NIELSEN & CHUANG EXERCISES

FARIS SBAHI

Contents

1. Chapter 2: Quantum Mechanics 1
2. Chapter 4: Quantum Circuits 10
2.1. Action by Hadamard on the Bloch Sphere 10
3. Chapter 5 18
4. Chapter 6: Quantum Search Algorithms 19
5. Chapter 11: Entropy and Information 20

1. Chapter 2: Quantum Mechanics

Exercise 1.1. *(2.11) Find the eigenvectors and eigenvalues of the Pauli matrices.*

Proof.

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$
$$X - \lambda I = \begin{bmatrix} -\lambda & 1 \\ 1 & -\lambda \end{bmatrix}$$
$$\lambda^2 - 1 = 0$$
$$\lambda_{\pm} = \pm 1$$
$$\begin{bmatrix} -1 & 1 \\ 1 & -1 \end{bmatrix} v_+ = 0$$
$$\Rightarrow v_+ = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$
$$\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} v_- = 0$$
$$\Rightarrow v_- = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$$

Similarly, Y has eigenvalues ± 1 with respective eigenvectors $\left\{ \begin{bmatrix} 1 \\ i \end{bmatrix}, \begin{bmatrix} 1 \\ -i \end{bmatrix} \right\}$. Z has eigenvalues ± 1 with respective eigenvectors $\left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\}$ □

Exercise 1.2. *(2.51) Verify that H is unitary*

$$\begin{aligned} HH^\dagger &= 1/2\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\\ &= 1/2\begin{pmatrix}2 & 0\\ 0 & 2\end{pmatrix}\\ &= I = H^\dagger H\end{aligned}$$

Exercise 1.3. *(2.52) Verify that $H^2 = I$*
Because H is hermitian we have that

$$\begin{aligned} H^2 &= HH^\dagger\\ &= I\end{aligned}$$

from H being unitary.

Exercise 1.4. *(2.53) What are the eigenvalues and eigenvectors of H?*

$$\begin{aligned} \det\frac{1}{\sqrt{2}}\begin{pmatrix}1-\lambda & 1\\ 1 & -1-\lambda\end{pmatrix} &= -(1-\sqrt{2}\lambda)(1+\sqrt{2}\lambda)-1=0\\ &= -1+2\lambda^2-1\\ \lambda &= \pm 1\\ \frac{1}{\sqrt{2}}\begin{pmatrix}1-\sqrt{2} & 1\\ 1 & -1+\sqrt{2}\end{pmatrix}v_1 &= 0\\ (1-\sqrt{2})v_{11}+v_{12} &= 0\\ v_{11}-(1-\sqrt{2})v_{12} &= 0\\ v_1 &= \begin{pmatrix}1+\sqrt{2}\\ 1\end{pmatrix}\\ \frac{1}{\sqrt{2}}\begin{pmatrix}1+\sqrt{2} & 1\\ 1 & -1-\sqrt{2}\end{pmatrix}v_2 &= 0\\ v_2 &= \begin{pmatrix}1-\sqrt{2}\\ 1\end{pmatrix}\end{aligned}$$

Exercise 1.5. *(2.54) Suppose $[A,B]=0$ and A,B are Hermitian. Prove that* $\exp(A)\exp(B) = \exp(A+B)$

Proof. From Theorem 2.2, A and B are simultaneously diagonalizable. Hence, there is a common set of orthonormal eigenvectors $\{|i\rangle\}$. Hence,
$A = \sum_i a_i |i\rangle\langle i|, B = \sum_i b_i |i\rangle\langle i|$. So,

$$\exp(A)\exp(B) = \sum_{k'=0}^{\infty}\sum_{i'}\frac{(b_{i'}|i'\rangle\langle i'|)^{k'}}{k'!}\sum_{k=0}^{\infty}\sum_{i}\frac{(a_i|i\rangle\langle i|)^k}{k!}$$

By orthonormality,

$$\begin{aligned}
&= \sum_i \Big[\sum_{k'=0}^{\infty} \frac{b_i^{k'} \left|i\right\rangle \left\langle i\right|}{k'!} \sum_{k=0}^{\infty} \frac{a_i^k \left|i\right\rangle \left\langle i\right|}{k!} \Big] \\
&= \sum_i \sum_{k'=0}^{\infty} \sum_{k=0}^{\infty} \frac{a_i^k b_i^{k'} \left|i\right\rangle \left\langle i\right|}{k!k'!} \\
&= \sum_i \sum_{l=0}^{\infty} \sum_{k=0}^{l} \frac{a_i^k b_i^{l-k} \left|i\right\rangle \left\langle i\right|}{k!(l-k)!} \\
&= \sum_i \sum_{l=0}^{\infty} \frac{1}{l!} \sum_{k=0}^{l} \binom{k}{l} a_i^k b_i^{l-k} \left|i\right\rangle \left\langle i\right| \\
&= \sum_i \sum_{l=0}^{\infty} \frac{(a_i + b_i)^l}{l!} \left|i\right\rangle \left\langle i\right| \\
&= \exp(A+B)
\end{aligned}$$

□

Exercise 1.6. *(2.56) Use the spectral decomposition to show that $K \coloneqq -i \log U$ is Hermitian for any unitary U and thus $U = \exp(iK)$ for some Hermitian K*

Proof. The eigenvalues of U can be given as $\exp(i\theta)$ by unitary. Furthermore, from spectral theorem, U is diagonalizable as $U = V\Lambda V^\dagger$ where V is unitary[1]. Hence, $U = V\Lambda V^\dagger$ where diagonal matrix Λ has elements of the form $\exp(i\theta)$ across the diagonal.

Furthermore, $(V\Lambda V^\dagger)^n = V\Lambda V^\dagger V\Lambda V^\dagger \cdots V\Lambda V^\dagger = V\Lambda^n V^\dagger \Rightarrow \exp\big(V\Lambda V^\dagger\big) = V\exp(\Lambda)V^\dagger$. Therefore, let $\Lambda' = \log(\Lambda)$ which therefore has elements of the form $i\theta$. Hence, $U = \exp\big(V\Lambda' V^\dagger\big)$

$$\begin{aligned}
K &= -i\log U \\
&= -i\log\big(\exp\big(V\Lambda' V^\dagger\big)\big) \\
&= -iV\Lambda' V^\dagger \\
&= V\Theta V^\dagger
\end{aligned}$$

where $\Theta = -i\Lambda'$ has elements of the form θ (and hence the elements are real along the diagonal and zero elsewhere $\Rightarrow \Theta^\dagger = \Theta$). Therefore, $K^\dagger = V^\dagger \Theta^\dagger V = V\Theta V^\dagger = K$. □

Exercise 1.7. *(2.55) Prove that $U(t_1, t_2)$ is unitary*

Proof. Using the result of 2.54,

$$\begin{aligned}
UU^\dagger = U^\dagger U &= \exp\left[\frac{-iH(t_2 - t_1)}{\hbar}\right] \exp\left[\frac{iH(t_2 - t_1)}{\hbar}\right] \\
&= \exp\big(\hat{0}\big) \\
&= I
\end{aligned}$$

□

[1] Quick proof: U can be written as $U = VTV^\dagger$ where V is unitary and T is upper triangular by Schur Decomposition. However, $UU^\dagger = U^\dagger U, VV^\dagger = I = V^\dagger V \Rightarrow T$ is normal $\Rightarrow T$ is diagonal.

