2

Exercises

8. Each $|v_{k+1}\rangle$ is scaled by its norm and hence normal.

   Orthogonality is proved by induction. Case $i = 1$: $\langle v_0|v_1\rangle \propto \langle v_0|w_1\rangle - \langle v_0| \langle v_0|w_1\rangle |v_0\rangle = \langle v_0|w_1\rangle - \langle v_0|w_1\rangle = 0$. Case $i = 2$:

$$\langle v_0|v_2\rangle \propto \langle v_0|w_2\rangle - \langle v_0| \langle v_0|w_2\rangle |v_0\rangle - \langle v_0| \langle w_2|v_1\rangle |v_1\rangle \tag{1}$$
$$= \langle v_0|w_2\rangle - \langle v_0|w_2\rangle = 0 \tag{2}$$
$$\langle v_1|v_2\rangle \propto \langle v_1|w_2\rangle - \langle v_1| \langle v_0|w_2\rangle |v_0\rangle - \langle v_1| \langle v_1|w_2\rangle |v_1\rangle = 0 \tag{3}$$

   Case $n + 1$: Given $\langle v_i|v_n\rangle = 0$ where $i = 0, \ldots, n - 1$:

$$\langle v_n|v_{n+1}\rangle \propto \langle v_n|w_{n+1}\rangle - \sum_{i=0}^{n} \langle v_n|v_i\rangle \langle v_i|w_{n+1}\rangle \tag{4}$$
$$= \langle v_n|w_{n+1}\rangle - \sum_{i=0}^{n-1} \langle v_n|v_i\rangle \langle v_i|w_{n+1}\rangle - \langle v_n|v_n\rangle \langle v_n|w_{n+1}\rangle \tag{5}$$
$$= \langle v_n|w_{n+1}\rangle - \langle v_n|w_{n+1}\rangle = 0 \tag{6}$$

18. Let $U^* = U^{-1}$ and let $|x\rangle$ be a normalized eigenvector of U with eigenvalue λ_x. Then $|\lambda_x|^2 = \lambda_x^* \lambda_x \langle x|x\rangle = \langle x| \lambda_x^* \lambda_x |x\rangle = (\langle x|U^*|)(|U|x\rangle) = \langle x|U^{-1}U|x\rangle = \langle x|x\rangle = 1$.

22. Let $A = A^*$, $A|x\rangle = \lambda_x |x\rangle$, and $A|y\rangle = \lambda_y |y\rangle$ be distinct eigenvectors (and hence $\lambda_x \neq \lambda_y$). Then $\langle x|A|y\rangle = \langle x|\lambda_y|y\rangle = \lambda_y \langle x|y\rangle$. But also, $\langle x|A|y\rangle = \langle x|A^*|y\rangle = \lambda_x \langle x|y\rangle$. Subtracting,

$$\lambda_x \langle x|y\rangle - \lambda_y \langle x|y\rangle = 0 \tag{7}$$
$$(\lambda_x - \lambda_y) \langle x|y\rangle = 0 \tag{8}$$
$$\langle x|y\rangle = 0 \tag{9}$$

23. Let P be a projector and let $P|x\rangle = \lambda |x\rangle$. Then $P|x\rangle = P^2|x\rangle = P\lambda |x\rangle = \lambda P|x\rangle = \lambda^2 |x\rangle$, thus $\lambda^2 - \lambda = \lambda(\lambda - 1) = 0$.

24. > "A special subclass of Hermitian operators is extremely important. This is the positive operators. A positive operator A is

defined to be an operator such that for any vector $|v\rangle$, $(|v\rangle, A|v\rangle)$ is a real, non-negative number."

If $A \in \mathbb{C}^{n\times n}$ is a positive operator, then $k = \langle x|A|x\rangle \geq 0$ is real and so, trivially, $k = k^* = \langle x|A^*|x\rangle = \langle x|A|x\rangle$, thus $A = A^*$.

Note that this argument fails for $B \in \mathbb{R}^{n\times n}$, since $\langle x|B|x\rangle = x^T Bx = \langle x|C|x\rangle$ does not imply that $B = C$; B could, for instance, be anti-symmetric.

25. $\langle x|A^*A|x\rangle = (\langle x|A^*)(A|x\rangle) = (A|x\rangle)^*(A|x\rangle) = \langle z|z\rangle \geq 0$.

