CS 593/MA 595 - Introduction to Quantum Computing

Quantum Computation and Quantum Information by *Isaac Chuang, Michael Nielsen*

Student: **Ralph Razzouk**

Homework 3

Do the following exercises from Nielsen and Chuang: 4.6, 4.11, 4.12, 4.17, 4.34, 4.35, 4.38, 4.39. For 4.17 and 4.39, just draw your answer, you do not need to justify it.

Problem 4.6
(Bloch sphere interpretation of rotations) One reason why the $R_{\hat{n}}(\theta)$ operators are referred to as rotation operators is the following fact, which you are to prove. Suppose a single qubit has a state represented by the Bloch vector $\vec{\lambda}$. Then the effect of the rotation $R_{\hat{n}}(\theta)$ on the state is to rotate it by an angle θ about the $\hat{n}$ axis of the Bloch sphere. This fact explains the rather mysterious looking factor of two in the definition of the rotation matrices.

Proof. Suppose a single qubit has a state represented by an arbitrary Bloch vector $\vec{\lambda}$. Without loss of generality, we can express $\vec{\lambda}$ in a coordinate system such that $\hat{n}$ is aligned with the $\hat{z}$ axis, so it suffices to consider how the state behaves under application $R_{\hat{z}}(\theta)$. Let $\vec{\lambda} = (\lambda_x, \lambda_y, \lambda_z)$ be the vector expressed in this coordinate system. By Exercise 2.72, the density operator ρ corresponding to this Bloch vector is given by:

$$\rho = \frac{\mathbb{I} + \vec{\lambda}\cdot\vec{\sigma}}{2}.$$

Observing how ρ transforms under conjugation by $R_{\hat{z}}(\theta)$, we have

$$\begin{aligned}
R_{\hat{z}}(\theta)\rho R_{\hat{z}}(\theta)^\dagger &= R_{\hat{z}}(\theta)\rho R_{\hat{z}}(-\theta)\\
&= R_{\hat{z}}(\theta)\left(\frac{\mathbb{I} + \vec{\lambda}\cdot\vec{\sigma}}{2}\right)R_{\hat{z}}(-\theta)\\
&= R_{\hat{z}}(\theta)\left(\frac{\mathbb{I} + \lambda_x\sigma_x + \lambda_y\sigma_y + \lambda_z\sigma_z}{2}\right)R_{\hat{z}}(-\theta).
\end{aligned}$$

Using $\sigma_j\sigma_k = \delta_{jk} + i\sum_l \epsilon_{jkl}\sigma_l$ and $\sigma_j\sigma_k = -\sigma_k\sigma_j$, we have

$$\begin{aligned}
R_{\hat{z}}(\theta)\sigma_x &= \left(\cos\left(\frac{\theta}{2}\right)\mathbb{I} - i\sin\left(\frac{\theta}{2}\right)\sigma_z\right)\sigma_x\\
&= \cos\left(\frac{\theta}{2}\right)\mathbb{I}\sigma_x - i\sin\left(\frac{\theta}{2}\right)\sigma_z\sigma_x\\
&= \cos\left(\frac{\theta}{2}\right)\sigma_x\mathbb{I} + i\sin\left(\frac{\theta}{2}\right)\sigma_x\sigma_z\\
&= \sigma_x\left(\cos\left(\frac{\theta}{2}\right)\mathbb{I} + i\sin\left(\frac{\theta}{2}\right)\sigma_z\right)\\
&= \sigma_x\left(\cos\left(-\frac{\theta}{2}\right)\mathbb{I} - i\sin\left(-\frac{\theta}{2}\right)\sigma_z\right)\\
&= \sigma_x R_{\hat{z}}(-\theta).
\end{aligned}$$

