

– **4.8-** *An arbitrary single qubit unitary operator can be written in the form*

$$U = e^{\imath\alpha} R_{\hat{n}}(\theta) \tag{1}$$

for some real numbers α, θ and a tridimensional unit vector $\hat{n}$.

1. *Prove this fact.*
2. *Find values for α, θ and $\hat{n}$ giving the Hadamard gate H.*
3. *Find values for α, θ and $\hat{n}$ giving the phase gate $S = \begin{bmatrix} 1 & 0 \\ 0 & \imath \end{bmatrix}$.*

□

If eq. (1) holds, since $H = (X + Z)/\sqrt{2}$, it follows that choosing $\alpha = -\pi/2, \theta = \pi/2$ and $\hat{n} = (1, 0, 1)/\sqrt{2}$ gives

$$-\imath\left\{\cos\pi/2 + \imath\sin\pi/2\left(\frac{X+Z}{\sqrt{2}}\right)\right\} = \frac{(X+Z)}{\sqrt{2}} = H\,.$$

In much the same way S is obtained in choosing $\alpha = \pi/4, \theta = -\pi/4$ and $\hat{n} = (0, 0, 1)$ giving

$$S = e^{\imath\pi/4}\, e^{-\imath\pi Z/4}\,.$$

Let now U be a 2×2 unitary matrix and it will be shown that (1) holds. First, $\det U$ is a pure phase. For indeed $|\det U|^2 = \det U \overline{\det U} = \det U \det U^\dagger = \det UU^\dagger = 1$. Therefore there is $\alpha \in \mathbb{R}$ such that $\det U = e^{2\imath\alpha}$. Hence $U = e^{\imath\alpha} W$ with W unitary and $\det W = 1$.

Since W is unitary, it is normal and thus can be diagonalized in an orthonormal basis with eigenvalues $\lambda_\pm$. Unitarity implies that both eigenvalues are pure phases. Since $\det W = \lambda_+\lambda_- = 1$ there is a real number θ such that $\lambda_\pm = e^{\pm \imath\theta}$. As a consequence $\mathrm{tr}\, W = 2\cos\theta$. As any 2×2 matrix, W can be decomposed in a unique way in the Pauli basis namely

$$W = w_0 I + w_x X + w_y Y + w_z Z\,, \qquad w_i \in \mathbb{C}\,.$$

Clearly $\mathrm{tr}\, W = 2w_0$ so that $w_0 = \cos\theta$. Moreover writing w_i as $u_i + \imath v_i$ with $u_i, v_i \in \mathbb{R}$ (for $i = x, y, z$), this gives, with $\vec{u} = (u_x, u_y, u_z)$ and $\vec{v} = (v_x, v_y, v_z)$,

$$W = \cos\theta\, I + \vec{u}\cdot\vec{\sigma} + \imath\vec{v}\cdot\vec{\sigma}\,, \qquad W^\dagger = \cos\theta\, I + \vec{u}\cdot\vec{\sigma} - \imath\vec{v}\cdot\vec{\sigma}\,.$$

By unitarity, it follows that

$$I = WW^\dagger = (\cos^2\theta + |\vec{u}|^2 + |\vec{v}|^2)\, I + (2\cos\theta\,\vec{u} + \vec{u}\wedge\vec{v})\cdot\vec{\sigma}\,,$$

giving

$$\cos^2\theta + |\vec{u}|^2 + |\vec{v}|^2 = 1\,, \qquad 2\cos\theta\,\vec{u} = -\vec{u}\wedge\vec{v}\,.$$

From the second equation, it follows that $2\cos\theta\,|\vec{u}|^2 = 0$ so that either $2\cos\theta = 0$ or $\vec{u} = 0$. If $\vec{u} \neq 0$, then $\vec{u}$ and $\vec{v}$ are colinear, and thanks to the *l.h.s*, $|\vec{u}|^2 + |\vec{v}|^2 = 1$ so that there is $\phi \in \mathbb{R}$ and a unit vector $\hat{n}$ such that $\vec{u} + \imath\vec{v} = e^{\imath\phi}\hat{n}$. Then, since $\det \hat{n}\vec{\sigma} = -1$ it implies that $\phi = \pi$ and eq. (1) holds with $\theta = \pi/2$.
If $\vec{u} = 0$, then $|\vec{v}|^2 = \sin^2\theta$ so that there is a unit vector $\hat{n}$ such that

$$W = \cos\theta\, I + \imath\sin\theta\,\hat{n}\cdot\vec{\sigma} = R_{\hat{n}}(\theta)\,.$$

and eq. (1) also holds.