26.

$$
\begin{aligned}
|\psi\rangle^{\otimes 2} &= \frac{1}{2}\left(|0\rangle|0\rangle + |1\rangle|0\rangle + |0\rangle|1\rangle + |1\rangle|1\rangle\right) && (10)\\
&= \frac{1}{2}\left(|00\rangle + |10\rangle + |01\rangle + |11\rangle\right) && (11)\\
|\psi\rangle^{\otimes 3} = |\psi\rangle^{\otimes 2} \otimes |\psi\rangle &= r^3\left(|000\rangle + |100\rangle + |010\rangle + |110\rangle\right) && (12)\\
&+ r^3\left(|001\rangle + |101\rangle + |011\rangle + |111\rangle\right) && (13)
\end{aligned}
$$

54. If A and B are Hermitian and commute then by the simultaneous diagonalization theorem, there exists an orthonormal basis $|i\rangle$ such that $A = \sum_i \lambda_i |i\rangle\langle i|$ and $B = \sum_i \gamma_i |i\rangle\langle i|$, with $\lambda_i, \gamma_i \in \mathbb{R}$. Then:

$$
\begin{aligned}
e^A e^B &= \left(\sum_i e^{\lambda_i}|i\rangle\langle i|\right)\left(\sum_i e^{\gamma_i}|i\rangle\langle i|\right) && (14)\\
&= \sum_i\sum_j e^{\lambda_i+\gamma_j}|i\rangle\langle i|j|\langle j| && (15)\\
&= \sum_i\sum_j e^{\lambda_i+\gamma_j}\delta_{ij}|i\rangle\langle j| && (16)\\
&= \sum_i e^{\lambda_i+\gamma_j}|i\rangle\langle i| && (17)\\
&= \exp\left(\sum_i(\lambda_i+\gamma_j)|i\rangle\langle i|\right) && (18)\\
&= \exp\left(\sum_i \lambda_i|i\rangle\langle i| + \sum_i \gamma_i|i\rangle\langle i|\right) && (19)\\
&= e^{A+B} && (20)
\end{aligned}
$$

55. Let H be a Hamiltonian (which is defined Hermitian) and let $A = -ih^{-1}H$. Then $A^* = (-ih^{-1}H)^* = ih^{-1}H^* = ih^{-1}H = -A$. Since A trivially commutes with $-A$,

$$\begin{aligned} UU^* &= e^{-At}\left(e^{-At}\right)^* && (21)\\ &= e^{-At}e^{(-A)^*t} && (22)\\ &= e^{-At}e^{At} && (23)\\ &= e^{-At+At} && (24)\\ &= e^0 = I && (25) \end{aligned}$$

In general, the exponent of a skew-Hermitian matrix is unitary.

56. If U is unitary, then it is trivially normal and thus there exists an orthonormal basis $|k\rangle$ where $U = \sum_k u_k |k\rangle\langle k| = \sum_k r_k \exp(i\theta_k)|k\rangle\langle k|$. Since $UU^* = I$, each $r_k = 1$. Then,

$$\begin{aligned} K^* = (-i\log U)^* &= i\left(\log\left(\sum_k e^{i\theta_k}|k\rangle\langle k|\right)\right)^* && (26)\\ &= i\left(\sum_k i\theta_k |k\rangle\langle k|\right)^* && (27)\\ &= -i\sum_k i\theta_k |k\rangle\langle k| && (28)\\ &= -i\sum_k \log\left(e^{i\theta_k}\right)|k\rangle\langle k| && (29)\\ &= -i\log\left(\sum_k e^{i\theta_k}|k\rangle\langle k|\right) && (30)\\ &= -i\log U = K && (31) \end{aligned}$$

This means that every unitary $U = \exp(iK)$ for some Hermitian K. But also, for every Hermitian K, iK is skew-Hermitian and thus $\exp(iK)$ is necessarily unitary. So there is a mapping between Hermitians and unitaries through e^{ix}, modulo 2π.

57. Given a quantum state $|\psi\rangle$ and two measurement operators L, M, the final state after measurement by M followed by L is:

$$\begin{aligned} |\psi\rangle &\xrightarrow{M} \langle\psi|M^*M|\psi\rangle^{-\frac{1}{2}} M|\psi\rangle = rM|\psi\rangle = r|\phi\rangle && (32)\\ r|\phi\rangle &\xrightarrow{L} \langle\phi|L^*r^2L|\phi\rangle^{-\frac{1}{2}} rL|\phi\rangle && (33)\\ &= \langle\phi|L^*L|\phi\rangle^{-\frac{1}{2}} L|\phi\rangle && (34) \end{aligned}$$

$$= \langle\psi|M^*L^*LM|\psi\rangle^{-\frac{1}{2}} LM|\psi\rangle \tag{35}$$

$$= \langle\psi|(LM)^*(LM)|\psi\rangle^{-\frac{1}{2}} LM|\psi\rangle \tag{36}$$

$$= \langle\psi|N^*N|\psi\rangle^{-\frac{1}{2}} N|\psi\rangle \tag{37}$$

which is the final state of a single measurement $N = LM$.