Similarly, $R_{\hat{z}}(\theta)\sigma_y = \sigma_y R_{\hat{z}}(-\theta)$ and $R_{\hat{z}}(\theta)\sigma_z = \sigma_z R_{\hat{z}}(\theta)$. Then, we have

$$\begin{aligned}
R_{\hat{z}}(\theta)\rho R_{\hat{z}}(\theta)^\dagger &= R_{\hat{z}}(\theta)\left(\frac{\mathbb{I} + \lambda_x\sigma_x + \lambda_y\sigma_y + \lambda_z\sigma_z}{2}\right)R_{\hat{z}}(-\theta)\\
&= \left(\frac{\mathbb{I}R_{\hat{z}}(\theta) + \lambda_x\sigma_x R_{\hat{z}}(-\theta) + \lambda_y\sigma_y R_{\hat{z}}(-\theta) + \lambda_z\sigma_z R_{\hat{z}}(\theta)}{2}\right)R_{\hat{z}}(-\theta)\\
&= \frac{\mathbb{I} + \lambda_x\sigma_x R_{\hat{z}}(-2\theta) + \lambda_y\sigma_y R_{\hat{z}}(-2\theta) + \lambda_z\sigma_z}{2}.
\end{aligned}$$

By term-by-term calculation, we have

$$\begin{aligned}
\sigma_x R_{\hat{z}}(-2\theta) &= \sigma_x \left(\cos\left(-\frac{2\theta}{2}\right) - i\sin\left(-\frac{2\theta}{2}\right)\sigma_z\right) \\
&= \sigma_x\left(\cos(\theta) + i\sin(\theta)\sigma_z\right) \\
&= \cos(\theta)\sigma_x + i\sin(\theta)\sigma_x\sigma_z \\
&= \cos(\theta)\sigma_x + i\sin(\theta)(-i\sigma_y) \\
&= \cos(\theta)\sigma_x + \sin(\theta)\sigma_y,
\end{aligned}$$

$$\begin{aligned}
\sigma_y R_{\hat{z}}(-2\theta) &= \sigma_y \left(\cos\left(-\frac{2\theta}{2}\right) - i\sin\left(-\frac{2\theta}{2}\right)\sigma_z\right) \\
&= \sigma_y\left(\cos(\theta) + i\sin(\theta)\sigma_z\right) \\
&= \cos(\theta)\sigma_y + i\sin(\theta)\sigma_y\sigma_z \\
&= \cos(\theta)\sigma_y + i\sin(\theta)(i\sigma_x) \\
&= \cos(\theta)\sigma_y - \sin(\theta)\sigma_x,
\end{aligned}$$

and substituting in the inital expression, we get

$$\begin{aligned}
R_{\hat{z}}(\theta)\rho R_{\hat{z}}(\theta)^\dagger &= \frac{\mathbb{I} + \lambda_x\sigma_x R_{\hat{z}}(-2\theta) + \lambda_y\sigma_y R_{\hat{z}}(-2\theta) + \lambda_z\sigma_z}{2} \\
&= \frac{\mathbb{I} + \lambda_x\left(\cos(\theta)\sigma_x + \sin(\theta)\sigma_y\right) + \lambda_y\left(\cos(\theta)\sigma_y - \sin(\theta)\sigma_x\right) + \lambda_z\sigma_z}{2} \\
&= \frac{\mathbb{I} + \left(\lambda_x\cos(\theta) - \lambda_y\sin(\theta)\right)\sigma_x + \left(\lambda_x\sin(\theta) + \lambda_y\cos(\theta)\right)\sigma_y + \lambda_z\sigma_z}{2}.
\end{aligned}$$

From this, the new Bloch vector $\vec{\lambda}'$, after conjugation by $R_{\hat{z}}(\theta)$ is expressed as

$$\vec{\lambda}' = (\lambda_x\cos(\theta) - \lambda_y\sin(\theta), \lambda_x\sin(\theta) + \lambda_y\cos(\theta), \lambda_z).$$

Notice that

$$\vec{\lambda}' = \begin{pmatrix} \cos(\theta) & -\sin(\theta) & 0 \\ \sin(\theta) & \cos(\theta) & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \lambda_x \\ \lambda_y \\ \lambda_z \end{pmatrix},$$

where the matrix is the 3-dimensional rotation matrix about $\hat{z}$ by an angle of θ.

Thus, the conjugation of ρ under $R_{\hat{z}}(\theta)$ has the equivalent effect to rotating the Bloch vector by θ about the z-axis, and hence, the effect of $R_{\hat{n}}(\theta)$ on a one qubit state is to rotate it by an angle θ about $\hat{n}$. ■

Problem 4.12
Give A, B, C, and α for the Hadamard gate

Proof. Since the Hadamard gate H is a unitary gate on a single qubit, then there exist unitary operators A, B, C on a single qubit such that $ABC = \mathbb{I}$ and $U = e^{i\alpha}AXBXC$, where α is some overall phase factor.