Exercise 1.8. *(2.57) Suppose $\{L_l\}$ and $\{M_m\}$ are two sets of measurement operators. Show that a measurement defined by the measurement operators $\{L_l\}$ followed by a measurement defined by the measurement operators $\{M_m\}$ is physically equivalent to a single measurement defined by measurement operators $\{N_{lm}\}$ with the representation $N_{lm} = M_m L_l$.*

Proof. Let $|\varphi\rangle$ be our initial state and recall that if l is measured then the post-measurement state is given by $\frac{L_l|\psi\rangle}{\sqrt{p(l)}}$. Furthermore, if we then measure m we have $\frac{M_m(L_l|\psi\rangle)}{\sqrt{p(m)}\sqrt{p(l)}} = \frac{N_{lm}|\psi\rangle)}{\sqrt{p(m)p(l)}}$.

Now,

$$\begin{aligned} p(m)p(l) &= \langle\psi| L_l^\dagger L_l |\psi\rangle \frac{\langle\psi| L_l^\dagger}{\sqrt{p(m)}} M_m^\dagger M_m \frac{L_l|\psi\rangle}{\sqrt{p(m)}} \\ &= p(l)\frac{\langle\psi| L_l^\dagger M_m^\dagger M_m L_l |\psi\rangle}{p(l)} \\ &= \langle\psi| N_{lm}^\dagger N_{lm} |\psi\rangle \\ &= p(lm) \end{aligned}$$

Hence, $\frac{N_{lm}|\psi\rangle}{\sqrt{p(m)p(l)}} = \frac{N_{lm}|\psi\rangle}{\sqrt{p(lm)}}$. Therefore, the representation is physically equivalent. □

Exercise 1.9. *(2.58) Suppose we prepare a quantum system in an eigenstate $|\psi\rangle$ of some observable M, with corresponding eigenvalue m. What is the average observed value of m and the standard deviation?*

Proof. First,

$$\begin{aligned} \langle M\rangle &= \langle\psi| M |\psi\rangle \\ &= \langle\psi| m |\psi\rangle = m \end{aligned}$$

Furthermore,

$$\begin{aligned} \langle M^2\rangle - \langle M\rangle^2 &= \langle\psi| M^2 |\psi\rangle - m^2 \\ &= \langle\psi| M^\dagger M |\psi\rangle - m^2 \\ &= m^2 - m^2 = 0 \end{aligned}$$

□

Exercise 1.10. *(2.59) Suppose we have a qubit in the state $|0\rangle$, and we measure the observable X. What is the average value of X? What is the standard deviation of X?*

Proof. X has eigenvalues $+1$ and -1 and eigenstates $|+\rangle$ and $|-\rangle$, respectively. Hence,

$$\begin{aligned} \langle X\rangle &= \langle\psi| X |\psi\rangle \\ &= \langle\psi| (|+\rangle\langle+| - |-\rangle\langle-|) |\psi\rangle \\ &= \langle 0|+\rangle\langle+|0\rangle - \langle 0|-\rangle\langle-|0\rangle \\ &= \frac{1}{2} - \frac{1}{2} = 0 \end{aligned}$$

Furthermore,

$$\begin{aligned}\langle M^2\rangle - \langle M\rangle^2 &= \langle\psi| M^2 |\psi\rangle - 0 \\ &= \langle\psi| \left(|+\rangle\langle+| + |-\rangle\langle-|\right) |\psi\rangle \\ &= \frac{1}{2} + \frac{1}{2} = 1\end{aligned}$$

□

Exercise 1.11. *(2.60) Show that $v \cdot \sigma$ has eigenvalues ± 1 and that the projectors onto the corresponding eigenspaces are given by $P_\pm = (I \pm v \cdot \sigma)/2$.*

Proof. First, $v \cdot \sigma$ is Hermitian so it's spectral decomposition is given by $v \cdot \sigma = U\Lambda U^\dagger$ for some unitary U, diagonal matrix Λ. Hence, using $(v \cdot \sigma)^2 = I$ we have

$$\begin{aligned} I = (v\cdot\sigma)^2 &= (U\Lambda U^\dagger)^2 \\ &= U\Lambda^2 U^\dagger \\ \Rightarrow U^\dagger I U &= \Lambda^2 \\ I &= \Lambda^2\end{aligned}$$

Therefore, Λ must have diagonal entries ± 1.

Next, $P_i P_j = \delta_{ij} P_j$ since if $i \neq j$ then $(I + v\cdot\sigma)(I - v\cdot\sigma) = I - (v\cdot\sigma)^2 = I - I = 0$. Furthermore, $P_+ + P_- = (I + v\cdot\sigma)/2 + (I - v\cdot\sigma)/2 = I$.

Finally, $(+1)P_+ + (-1)P_- = (I + v\cdot\sigma)/2 - (I - v\cdot\sigma)/2 = v\cdot\sigma$. □

Exercise 1.12. *(2.61) Calculate the probability of obtaining result $+1$ for a measurement of $v \cdot \sigma$, given that the state prior to measurement is $|0\rangle$. What is the state of the system after measurement if $+1$ is obtained?*

Proof. First,

$$\begin{aligned} p(+1) &= \langle\psi| P_+ |\psi\rangle \\ &= \langle\psi| (I + v\cdot\sigma)/2 |\psi\rangle \\ &= 1 + \frac{1}{2}[v_1 \langle 0| X |0\rangle + v_2 \langle 0| Y |0\rangle + v_3 \langle 0| Z |0\rangle] \\ &= 1 + \frac{1}{2}[v_1 \langle 0|1\rangle + iv_2 \langle 0|1\rangle + v_3 \langle 0|0\rangle] \\ &= 1 + \frac{v_3}{2}\end{aligned}$$

Furthermore, after measurement of $+1$ we have

$$\begin{aligned}(I + v\cdot\sigma)/2 |0\rangle &= |0\rangle + \frac{1}{2}[v_1 |1\rangle + iv_2 |1\rangle + v_3 |0\rangle] \\ &= \left[\left(\frac{v_3}{2} + 1\right)|0\rangle + \frac{v_1 + iv_2}{2} |1\rangle\right] / \sqrt{1 + \frac{v_3}{2}}\end{aligned}$$