60. For a normal vector $\vec{v} \in \mathbb{R}^3$, the observable

$$V = \vec{v}\cdot\vec{\sigma} = \begin{pmatrix} v_2 & v_0 - iv_1 \\ v_0 + iv_1 & -v_2 \end{pmatrix} = \begin{pmatrix} v_2 & c^* \\ c & -v_2 \end{pmatrix}$$

has characteristic polynomial

$$\lambda I - V = \lambda^2 - v_2^2 - \left(v_0^2 + v_1^2\right) = \lambda^2 - \|v\|^2 = \lambda^2 - 1$$

and thus eigenvalues $\lambda = \pm 1$. For $\lambda = 1$, its eigenvectors are:

$$\begin{pmatrix} v_2 & c^* \\ c & -v_2 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} \tag{38}$$

$$\Rightarrow xv_2 + yc^* = x \Rightarrow y = x\frac{1-v_2}{c^*} \tag{39}$$

$$\Rightarrow |\hat{\psi_+}\rangle = \begin{pmatrix} 1 & \frac{1-v_2}{c^*} \end{pmatrix}^T \tag{40}$$

Normalize:

$$\langle\hat{\psi_+}|\hat{\psi_+}\rangle = 1 + \frac{1 - 2v_2 + v_2^2}{v_0^2 + v_1^2} \tag{41}$$

$$= \frac{1 - v_2^2 + 1 - 2v_2 + v_2^2}{1 - v_2^2} \tag{42}$$

$$= \frac{2 - 2v_2}{(1-v_2)(1+v_2)} \tag{43}$$

$$= \frac{2}{1+v_2} \tag{44}$$

$$|\psi_+\rangle = \sqrt{\frac{1+v_2}{2}}\begin{pmatrix} 1 & \frac{1-v_2}{c^*} \end{pmatrix}^T \tag{45}$$

Projector:

$$|\psi_+\rangle\langle\psi_+| = \frac{1+v_2}{2}\begin{pmatrix} 1 & \frac{1-v_2}{c} \\ \frac{1-v_2}{c^*} & \frac{(1-v_2)^2}{v_0^2+v_1^2} \end{pmatrix} \tag{46}$$

$$= \frac{1}{2}\begin{pmatrix} 1+v_2 & \frac{1-v_2^2}{c} \\ \frac{1-v_2^2}{c^*} & \frac{\left(1-v_2^2\right)(1-v_2)}{1-v_2^2} \end{pmatrix} \tag{47}$$

$$= \frac{1}{2}\begin{pmatrix} 1+v_2 & \frac{c^*c}{c} \\ \frac{c^*c}{c^*} & 1-v_2 \end{pmatrix} = \frac{1}{2}(I+V) \tag{48}$$

Similarly, For $\lambda = -1$:

$$\begin{pmatrix} v_2 & c^* \\ c & -v_2 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = -\begin{pmatrix} x \\ y \end{pmatrix} \tag{49}$$

$$\Rightarrow xv_2 + yc^* = -x \Rightarrow y = -x\frac{1+v_2}{c^*} \tag{50}$$

$$\Rightarrow |\hat{\psi_-}\rangle = \begin{pmatrix} 1 & \frac{1+v_2}{c^*} \end{pmatrix}^T \tag{51}$$

Normalize:

$$\langle\hat{\psi_-}|\hat{\psi_-}\rangle = 1 + \frac{1+2v_2+v_2^2}{v_0^2+v_1^2} = \frac{2}{1-v_2} \tag{52}$$

$$|\psi_-\rangle = \sqrt{\frac{1-v_2}{2}}\,|\hat{\psi_-}\rangle \tag{53}$$

Projector:

$$|\psi_-\rangle\langle\psi_-| = \frac{1-v_2}{2}\begin{pmatrix} 1 & \frac{1+v_2}{c} \\ \frac{1+v_2}{c^*} & \frac{(1+v_2)^2}{1-v_2^2} \end{pmatrix} \tag{54}$$

$$= \frac{1}{2}\begin{pmatrix} 1-v_2 & \frac{c^*c}{c} \\ \frac{c^*c}{c^*} & 1+v_2 \end{pmatrix} = \frac{1}{2}(I-V) \tag{55}$$

61. Using V as defined in Exercise 60, $\mathrm{p}(+1; |0\rangle) = \langle 0|P_+|0\rangle = \frac{1}{2}\langle 0|I+V|0\rangle = \frac{1}{2}(1+v_2)$. If $+1$ is gotten, then the post-measurement state will be

$$\frac{P_+|0\rangle}{\sqrt{\langle 0|P_+|0\rangle}} = \frac{(1+v_2)|0\rangle + c|1\rangle}{2\sqrt{\frac{1+v_2}{2}}} = \frac{(1+v_2)|0\rangle + c|1\rangle}{\sqrt{2(1+v_2)}}$$

62. Trivially, $E_m = M_m^*M_m = E_m^*$. If $E_m = M_m$, then $M_m^* = E_m^* = E_m = M_m$ and $M_m^2 = M_mM_m = M_m^*M_m = E_m = M_m$, thus making M_m a projector.

