Ph219a/CS219a

Solutions
Nov 8, 2013

Problem 3.1

(a) Constructing the unitary transformation $\mathbf{U}_1$ as given in the circuit, we have $\mathbf{U}_1 = (\mathbf{H} \otimes \mathbf{I})\Lambda(\mathbf{P})(\mathbf{H} \otimes \mathbf{I})$. In the standard basis, $\mathbf{H}$ and $\mathbf{P}$ are given by

$$\mathbf{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad P = \begin{pmatrix} 1 & 0 \\ 1 & i \end{pmatrix} \tag{1}$$

so that $\mathbf{H} \otimes \mathbf{I}$ and $\Lambda(\mathbf{P})$ have the block diagonal form:

$$\mathbf{H} \otimes \mathbf{I} = \frac{1}{\sqrt{2}} \begin{pmatrix} \mathbf{I} & \mathbf{I} \\ \mathbf{I} & -\mathbf{I} \end{pmatrix} \quad \Lambda(\mathbf{P}) = \begin{pmatrix} \mathbf{I} & \emptyset \\ \emptyset & \mathbf{P} \end{pmatrix} \tag{2}$$

where $\emptyset$ is the 2×2 zero matrix and $\mathbf{I}$ is the 2×2 identity matrix. Thus,

$$\mathbf{U}_1 = \frac{1}{2} \begin{pmatrix} \mathbf{I}+\mathbf{P} & \mathbf{I}-\mathbf{P} \\ \mathbf{I}-\mathbf{P} & \mathbf{I}+\mathbf{P} \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 1+i & 0 & 1-i \\ 0 & 0 & 2 & 0 \\ 0 & 1-i & 0 & 1+i \end{pmatrix} \tag{3}$$

Similarly, $\mathbf{U}_2$ is given by $\mathbf{U}_2 = (\mathbf{I} \otimes \mathbf{H})\Lambda(\mathbf{P})(\mathbf{I} \otimes \mathbf{H}) = (\mathbf{SWAP})\mathbf{U}_1(\mathbf{SWAP})$, since $\Lambda(\mathbf{P})$ acts symmetrically on the input qubits. Interchanging the second and third rows and columns of $\mathbf{U}_1$, we have,

$$\mathbf{U}_2 = \frac{1}{2} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 1+i & 1-i \\ 0 & 0 & 1-i & 1+i \end{pmatrix} \tag{4}$$

It is easy to see that $\mathbf{U}_1$ and $\mathbf{U}_2$ act trivially on the states $|u_1\rangle = |00\rangle$ and $|u_2\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle + |11\rangle)$

$$\begin{aligned} \mathbf{U}_1 |00\rangle &= |00\rangle \quad \mathbf{U}_1 \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle + |11\rangle) \\ \mathbf{U}_2 |00\rangle &= |00\rangle \quad \mathbf{U}_2 \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle + |11\rangle) \end{aligned} \tag{5}$$

(b) Notice that $|u_3\rangle = \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle)$ and $|u_4\rangle = \frac{1}{\sqrt{6}}(|01\rangle + |10\rangle - 2\,|11\rangle)$, together with $|u_1\rangle$ and $|u_2\rangle$, form an orthonormal basis for the 2-qubit space. The unitary matrix that transforms from the computational basis to the $\{|u_i\rangle\}$ basis is

$$\mathbf{V} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} \\ 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} & -\frac{2}{\sqrt{6}} \end{pmatrix} \tag{6}$$

To express $\mathbf{U}_1$ and $\mathbf{U}_2$ in the new basis, we simply need to conjugate with $\mathbf{V}$

$$\begin{aligned} (\mathbf{U}_1)_{\text{new}} &= \mathbf{V}\mathbf{U}_1\mathbf{V}^\dagger = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{3+i}{4} & \frac{\sqrt{3}(-1+i)}{4} \\ 0 & 0 & \frac{\sqrt{3}(-1+i)}{4} & \frac{1+3i}{4} \end{pmatrix} \\ (\mathbf{U}_2)_{\text{new}} &= \mathbf{V}\mathbf{U}_2\mathbf{V}^\dagger = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{3+i}{4} & \frac{\sqrt{3}(1-i)}{4} \\ 0 & 0 & \frac{\sqrt{3}(1-i)}{4} & \frac{1+3i}{4} \end{pmatrix} \end{aligned} \tag{7}$$

Thus, when restricted to the two dimensional subspace spanned by $|u_3\rangle$ and $|u_4\rangle$,

$$(\mathbf{U}_1)_{\text{new}} = \begin{pmatrix} \frac{3+i}{4} & \frac{\sqrt{3}(-1+i)}{4} \\ \frac{\sqrt{3}(-1+i)}{4} & \frac{1+3i}{4} \end{pmatrix} \quad (\mathbf{U}_2)_{\text{new}} = \begin{pmatrix} \frac{3+i}{4} & \frac{\sqrt{3}(1-i)}{4} \\ \frac{\sqrt{3}(1-i)}{4} & \frac{1+3i}{4} \end{pmatrix} \tag{8}$$