□

Exercise 1.13. *(2.62) Show that any measurement where the measurement operators and the POVM elements coincide is a projective measurement*

Proof. We would then have $M_m = E_m = M_m^\dagger M_m$. Furthermore, E_m is a positive operator $\Rightarrow$ $M_m = M_m^\dagger M_m = M_m M_m^\dagger = M_m^\dagger$ so M_m is Hermitian. Hence, $M_m = M_m^2$ so the measurement is projective. □

Exercise 1.14. *(2.63) Suppose a measurement is described by measurement operators M_m. Show that there exist unitary operators U_m such that $M_m = U_m\sqrt{E_m}$ where E_m is the POVM associated to the measurement.*

Proof. From SVD, we have that $M_m = UDV$ for U, V unitary and D real, diagonal. Hence,

$$\begin{aligned}\sqrt{E_m} &= \sqrt{M_m^\dagger M_m} = \sqrt{V^\dagger D U^\dagger U D V} \\ &= \sqrt{V^\dagger D^2 V} \\ &= V^\dagger D V = V^\dagger U^\dagger U D V \\ &= U_m^\dagger M_m\end{aligned}$$

where $U_m \coloneqq UV$. Therefore, there exists the unitary transformation of interest.

□

Exercise 1.15. *(2.64) Suppose Bob is given a quantum state chosen from a set $S = |\psi_1\rangle, \cdots, |\psi_m\rangle$ of linearly independent states. Construct a POVM $\{E_1, \cdots, E_{m+1}\}$ such that if outcome E_i occurs, $1 \leq i \leq m$, then Bob knows with certainty that he was given state $|\psi_i\rangle$.*

Proof. To distinguish the states we require $\langle\psi_i| E_j |\psi_i\rangle = p_i \delta_{ij}$ where $p_i > 0$ and $1 \leq i, j \leq m$.

So, we can use the Gram-Schmidt process using S as our linearly independent set. This will give us an orthonormal set $U = |\varphi_1\rangle, \cdots, |\varphi_m\rangle$ that spans the same subspace as S. Next, we can represent each $|\psi_i\rangle$ in this orthonormal basis, U. Finally, for each i we can find a vector $|\psi_i'\rangle$ in the span of U that is orthogonal to all $|\psi_j\rangle, j \neq i$. Hence, we can define $E_i = |\psi_i'\rangle\langle\psi_i'|, 1 \leq i \leq m$. Finally, take $E_{m+1} = I - \sum_m E_i$.

Creating an optimal POVM is much trickier (in the sense of minimizing the probability p_{m+1}). □

From this exercise, we see that POVMs present a reliable way to distinguish non-orthogonal (but linearly independent) states given that we allow for the slack of an "inconclusive" measurement (E_{m+1}).

Exercise 1.16. *(2.65) Express the states $(|0\rangle + |1\rangle)/\sqrt{2}$ and $(|0\rangle - |1\rangle)/\sqrt{2}$ in a basis in which they are not the same up to relative phase shift.*

Proof. Trivially, the $|+\rangle$ and $|-\rangle$ suffices as a basis where they are not the same up to relative phase shift. □

Exercise 1.17. *(2.66) Show that the average value of the observable $X_1 Z_2$ (X acting on the first qubit and Z on the second) for a two qubit system measured in the state $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$ is zero.*

Proof. Let observable $M = X_1 Z_2$. Hence,

$$\begin{aligned}\langle M\rangle &= \frac{\langle 00| + \langle 11|}{\sqrt{2}} M \frac{|00\rangle + |11\rangle}{\sqrt{2}} \\ &= \frac{\langle 00| + \langle 11|}{\sqrt{2}} \frac{X_1 |0\rangle Z_2 |0\rangle + X_1 |1\rangle Z_2 |1\rangle}{\sqrt{2}} \\ &= \frac{\langle 00| + \langle 11|}{\sqrt{2}} \frac{|1\rangle |0\rangle - |0\rangle |1\rangle}{\sqrt{2}} \\ &= 0\end{aligned}$$

□

Exercise 1.18. *(2.67)*

Exercise 1.19. *(2.68) Prove that $|\psi\rangle \neq |a\rangle |b\rangle$ for all single qubit state $|a\rangle$ and $|b\rangle$ where $|\psi\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$.*

Proof. First, decompose the qubit state in their basis, $|a\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$ and $|b\rangle = \beta_0 |0\rangle + \beta_1 |1\rangle$. Now, we prove by contradiction

$$\begin{aligned}|a\rangle |b\rangle &= \alpha_0\beta_0 |00\rangle + \alpha_0\beta_1 |01\rangle + \alpha_1\beta_0 |10\rangle + \alpha_1\beta_1 |11\rangle \\ &= \frac{|00\rangle + |11\rangle}{\sqrt{2}}\end{aligned}$$

which would imply that either α_0 or β_1 are zero in order to remove the $|01\rangle$ term. However, this would also remove either the $|00\rangle$ or $|11\rangle$ term, so we have a contradiction. □

Exercise 1.20. *(2.69) Verify that the Bell basis forms an orthonormal basis for the two qubit state space.*

Proof. Two qubit state space consists of states of the form $|\psi\rangle = a |00\rangle + b |01\rangle + c |10\rangle + d |11\rangle$. Evidently, $|00\rangle = \frac{\sqrt{2}}{2}\left[\frac{|00\rangle+|11\rangle}{\sqrt{2}} + \frac{|00\rangle-|11\rangle}{\sqrt{2}}\right], |01\rangle = \frac{\sqrt{2}}{2}\left[\frac{|10\rangle+|01\rangle}{\sqrt{2}} - \frac{-|10\rangle+|01\rangle}{\sqrt{2}}\right]$ and similarly for the others. Hence, we span the same space.

Furthermore, $\langle\beta_{00}|\beta_{00}\rangle = \frac{\langle 00|+\langle 11|}{\sqrt{2}} \frac{|00\rangle+|11\rangle}{\sqrt{2}} = (\langle 00|00\rangle + \langle 11|11\rangle)/2 = 1$. Also, $\langle\beta_{00}|\beta_{01}\rangle = \frac{\langle 00|+\langle 11|}{\sqrt{2}} \frac{|00\rangle-|11\rangle}{\sqrt{2}} = (\langle 00|00\rangle - \langle 11|11\rangle)/2 = 0$. The other combinations follow similarly.