63. Let M_m be a measurement operator. Then $E_m = M_m^*M_m$ is Hermitian and will thus have a spectral decomposition $U\Lambda U^*$ with unitary U. We contend that U satisfies $M_m = U\sqrt{E_m}$:

$$M_m^*M_m = \left(U\sqrt{E_m}\right)^* U\sqrt{E_m} \tag{56}$$

$$= \left(\sqrt{E_m}\right)^* U^* U \sqrt{E_m} \tag{57}$$

$$= \sqrt{E_m^*}\sqrt{E_m} \tag{58}$$

$$= \sqrt{E_m}\sqrt{E_m} = E_m \tag{59}$$

65. If $|a\rangle = 2^{-\frac{1}{2}}(|0\rangle + |1\rangle)$ and $|b\rangle = 2^{-\frac{1}{2}}(|0\rangle + |1\rangle)$, the two will be distinct in the basis $|+\rangle = |a\rangle$ and $|-\rangle = |b\rangle$. In other words, the Hermitian observable $M = m_+ |+\rangle\langle+| + m_- |-\rangle\langle-|$ will have expectation $E_{|a\rangle}[M] = m_+$ while $E_{|b\rangle}[M] = m_-$.

    More generally, if $|a\rangle = \alpha|0\rangle + \beta e^{i\theta_a}|1\rangle$ and $|b\rangle = \alpha|0\rangle + \beta e^{i\theta_b}|1\rangle$ where $\theta_a, \theta_b, \alpha, \beta \in \mathbb{R}$ and $\theta_a \neq \theta_b$ and $\langle a|a\rangle = \langle b|b\rangle = 1$, we can use Gram-Schmidt to construct a Hermitian observable under which the two will have differing expectations:

$$|+\rangle = |a\rangle \tag{60}$$

$$|-\rangle = N\left(|b\rangle - \mathbf{proj}_a(b)\right), N \in \mathbb{R} \tag{61}$$

$$= N\left(|b\rangle - \langle a|b\rangle|a\rangle\right) \tag{62}$$

    Here, N is a normalization constant to ensure that $\langle -|-\rangle = 1$. Under this basis, $\langle b|-\rangle = N(\langle b|b\rangle - \langle a|b\rangle\langle b|a\rangle) = N(1 - z^*z)$ where $z = \alpha^2 + \beta^2 e^{ik} = u + ve^{ik}$ and $k = \theta_a - \theta_b \in (0, 2\pi) \Rightarrow \cos k < 1$. We know that u and v are strictly non-zero (or else one of α or β would be zero, which would make $|a\rangle$ and $|b\rangle$ identical or differing by a global phase, respectively):

$$z^*z = u^2 + v^2 + 2uv\cos k \tag{63}$$

$$< u^2 + v^2 + 2uv \tag{64}$$

$$= (u+v)^2 \tag{65}$$

$$= 1^2 = 1 \tag{66}$$

    So $\langle b|-\rangle = N(1 - z^*z) \neq 0$ but $\langle a|-\rangle = 0$ by construction. Thus, they would be distinguishable under the measurement operator $|-\rangle\langle-|$.

66. Expand into matrix form:

$$X_1 Z_2 = X \otimes Z = \begin{pmatrix} 0 & Z \\ Z & 0 \end{pmatrix} \tag{67}$$

$$= \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix} \tag{68}$$

Since $X \otimes Z$ is Hermitian, the expectation would be $\langle\psi|X \otimes Z|\psi\rangle$ for $\psi = (|00\rangle + |11\rangle)/\sqrt{2}$:

$$\frac{1}{2}\begin{pmatrix}1 & 0 & 0 & 1\end{pmatrix}(X \otimes Z)\begin{pmatrix}1\\0\\0\\1\end{pmatrix} = \frac{1}{2}\begin{pmatrix}1 & 0 & 0 & 1\end{pmatrix}\begin{pmatrix}0\\-1\\1\\0\end{pmatrix} \tag{69}$$

$$= 0 \tag{70}$$

67. Since W is a subspace of V, one can choose an orthonormal basis $|0\rangle, |1\rangle, \ldots, |d-1\rangle$ for W and then extend it via Gram-Schmidt into an orthonormal basis $|0\rangle, \ldots, |k-1\rangle$ for V, with $d < k$. Letting $A : W \to V$ be a linear operator,

$$A = I_V A I_W = \left(\sum_{i=0}^{k-1} |i\rangle\langle i|\right) A \left(\sum_{j=0}^{d-1} |j\rangle\langle j|\right) \tag{71}$$

$$= \sum_i \sum_j \langle i|A|j\rangle |i\rangle\langle j| \tag{72}$$

$$= \sum_j \left(\sum_i \langle i|A|j\rangle |i\rangle\right)\langle j| \tag{73}$$

$$= \sum_j |u_j\rangle\langle j| \tag{74}$$

Each $|u_j\rangle$ can be viewed as a column in the matrix representations of A:

$$|u_0\rangle = \sum_i \langle i|A|0\rangle |i\rangle = \sum_i A_{i0} |i\rangle$$