(c) Working in the basis consisting of identity and the Pauli matrices, suppose $\mathbf{U}_1 = \alpha_1\mathbf{I} + \beta_1\mathbf{X} + \gamma_1\mathbf{Y} + \delta_1\mathbf{Z}$. Equation(7) gives:

$$\begin{aligned} \text{Tr}(\mathbf{U}_1\mathbf{I}) &= 2\alpha_1 = 1+i \;\Rightarrow\; \alpha_1 = \frac{1+i}{2} = \sqrt{\frac{i}{2}} \\ \text{Tr}(\mathbf{U}_1\mathbf{X}) &= 2\beta_1 = \frac{\sqrt{3}(-1+i)}{2} \;\Rightarrow\; \beta_1 = \sqrt{\frac{i}{2}}(\frac{\sqrt{3}i}{2}) \\ \text{Tr}(\mathbf{U}_1\mathbf{Y}) &= 2\gamma_1 = 0 \;\Rightarrow\; \gamma_1 = 0 \\ \text{Tr}(\mathbf{U}_1\mathbf{Z}) &= 2\delta_1 = \frac{1-i}{2} \;\Rightarrow\; \delta_1 = \sqrt{\frac{i}{2}}(\frac{-i}{\sqrt{2}}) \end{aligned} \tag{9}$$

Thus,

$$\mathbf{U}_1 = \sqrt{i}\left(\frac{1}{\sqrt{2}} - i\frac{1}{\sqrt{2}}\hat{n_1}.\vec{\sigma}\right) \tag{10}$$

with $\hat{n_1} = (-\sqrt{3}/2, 0, 1/2)^{\text{T}}$.
Similarly, solving for the expansion coefficients of $\mathbf{U}_2$, we get, $\alpha_2 = \sqrt{i/2}$, $\beta_2 = \sqrt{i/2}(-\sqrt{3}i/2)$, $\gamma_2 = 0$ and $\delta_2 = \sqrt{i/2}(-i/\sqrt{2})$, so that,

$$\mathbf{U}_2 = \sqrt{i}\left(\frac{1}{\sqrt{2}} - i\frac{1}{\sqrt{2}}\hat{n_2}.\vec{\sigma}\right) \tag{11}$$

where $\hat{n_2} = (\sqrt{3}/2, 0, 1/2)^{\text{T}}$.

(d) Using the results of part(c), we have,

$$\begin{aligned}\mathbf{U}_2^{-1}\mathbf{U}_1 &= \sqrt{-i^2}\left(\frac{1}{\sqrt{2}}\mathbf{I}+\frac{i}{\sqrt{2}}\hat{n_1}.\vec{\sigma}\right)\left(\frac{1}{\sqrt{2}}\mathbf{I}-\frac{i}{\sqrt{2}}\hat{n_2}.\vec{\sigma}\right)\\ &= \frac{1}{2}-\frac{i}{2}(\hat{n_1}-\hat{n_2}).\vec{\sigma}+\frac{1}{2}(\hat{n_1}.\vec{\sigma})(\hat{n_2}.\vec{\sigma}) \qquad (12)\end{aligned}$$

Now using the identity $(\hat{n_1}.\vec{\sigma})(\hat{n_2}.\vec{\sigma}) = \hat{n_1}.\hat{n_2} + i\vec{\sigma}(\hat{n_1}\times\hat{n_2})$, and computing $\hat{n_1}.\hat{n_2} = -1/2$ and $\hat{n_1}\times\hat{n_2} = (0,\sqrt{3}/2,0)^T$, we have,

$$\mathbf{U}_2^{-1}\mathbf{U}_1 = \frac{1}{4}\mathbf{I} - i\frac{\sqrt{15}}{4}\hat{k}.\vec{\sigma} \qquad (13)$$

with $\hat{k} = (-2/\sqrt{5}, 1/\sqrt{5}, 0)^{\mathrm{T}}$. Thus we see that the operation $\mathbf{U}_2^{-1}\mathbf{U}_1$ is a rotation about the axis $\hat{k}$, by an angle θ such that $\cos(\frac{\theta}{2}) = \frac{1}{4}$.

Problem 3.2

(a) A monic rational polynomial of degree 1 has exactly one rational root. Therefore the minimal degree monic rational polynomial that has $e^{i\frac{\theta}{2}}$ as a root must be of atleast degree 2. Since complex roots of rational polynomials must occur in pairs, we can construct the monic rational polynomial of degree 2 as follows -

$$P(x) = (x-e^{i\frac{\theta}{2}})(x-e^{-i\frac{\theta}{2}}) = x^2 - 2\cos(\frac{\theta}{2})x + 1 = x^2 - \frac{1}{2}x + 1 \qquad (14)$$

(b) Let $A(x) = x^n - 1$. Dividing $A(x)$ by the rational polynomial $P(x)$, we obtain rational polynomials $Q(x)$ and $R(x)$ such that

$$A(x) = P(x)Q(x) + R(x) \qquad (15)$$

where $R(x)$ has degree less than that of $P(x)$. Substituting the value $x = a$, we see that $A(a) = 0$ and $P(a) = 0$, implying that $R(a) = 0$. This leads to a contradiction since $P(x)$ is given to be the minimal degree rational polynomial with root a. Therefore, $R(x)$ must vanish for all values of x, ie. $R(x) = 0, \forall x$, so that $A(x) = x^n - 1 = P(x)Q(x)$.