– **4.9-** *Explain why a single qubit unitary operator can be written as*

$$U = \begin{bmatrix} e^{\imath(\alpha-\beta/2-\delta/2)}\cos\gamma/2 & -e^{\imath(\alpha-\beta/2+\delta/2)}\sin\gamma/2 \\ e^{\imath(\alpha+\beta/2-\delta/2)}\sin\gamma/2 & e^{\imath(\alpha+\beta/2+\delta/2)}\cos\gamma/2 \end{bmatrix} \qquad (2)$$

□

Any 2×2 unitary matrix can be written as

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

where the two columns makes an orthonormal basis, namely

$$|a|^2 + |c|^2 = 1\,, \qquad |b|^2 + |d|^2 = 1\,, \qquad a\bar{b} + c\bar{d} = 0\,. \qquad (3)$$

If $c = 0$ (resp. $b = 0$) this implies $b = 0$ (resp. $c = 0$) and both a, d are pure phases, so that it is always possible to find (non unique) real numbers α, β, δ such that $a = e^{\imath(\alpha-\beta/2-\delta/2)}$ and $d = e^{\imath(\alpha+\beta/2+\delta/2)}$ and eq. (2) holds. Similarly if $a = 0$ (resp. $d = 0$) then $d = 0$ (resp. $a = 0$) and it is always possible to find (non unique) real numbers α, β, δ such that $b = -e^{\imath(\alpha-\beta/2+\delta/2)}$ and $c = e^{\imath(\alpha+\beta/2-\delta/2)}$ so that eq. (2) holds again.

Therefore it is possible to assume that none of the cœfficients a, b, c, d vanish. In particular, there are real numbers $0 < \gamma, \gamma' < \pi$ such that $|a| = \cos\gamma/2$, $|c| = \sin\gamma/2$, $|d| = \cos\gamma'/2$

and $|b| = \sin\gamma'/2$. In addition, since $a\bar{b} = -c\bar{d}$, it follows that $0 = |a||b| - |c||d| = \sin(\gamma' - \gamma)/2$ and therefore $\gamma = \gamma'$ since both belong to $(0, \pi)$. Thus, there are real numbers $\theta_a, \theta_b, \theta_c, \theta_d$ such that

$$\begin{aligned} a &= \cos\gamma/2\, e^{\imath\theta_a} & b &= -\sin\gamma/2\, e^{\imath\theta_b} \\ c &= \sin\gamma/2\, e^{\imath\theta_c} & d &= \cos\gamma/2\, e^{\imath\theta_d} \end{aligned}$$

From eq. (3), it follows that $\theta_c - \theta_d = \theta_a - \theta_b$ or equivalently, there is a real number α such that

$$\theta_a + \theta_d = \theta_c + \theta_b = 2\alpha\,.$$

Therefore it is possible to find real numbers ϕ and ϕ' such that

$$\begin{aligned} \theta_a &= \alpha - \phi & \theta_b &= \alpha - \phi' \\ \theta_c &= \alpha + \phi' & \theta_d &= \alpha + \phi \end{aligned}$$

Setting $\phi + \phi' = \beta$ and $\phi - \phi' = \delta$ gives eq. (2).

– **4.13- (Circuit identities)***It is useful to be able to simplify circuits by inspection, using well-known identities. Prove the following three identities*

$$HXH = Z\,, \qquad HYH = -Y\,, \qquad HZH = X\,. \tag{4}$$

□

By definition, $XZ = -ZX$, $X^2 = I = Z^2$ and $ZX = \imath Y$. Moreover the Hadamard operator can be written as $H = (X + Z)/\sqrt{2}$. These definitions leads to

$$H^\dagger = H\,, \qquad H^2 = \frac{X^2 + XZ + ZX + Z^2}{2} = I\,.$$

In addition

$$HXH = \frac{X^3 + X^2Z + ZX^2 + ZXZ}{2} = \frac{X + 2Z - X}{2} = Z$$

Consequently, multiplying to the right and to the left by H gives $HZH = X$, since $H^2 = I$. At last, $Y = -\imath ZX = \imath XZ$ so that $HYH = \imath HXHHZH = \imath ZX = -Y$.

