Quantum Computing Assignment 6

Brennan W. Fieck

March 1, 2017

Problem 4.2.3.

(a) Prove $XR_y(\theta)X = R_y(-\theta)$ and $XR_z(\theta)X = R_z(-\theta)$.

(b) Prove Corollary 4.2.1:
   Any 1-qubit gate U can be written in the form

$$U = e^{i\alpha}AXBXC$$

Solution.

(a) Via direct application:

$$XR_y(\theta)X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \cos\left(\frac{\theta}{2}\right) & -\sin\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \\ \cos\left(\frac{\theta}{2}\right) & -\sin\left(\frac{\theta}{2}\right) \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} \cos\left(\frac{\theta}{2}\right) & \sin\left(\frac{\theta}{2}\right) \\ -\sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{bmatrix}$$

Now, since cos is an even function, and sin is an odd function, if we let $\theta = -\theta$ this becomes

$$\begin{bmatrix} \cos\left(\frac{-\theta}{2}\right) & \sin\left(\frac{-\theta}{2}\right) \\ -\sin\left(\frac{-\theta}{2}\right) & \cos\left(\frac{-\theta}{2}\right) \end{bmatrix} = \begin{bmatrix} \cos\left(\frac{\theta}{2}\right) & -\sin\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{bmatrix}$$

$$\rightarrow XR_y(\theta)X = R_y(-\theta)$$

and now

$$XR_z(\theta)X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} e^{-i\theta} & 0 \\ 0 & e^{i\theta} \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & e^{i\theta} \\ e^{-i\theta} & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{bmatrix} = R_z(-\theta)$$

(b) Well, first of all it may be helpful to figure out what U looks like.

$$U = e^{i\alpha} \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} c_1 & c_2 \\ c_3 & c_4 \end{bmatrix}$$

$$= e^{i\alpha} \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \begin{bmatrix} b_4 & b_3 \\ b_2 & b_1 \end{bmatrix} \begin{bmatrix} c_1 & c_2 \\ c_3 & c_4 \end{bmatrix} = e^{i\alpha} \begin{bmatrix} a_1b_4 + a_2b_2 & a_1b_3 + a_2b_1 \\ a_3b_4 + a_4b_2 & a_3b_3 + a_4b_1 \end{bmatrix} \begin{bmatrix} c_1 & c_2 \\ c_3 & c_4 \end{bmatrix}$$

$$= e^{i\alpha} \begin{bmatrix} c_1(a_1b_4 + a_2b_2) + c_3(a_1b_3 + a_2b_1) & c_2(a_1b_4 + a_2b_2) + c_4(a_1b_3 + a_2b_1) \\ c_1(a_3b_4 + a_4b_2) + c_3(a_3b_3 + a_4b_1) & c_2(a_3b_4 + a_4b_2) + c_4(a_3b_3 + a_4b_1) \end{bmatrix}$$

So it may be difficult to see in all that mess, but the gist of it is we have 4 expressions and 4 totally independent degrees of freedom, which means that it's possible to define each entry of U independently. This, in turn implies that any $\mathbb{C}^{2\times 2}$ object can be defined. Furthermore, the leading exponential allows the application of arbitrary global phase factors, and together these meet the criteria of being able to express any 1-qubit gate.

$\square$

Problem 4.2.4. Describe the effect of the CNOT gate with respect to the following bases

(a)
$$B_1 = \left\{ |0\rangle \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right), |0\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right), |1\rangle \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right), |1\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \right\}$$

(b)
$$B_2 = \left\{ \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right), \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right), \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right), \right.$$
$$\left. \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \right\} \quad (1)$$

Solution.

(a) First, it'll make everything easier to simplify the basis.

$$B_1 = \left\{ \frac{1}{\sqrt{2}} \left(|00\rangle + |01\rangle \right), \frac{1}{\sqrt{2}} \left(|00\rangle - |01\rangle \right), \frac{1}{\sqrt{2}} \left(|10\rangle + |11\rangle \right), \frac{1}{\sqrt{2}} \left(|10\rangle + |11\rangle \right) \right\}$$

application of the CNOT gate to these states gives

$$\left\{ \frac{1}{\sqrt{2}} \left(|00\rangle + |01\rangle \right), \frac{1}{\sqrt{2}} \left(|00\rangle - |01\rangle \right), \frac{1}{\sqrt{2}} \left(|11\rangle + |10\rangle \right), \frac{1}{\sqrt{2}} \left(|11\rangle + |10\rangle \right) \right\}$$

which is actually just the same as the original basis, which seems to imply that in this basis, CNOT acts as an identity.

(b) First, it'll make everything easier to simplify the basis.

$$B_2 = \left\{ \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2}, \frac{|00\rangle - |01\rangle + |10\rangle - |11\rangle}{2}, \frac{|00\rangle + |01\rangle - |10\rangle - |11\rangle}{2}, \right.$$
$$\left. \frac{|00\rangle - |01\rangle - |10\rangle + |11\rangle}{2} \right\} \quad (2)$$

Now we apply the `CNOT` gate to each component of this basis and see what happens

$$B_2 = \left\{ \frac{|00\rangle + |01\rangle + |11\rangle + |10\rangle}{2}, \frac{|00\rangle - |01\rangle + |11\rangle - |10\rangle}{2}, \frac{|00\rangle + |01\rangle - |11\rangle - |10\rangle}{2}, \right.$$
$$\left. \frac{|00\rangle - |01\rangle - |11\rangle + |10\rangle}{2} \right\} \quad (3)$$