(c) Let $A(x) = \sum_l a_l x^l$ and $B(x) = \sum_m b_m x^m$, so that,

$$C(x) = \sum_k c_k x^k = A(x)B(x) = \sum_{l,m} a_l b_m x^{l+m} \qquad (16)$$

Clearly, given that $A(x)$ and $B(x)$ are integral, so is $C(x)$. Lets assume $C(x)$ is not primitive, ie. say there exists a prime p that divides all of the coefficients c_k. Since $A(x)$ and $B(x)$ are primitive, p does not divide all the a_l's or b_m's. Let a_r be the lowest-order coefficient of $A(x)$ that is not divisible by p and let b_s be the lowest-order coefficient of $B(x)$ that is not divisible by p. Consider the $(r+s)^{\text{th}}$ order coefficient of $C(x)$. From equation(15),

$$c_{r+s} = a_r b_s + \sum_{l\neq r, m\neq s: l+m=r+s} a_l b_m \qquad (17)$$

By our assumption, c_{r+s} is divisible by p, and so are all the terms in the summation on the RHS - for every term, either $l < r$ so that a_l is divisible by p or $m < s$ and b_m is divisible by p. This implies that $a_r b_s$ is divisible by p, ie. one of a_r or b_s is divisible by p, thus leading to a contradiction. By *reductio ad absurdum*, $C(x)$ must be primitive.

(d) Let r be the lowest common denominator of the coefficients of $A(x)$. Therefore, r is the smallest integer such that $rA(x) = \tilde{A(x)}$ where $\tilde{A(x)}$ is integral. Now, suppose $\tilde{A(x)}$ is not primitive. Then there exists an integer $k > 1$ such that $\frac{1}{k}\tilde{A(x)}$ is integral or equivalently, $\frac{r}{k}A(x)$ is integral. Since $A(x)$ is monic, the highest order coefficient of $\frac{r}{k}A(x)$ is $\frac{r}{k}$, and since $\frac{r}{k}A(x)$ is integral, k must divide r. Thus we have found an integer $\frac{r}{k} = l < r$ such that $\tilde{A'(x)} = lA(x)$ is integral. This contradicts our initial assumption that r is the smallest integer such that $rA(x)$ is integral. By *reductio ad absurdum*, $\tilde{A(x)} = rA(x)$ must be primitive. By a similar argument, we can find an integer s such that $B(x) = \frac{1}{s}\tilde{B(x)}$ where $\tilde{B(x)}$ is primitive integral.
Given $P(x) = A(x)B(x) = \frac{1}{rs}\tilde{A(x)}\tilde{B(x)}$ is a monic integral polynomial. Using the result of part(c), $\tilde{A(x)}\tilde{B(x)}$ is primitive integral, since $\tilde{A(x)}$ and $\tilde{B(x)}$ are primitive integral. Since $P(x)$ is integral, either rs must divide all the coefficients of $\tilde{A(x)}\tilde{B(x)}$ or $rs = 1$. The first alternative is not possible, since $\tilde{A(x)}\tilde{B(x)}$ is primitive. Therefore, $rs = 1$ or equivalently, $r = s = 1$.

(e) Let a be a root of unity, ie. $a^n = 1$, for some integer n and $P(x)$ be the minimal degree monic rational polynomial that has a as a root. Then part(b) implies that there exists a monic rational polynomial $Q(x)$ such that $x^n - 1 = P(x)Q(x)$. Finally, using part(d), since $x^n - 1$ is integral, $P(x)$ must be integral too. QED!

Problem 3.3

(a) Representing all gates in the standard basis,

$$\begin{aligned}
\mathbf{HXH} &= \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \mathbf{Z} \\
\mathbf{HYH} &= \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}\frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} = -\mathbf{Y} \\
\mathbf{HZH} &= \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \mathbf{X} \\
\mathbf{PXP}^{-1} &= \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} = \mathbf{Y} \\
\mathbf{PYP}^{-1} &= \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}\begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \mathbf{X} \\
\mathbf{PYP}^{-1} &= \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \mathbf{Z}
\end{aligned} \tag{18}$$

(b) The action of $\mathbf{K}$ on the standard basis is given by

$$\mathbf{K} = \mathbf{HP}^{-1}\mathbf{HPH} = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 & 1-i \\ 1+i & 0 \end{pmatrix} \tag{19}$$

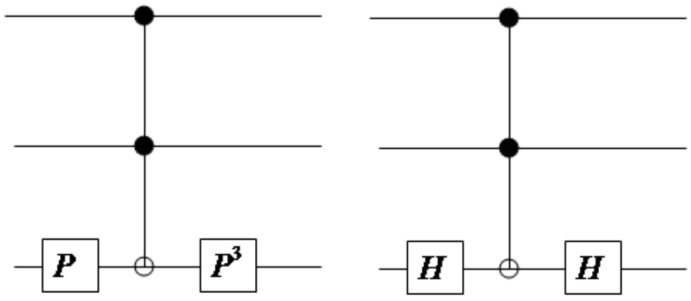
Once again, by simple matrix multiplication we can prove the following identities -

$$\begin{aligned}
\mathbf{KXK} &= \frac{1}{\sqrt{2}}\begin{pmatrix} 0 & 1-i \\ 1+i & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} 0 & 1-i \\ 1+i & 0 \end{pmatrix} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = \mathbf{Y} \\
\mathbf{KYK} &= \frac{1}{\sqrt{2}}\begin{pmatrix} 0 & 1-i \\ 1+i & 0 \end{pmatrix}\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} 0 & 1-i \\ 1+i & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \mathbf{X} \\
\mathbf{KZK} &= \frac{1}{\sqrt{2}}\begin{pmatrix} 0 & 1-i \\ 1+i & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} 0 & 1-i \\ 1+i & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = -\mathbf{Z}
\end{aligned}$$