– **4.17- (Building** CNOT **from the controlled-Z gate)** *Construct a* CNOT *gate from one controlled-Z gate, that is, the gate whose action on the computational basis is specified by the unitary matrix*

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \tag{5}$$

and the two Hadamard gates, specifying the control and the target qubits. □

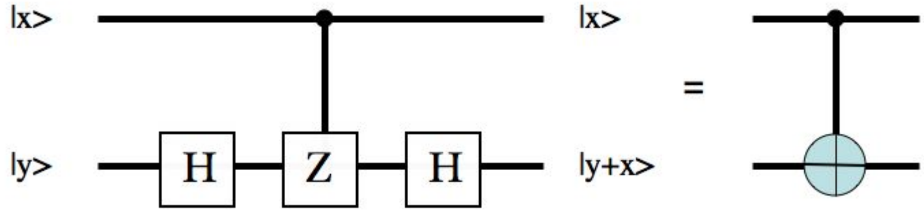

FIG. 1 – How to construct CNOT from the controlled-Z gate

The controlled-Z gate can be described algebraically as $C^1(Z)|x,y\rangle = |x\rangle \otimes Z^x|y\rangle$. It is easy to check that its matrix is given by eq. (5) in the computational basis. Since $X = HZH$ (see eq. (4)), $\text{CNOT}|x,y\rangle = |x\rangle \otimes X^x|y\rangle = |x\rangle \otimes (HZH)^x|y\rangle = |x\rangle \otimes HZ^xH|y\rangle = I \otimes H \cdot C^1(Z) \cdot I \otimes H|x,y\rangle$ giving the result described in Figure 1.

– **4.18-** *Show that* □

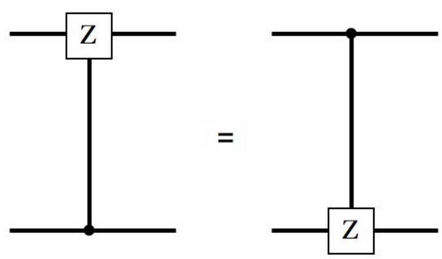

FIG. 2 –

By construction $C^1(Z)|x,y\rangle = |x\rangle \otimes Z^x|y\rangle = |x\rangle \otimes (-1)^{xy}|y\rangle = (-1)^{xy}|x,y\rangle = Z^y|x\rangle \otimes |y\rangle$ which is exactly what Figure 2 expresses.

– **4.21-** *Verify that Figure 3 implements the $C^2(U)$ operation* □

As can be seen from Figure 3, there are five gates in the circuit of the *r.h.s.* Therefore the quantum states describing the computer can be labeled by $|\psi_0\rangle, \cdots, |\psi_5\rangle$ if $|\psi_0\rangle$ denotes the input, while $|\psi_s\rangle$ denotes the state after the s-th gate. So that $|\psi_5\rangle$ is the output. If the input is given by $|\psi_0\rangle = |x,y,z\rangle$ then

$$\begin{aligned}
|\psi_1\rangle &= |x\rangle \otimes |y\rangle \otimes V^y|z\rangle \\
|\psi_2\rangle &= |x\rangle \otimes |y+x\rangle \otimes V^y|z\rangle \\
|\psi_3\rangle &= |x\rangle \otimes |y+x\rangle \otimes (V^\dagger)^{x+y}V^y|z\rangle \\
|\psi_4\rangle &= |x\rangle \otimes |y+2x\rangle \otimes (V^\dagger)^{x+y}V^y|z\rangle \\
&= |x\rangle \otimes |y\rangle \otimes (V^\dagger)^{x+y}V^y|z\rangle \\
|\psi_5\rangle &= |x\rangle \otimes |y\rangle \otimes V^x(V^\dagger)^{x+y}V^y|z\rangle
\end{aligned}$$

In the last expression, giving the output, $x+y$ has to be understood *modulo* 2. Namely $|\psi_{out}\rangle = |x,y\rangle \otimes V^x(V^\dagger)^{x+y}V^y|z\rangle$. So that if $(x,y) \neq (1,1)$ then the one-qubit operation