Therefore, we have an orthonormal basis. □

Exercise 1.21. *(2.70) Suppose E is any positive operator acting on Alices qubit. Show that $\langle\psi| E \otimes I |\psi\rangle$ takes the same value when $|\psi\rangle$ is any of the four Bell states. Suppose some malevolent third party ('Eve') intercepts Alices qubit on the way to Bob in the superdense coding protocol. Can Eve infer anything about which of the four possible bit strings 00, 01, 10, 11 Alice is trying to send? If so, how, or if not, why not?*

Proof.

$$\begin{aligned}
\langle 00| + \langle 11| (E \otimes I) |00\rangle + |11\rangle &= \langle 0| E |0\rangle + \langle 1| E |1\rangle \\
\langle 00| - \langle 11| (E \otimes I) |00\rangle - |11\rangle &= \langle 0| E |0\rangle + \langle 1| E |1\rangle \\
\langle 10| + \langle 01| (E \otimes I) |10\rangle + |01\rangle &= \langle 0| E |0\rangle + \langle 1| E |1\rangle \\
-\langle 10| + \langle 01| (E \otimes I) - |10\rangle + |01\rangle &= \langle 0| E |0\rangle + \langle 1| E |1\rangle
\end{aligned}$$

Hence, Eve can't infer anything. The states are only distinguishable if one can perform a measurement that acts on both qubits. □

Exercise 1.22. *(2.71) Let ρ be a density operator. Show that $\mathrm{tr}(\rho^2) \leq 1$ with equality iff ρ is a pure state.*

Proof.

$$\begin{aligned}
\rho^2 &= \sum_i p_i |\psi_i\rangle \langle\psi_i| \sum_{i'} p_{i'} |\psi_{i'}\rangle \langle\psi_{i'}| \\
&= \sum_i p_i^2 |\psi_i\rangle \langle\psi_i|
\end{aligned}$$

by orthonormality. Hence,

$$\mathrm{tr}\, \rho^2 = \sum_i \sum_j p_i^2 \psi_{i,jj}^2$$

And $\sum_j \psi_{i,jj}^2 = 1$ by normalization

$$= \sum_i p_i^2$$

Now, we have that $\sum_i p_i = 1 \Rightarrow \sum_i p_i^2 = 1 \Leftrightarrow p_i = 1$. If $p_i = 1$, then there is only one index and hence we have a pure state. Otherwise, $\sum_i p_i^2 < 1$ and we have a mixed state. □

Exercise 1.23. *(2.72) Bloch Sphere for mixed states.*
(1) Show that an arbitrary density matrix for a mixed state qubit can be written as

$$\rho = \frac{I + r \cdot \sigma}{2}$$

where r is a real 3-D vector such that $\|r\| \leq 1$. This vector is known as the Bloch vector for the state ρ.

Proof. Let ρ be an arbitrary density matrix, and so $\rho = \sum_i p_i |\psi_i\rangle \langle\psi_i|$. □

(2) What is the Bloch vector representation for the state $\rho = I/2$?
(3) Show that a state ρ is pure iff $\|r\| = 1$.

Proof. □

(4) Show that for pure states the description of the Bloch vector we have given coincides with that in Section 1.2

Proof. □

Exercise 1.24. *(2.73) Let ρ be a density operator. A minimal ensemble for ρ is an ensemble $\{p_i, |\psi_i\rangle\}$ containing a number of elements equal to the rank of ρ.*

Proof. □

Exercise 1.25. *(2.74) Suppose a composite of systems A and B is in state $|a\rangle|b\rangle$, where $|a\rangle$ is a pure state of system A and $|b\rangle$ is a pure state of system B. Show that the reduced density operator of system A alone is a pure state.*

Proof.

$$\rho = |a\rangle|b\rangle\langle a|\langle b|$$
$$\rho^A = |a\rangle\langle a|\langle b|b\rangle = |a\rangle\langle a|$$

where we were given that $|a\rangle$ is a pure state. □

Exercise 1.26. *(2.75) For each of the four Bell states, find the reduced density operator for each qubit*

Proof. First, $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$

$$\begin{aligned}
\rho &= \frac{|00\rangle + |11\rangle}{\sqrt{2}}\frac{\langle 00| + \langle 11|}{\sqrt{2}} \\
\rho^1 &= \frac{|0\rangle\langle 0|\langle 0|0\rangle + |1\rangle\langle 0|\langle 0|1\rangle + |0\rangle\langle 1|\langle 1|0\rangle + |1\rangle\langle 1|\langle 1|1\rangle}{2} \\
&= \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} = \frac{I}{2} \\
\rho^2 &= \frac{|0\rangle\langle 0|\langle 0|0\rangle + |1\rangle\langle 0|\langle 0|1\rangle + |0\rangle\langle 1|\langle 1|0\rangle + |1\rangle\langle 1|\langle 1|1\rangle}{2} \\
&= \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} = \frac{I}{2}
\end{aligned}$$

Next, $\frac{|00\rangle-|11\rangle}{\sqrt{2}}$

$$\begin{aligned}
\rho &= \frac{|00\rangle - |11\rangle}{\sqrt{2}}\frac{\langle 00| - \langle 11|}{\sqrt{2}} \\
\rho^1 &= \frac{|0\rangle\langle 0|\langle 0|0\rangle - |1\rangle\langle 0|\langle 0|1\rangle - |0\rangle\langle 1|\langle 1|0\rangle + |1\rangle\langle 1|\langle 1|1\rangle}{2} \\
&= \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} = \frac{I}{2} \\
\rho^2 &= \frac{|0\rangle\langle 0|\langle 0|0\rangle - |1\rangle\langle 0|\langle 0|1\rangle - |0\rangle\langle 1|\langle 1|0\rangle + |1\rangle\langle 1|\langle 1|1\rangle}{2} \\
&= \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} = \frac{I}{2}
\end{aligned}$$

The remaining two are similar. □

Exercise 1.27. *(2.76)*

Exercise 1.28. *(2.77)*

Exercise 1.29. *(2.78)*

Exercise 1.30. *(2.79)*

Exercise 1.31. *(2.80)*

Exercise 1.32. *(2.81)*

Exercise 1.33. *(2.82)*

2. Chapter 4: Quantum Circuits

Exercise 2.1. *(4.1) Find the points on the Bloch sphere which correspond to the normalized eigenvectors of the different Paul matrices.*

Proof. Recall that, from Exercise 2.11, X has eigenvalues ± 1 with respective eigevectors $\left\{\frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}, \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}\right\}$. Similarly, Y has eigenvalues ± 1 with respective eigenvectors $\left\{\frac{1}{\sqrt{2}}\begin{bmatrix}1\\i\end{bmatrix}, \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-i\end{bmatrix}\right\}$. Finally, Z has eigenvalues ± 1 with respective eigenvectors $\left\{\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}\right\}$.

First, we solve for X.

$\left\{\frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}, \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}\right\} \Leftrightarrow \{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$. First, for $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, we have that $\cos(\theta/2) = \frac{1}{\sqrt{2}}$. Hence, $\theta = \pi/2$. Now, $e^{i\varphi}\sin(\theta/2) = e^{i\varphi}/\sqrt{2} = 1/\sqrt{2}$. Hence, $\varphi = 0$.