(c) To construct $\Lambda^2(\mathbf{Y})$ using the gate set $\{\mathbf{H}, \mathbf{P}, \Lambda^2(\mathbf{X})\}$, we use the identity $\mathbf{PXP}^{-1} = \mathbf{PXP}^3 = \mathbf{Y}$ (proved above), so that

$$\begin{aligned}
\Lambda^2(\mathbf{Y}) &= |00\rangle\langle 00| \otimes \mathbf{I} + |01\rangle\langle 01| \otimes \mathbf{I} + |10\rangle\langle 10| \otimes \mathbf{I} + |11\rangle\langle 11| \otimes \mathbf{Y} \\
&= (|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10|) \otimes \mathbf{PP}^{-1} + |11\rangle\langle 11| \otimes \mathbf{PXP}^{-1} \\
&= (\mathbf{I} \otimes \mathbf{P})\left[(|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10|) \otimes \mathbf{I} + |11\rangle\langle 11| \otimes \mathbf{X}\right](\mathbf{I} \otimes \mathbf{P}^{-1}) \\
&= (\mathbf{I} \otimes \mathbf{P})\Lambda^2(\mathbf{X})(\mathbf{I} \otimes \mathbf{P}^3) \qquad (20)
\end{aligned}$$

Similarly, to construct $\Lambda^2(\mathbf{Z})$ we use the identity $\mathbf{HXH} = \mathbf{Z}$ so that $\Lambda^2(\mathbf{Z}) = (\mathbf{I} \otimes \mathbf{H})\Lambda^2(\mathbf{X})(\mathbf{I} \otimes \mathbf{H})$. Schematically,



(a) $\Lambda(\mathbf{Y})$ (b) $\Lambda(\mathbf{Z})$

Finally, we can trivially construct $\Lambda(\mathbf{P}) \otimes \mathbf{I}$ using $\Lambda^2(\mathbf{X}), \Lambda^2(\mathbf{Y})$ and $\Lambda^2(\mathbf{Z})$, since

$$\begin{aligned}
\Lambda(\mathbf{P}) \otimes \mathbf{I} &= \mathrm{diag}(\mathbf{I}, \mathbf{I}, \mathbf{I}, i\mathbf{I}) \\
&= \mathrm{diag}(\mathbf{I}, \mathbf{I}, \mathbf{I}, \mathbf{XYZ}) \\
&= \Lambda^2(\mathbf{XYZ}) = \Lambda^2(\mathbf{X})\Lambda^2(\mathbf{Y})\Lambda^2(\mathbf{Z}) \qquad (21)
\end{aligned}$$

where we have used $\mathbf{XYZ} = i\mathbf{Z}^2 = i\mathbf{I}$.

(d) Recall that $\Lambda(\mathbf{P}) = \mathrm{diag}(1, 1, 1, i)$. The real orthogonal matrix corresponding to this, $\Lambda(\mathbf{P})_R$, acts as follows:

$$\begin{aligned}
\Lambda(\mathbf{P})_R : |x, y, 0\rangle &\rightarrow (\mathrm{diag}(1, 1, 1, 0)\,|x, y\rangle) \otimes |0\rangle + (\mathrm{diag}(0, 0, 0, 1)\,|x, y\rangle) \otimes |1\rangle \\
|x, y, 1\rangle &\rightarrow (-\mathrm{diag}(0, 0, 0, 1)\,|x, y\rangle) \otimes |0\rangle + (\mathrm{diag}(1, 1, 1, 0)\,|x, y\rangle) \otimes |1\rangle \qquad (22)
\end{aligned}$$

Thus $\Lambda(\mathbf{P})_R$ acts trivially on all inputs except those with $x = y = 1$. In this case, it leaves the first two qubits unchanged and acts on the third qubit as follows: $|0\rangle \to |1\rangle$ and $|1\rangle \to -|0\rangle$. This corresponds to doing an **XZ** gate on the third qubit (conditioned on the first two qubits being in the $|11\rangle$ state), since

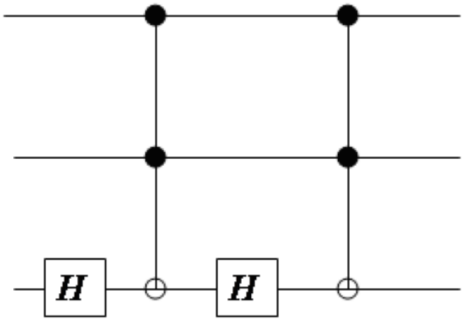
$$\mathbf{XZ} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \tag{23}$$

Hence $\Lambda(\mathbf{P})_R$ is simply a controlled-controlled-**XZ** gate, ie. $\Lambda(\mathbf{P})_R = \Lambda^2(\mathbf{XZ})$.

(e) First we note that $\Lambda^2(\mathbf{XZ}) = \Lambda^2(\mathbf{X})\Lambda^2(\mathbf{Z})$

$$\begin{aligned} \Lambda^2(\mathbf{X}) &= (|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10|) \otimes \mathbf{I} + |11\rangle\langle 11| \otimes \mathbf{X} \\ \Lambda^2(\mathbf{Z}) &= (|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10|) \otimes \mathbf{I} + |11\rangle\langle 11| \otimes \mathbf{Z} \\ \Rightarrow \Lambda^2(\mathbf{X})\Lambda^2(\mathbf{Z}) &= (|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10|) \otimes \mathbf{I} + |11\rangle\langle 11| \otimes \mathbf{XZ} \\ &= \Lambda^2(\mathbf{XZ}) \end{aligned} \tag{24}$$