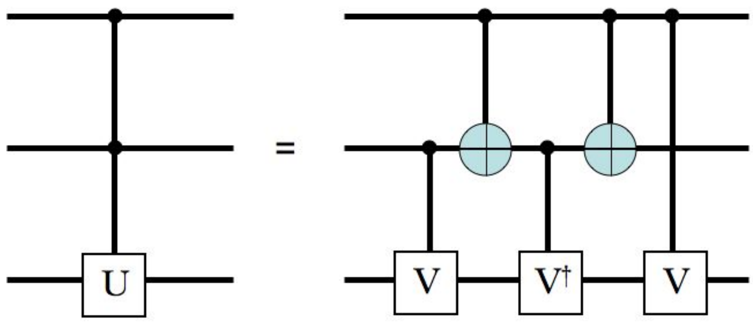

FIG. 3 – Circuit for the $C^2(U)$ gate. V is any unitary satisfying $V^2 = U$. The special case $V = (1-\imath)(I+\imath X)/2$ corresponds to the Toffoli gate

$V^x(V^\dagger)^{x+y}V^y$ is always the indentity I, since $V^\dagger = V^{-1}$. However, if $x = y = 1$ then $x + y = 0, \bmod 2$ and $V^x(V^\dagger)^{x+y}V^y = V^2 = U$. Thus $V^x(V^\dagger)^{x+y}V^y = U^{xy}$ for all $(x, y) \in \{0,1\}^{\times 2}$. And therefore $|\psi_{out}\rangle = |x, y\rangle \otimes U^{xy}|z\rangle = C^2(U)|x, y, z\rangle$.
It is easy to check that if $V = (1-\imath)(I+\imath X)/2 = e^{-\imath\pi/4}\, e^{\imath\pi X/4}$, $V^2 = -\imath(\cos\pi/2 + \imath\sin\pi/2X) = X$. So that the previous circuit implements the Toffoli gate.

– **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 from three to two ?* □

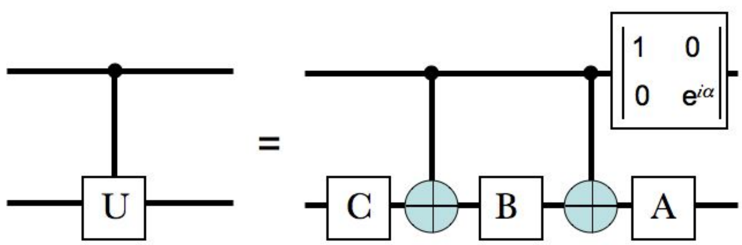

FIG. 4 – Circuit implementing $C^1(U)$: here $ABC = I$ and $U = e^{\imath\alpha}AXBXC$.

The quantum circuit in Figure 4 describes how to implement a $C^1(U)$ gate from using only one-qubit and CNOT gates.

By construction $\det U = e^{\imath\alpha}$. If $U = R_y(\theta) = e^{\imath\theta Y}$ then $\alpha = 0$. Moreover, taking $A = I, B = e^{-\imath\theta Y/2}$ and $C = e^{\imath\theta Y/2}$, leads to $ABC = BC = I$ and $AXBXC = XBXC = e^{\imath\theta Y/2}e^{\imath\theta Y/2} = e^{\imath\theta Y}$ since $XYX = -Y$ (see Exercise **4.7**). In this case then, only the two 1-qubit gates B, C are needed. Actually A and C could be interchanged here.

If $U = R_x(\theta)$ however, a solution is given by $A = H, B = e^{-\imath\theta Z/2}$ and $C = e^{\imath\theta Z/2}H$. This is because $HZH = X$ and $XZX = -Z$ (see Exercise **4.13**). It does not seem possible to reduce the number of single qubit gates then.