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = e^{i\frac{\pi}{2}} R_z(\pi) R_y\left(-\frac{\pi}{2}\right) R_z(0).$$

Thus,

$$\begin{aligned}
A &= R_z(\pi)R_y\left(-\frac{\pi}{4}\right) \\
B &= R_y\left(\frac{\pi}{4}\right)R_z\left(-\frac{\pi}{2}\right) \\
C &= R_z\left(-\frac{\pi}{2}\right) \\
\alpha &= \frac{\pi}{2}.
\end{aligned}$$

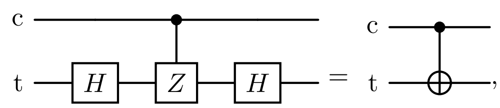
■

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

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

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

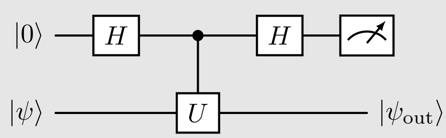
Proof. From Exercise 4.13, we have that $HZH = X$. To obtain a CNOT gate from a single controlled-Z gate, we can conjugate the target qubit with Hadamard gates



which is
$$\begin{pmatrix} H & 0 \\ 0 & H \end{pmatrix}\begin{pmatrix} I & 0 \\ 0 & Z \end{pmatrix}\begin{pmatrix} H & 0 \\ 0 & H \end{pmatrix} = \begin{pmatrix} HH & 0 \\ 0 & HZH \end{pmatrix} = \begin{pmatrix} I & 0 \\ 0 & X \end{pmatrix} = CNOT.$$

∎

Problem 4.34
(Measuring an operator) 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. That is, we desire to obtain a measurement result indicating one of the two eigenvalues, and leaving a post-measurement state which is the corresponding eigenvector. How can this be implemented by a quantum circuit? Show that the following circuit implements a measurement of U:



Proof. We can obtain a measurement result indicating one of the two eigenvalues, while leaving a post-measurement state which is the corresponding eigenvector by using a controlled gate to entangle the system to a qubit whose measurement will collapse the state into +1 or -1, while also giving us the state of the original qubit. Additionally, since U is both Hermitian and unitary, then it is also an involutory matrix, i.e. $1 = U^\dagger U = UU = U^2$. The circuit will execute as follows

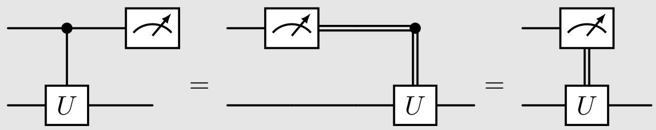
$$\begin{aligned} |0\rangle|\psi\rangle &\to^H \frac{1}{\sqrt{2}}(|0\rangle|\psi\rangle + |1\rangle|\psi\rangle) \\ &\to^{CU} \frac{1}{\sqrt{2}}(|0\rangle|\psi\rangle + |1\rangle U|\psi\rangle) \\ &\to^H \frac{1}{2}\left[|0\rangle|\psi\rangle + |1\rangle|\psi\rangle + |0\rangle U|\psi\rangle + |1\rangle U|\psi\rangle\right] \\ &= \frac{1}{2}\left[|0\rangle(\mathbb{I}+U)|\psi\rangle + |1\rangle(\mathbb{I}-U)|\psi\rangle\right]. \end{aligned}$$

- If the measurement value is $|0\rangle$, then the state is in $|\psi_{out}\rangle = (\mathbb{I}+U)|\psi\rangle$, where $U|\psi_{out}\rangle = U(\mathbb{I}+U)|\psi\rangle = (\mathbb{I}+U)|\psi\rangle$, and thus has an eigenvalue of +1.

- If the measurement value is $|1\rangle$, then the state is in $|\psi_{out}\rangle = (\mathbb{I}-U)|\psi\rangle$, where $U|\psi_{out}\rangle = U(\mathbb{I}-U)|\psi\rangle = -(\mathbb{I}-U)|\psi\rangle$, and thus has an eigenvalue of -1.

■

Problem 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:



(Recall that the 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.