Then, as shown in part(c), we can construct $\Lambda^2(\mathbf{Z})$ using the Toffoli gate and the Hadamard gate: $\Lambda^2(\mathbf{Z}) = (\mathbf{I}\otimes\mathbf{H})\Lambda^2(\mathbf{X})(\mathbf{I}\otimes\mathbf{H})$. Therefore, $\Lambda^2(\mathbf{XZ}) = \Lambda^2(\mathbf{X})\Lambda^2(\mathbf{Z}) = \Lambda^2(\mathbf{X})(\mathbf{I}\otimes\mathbf{H})\Lambda^2(\mathbf{X})(\mathbf{I}\otimes\mathbf{H})$. Schematically,



Problem 3.4

(a) Recall that the action of the **SWAP** gate on the computational basis is given by

$$\mathbf{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{25}$$

Writing out $\mathbf{X}\otimes\mathbf{X} + \mathbf{Y}\otimes\mathbf{Y} + \mathbf{Z}\otimes\mathbf{Z}$ in the computational basis, we see that,

$$\mathbf{X}\otimes\mathbf{X} + \mathbf{Y}\otimes\mathbf{Y} + \mathbf{Z}\otimes\mathbf{Z} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 2 & 0 \\ 0 & 2 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = 2(\mathbf{SWAP}) - \mathbf{I}_4 \tag{26}$$

where $\mathbf{I}_4$ is the 4×4 identity matrix. Therefore,

$$\begin{aligned}
\mathbf{V}(\frac{\pi}{4}, \frac{\pi}{4}, \frac{\pi}{4}) &= \exp[\, i\frac{\pi}{4}(\mathbf{X}\otimes\mathbf{X} + \mathbf{Y}\otimes\mathbf{Y} + \mathbf{Z}\otimes\mathbf{Z})\,] \\
&= \exp[\, i\frac{\pi}{4}(2\mathbf{SWAP} - \mathbf{I}_4)\,] \\
&= e^{-i\frac{\pi}{4}}\exp[\, i\frac{\pi}{2}\mathbf{SWAP}] \\
&= e^{-i\frac{\pi}{4}}[\, (\cos\frac{\pi}{2})\mathbf{I} + i(\sin\frac{\pi}{2})\mathbf{SWAP}\,] \\
&= e^{i\frac{\pi}{4}}\mathbf{SWAP} \qquad (27)
\end{aligned}$$

In the penultimate step, we have used the identity $e^{i\theta\mathbf{A}} = (\cos\theta)\mathbf{I} + i(\sin\theta)\mathbf{A}$ for any real θ and any $\mathbf{A}$ such that $(\mathbf{A})^2 = \mathbf{I}$.
Thus, upto an overall phase, $\mathbf{V}(\frac{\pi}{4}, \frac{\pi}{4}, \frac{\pi}{4})$ is simply the **SWAP** operation.

(b) Writing down $\mathbf{V}(0, 0, \frac{\pi}{4})$ in the computational basis, we have,

$$\begin{aligned}
\mathbf{V}(0, 0, \frac{\pi}{4}) &= \exp[\, i\frac{\pi}{4}\mathbf{Z}\otimes\mathbf{Z}] \\
&= e^{i\frac{\pi}{4}}\mathrm{diag}(1, -i, -i, 1) \\
&= e^{i\frac{\pi}{4}}(|0\rangle\langle 0|\otimes\mathbf{P}^{-1} - i\,|1\rangle\langle 1|\otimes\mathbf{P}) \qquad (28)
\end{aligned}$$

Then,

$$\begin{aligned}
e^{-i\frac{\pi}{4}}(\mathbf{P}\otimes\mathbf{P})\mathbf{V}(0, 0, \frac{\pi}{4}) &= |0\rangle\langle 0|\otimes\mathbf{I} + |1\rangle\langle 1|\otimes\mathbf{P}^2 \\
&= \Lambda(\mathbf{Z}) \qquad (29)
\end{aligned}$$

since $\mathbf{P}^2 = \mathbf{Z}$. Now to get the CNOT operation, we simply conjugate with the Hadamard gate, so that

$$\Lambda(\mathbf{X}) = e^{-i\frac{\pi}{4}}(\mathbf{I}\otimes\mathbf{H})(\mathbf{P}\otimes\mathbf{P})\mathbf{V}(0, 0, \frac{\pi}{4})(\mathbf{I}\otimes\mathbf{H}) \qquad (30)$$

showing that $\mathbf{V}(0, 0, \frac{\pi}{4})$ is indeed locally equivalent to $\Lambda(\mathbf{X})$.

(c) Given any operator $\mathbf{A}$ and a unitary $\mathbf{U}$,

$$\mathbf{U}e^{i\mathbf{A}}\mathbf{U}^\dagger = e^{\mathbf{U}(i\mathbf{A})\mathbf{U}^\dagger} \qquad (31)$$