Similarly, for the second eigenvector, $\theta = \pi/2$ but $\varphi = -\pi$.

Therefore, for the first eigenvector,

$$\begin{aligned}(\cos\varphi\sin\theta, \sin\varphi\sin\theta, \cos\theta) &= (\cos(0)\sin(\pi/2), \sin(0)\sin(\pi/2), \cos(\pi/2))\\ &= (1,0,0)\end{aligned}$$

And for the second we have,

$$\begin{aligned}&(\cos(\pi)\sin(\pi/2), \sin(\pi)\sin(\pi/2), \cos(\pi/2))\\ &\qquad = (-1,0,0)\end{aligned}$$

Similarly, we find the Bloch vectors $(0,\pm 1,0)$ for Y and $(0,0,\pm 1)$ for Z. □

2.1. **Action by Hadamard on the Bloch Sphere.** On the Bloch sphere, $|0\rangle = (0,0,1), |1\rangle = (0,0,-1), |+\rangle = (1,0,0), |-\rangle = (-1,0,0)$. This can often aid intuition. For example, we know that Hadamard operator H is defined s.t. $|0\rangle \to^H |+\rangle$.

Hence, on the Bloch sphere, this transformation is equivalent to $(0,0,1) \to^H (1,0,0)$. So, we can define a series of rotations to emulate the action of H, by considering its action on a basis of the Bloch sphere. So we note the additional transformations, $H^2 = I \Rightarrow |+\rangle \to |0\rangle \Leftrightarrow (1,0,0) \to (0,0,1)$ and $H\begin{bmatrix}1\\i\end{bmatrix} = \begin{bmatrix}1+i\\1-i\end{bmatrix} = \begin{bmatrix}1\\-i\end{bmatrix}$ (up to a global phase) $\Leftrightarrow (0,1,0) \to (0,-1,0)$.

Geometrically, we can convince ourselves that the following procedure suffices. For example, consider the effect of this procedure on $|0\rangle$:

(1) Begin with state $|0\rangle = (0,0,1)$
(2) Rotate by $-\pi/2$ about the $\hat{x}$ axis. Hence, we then have $(0,1,0)$.
(3) Rotate by $-\pi/2$ about the $\hat{z}$ axis. This gives $(1,0,0)$.
(4) Rotate by $-\pi/2$ about the $\hat{x}$ axis. This keeps us at $(1,0,0) = |+\rangle$

Similarly, using the same procedure

(1) $\begin{bmatrix}1\\ i\end{bmatrix} = (0, 1, 0)$.
(2) $(0, 0, -1)$.
(3) $(0, 0, -1)$.
(4) $(0, -1, 0)$.
The reader can verify the above for $|+\rangle$.

Exercise 2.2. *(4.2) Let $x \in \mathbb{R}$ and A be a matrix that satisfies $A^2 = I$. Show that*

$$\exp(iAx) = \cos(x)I + i\sin(x)A$$

Proof. From the power series definition of e^z, we have that

$$\begin{aligned}
\exp(iAx) &= \sum_{n=0}^{\infty} \frac{(iAx)^n}{n!} \\
&= \sum_{n=0}^{\infty} \frac{(iAx)^{2n}}{(2n)!} + \sum_{n=0}^{\infty} \frac{(iAx)^{2n+1}}{(2n+1)!} \\
\sum_{n=0}^{\infty} \frac{(iAx)^{2n}}{(2n)!} &= \sum_{n=0}^{\infty} \frac{i^{2n} A^{2n} x^{2n}}{(2n)!} \\
&= \sum_{n=0}^{\infty} \frac{(-1)^{2n} I x^{2n}}{(2n)!} \\
&= I \sum_{n=0}^{\infty} \frac{(-1)^{2n} x^{2n}}{(2n)!} = \cos(x)I \\
\sum_{n=0}^{\infty} \frac{(iAx)^{2n+1}}{(2n+1)!} &= \sum_{n=0}^{\infty} \frac{i^{2n+1} A^{2n+1} x^{2n+1}}{(2n+1)!} \\
&= \sum_{n=0}^{\infty} \frac{i(-1)^{2n+1} A x^{2n+1}}{(2n+1)!} \\
&= iA \sum_{n=0}^{\infty} \frac{(-1)^{2n+1} x^{2n+1}}{(2n+1)!} = i\sin(x)A
\end{aligned}$$

□

Exercise 2.3. *(4.3) Show that, up to a global phase, the $\pi/8$ gate satisfies $T = R_z(\pi/4)$.*

Proof. Note that

$$T = \begin{bmatrix}1 & 0\\ 0 & \exp(i\pi/4)\end{bmatrix} = \exp(i\pi/8) \begin{bmatrix}\exp(-i\pi/8) & 0\\ 0 & \exp(i\pi/8)\end{bmatrix}$$

Now, using the definition of R_z,

$$\begin{aligned} e^{-iZ\frac{\pi}{8}} &= \cos(-\pi/8)I + i\sin(-\pi/8)Z \\ &= \cos(\pi/8)I - i\sin(\pi/8)Z \\ &= \begin{bmatrix} \cos(\pi/8) - i\sin(\pi/8) & 0 \\ 0 & \cos(\pi/8) + i\sin(\pi/8) \end{bmatrix} \\ &= \begin{bmatrix} \exp(-i\pi/8) & 0 \\ 0 & \exp(i\pi/8) \end{bmatrix} \end{aligned}$$

□

Exercise 2.4. *(4.4) Express the Hadamard gate H as a product of R_x and R_z rotations and $e^{i\varphi}$ for some φ.*

Proof. In section 2.1 we discussed a procedure for expressing H as a product of rotations on the Bloch sphere, by considering its actions on a basis of the Bloch sphere. We showed that $R_x(-\pi/2)R_z(-\pi/2)R_x(-\pi/2)$ suffices. We can verify this result a second way by considering the respective rotation matrices.

We know that $H = \frac{1}{\sqrt{2}}(X+Z)$. Furthermore,

$$\begin{aligned} R_x(-\pi/2) &= \begin{bmatrix} \cos(\pi/4) & i\sin(\pi/4) \\ i\sin(\pi/4) & \cos(\pi/4) \end{bmatrix} \\ &= \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix} = \frac{1}{\sqrt{2}}(I + iX) \\ R_z(-\pi/2) &= \begin{bmatrix} \cos(\pi/4) + i\sin(\pi/4) & 0 \\ 0 & \cos(\pi/4) - i\sin(\pi/4) \end{bmatrix} \\ &= \frac{1}{\sqrt{2}}\begin{bmatrix} 1+i & 0 \\ 0 & 1-i \end{bmatrix} = \frac{1}{\sqrt{2}}(I + iZ) \end{aligned}$$

We'll use that

$$\begin{aligned} XZ &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \\ &= \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = iY \\ ZX &= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \\ &= \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = -iY \\ \Rightarrow XZ + ZX &= 0 \\ \Rightarrow XZX + ZX^2 &= 0 \\ \Rightarrow XZX &= -Z \end{aligned}$$

Note that the above is simply showing that the anti-commutator of X and Z, $\{X, Z\} = 0$. This holds for any pair of distinct Pauli matrices (Exercise 2.41).