$$|u_1\rangle = \sum_i \langle i|A|1\rangle |i\rangle = \sum_i A_{i1} |i\rangle$$

$$\vdots$$

We also had $\langle x|A^*A|y\rangle = \langle x|y\rangle$, so A^*A is necessarily the identity. In other words,

$$A^*A = I \tag{75}$$

$$\left(\sum_{m=0}^{d-1} |m\rangle\langle u_m|\right)\left(\sum_{n=0}^{d-1} |u_n\rangle\langle n|\right) = \sum_k |k\rangle\langle k| \tag{76}$$

$$\sum_m \sum_n |m\rangle\langle u_m|u_n\rangle\langle n| = \sum_k |k\rangle\langle k| \tag{77}$$

$$\langle u_m|u_n\rangle = \delta_{mn} \tag{78}$$

This means that $\{|u_i\rangle\}_{i=0}^{d-1}$ is necessarily an orthonormal subset of V. Since V is a k-dimensional space, we can once again employ Gram-Schmidt to derive the remaining $|u_d\rangle, \dots, |u_{k-1}\rangle$ so that the entire set $\{|u_i\rangle\}_{i=0}^{k-1}$ is an orthnormal basis of V. Using this, we can form unitary extension of A:

$$A' = \sum_{j=0}^{k-1} |u_j\rangle \langle j| \tag{79}$$

68. Suppose $|\psi\rangle = |00\rangle + |11\rangle$ could be expressed as $|a_0\rangle \otimes |a_1\rangle$, where $|a_i\rangle = u_i |0\rangle + v_i |1\rangle$ Then we have $|a_0\rangle \otimes |a_1\rangle = u_0u_1 |00\rangle + u_0v_1 |01\rangle + v_0u_1 |10\rangle + v_0v_1 |11\rangle$ and $u_0u_1 = v_0v_1 = 1$, which means that each of $u_0, u_1, v_0, v_1 \neq 0$. On the other hand, $u_0v_1 = v_0u_1 = 0$, which implies that one of $u_0, u_1, v_0, v_1 = 0$, leading to a contradiction. Thus, $|\psi\rangle$ is non-separable.

70. Since E is a positive operator, it is also Hermitian. Letting $E = \begin{pmatrix} u & v \\ v^* & w \end{pmatrix}$ $(u, w \in \mathbb{R})$ and computing the Kronecker product:

$$E \otimes I = \begin{pmatrix} u & 0 & v & 0 \\ 0 & u & 0 & v \\ v^* & 0 & w & 0 \\ 0 & v^* & 0 & w \end{pmatrix} \tag{80}$$

Case $|\psi_0\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$:

$$\langle\psi_0|E \otimes I|\psi_0\rangle = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} u \\ v \\ v^* \\ w \end{pmatrix} \tag{81}$$

$$= \frac{u+w}{2} \tag{82}$$

Case $|\psi_1\rangle = (|00\rangle - |11\rangle)/\sqrt{2}$:

$$\langle\psi_1|E \otimes I|\psi_1\rangle = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & -1 \end{pmatrix}\begin{pmatrix} u \\ v \\ v^* \\ -w \end{pmatrix} \tag{83}$$

$$= \frac{u+w}{2} \tag{84}$$

Case $|\psi_2\rangle = (|01\rangle + |10\rangle)/\sqrt{2}$: $\frac{1}{2}\begin{pmatrix} 0 & 1 & 1 & 0 \end{pmatrix}\begin{pmatrix} v \\ u \\ w \\ v^* \end{pmatrix} = \frac{u+w}{2}$.

Case $|\psi_3\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$: $\frac{1}{2}\begin{pmatrix}0 & 1 & -1 & 0\end{pmatrix}\begin{pmatrix}v\\u\\-w\\v^*\end{pmatrix} = \frac{u+w}{2}$.

So it would be impossible to distinguish between Bell states via measurement of only one half of the entangled pair.

71. In an orthnormal basis $\{|i\rangle\}$,

$$\mathrm{tr}\left[|\alpha\rangle\langle\beta|\right] = \mathrm{tr}\left[\left(\sum_i a_i |i\rangle\right)\left(\sum_j b_j^* \langle j|\right)\right] \tag{85}$$

$$= \mathrm{tr}\left[\sum_{i,j} a_i b_j^* |i\rangle\langle j|\right] \tag{86}$$

$$= \sum_{i,j} a_i b_j^* \mathrm{tr}\left[|i\rangle\langle j|\right] \tag{87}$$

$$= \sum_{i,j} a_i b_j^* \delta_{ij} = \langle\beta|\alpha\rangle \tag{88}$$

Now let $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ be a density operator where $\{|\psi_i\rangle\}$ are all normal but may not necessarily be orthogonal to each other. Then, $\rho^2 = \sum_{i,j} p_i p_j \langle\psi_i|\psi_j\rangle |\psi_i\rangle\langle\psi_j|$ and:

$$\mathrm{tr}\left[\rho^2\right] = \sum_{i,j} p_i p_j \langle\psi_i|\psi_j\rangle \mathrm{tr}\left[|\psi_i\rangle\langle\psi_j|\right] \tag{89}$$

$$= \sum_{i\neq j} p_i p_j \langle\psi_i|\psi_j\rangle \mathrm{tr}\left[|\psi_i\rangle\langle\psi_j|\right] + \sum_k p_k^2 \mathrm{tr}\left[|\psi_k\rangle\langle\psi_k|\right] \tag{90}$$

$$= \sum_{i\neq j} p_i p_j \left|\langle\psi_j|\psi_i\rangle\right|^2 + \sum_k p_k^2 \langle\psi_k|\psi_k\rangle \tag{91}$$

$$\leq \sum_{i\neq j} p_i p_j + \sum_k p_k^2 \tag{92}$$

$$= \left(\sum_i p_i\right)^2 = 1 \tag{93}$$

In a pure state, $p_r = 1$ for some fixed r and necessarily, all other $p_i = 0$ (thus, $p_i p_r = \delta_{ir}$). Then:

$$\mathrm{tr}\left[\rho^2\right] = \sum_{i\neq j} p_i p_j \left|\langle\psi_j|\psi_i\rangle\right|^2 + \sum_k p_k^2 \langle\psi_k|\psi_k\rangle \tag{94}$$

$$= \sum_k p_k^2 \langle\psi_k|\psi_k\rangle \tag{95}$$

$$= p_r^2 \langle\psi_r|\psi_r\rangle = 1^2 \cdot 1 = 1 \tag{96}$$

Conversely, suppose that $\mathrm{tr}\left[\rho^2\right] = 1$. Then,

$$\sum_{i\neq j} p_i p_j \left|\langle\psi_j|\psi_i\rangle\right|^2 + \sum_k p_k^2 \langle\psi_k|\psi_k\rangle = 1 \tag{97}$$

$$\sum_{i\neq j} p_i p_j \left|\langle\psi_j|\psi_i\rangle\right|^2 + \sum_k p_k^2 = \left(\sum_k p^k\right)^2 \tag{98}$$

$$= \sum_{i\neq j} p_i p_j + \sum_k p_k^2 \tag{99}$$

$$\sum_{i\neq j} p_i p_j \left|\langle\psi_j|\psi_i\rangle\right|^2 = \sum_{i\neq j} p_i p_j \tag{100}$$

$$p_i p_j \left|\langle\psi_j|\psi_i\rangle\right|^2 = p_i p_j, \quad i \neq j \tag{101}$$

Suppose that there exists a pair $r \neq s$ such that $p_r p_s > 0$. Then:

$$p_r p_s \left|\langle\psi_s|\psi_r\rangle\right|^2 = p_r p_s \Rightarrow \left|\langle\psi_s|\psi_r\rangle\right|^2 = 1 \Rightarrow |\psi_r\rangle = |\psi_s\rangle \Rightarrow r = s$$

leading to a contradiction. So the product of probabilities for every pair of distinct states must be zero, which means that there can be at most one non-zero p_r. They cannot all be zero either, because $\sum_k p_k = 1$. Thus, $\sum_k p_k = p_r = 1$.

72. **Setup**: Let $\{p_j, |\psi_j\rangle\}$ be an ensemble of qubit states. Each individual $|\psi_j\rangle = \cos(\theta_j/2)|0\rangle + e^{i\phi_j}\sin(\theta_j/2)|1\rangle$ has a corresponding point on the Bloch sphere $(x_j, y_j, z_j) = (\cos\phi_j \sin\theta_j, \sin\phi_j \sin\theta_j, \cos\theta_j)$. Then we have

$$|\psi_j\rangle\langle\psi_j| = \begin{pmatrix} \cos^2\frac{\theta_j}{2} & e^{-i\phi_j}\cos\left(\frac{\theta_j}{2}\right)\sin\left(\frac{\theta_j}{2}\right) \\ e^{i\phi_j}\cos\left(\frac{\theta_j}{2}\right)\sin\left(\frac{\theta_j}{2}\right) & -\sin^2\frac{\theta_j}{2} \end{pmatrix} \tag{102}$$

$$= \begin{pmatrix} \frac{1+\cos\theta_j}{2} & e^{-i\phi_j}\frac{\sin\theta_j}{2} \\ e^{i\phi_j}\frac{\sin\theta_j}{2} & \frac{1-\cos\theta_j}{2} \end{pmatrix} \tag{103}$$

$$= \frac{1}{2}\begin{pmatrix} 1+z_j & x_j - iy_j \\ x_j + iy_j & 1 - z_j \end{pmatrix} \tag{104}$$

$$= \frac{1}{2}\left(I + (x_j, y_j, z_j)\cdot\vec{\sigma}\right) = \frac{I + \vec{n_j}\cdot\vec{\sigma}}{2} \tag{105}$$