Since the Pauli operators are unitary, we can use this identity to get,

$$\begin{aligned}
(\mathbf{I}\otimes\mathbf{X})\mathbf{V}(\theta_x, \theta_y, \theta_z)(\mathbf{I}\otimes\mathbf{X})\mathbf{V}(\theta_x, \theta_y, \theta_z) &= \exp[\, i(\mathbf{I}\otimes\mathbf{X})(\theta_x\mathbf{X}\otimes\mathbf{X} + \theta_y\mathbf{Y}\otimes\mathbf{Y} + \theta_z\mathbf{Z}\otimes\mathbf{Z})(\mathbf{I}\otimes\mathbf{X})\,]\mathbf{V} \\
&= \exp[\, i(\theta_x\mathbf{X}\otimes\mathbf{X} + \theta_y\mathbf{Y}\otimes\mathbf{XYX} + \theta_z\mathbf{Z}\otimes\mathbf{XZX})\,]\mathbf{V} \\
&= \exp[\, i(\theta_x\mathbf{X}\otimes\mathbf{X} - \theta_y\mathbf{Y}\otimes\mathbf{Y} - \theta_z\mathbf{Z}\otimes\mathbf{Z})\,]\mathbf{V}(\theta_x, \theta_y, \theta_z) \\
&= \mathbf{V}(\theta_x, -\theta_y, -\theta_z)\mathbf{V}(\theta_x, \theta_y, \theta_z) \\
&= \mathbf{V}(2\theta_x, 0, 0) \qquad (32)
\end{aligned}$$

Similarly, we can show,

$$\begin{aligned}
(\mathbf{I}\otimes\mathbf{Y})\mathbf{V}(\theta_x, \theta_y, \theta_z)(\mathbf{I}\otimes\mathbf{Y})\mathbf{V}(\theta_x, \theta_y, \theta_z) &= \mathbf{V}(0, 2\theta_y, 0) \\
(\mathbf{I}\otimes\mathbf{Z})\mathbf{V}(\theta_x, \theta_y, \theta_z)(\mathbf{I}\otimes\mathbf{Z})\mathbf{V}(\theta_x, \theta_y, \theta_z) &= \mathbf{V}(0, 0, 2\theta_z) \qquad (33)
\end{aligned}$$

(d) Once again, working in the computational basis,

$$\begin{aligned}\mathbf{V}(0,0,\theta) &= \exp[i\theta\mathbf{Z}\otimes\mathbf{Z}] = \mathrm{diag}(e^{i\theta}, e^{-i\theta}, e^{-i\theta}, e^{i\theta}) \\ &= |0\rangle\langle 0| \otimes \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix} + |1\rangle\langle 1| \otimes \begin{pmatrix} e^{-i\theta} & 0 \\ 0 & e^{i\theta} \end{pmatrix} \end{aligned} \tag{34}$$

Let

$$\Theta = \begin{pmatrix} e^{-i\theta} & 0 \\ 0 & e^{i\theta} \end{pmatrix} \tag{35}$$

Then, equation(34) implies

$$\begin{aligned}[\mathbf{I}\otimes\Theta]\mathbf{V}(0,0,\theta) &= |0\rangle\langle 0| \otimes \mathbf{I} + |1\rangle\langle 1| \otimes \begin{pmatrix} e^{-2i\theta} & 0 \\ 0 & e^{2i\theta} \end{pmatrix} \\ &= |0\rangle\langle 0| \otimes \mathbf{I} + |1\rangle\langle 1| \otimes \mathbf{R}(\hat{z}, 4\theta) \\ \Rightarrow (\mathbf{I}\otimes\Theta)\mathbf{V}(0,0,\theta) &= \Lambda[\mathbf{R}(\hat{z}, 4\theta)] \end{aligned} \tag{36}$$

where $\mathbf{R}(\hat{z}, 4\theta) = e^{-2i\theta\mathbf{Z}}$ is a rotation about the $\hat{z}$ axis. This shows an equivalence between $\mathbf{V}(0,0,\theta)$ and $\Lambda[\mathbf{R}(\hat{z}, 4\theta)]$ ie. a controlled rotation by 4θ about the $\hat{z}$ axis. Now to get a controlled rotation about an arbitrary axis $\hat{n}$, we need to conjugate by a unitary that rotates between the eigenvectors of $\hat{z}.\vec{\sigma}$ $(= \mathbf{Z})$ and $\hat{n}.\vec{\sigma}$. If $|\hat{n}, +\rangle$ and $|\hat{n}, -\rangle$ denote the eigenvectors of $\hat{n}.\sigma$, the required unitary operation is

$$\mathbf{U}_{\hat{n}} = |\hat{n}, +\rangle\langle 0| + |\hat{n}, -\rangle\langle 1| \tag{37}$$

so that

$$\begin{aligned}\mathbf{U}_{\hat{n}}\mathbf{R}(\hat{z}, 4\theta)\mathbf{U}_{\hat{n}}^{\dagger} &= \mathbf{U}_{\hat{n}} \begin{pmatrix} e^{-2i\theta} & 0 \\ 0 & e^{2i\theta} \end{pmatrix} \mathbf{U}_{\hat{n}}^{\dagger} \\ &= e^{-2i\theta}|\hat{n}, +\rangle\langle\hat{n}, +| + e^{2i\theta}|\hat{n}, -\rangle\langle\hat{n}, -| \\ &= \mathbf{R}(\hat{n}, 4\theta) \end{aligned} \tag{38}$$

Thus, conjugating both sides of equation(36) with $\mathbf{I}\otimes\mathbf{U}_{\hat{n}}$, we have,

$$(\mathbf{I}\otimes\mathbf{U}_{\hat{n}})(\mathbf{I}\otimes\Theta)\mathbf{V}(0,0,\theta)(\mathbf{I}\otimes\mathbf{U}_{\hat{n}}^{\dagger}) = \Lambda[\mathbf{R}(\hat{n}, 4\theta)] \tag{39}$$

showing that $\mathbf{V}(0,0,\theta)$ is indeed locally equivalent to a controlled rotation about an arbitrary axis on the Bloch sphere.