In this basis, the first and third components remain unchanged under a `CNOT` transformation, and the values of the second and fourth are exchanged. If we represent this basis symbolically like so

$$B_2 = \{|A\rangle, |B\rangle, |C\rangle, |D\rangle\}$$

then any state $|\psi\rangle$ can be expressed as a linear combination of these basis states $|\psi\rangle = a|A\rangle + b|B\rangle + c|C\rangle + d|D\rangle$. In this basis, application of the `CNOT` gate transforms an arbitrary state $|\psi\rangle$ like this:

$$\texttt{CNOT}|\psi\rangle = a|A\rangle + d|B\rangle + c|C\rangle + b|D\rangle$$

$\square$

Problem 4.2.5. Prove that the c-U gate corresponds to the operator

$$|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U$$

Solution.
This expression must satisfy the following two conditions:

$$c\text{-}U|0\rangle|\psi\rangle = |0\rangle|\psi\rangle$$

and

$$c\text{-}U|1\rangle|\psi\rangle = |1\rangle U|\psi\rangle$$

So let's just try direct application:

$$(|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U)|0\rangle|\psi\rangle$$

$$= (|0\rangle\langle 0| \otimes I)|0\rangle|\psi\rangle + (|1\rangle\langle 1| \otimes U)|0\rangle|\psi\rangle$$
$$= (|0\rangle\langle 0|0\rangle) \otimes (I|\psi\rangle) + (|1\rangle\langle 1|0\rangle) \otimes (U|\psi\rangle)$$
$$= |0\rangle \otimes |\psi\rangle = |0\rangle|\psi\rangle$$

so that works, now the other one:

$$(|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U)|1\rangle|\psi\rangle$$

$$= (|0\rangle\langle 0| \otimes I)|1\rangle|\psi\rangle + (|1\rangle\langle 1| \otimes U)|1\rangle|\psi\rangle$$
$$= (|0\rangle\langle 0|1\rangle) \otimes (I|\psi\rangle) + (|1\rangle\langle 1|1\rangle) \otimes (U|\psi\rangle)$$
$$= |1\rangle \otimes |\psi\rangle = |1\rangle|\psi\rangle$$

so that definition of c-U checks out. $\square$

Problem 4.2.6. We know that U and $e^{i\theta}U$ are equivalent since they only differ by a global phase. However, prove that $c\text{-}U \neq c\text{-}(e^{i\theta}U)$ for θ not equal to an integer multiple of 2π.

Solution.
From the solution to 4.2.5, the $c\text{-}(e^{i\theta}U)$ gate would operate like so:

$$|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes e^{i\theta}U$$

Note that the phase term is not applied *globally*, meaning that the gate is now composed of a combination of two different phases - which are usually orthogonal. However, if θ happens to be an integer multiple of 2π, the phases of those two terms will match, and in that case $c\text{-}U = c\text{-}(e^{i\theta}U)$. $\qquad\square$

Problem 4.2.7. For a given 1-qubit gate U, use the result of Corollary 4.2.1 to construct a circuit for implementing a $c\text{-}U$ gate using only CNOT gates, and single-qubit gates.

Solution.
Given the results of corollary 4.2.1, any arbitrary gate U can be deconstructed to the form

$$U = e^{i\alpha}AXBXC$$

So to make a controlled version of U, it suffices to make controlled versions of its constituent gates. The global phase factor will be ignored. Recall that the controlled version of X is a CNOT gate.
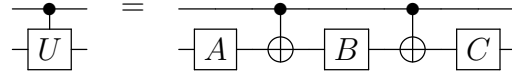
Now, to prove that this works, let's find the circuit's transfer function:

$$c\text{-}U = (I \otimes A)(\texttt{CNOT})(I \otimes B)(\texttt{CNOT})(I \otimes C)$$

$$= \left[\begin{array}{c|c} A & 0 \\ \hline 0 & A \end{array}\right]\left[\begin{array}{c|c} I_2 & 0 \\ \hline 0 & X \end{array}\right]\left[\begin{array}{c|c} B & 0 \\ \hline 0 & B \end{array}\right]\left[\begin{array}{c|c} I_2 & 0 \\ \hline 0 & X \end{array}\right]\left[\begin{array}{c|c} C & 0 \\ \hline 0 & C \end{array}\right]$$

$$= \left[\begin{array}{c|c} A & 0 \\ \hline 0 & AX \end{array}\right]\left[\begin{array}{c|c} B & 0 \\ \hline 0 & BX \end{array}\right]\left[\begin{array}{c|c} C & 0 \\ \hline 0 & C \end{array}\right]$$

$$= \left[\begin{array}{c|c} A & 0 \\ \hline 0 & AX \end{array}\right]\left[\begin{array}{c|c} BC & 0 \\ \hline 0 & BXC \end{array}\right]$$

$$= \left[\begin{array}{c|c} ABC & 0 \\ \hline 0 & AXBXC \end{array}\right] = \left[\begin{array}{c|c} I_2 & 0 \\ \hline 0 & U \end{array}\right]$$

$\qquad\square$

Problem F1. Find the left and right polar decompositions of the matrix

$$A = \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}$$

Solution.
Right and left polar decompositions of a matrix M take the form UP and $P'U$ respectively, where $P = \sqrt{MM^*}$ and $P' = \sqrt{M^*M}$. So first it's prudent to find A^*:

$$A^* = \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix} = A$$

which is fortunate, because it means that $A^*A = AA^* = A^2$, which means that P and P' must both be exactly $\sqrt{A^2} = A$, and thus the only value U can have is the 2×2 Identity, so the answer is simply:

- Right

$$A = AI$$

- Left

$$A = IA$$

$\square$