Hence,

$$\begin{aligned}\frac{1}{2\sqrt{2}}(I+iX)(I+iZ)(I+iX) &= \frac{1}{2\sqrt{2}}[I+iX+iZ+i^2ZX+iX+i^2X^2+i^2XZ+i^3XZX] \\ &= \frac{1}{2\sqrt{2}}[I+iX+iZ-ZX+iX-I-XZ+i^3XZX] \\ &= \frac{1}{2\sqrt{2}}[i(X+Z)+iX-iXZX] \\ &= \frac{1}{2\sqrt{2}}[i(X+Z)+iX+iZ] \\ &= \frac{1}{\sqrt{2}}[i(X+Z)]\end{aligned}$$

which gives the Hadamard transform with phase e^{i0}.

□

Exercise 2.5. *(4.5) Prove that $(\hat{n}\cdot\hat{\sigma})^2 = I$, and use this to verify the following equation*

$$R_n(\theta) \equiv \exp(-i\theta n\cdot\sigma/2) = \cos(\theta/2)I - i\sin(\theta/2)(n_xX+n_yY+n_zZ)$$

Proof. Evidently, $\hat{n}\cdot\hat{\sigma} = (n_xX+n_yY+n_zZ)$ so, recalling that distinct Pauli matrices anti-commute,

$$\begin{aligned}(n_xX+n_yY+n_zZ)^2 &= n_x^2X^2+n_xn_yXY+n_xn_zXZ+n_xn_yYX+n_y^2Y^2+n_yn_zYZ+n_xn_zZX+n_yn_zZY+n_zZ^2 \\ &= (n_x^2+n_y^2+n_z^2)I+n_xn_z(XZ+ZX)+n_yn_z(YZ+ZY)+n_xn_y(XY+YX) \\ &= (n_x^2+n_y^2+n_z^2)I = I\end{aligned}$$

because $\hat{n}$ is a unit vector.

Therefore, using Exercise 4.2 (Nielsen & Chuang), if we let $A = \hat{n}\cdot\hat{\sigma}$, then the result follows directly. □

Exercise 2.6. *(4.7) Show that $XYX = Y$ and use this to prove that $XR_y(\theta)X = R_y(-\theta)$.*

Proof. From above, we have that distinct Pauli matrices anti-commute. Furthermore, the Pauli matrices are hermitian and unitary $\Rightarrow \sigma_i^2 = 0, i \in \{x,y,z\}$. Hence,

$$\begin{aligned}XY+YX &= 0 \\ XYX+YX^2 &= 0 \\ XYX+Y &= 0 \\ XYX &= -Y\end{aligned}$$

So,

$$\begin{aligned} XR_y(\theta)X &= X\big[\cos(\theta/2)I - i\sin(\theta/2)Y\big]X \\ &= \cos(\theta/2)X^2 - i\sin(\theta/2)XYX \\ &= \cos(\theta/2)I + i\sin(\theta/2)Y \\ &= \cos(-\theta/2)I - i\sin(-\theta/2)Y \\ &= R_y(-\theta) \end{aligned}$$

using that $\cos(-x) = \cos(x), \sin(-x) = -\sin(x)$. □

Exercise 2.7. *(4.12) Give A, B, C, and α for the Hadamard gate.*

Proof. Using Lemma **??** above we can solve, assuming $\gamma = \pi/2$,

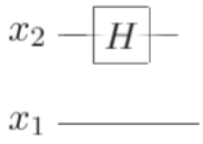
$$\begin{aligned} H = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} &= \begin{bmatrix} e^{i(\alpha-\beta/2-\delta/2)} & -e^{i(\alpha-\beta/2+\delta/2)} \\ e^{i(\alpha+\beta/2-\delta/2)} & e^{i(\alpha+\beta/2+\delta/2)} \end{bmatrix} \\ \alpha - \beta/2 - \delta/2 &= 0 \\ \alpha - \beta/2 + \delta/2 &= \pi \\ \alpha + \beta/2 - \delta/2 &= 0 \\ (\alpha + \beta/2 + \delta/2) &= \pi \\ \Rightarrow \alpha = \pi/2, \beta = 0, \delta &= \pi \end{aligned}$$

So, the proof of Corollary **??** in Nielsen & Chuang tells us to set

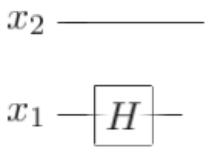
$$\begin{aligned} A &= R_z(\beta)R_y(\gamma/2) \\ &= R_z(0)R_y(\pi/4) \\ &= \begin{bmatrix} \cos(\pi/8) & -\sin(\pi/8) \\ \sin(\pi/8) & \cos(\pi/8) \end{bmatrix} \\ B &= R_y(-\gamma/2)R_z(-(\delta+\beta)/2) \\ &= R_y(-\pi/4)R_z(-\pi/2) \\ &= \begin{bmatrix} \cos(\pi/8) & \sin(\pi/8) \\ -\sin(\pi/8) & \cos(\pi/8) \end{bmatrix} \begin{bmatrix} e^{i\pi/4} & 0 \\ 0 & e^{-i\pi/4} \end{bmatrix} \\ C &= R_z((\delta-\beta)/2) \\ &= R_z(\pi/2) \\ &= \begin{bmatrix} e^{i\pi/4} & 0 \\ 0 & e^{-i\pi/4} \end{bmatrix} \end{aligned}$$

and α remains set $\alpha = \pi/2$. □

Exercise 2.8. *(4.16)*
What is the 4×4 unitary matrix for the circuit



in the computational basis? What is the unitary matrix for the circuit



in the computational basis?

Proof. For the first circuit, we consider action on the computational basis.

$$|x_1\rangle |x_2\rangle \to |x_1\rangle H |x_2\rangle = (I \otimes H) |x_1\rangle |x_2\rangle$$

Now, given that $H = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ w.r.t the computation basis, then

$$(I \otimes H) = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}$$

Similarly, for the second circuit we have

$$(H \otimes I) = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix}$$

□

Exercise 2.9. *(4.17) 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. Recall that, in terms of the computational basis, the action of the `CNOT` is given by $|c\rangle|t\rangle \to |c\rangle|t \oplus c\rangle$ and that $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.