(e) We know from parts (c) and (d) that any 2-qubit, entangling gate of the form $\mathbf{V}(\theta_x, \theta_y, \theta_z)$ can be used, in combination with single qubit unitaries to realize a gate of the form $\mathbf{V}(0,0,2\theta_z)$. Further, this is locally equivalent to $\Lambda[\mathbf{R}(\hat{z}, 4\theta_z)]$, a controlled rotation by $2\theta_z$ about the z-axis. Now, to prove the Lemma, let us consider the following two cases:
(i) $\pi/4$ is an integral multiple of $2|\theta_z|$:-
In this case, $2q|\theta_z| = \pi/4$ for some positive integer q, and the Lemma is proved trivially -

$$\begin{aligned}\mathbf{V}(\theta_x, \theta_y, \theta_z) &\equiv \Lambda[\mathbf{R}(\hat{z}, 4\theta_z)] \\ &\rightarrow \ (q \text{ times}) \ \Lambda^q[\mathbf{R}(\hat{z}, 4\theta_z)] = \Lambda[\mathbf{R}(\hat{z}, 4q\theta_z)] \\ &= \Lambda[\mathbf{R}(\hat{z}, \pi/2)] \equiv \mathbf{V}(0, 0, \frac{\pi}{2}) \\ &\equiv \Lambda(\mathbf{X}) \ \text{ (from part(b))} \end{aligned} \tag{40}$$

where $\equiv$ implies that two gates are locally equivalent.

(ii) $\pi/4$ is not an integral multiple of $2|\theta_z|$:-
In this case, we need to use another gate to make up for the difference. Let $q = [\,\pi/8|\theta_z|\,]$, where [.] denotes the greatest integer function. Then, we need to implement $\Lambda[\mathbf{R}(\hat{z},\alpha)]$, ie. a controlled rotation by $0 < |\alpha| = \pi/4 - 2q|\theta_z| < 2|\theta_z|$ about the z-axis, to realize $\Lambda(\mathbf{X})$.
To construct such a gate, first note that the product of two controlled rotations $\Lambda[\mathbf{R}(\hat{n},\theta)]$ and $\Lambda[\mathbf{R}(\hat{n'},\theta')]$ is also a controlled rotation whose axis of rotation and magnitude depends on $\hat{n}, \hat{n'}, \theta$, and θ'. Thus, if we construct the gate $\Lambda[\mathbf{R}(\hat{n},\theta_z)]$ for some arbitrary axis $\hat{n}$ (as described in part(d)), the product $\Lambda[\mathbf{R}(\hat{z},\theta_z)]\Lambda[\mathbf{R}(\hat{n},\theta_z)]$ is a controlled rotation $\Lambda[\mathbf{R}(\hat{m},\alpha)]$, whose axis of rotation $\hat{m}$ and angle of rotation α are given by

$$\begin{aligned} \cos(\alpha) &= \cos^2(\theta_z) - \sin^2(\theta_z)\hat{z}.\hat{n} \\ \sin(\alpha)\hat{m} &= \sin(\theta_z)\cos(\theta_z)(\hat{z}+\hat{n}) - \sin^2(\theta_z)(\hat{n}\otimes\hat{z}) \end{aligned} \tag{41}$$

For a given θ_z, α varies continuously as a function of $\hat{n}$. Then, by the Intermediate Value Theorem[1], it takes all possible values in the interval $[0, 2\theta_z]$. It is therefore possible to choose $\hat{n}$ such that we get the desired angle of rotation, $\alpha = \pi/4 - 2q|\theta_z|$. Finally, to rotate the axis of rotation from $\hat{m}$ to the z-axis, we need to implement the local unitary $\mathbf{U}^\dagger_{\hat{m}}$, which was defined in equation(37) above. To summarize,

$$\begin{aligned} \mathbf{V}(\theta_x,\theta_y,\theta_z) &\equiv \Lambda[\mathbf{R}(\hat{z},\theta_z)] \equiv \Lambda[\mathbf{R}(\hat{n},\theta_z)] \\ (\mathbf{I}\otimes\mathbf{U}^\dagger_{\hat{m}})\Lambda[\mathbf{R}(\hat{z},\theta_z)]\Lambda[\mathbf{R}(\hat{n},\theta_z)](\mathbf{I}\otimes\mathbf{U}_{\hat{m}}) &= (\mathbf{I}\otimes\mathbf{U}^\dagger_{\hat{m}})\Lambda[\mathbf{R}(\hat{m},\alpha)](\mathbf{I}\otimes\mathbf{U}_{\hat{m}}) \\ &= \Lambda[\mathbf{R}(\hat{z},\frac{\pi}{4}-2q|\theta_z|)] \end{aligned} \tag{42}$$

Putting together cases (i) and (ii), we see that

$$\begin{aligned} \Lambda(\mathbf{X}) &\equiv \Lambda[\mathbf{R}(\hat{z},\frac{\pi}{2})] \\ &= \Lambda[\mathbf{R}(\hat{z},4q\theta_z)]\Lambda[\mathbf{R}(\hat{z},\frac{\pi}{4}-2q|\theta_z|)] \\ &= \Lambda^q[\mathbf{R}(\hat{z},4\theta_z)](\mathbf{I}\otimes\mathbf{U}^\dagger_{\hat{m}})\Lambda[\mathbf{R}(\hat{z},\theta_z)]\Lambda[\mathbf{R}(\hat{n},\theta_z)](\mathbf{I}\otimes\mathbf{U}_{\hat{m}}) \\ &\equiv \Lambda^q[\mathbf{R}(\hat{z},4\theta_z)]\Lambda[\mathbf{R}(\hat{z},\theta_z)]\Lambda[\mathbf{R}(\hat{n},\theta_z)] \end{aligned} \tag{43}$$

for an appropriate choice of $\hat{n}$, obtained by solving equations(41). The gates in the final step are all locally equivalent to a generic 2-qubit gate of the form $\mathbf{V}(\theta_x,\theta_y,\theta_z)$ (provided $\theta_x = \theta_y = \theta_z) \neq \{0, \frac{\pi}{4}\}$), thus proving the Lemma!