– **4.24-** *Verify that Figure 5 implements the Toffoli gate* □

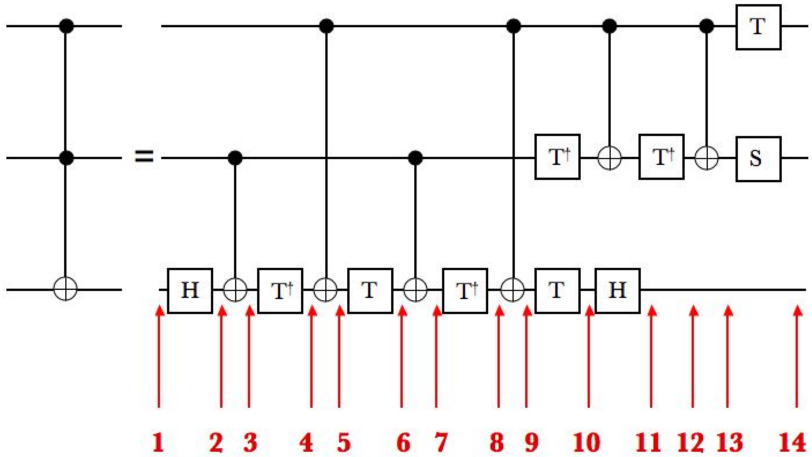

FIG. 5 – Implementation of the Toffoli gate

To compute the outcome of the *r.h.s.* it will be convenient to proceed gate by gate as indicated by the arrows in Figure 5. Since $T = e^{\imath\pi/8}e^{-\imath\pi Z/8}$ and since $XZX = -Z$ it follows that $XT^\dagger X = e^{-\imath\pi/4}T$. It is easy to jump directly to the step #9. This gives

$$|\psi_1\rangle = |x,y,z\rangle\,, \qquad |\psi_9\rangle = |x,y\rangle \otimes X^xT^\dagger X^yTX^xT^\dagger X^yH|z\rangle$$

$$\begin{aligned}
|\psi_{10}\rangle &= |x\rangle \otimes T^\dagger|y\rangle \otimes TX^xT^\dagger X^yTX^xT^\dagger X^yH|z\rangle\\
|\psi_{11}\rangle &= |x\rangle \otimes X^xT^\dagger|y\rangle \otimes HTX^xT^\dagger X^yTX^xT^\dagger X^yH|z\rangle\\
|\psi_{12}\rangle &= |x\rangle \otimes T^\dagger X^xT^\dagger|y\rangle \otimes HTX^xT^\dagger X^yTX^xT^\dagger X^yH|z\rangle\\
|\psi_{13}\rangle &= |x\rangle \otimes X^xT^\dagger X^xT^\dagger|y\rangle \otimes HTX^xT^\dagger X^yTX^xT^\dagger X^yH|z\rangle\\
|\psi_{14}\rangle &= e^{\imath\pi x/4}|x\rangle \otimes SX^xT^\dagger X^xT^\dagger|y\rangle \otimes HTX^xT^\dagger X^yTX^xT^\dagger X^yH|z\rangle
\end{aligned}$$

where $T|x\rangle = e^{\imath\pi x/4}|x\rangle$ has been used. If $x = 0$ then

$$|\psi_{out}\rangle = |0\rangle \otimes |y\rangle \otimes |z\rangle = \text{TOFFOLI}|0,y,z\rangle\,.$$

as can be checked immediately. If $x = 1$ then $e^{\imath\pi x/4}SX^xT^\dagger X^xT^\dagger|y\rangle = e^{\imath\pi/4}SXT^\dagger XT^\dagger|y\rangle = S|y\rangle = (\imath)^y|y\rangle$. Thus, whenever $y = 0$ this gives

$$|\psi_{out}\rangle = |1\rangle \otimes |0\rangle \otimes HTXT^\dagger TXT^\dagger H|z\rangle = |1,0,z\rangle$$

If now $x = y = 1$ then

$$|\psi_{out}\rangle = |1,1\rangle \otimes \imath HTXT^\dagger XTXT^\dagger XH|z\rangle = \text{TOFFOLI}|1,0,z\rangle\,.$$

noindent However it is easy to check that

$$TXT^\dagger X = \begin{bmatrix} e^{-\imath\pi/4} & 0 \\ 0 & e^{\imath\pi/4} \end{bmatrix} \qquad \Rightarrow \qquad (TXT^\dagger X)^2 = -\imath Z\,.$$

So that

$$|\psi_{out}\rangle = |1,1\rangle \otimes HZH|z\rangle = |1,1\rangle \otimes X|z\rangle = \text{TOFFOLI}|1,1,z\rangle\,.$$

Hence the result is the same as for the Toffoli gate for all values of (x, y, z).