We construct our algorithm by first making the observation that $H|+\rangle = |0\rangle$ and $H|-\rangle = |1\rangle$. Hence, beginning with state $|c\rangle|t\rangle$ we can initially apply H to $|t\rangle$. Now, using the control-Z gate with $|c\rangle$ as the control and $H|t\rangle$ as the target, we have two cases:

(1) If $|c = 1\rangle$, then the second qubit will swap either from $|+\rangle$ to $|-\rangle$ or vis versa. Therefore, we can apply another Hadamard to the second qubit and have $|t \oplus c\rangle$ at the second qubit, as expected. The first qubit is unaltered, as expected.

(2) If $|c = 1\rangle$, then the second qubit will remain unchanged. Hence, if we apply another Hadamard to the second qubit, then $|t\rangle$ is recovered since $H^2 = I$. So, we have the expected behavior.

In summary, we have the circuit, beginning with state $|c\rangle|t\rangle$:

(1) Apply H to the second qubit

(2) Controlled-Z with the first qubit as the control and second as the target

(3) Apply H to the second qubit. □

Exercise 2.10. *(4.19) The `CNOT` gate is a simple permutation whose action on a density matrix ρ is to rearrange the elements in the matrix. Write out this action explicitly in the computational basis.*

Proof.

$$|00\rangle\langle 00| = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$|01\rangle\langle 01| = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$|10\rangle\langle 10| = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$|11\rangle\langle 11| = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Now,

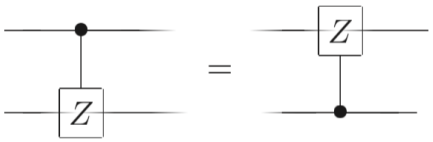
$$\begin{aligned} C_1(X)|00\rangle &= |00\rangle \\ C_1(X)|01\rangle &= |01\rangle \\ C_1(X)|10\rangle &= |11\rangle \\ C_1(X)|11\rangle &= |10\rangle \end{aligned}$$

Hence, the permutation matrix acting on the computational basis as

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

satisfies this permutation. □

Exercise 2.11. *(4.18) Show that*



Proof. We simply prove the statement for the computational basis.

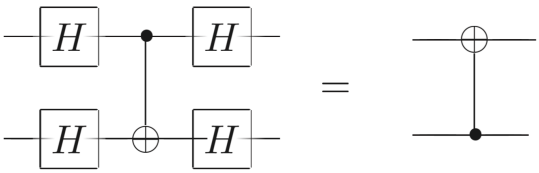
(1) $|0\rangle|0\rangle$: Both circuits give the identity transform since they are conditioned on a qubit which is $|0\rangle$, in either case.

(2) $|1\rangle|0\rangle$: The first circuit is conditioned on $|1\rangle$, so it applies Z to $|0\rangle$ which gives $|0\rangle$. Hence, we have $|1\rangle|0\rangle$. The second circuit is conditioned on $|0\rangle$, so we have the identity transform which gives $|1\rangle|0\rangle$, similarly.

(3) $|0\rangle|1\rangle$: By symmetry, we have the same outcome as in (2).

(4) $|1\rangle|1\rangle$: The first circuit is conditioned on the first $|1\rangle$, so it applies Z to the second qubit which gives $-|1\rangle|1\rangle$. Similarly, the second circuit gives $-|1\rangle|1\rangle$. □

Exercise 2.12. *(4.20) Unlike ideal classical gates, ideal quantum gates do not have (as electrical engineers say) high-impedance inputs. In fact, the role of control and target are arbitrary they depend on what basis you think of a device as operating in. We have described how the* `CNOT` *behaves with respect to the computational basis, and in this description the state of the control qubit is not changed. However, if we work in a different basis then the control qubit does change: we will show that its phase is flipped depending on the state of the target qubit! Show that*



Introducing basis states $|\pm\rangle$ *use this circuit identity to show that the effect of a* `CNOT` *with the first qubit as control and the second qubit as target is as follows:*

$$|+\rangle|+\rangle \to |+\rangle|+\rangle$$
$$|-\rangle|+\rangle \to |-\rangle|+\rangle$$
$$|+\rangle|-\rangle \to |-\rangle|-\rangle$$
$$|-\rangle|-\rangle \to |+\rangle|-\rangle$$

Thus, with respect to this new basis, the state of the target qubit is not changed, while the state of the control qubit is flipped if the target starts as $|-\rangle$, otherwise it is left alone. That is, in this basis, the target and control have essentially interchanged roles!

Proof. Consider action on $|c\rangle|t\rangle$ by the circuit on the LHS. The action of this circuit is given by $(H\otimes H)C^1(X)|c\rangle|t\rangle(H\otimes H)$ using c as the control and t as the target for the controlled operation. So, in Exercise 4.17, we showed that we can decompose $C^1(X)$ as $HC^1(Z)H$ using the same control and target as used for $C^1(X)$ originally, and with the H transforms acting on the target qubit. Hence, we can rewrite action by the LHS circuit as $(H\otimes H)(I\otimes H)C^1(Z)|c\rangle|t\rangle(I\otimes H)(H\otimes H) = (H\otimes I)C^1(Z)|c\rangle|t\rangle(H\otimes I)$.

Similarly, for the circuit on the RHS, action on $|c\rangle|t\rangle$ is given by $C^1(X)|c\rangle|t\rangle$ where in this case t is the control and c is the target. Hence, using the same result, we can rewrite this as $(H\otimes I)C^1(Z)|c\rangle|t\rangle(H\otimes I)$ with t as control and c as target. Finally, using Exercise 4.18, we can swap which qubits we regard as control/target in a controlled-Z operation. Hence, we have the action $(H\otimes I)C^1(Z)|c\rangle|t\rangle(H\otimes I)$ with c as control and t as target, as in the LHS.

Now, using that $H^2=I$, we note that the identity given by the circuit is equivalent to $C^1(X)(H\otimes H)|c\rangle|t\rangle = C^1(X)|t\rangle|c\rangle(H\otimes H)$ (applying $H\otimes H$ to the end of both circuits). Hence, this directly gives the effect of `CNOT` on the basis $|\pm\rangle$.