where $\|n_j\| = 1$. The corresponding density matrix is

$$\rho = \sum_j p_j |\psi_j\rangle\langle\psi_j| \tag{106}$$

$$= \frac{1}{2} \sum_j p_j \left(I + \vec{n_j} \cdot \vec{\sigma} \right) \tag{107}$$

$$= \frac{1}{2} \left(\sum_j p_j I + \vec{\sigma} \cdot \sum_j p_j \vec{n_j} \right) \tag{108}$$

$$= \frac{1}{2} \left(I + \vec{\sigma} \cdot \vec{n} \right) \tag{109}$$

where $\sum_j p_j I = I \sum_j p_j = I$ and we have defined $\vec{n} = \sum_j p_j \vec{n_j}$.

(a) By the triangle inequality, $\|n\| = \left\| \sum_j p_j n_j \right\| \leq \sum_j p_j \|n_j\| = \sum_j p_j = 1$.

(b) If $\rho = I/2$, then it must be that $\vec{n} \cdot \vec{\sigma} = 0 \Rightarrow \vec{n} = 0 = \sum_j p_j \vec{n_j}$ which must mean that all p_j are identical.

(c) In a pure state, $p_j = \delta_{jr}$ for some fixed r. Thus, $\|\vec{n}\| = \|\vec{n_r}\| = 1$. Conversely, if $\|\vec{n}\| = 1$, then $\|\vec{n}\| = \sum_j \|p_j \vec{n_j}\|$. Suppose there was a pair $p_r, p_s > 0$. Then by the triangle inequality, $\vec{n_r}$ must be a multiple of $\vec{n_s}$. But we know that in a mixed state, each pair of the ensemble must be linearly independent. Thus, there can be at most one $p_r > 0$, and since $\sum_j p_j = 1 = p_r$, this must be a pure state.

(d) For pure states, $\rho = |\psi_r\rangle \langle\psi_r| = \frac{1}{2} \left(I + \vec{n_r} \cdot \vec{\sigma} \right)$. Letting

$$\vec{n_r} = (\cos\phi_r \sin\theta_r, \sin\phi_r \sin\theta_r, \cos\theta_r)$$

and repeating in reverse the steps of the above setup will lead back to $|\psi_r\rangle = \cos\theta_r |0\rangle + e^{i\phi} \sin\theta_r |1\rangle$. Thus, the Bloch vector for pure states corresponds to the point on the Bloch sphere.

74. Suppose the composite system AB is in the states $|a\rangle |b\rangle$, where $|a\rangle$ and $|b\rangle$ are pure states of A and B, respectively. Then, the reduced density operator for A is:

$$\rho_A = \mathrm{tr}_B \left(\rho_{AB} \right) \tag{110}$$

$$= \mathrm{tr}_B \left(|a\rangle \langle a| \otimes |b\rangle \langle b| \right) \tag{111}$$

$$= |a\rangle \langle a| \, \mathrm{tr}_B \left(|b\rangle \langle b| \right) \tag{112}$$

$$= |a\rangle \langle a| \langle b|b\rangle \tag{113}$$

$$= |a\rangle \langle a| \tag{114}$$

Similarly, ρ_B is a pure state as well.

75. **Reduced density operators for Bell states**. For $2^{-1/2}(|00\rangle + |11\rangle)$:

$$\rho_0 = \frac{\mathrm{tr}_0\left(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|\right)}{2} \tag{115}$$
$$= \frac{I}{2} \tag{116}$$
$$\rho_1 = \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} \tag{117}$$
$$= \frac{I}{2} \tag{118}$$

For $2^{-1/2}(|00\rangle - |11\rangle)$:

$$\rho_0 = \frac{\mathrm{tr}_0\left(|00\rangle\langle 00| - |00\rangle\langle 11| - |11\rangle\langle 00| + |11\rangle\langle 11|\right)}{2} \tag{119}$$
$$= \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} \tag{120}$$
$$= \frac{I}{2} \tag{121}$$
$$\rho_1 = \rho_0 \tag{122}$$

For $2^{-1/2}(|01\rangle + |10\rangle)$:

$$\rho_0 = \frac{\mathrm{tr}_0\left(|01\rangle\langle 01| + |01\rangle\langle 10| + |10\rangle\langle 01| + |10\rangle\langle 10|\right)}{2} \tag{123}$$
$$= \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} \tag{124}$$
$$= \frac{I}{2} \tag{125}$$
$$\rho_1 = \rho_0 \tag{126}$$

For $2^{-1/2}(|01\rangle - |10\rangle)$:

$$\rho_0 = \frac{\mathrm{tr}_0\left(|01\rangle\langle 01| - |01\rangle\langle 10| - |10\rangle\langle 01| + |10\rangle\langle 10|\right)}{2} \tag{127}$$
$$= \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} \tag{128}$$
$$= \frac{I}{2} \tag{129}$$
$$\rho_1 = \rho_0 \tag{130}$$

76. **General case of the Schmidt decomposition**: Let $|\psi\rangle$ be a pure state of the composite system AB, where A and B have dimensions m and n, respectively. Assume without loss of generality that $m < n$.