– **4.25-** *Recall that the Fredkin (controlled-*SWAP*) gate performs the transform*

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \tag{6}$$

1. *Give a quantum circuit which uses 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 with the circuit of Figure 3 to obtain a Fredkin gate construction using only six two-qubit gates.*
4. *Can you come up with an even simpler construction, with five two-qubit gates ?*

□

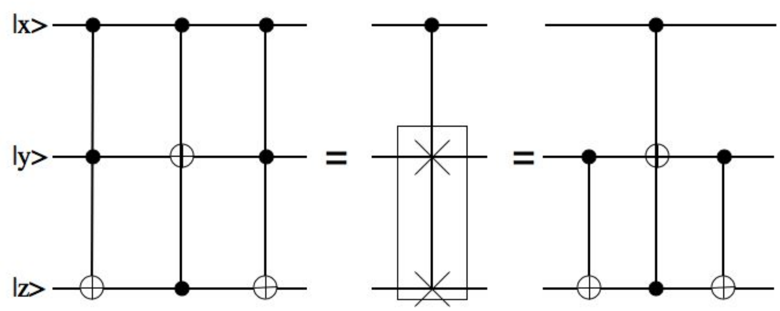

FIG. 6 – The Fredkin gate is a controlled-SWAP gate

1. As can be seem from eq. (6), the Fredkin gate acts on the computational basis as $F|0,y,z\rangle = |0,y,z\rangle$ and $F|1,y,z\rangle = |1,z,y\rangle$. In other words if $\text{SWAP}|y,z\rangle = |z,y\rangle$ then it can be written as $F|x,y,z\rangle = |x\rangle \otimes (\text{SWAP})^x|y,z\rangle$. Hence the Fredkin gate is nothing but a controlled-SWAP. The SWAP-gate can be implemented by three alternating CNOT-gates, suggesting that the Fredkin gate be given by the quantum circuit described on the *l.h.s.* of Figure 6. A direct calculation of the outcome of this quantum circuit gives indeed, if $|\psi_i\rangle$ represents the quantum state of the computer after the i-th gate,

$$\begin{aligned}
|\psi_1\rangle &= |x, y, z + xy\rangle \\
|\psi_2\rangle &= |x, y + xz + x^2y, z + xy\rangle \\
&= |x, \overline{x}y + xz, z + xy\rangle \\
|\psi_{out}\rangle = |\psi_3\rangle &= |x, \overline{x}y + xz, z + xy + x\overline{x}y + x^2z\rangle \\
&= |x, \overline{x}y + xz, \overline{x}z + xy\rangle
\end{aligned}$$

In these equations, $x = x^2, \overline{x} = 1 - x = 1 + x, x\overline{x} = 0$ have been used. If $x = 0$ the outcome is therefore $|0, y, z\rangle$ while if $x = 1$ it is $|1, z, y\rangle$. Hence the *l.h.s.* of Figure 6 implements indeed the Fredkin gate.

2. Actually the left and the right Toffoli gates can be replaced by a simple CNOT gate, as in the *r.h.s.* of Figure 6. For indeed the same calculation performed now on the *r.h.s.* gives

$$\begin{aligned}
|\psi_1\rangle &= |x, y, z + y\rangle \\
|\psi_2\rangle &= |x, y + xz + xy, z + y\rangle \\
&= |x, \overline{x}y + xz, z + y\rangle \\
|\psi_{out}\rangle = |\psi_3\rangle &= |x, \overline{x}y + xz, z + y + \overline{x}y + xz\rangle \\
&= |x, \overline{x}y + xz, \overline{x}z + xy\rangle
\end{aligned}$$

giving indeed the same result.

3. Replacing the Toffoli gate in the middle by the quantum circuit given in Figure 3, will give Figure 7, where $V = e^{-\imath\pi/4}(I + \imath X)/\sqrt{2}$. In such a case $V^2 = X$, or, equivalently $(V^\dagger)^2 = X$. It can be checked directly that the *r.h.s.* of Figure 7 gives indeed the Fredkin gate for, using the same type of computation as before,

$$\begin{aligned}
|\psi_1\rangle &= |x, y, z \oplus y\rangle \\
|\psi_2\rangle &= |x\rangle \otimes V^{y\oplus z}|y\rangle \otimes |y \oplus z\rangle \\
|\psi_3\rangle &= |x\rangle \otimes V^{y\oplus z}|y\rangle \otimes |x \oplus y \oplus z\rangle \\
|\psi_4\rangle &= |x\rangle \otimes (V^\dagger)^{x\oplus y\oplus z}V^{y\oplus z}|y\rangle \otimes |x \oplus y \oplus z\rangle \\
|\psi_5\rangle &= |x\rangle \otimes (V^\dagger)^{x\oplus y\oplus z}V^{y\oplus z}|y\rangle \otimes |y \oplus z\rangle \\
|\psi_6\rangle &= |x\rangle \otimes V^x(V^\dagger)^{x\oplus y\oplus z}V^{y\oplus z}|y\rangle \otimes |y \oplus z\rangle \\
&= |x\rangle \otimes |u\rangle \otimes |y \oplus z\rangle \\
|\psi_{out}\rangle = |\psi_7\rangle &= |x\rangle \otimes |u\rangle \otimes |u \oplus y \oplus z\rangle
\end{aligned}$$