Problem3 3.5

a) A problem of size n is in BQP if there exists a polynomial-size uniform circuit family that depends on n, where for each such circuit the state for the first output qubit is $|0\rangle$ (resp. $|1\rangle$)

[1]Suppose that $f : [a,b] \to \mathbb{R}$ is continuous and that u is a real number satisfying $f(a) < u < f(b)$ or $f(a) > u > f(b)$. Then for some $c \in [a,b], f(c) = u$

with probability at least 2/3 if the correct answer is 0 (resp. 1). Recall that, according to our model, the input qubits to each circuit are prepared in the standard state $|0\rangle^{\otimes n}$ which we will denote as $|0\rangle$ for simplicity. If U is the unitary implemented by the quantum circuit, the output state is therefore $U|0\rangle$. Let P_0 be the projector onto the state $(|0\rangle\langle 0|)_1$ on the first qubit. Then, the probability of obtaining the outcome 0 after measuring the first output qubit is

$$P(0) = \langle 0|U^\dagger (P_0 \otimes I_{n-1}) U|0\rangle \ . \tag{44}$$

where I_{n-1} is the identity operator acting on all qubits except for the first.

We can now view $V = U^\dagger (P_0 \otimes I_{n-1})U$ as a new matrix, so that the classical simulation of the quantum computation executed by U reduces to the calculation of the matrix element $\langle 0|V|0\rangle$. We note that V consists first of the unitary U, then of the projector onto the $|0\rangle$ state on the first qubit, and finally of the inverse of the quantum circuit U^{-1}. This is reminiscent of the idea used by Bennett to show that reversible classical computation (i.e., computation in which no "junk" bits are produced and which can be performed with zero thermodynamic cost) is possible.

b) We can write $V = V_L \dots V_2 V_1$ where each V_i is either a Hadamard gate (H), or a Toffoli gate ($\Lambda(X)$), or a projection P_0 tensored with the identity on all qubits on which it acts trivially. Therefore, our classical simulation will need to compute the matrix element $\langle 0|V_L \dots V_2 V_1|0\rangle$.

For every Toffoli gate in this expression, we can insert the identity in the form $I = H^2$ following it on its target qubit. This way we obtain a new V, say V', of size $S \leq 2L$, and let us denote by h the number of Hadamard gates it contains. Then we need to compute

$$P(0) = \frac{1}{\sqrt{2^h}} \langle 0|V'_S \dots V'_2 V'_1|0\rangle \ , \tag{45}$$

where for every Hadamard gate in V' we have collected the $1/\sqrt{2}$ normalization in front of the expression and replaced the corresponding gate $V'_a = H$ by the gate $V'_a = \sqrt{2}H$.

We now note that $\sqrt{2}H$ acts in the computation basis as

$$\sqrt{2}H \ : \ |i\rangle \mapsto \sum_{j=0}^{1} (-1)^{ij} |j\rangle \ . \tag{46}$$

Similarly, for the Toffoli gate

$$\Lambda(X) \ : \ |i,j,k\rangle \mapsto |i,j,k \oplus ij\rangle \ , \tag{47}$$

which, when combined with the two Hadamard gates following it by the construction of V', becomes

$$\begin{aligned} (I \otimes I \otimes H)\Lambda(X) \quad &: \quad |i,j,k\rangle \mapsto \sum_{l=0}^{1} (-1)^{(k\oplus ij)l} |i,j,l\rangle \ , \\ (I \otimes I \otimes H^2)\Lambda(X) \quad &: \quad |i,j,k\rangle \mapsto \sum_{l=0}^{1} \sum_{m=0}^{1} (-1)^{(k\oplus ij\oplus m)l} |i,j,m\rangle \ . \end{aligned} \tag{48}$$

The result now follows. The initial state is a state in the computation basis (i.e., all qubits in the state $|0\rangle$). For every Hadamard gate initially in V, we can use Eq. (46) to generate a new

index and express the output state in the computation basis. For every $\Lambda(X)$ gate initially in V, we can group it with the two Hadamard gates we inserted to obtains V' and use Eq. (48) to generate two new indices. At the end of the computation we "project" onto the $|0\rangle$ state, so that all free indices at that point are forced to take the value 0. Thus we have reduced the calculation of $P(0)$ in Eq. (45) to the calculation of a sum over $h \leq 2L$ intermediate binary indices of the form

$$P(0) = \frac{1}{\sqrt{2^h}} \sum_x (-1)^{\phi(x)} \; , \tag{49}$$

where x is a binary vector with the h intermediate indices as components and $\phi(x)$ is a polynomial of degree at most three in the intermediate indices. If N_0 (resp. N_1) is the number of values of x for which $\phi(x) = 0$ (resp. $\phi(x) = 1$), it follows that

$$P(0) = \frac{1}{\sqrt{2^h}} (N_0 - N_1) \; . \tag{50}$$