□

Exercise 2.13. *(4.21) Verify that Figure 4.8 implements the $C^2(U)$ operation.*

Proof. □

3. Chapter 5

Exercise 3.1. *(5.2) Explicitly compute the Fourier transform of the n qubit state $|00\cdots0\rangle$.*

Proof. $|00\cdots0\rangle$ corresponds to state $|0\rangle$ in the size $N=2^n$ computational basis. Hence, using the formula above we have

$$\begin{aligned}|0\rangle &\to \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}|k\rangle\\ &= \frac{|0\rangle+|1\rangle+\cdots+|N-1\rangle}{\sqrt{N}}\end{aligned}$$

□

Exercise 3.2. *(5.7) Additional insight into the circuit above may be obtained by showing, as you should now do, that the effect of the sequence of controlled-U operations like that in the figure is to take the state $|j\rangle|u\rangle$ to $|j\rangle U^j|u\rangle$. (Note that this does not depend on $|u\rangle$ being an eigenstate of U.)*

Proof. Consider an arbitrary j in its binary representation $j_0j_1\cdots j_{t-1}$ where $j_i\in\{0,1\}$. Hence, for each $|j_i\rangle$, the control-U acts on $|j_i\rangle|u\rangle$ such that $|j_i\rangle|u\rangle\mapsto|j_i\rangle U^{j_i2^i}|u\rangle$. Therefore, the final state is given by

$$\begin{aligned}|j_0\rangle\cdots|j_{t-1}\rangle\, U^{j_0 2^0}\cdots U^{j_{t-1}2^{t-1}}\,|u\rangle &= |j\rangle\, U^{j_0 2^0}\cdots U^{j_{t-1}2^{t-1}}\,|u\rangle \\ &= |j\rangle\, U^{j_0 2^0 + j_{t-1}2^{t-1}}\,|u\rangle \\ &= |j\rangle\, U^{j}\,|u\rangle\end{aligned}$$

□

4. Chapter 6: Quantum Search Algorithms

Exercise 4.1. *(6.1) Show that the Unitary operator corresponding to the phase shift in the Grover iteration is* $2\,|0\rangle\langle 0| - I$.

Proof. Consider arbitrary state $|x\rangle$. There are two cases:
(1) $|x\rangle = |0\rangle$. Hence,

$$\begin{aligned}(2\,|0\rangle\langle 0| - I)\,|0\rangle &= 2\,|0\rangle\langle 0|0\rangle - |0\rangle \\ &= |0\rangle\end{aligned}$$

as expected.
(2) $|x\rangle \neq |0\rangle$. Hence,

$$\begin{aligned}(2\,|0\rangle\langle 0| - I)\,|x\rangle &= 2\,|0\rangle\langle 0|x \neq 0\rangle - |x\rangle \\ &= 0 - |x\rangle = -\,|x\rangle\end{aligned}$$

as expected. □

Exercise 4.2. *(6.2) Show that the operation* $(2\,|\psi\rangle\langle\psi| - I)$ *(where* $|\psi\rangle$ *is the equally weighted superposition of states) applied to general state* $\sum_k \alpha_k\,|k\rangle$ *produces*

$$\sum_k [-\alpha_k + 2\langle\alpha\rangle]\,|k\rangle$$

where $\langle\alpha\rangle \equiv \sum_k \alpha_k/N$ *is the mean value of* α_k.

Proof.

$$\begin{aligned}(2\,|\psi\rangle\langle\psi| - I)\sum_k \alpha_k\,|k\rangle &= \Big(2\frac{1}{N^{1/2}}\,|x\rangle\,\frac{1}{N^{1/2}}\sum_{x'=0}^{N-1}\langle x'| - I\Big)\sum_k \alpha_k\,|k\rangle \\ &= 2\frac{1}{N}\sum_{x=0}^{N-1}|x\rangle\langle x'|\sum_k \alpha_k\,|k\rangle - \sum_k \alpha_k\,|k\rangle \\ &= \frac{2}{N}\sum_k |k\rangle\,\alpha_k - \sum_k \alpha_k\,|k\rangle \\ &= \sum_k [2\langle\alpha\rangle - \alpha_k]\,|k\rangle\end{aligned}$$

□

5. Chapter 11: Entropy and Information

Exercise 5.1. *(11.8)*
Let X, Y be i.i.d random variables uniformly distributed over set $\{0,1\}$. Hence,

$$\begin{aligned} H(X) &= H(1/2) = 1 = H(Y) \\ H(X,Y) &= -4[1/4\log(1/4)] = 2 \\ H(X \mid Y) &= H(X,Y) - H(Y) \\ &= 2 - 1 = 1 \\ &= H(Y \mid X) \\ I(X:Y) &= H(X) - H(X \mid Y) \\ &= 0 \end{aligned}$$

Now, let $Z = X \oplus Y$. Then,

$$\begin{aligned} H(Z) &= H(1/2) = 1 \\ H(X,Y,Z) &= -4[1/4\log(1/4)] = 2 \\ H(X,Y \mid Z) &= H(X,Y,Z) - H(Z) \\ &= 1 \\ I(X,Y:Z) &= H(X,Y) - H(X,Y \mid Z) \\ &= 2 - 1 = 1 \end{aligned}$$

Furthermore,

$$\begin{aligned} H(X,Z) &= 2 \\ H(X \mid Z) &= H(X,Z) - H(Z) \\ &= 2 - 1 = 1 \\ I(X:Z) &= H(X) - H(X \mid Z) \\ &= 1 - 1 = 0 \end{aligned}$$

Similarly, $I(Y:Z) = 0$).
$\therefore I(X:Z) + I(Y:Z) < I(X,Y:Z)$ in this case.
Thinking through this problem intuitively, it just says that if we've specified both X, Y, then we don't need to send a bit for Z through our channel since we can compute its value readily. However, if we send just X or Y, the XOR function provides uniform outcomes across Z.

Exercise 5.2. *(11.9) Let r.v. X_1 be uniformly distributed across $\{0,1\}$. Furthermore, require that $X_2 = Y_2 = Y_1 = X_1$ (identically).*
In this case,

$$\begin{aligned} H(X_1 \mid Y_1) &= H(X_1, Y_1) - H(Y_1) \\ &= H(1/2) - H(1/2) = 0 \\ I(X_1 : Y_1) &= H(X_1) - H(X_1 \mid Y_1) \\ 1 - 0 &= 1 \\ &= I(X_2 \mid Y_2) \end{aligned}$$

However,

$$\begin{aligned} H(X_1, X_2 \mid Y_1, Y_2) &= H(X_1, X_2, Y_1, Y_2) - H(X_1, X_2) \\ &= H(1/2) - H(1/2) = 0 \\ I(X_1 : Y_1) &= H(X_1, X_2) - H(X_1, X_2 \mid Y_1, Y_2) \\ &= 1 - 0 = 0 \end{aligned}$$

$\therefore I(X_1 : Y_1) + I(X_2 : Y_2) > I(X_1, X_2 : Y_1, Y_2)$ *in this case.*

Intuitively, the random variables are distributed identically, so we always only need a single bit to communicate their distribution across a channel. Hence, there will always be a single bit of mutual information across the r.v.'s since their conditional entropy will be zero bits (we know everything we need to know given one variable's value) and their joint entropy will be a single bit.

Conclusion from the above two exercises: mutual information is neither sub-additive nor super-additive.