Proof. Let the system be in the state $a|0\rangle|\psi\rangle + b|1\rangle|\psi\rangle$. Then the effect of the circuits are

- **Circuit 1:**

$$\begin{aligned} a|0\rangle|\psi\rangle + b|1\rangle|\psi\rangle &\rightarrow^{CU} a|0\rangle|\psi\rangle + b|1\rangle U|\psi\rangle \\ &\rightarrow^{M} \begin{cases} |0\rangle, & \text{with } p = |a|^2 \text{ and state } |\psi\rangle, \\ |1\rangle, & \text{with } p = |b|^2 \text{ and state } U|\psi\rangle \end{cases} \end{aligned}$$

- **Circuit 2:**

$$\begin{aligned} a|0\rangle|\psi\rangle + b|1\rangle|\psi\rangle &\rightarrow^{M} \begin{cases} |0\rangle, & \text{with } p = |a|^2 \text{ and state } |\psi\rangle, \\ |1\rangle, & \text{with } p = |b|^2 \text{ and state } |\psi\rangle \end{cases} \\ &\rightarrow^{CU} \begin{cases} |0\rangle, & \text{with } p = |a|^2 \text{ and state } |\psi\rangle, \\ |1\rangle, & \text{with } p = |b|^2 \text{ and state } U|\psi\rangle \end{cases} \end{aligned}$$

■

Problem 4.38
Prove that 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.

Proof. Suppose U is a $d \times d$ unitary matrix which can be decomposed using less than $d-1$ two-level unitaries.

We can think of each two-level unitary as an "edge" linking some pair of nodes $|i\rangle$ and $|j\rangle$, interpreting each node as a vertex. Let $U = U_{d-1}U_{d-2}\cdots U_2U_1$, where U_k is a two-level unitary. The graph corresponding to U has at most $d-1$ edges corresponding to the U_k operators, but we have d vertices, then there must be two subsets of nodes on which U acts independently. Hence, U must be block diagonal in some rearrangement of the initial basis. A one-component graph would require more than $d-1$ edges. A non-block diagonal operator cannot be written with less than d operators U_k.

Clearly not every U has this form. To name one example, the Quantum Fourier Transform matrix doesn't.

Thus, by contradiction, there exists a $d \times d$ matrix U which cannot be decomposed as a product of fewer than $d-1$ two-level unitary matrices.

■

Problem 4.39
Find a quantum circuit using single qubit operations and CNOTs to implement the transformation

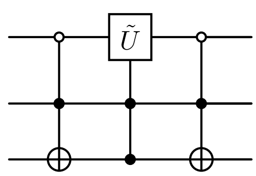
$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & a & 0 & 0 & 0 & 0 & c \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & b & 0 & 0 & 0 & 0 & d \end{bmatrix}$$

where $\tilde{U} = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ is an arbitrary 2×2 unitary matrix.

Proof. From the entries of the matrix, we can see that it acts non-trivially on the states $|010\rangle$ and $|111\rangle$. We write a Gray code connecting 010 and 111:

$$\begin{array}{c} ABC \\ 0\,1\,0 \\ 0\,1\,1 \\ 1\,1\,1 \end{array}$$

From this we read off the required circuit to be



∎

Problem 2
Give an example of a unitary 2-qubit gate $U : \left(\mathbb{C}^2\right)^{\otimes 2} \to \left(\mathbb{C}^2\right)^{\otimes 2}$ that is "entangling," that is, can not be expressed as a tensor product $U_1 \otimes U_2$ where U_1 and U_2 are two 1-qubit gates $U_1, U_2 : \mathbb{C}^2 \to \mathbb{C}^2$. Justify your example.

Proof. An example of a unitary 2-qubit gate that is "entangling" is the CNOT gate, given by

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} \mathbb{I}_2 & 0 \\ 0 & X \end{pmatrix}.$$

This gate is not separable (entangling) as it cannot be written as the tensor product of two matrices. In fact, if it separable, then

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \otimes B = \begin{pmatrix} a_{11}B & a_{12}B \\ a_{21}B & a_{22}B \end{pmatrix} \implies \begin{cases} \mathbb{I}_2 = a_{11}B \\ X = a_{22}B \end{cases} \implies \mathbb{I}_2 = bX,$$

where $b = \frac{a_{11}}{a_{22}}$ is some scalar, which is a contradiction.
Therefore, CNOT is an entangling gate. ∎