where

$$|u\rangle = V^x(V^\dagger)^{x\oplus y\oplus z}V^{y\oplus z}|y\rangle\,.$$

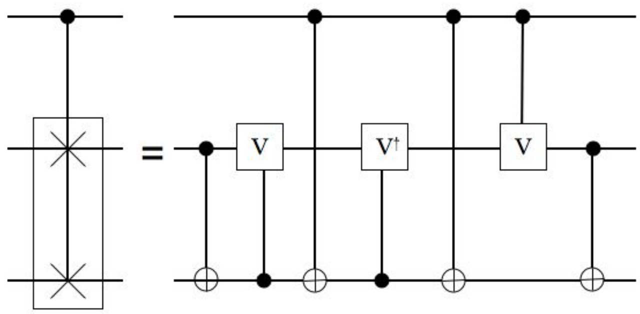

FIG. 7 – Quantum circuit implementing the Fredkin gate

Hence if $x = 0$ then $|u\rangle = |y\rangle$ and $|u \oplus y \oplus z\rangle = |z\rangle$. If $x = 1$ then $|u\rangle = V(V^\dagger)^{1-y\oplus z}V^{y\oplus z}|y\rangle = V^{2\{y\oplus z\}}|y\rangle = X^{y\oplus z}|y\rangle = |y\oplus y\oplus z\rangle = |z\rangle$. Then $|u\oplus y\oplus z\rangle = |y\rangle$. Thus

$$|\psi_{out}\rangle = |x\rangle \otimes (\text{SWAP})^x|y,z\rangle = F|x,y,z\rangle\,.$$

This circuit requires seven elementary two-qubit-gates and not six as suggested. However, the product of two such gates is a two-qubit gate so that the product of the first gates on the *r.h.s.* of Figure 7 can be considered as a unique two-qubit gate, meaning that only 6 such gates are necessary. If G denotes this product then

$$G|y,z\rangle = e^{-\imath\pi/4}\frac{(|y\rangle + \imath|z\rangle)}{\sqrt{2}}$$

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

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

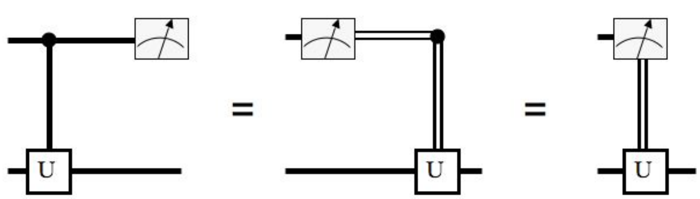

FIG. 8 –

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

If $|x, y\rangle$ is the input in these circuit, then on the leftmost circuit, the quantum state of the computer before measurement is $|x\rangle \otimes U^x|y\rangle$. In general then the input will be a linear combinations $\sum_{x,y} \alpha_{xy}|x, y\rangle$ of the computational basis. The measurement will give an outcome for the value of the first qubit. If this outcome is x, then then, thanks to the axioms about measurement, the output will be given by

$$|\psi_{out}\rangle = \frac{\sum_y \alpha_{xy} U^x |y\rangle}{\sqrt{\sum_y |\alpha_{xy}|^2}} = U^x \, \frac{\sum_y \alpha_{xy} |y\rangle}{\sqrt{\sum_y |\alpha_{xy}|^2}}$$

In the middle circuit, the measurement of the first qubit is made first. If x is the outcome then the new state, right after the measurement is given by

$$|\psi_{meas}\rangle = \frac{\sum_y \alpha_{xy} |y\rangle}{\sqrt{\sum_y |\alpha_{xy}|^2}}$$

The classical bit x is then applied to control the gate U so that the output will be $U^x|\psi_{meas}\rangle$ which the same output as for the leftmost circuit.