Then $|\psi\rangle = \sum_{j=0}^{m-1} \sum_{k=0}^{n-1} w_{jk} |j_A\rangle |k_B\rangle$ and the coefficients w_{jk} can be organized into a $m \times n$ rectangular matrix W:

$$|\psi\rangle = \underbrace{\begin{pmatrix} |0_A\rangle & |1_A\rangle & \cdots \end{pmatrix}}_{1\times m} \underbrace{\begin{pmatrix} w_{0,0} & \cdots \\ \vdots & \ddots \end{pmatrix}}_{m\times n} \underbrace{\begin{pmatrix} |0_B\rangle \\ |1_B\rangle \\ \vdots \end{pmatrix}}_{n\times 1} \tag{131}$$

$$= AWB \tag{132}$$

By the singular value decomposition theorem, $W = U\Sigma V^*$ where U, V are $m \times m$ and $n \times n$ unitary, respectively, and Σ is $m \times n$ diagonal:

$$|\psi\rangle = AWB \tag{133}$$

$$= AU\Sigma V^* B \tag{134}$$

$$= A'\Sigma B' \tag{135}$$

$$= \underbrace{\begin{pmatrix} |0_{A'}\rangle & |1_{A'}\rangle & \cdots \end{pmatrix}}_{1\times m} \underbrace{\begin{pmatrix} \lambda_0 & 0 & \cdots \\ 0 & \ddots & 0 \\ 0 & \cdots & \lambda_{n-1} \\ 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \end{pmatrix}}_{m\times n} \underbrace{\begin{pmatrix} |0_{B'}\rangle \\ |1_{B'}\rangle \\ \vdots \end{pmatrix}}_{n\times 1} \tag{136}$$

$$= \underbrace{\begin{pmatrix} |0_{A'}\rangle & |1_{A'}\rangle & \cdots & |(n-1)_{A'}\rangle \end{pmatrix}}_{1\times n} \underbrace{\begin{pmatrix} \lambda_0 & 0 & \cdots \\ 0 & \ddots & 0 \\ 0 & \cdots & \lambda_{n-1} \end{pmatrix}}_{n\times n} \underbrace{\begin{pmatrix} |0_{B'}\rangle \\ |1_{B'}\rangle \\ \vdots \end{pmatrix}}_{n\times 1} \tag{137}$$

$$= \sum_{k=0}^{n-1} \lambda_k |k_{A'}\rangle |k_{B'}\rangle \tag{138}$$

where A' (and similarly, B') is necessarily unitary and orthonormal:

$$(A')^* A' = U^* A^* A U \tag{139}$$

$$= U^* U \tag{140}$$

$$= I \tag{141}$$

78. **Equivalency of product states and Schmidt number 1**: Suppose $|\psi\rangle = |\psi_A\rangle |\psi_B\rangle$. Then, via Gram-Schmidt, an orthonormal basis can be

chosen to contain $|\psi_A\rangle$ and $|\psi_B\rangle$ for spaces A and B, respectively. Under this basis, $|\psi\rangle$ will have a Schmidt number of 1.

On the other hand, if $|\psi\rangle$ has a Schmidt number of 1, then it is trivially a product state.

Equivalency of product states and pure state reduced operators:

$$\mathrm{tr}_B\left(|\psi\rangle\langle\psi|\right) = \mathrm{tr}_B\left(|\psi_A\rangle\langle\psi_A| \otimes |\psi_B\rangle\langle\psi_B|\right) = |\psi_A\rangle\langle\psi_A|\langle\psi_B|\psi_B\rangle = |\psi_A\rangle\langle\psi_A|$$
$$\mathrm{tr}_A\left(|\psi\rangle\langle\psi|\right) = \mathrm{tr}_A\left(|\psi_A\rangle\langle\psi_A| \otimes |\psi_B\rangle\langle\psi_B|\right) = \langle\psi_A|\psi_A\rangle|\psi_B\rangle\langle\psi_B| = |\psi_B\rangle\langle\psi_B|$$

So $|\psi\rangle$ being a two-system product state is equivalent to both its reduced operators being pure states.

79. **Schmidt decompositions**: $|\psi_0\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$ is already its own decomposition.

$|\psi_1\rangle = \frac{|00\rangle+|01\rangle+|10\rangle+|11\rangle}{2}$ has a Hermitian coefficient matrix and so its SVD will coincide with its spectral decomposition:

$$\frac{1}{2}\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix} = \left[\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\right]\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\left[\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\right]$$

So $|\psi_1\rangle = \left(\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)\right)^{\otimes 2}$.

$|\psi_2\rangle = \frac{|00\rangle+|01\rangle+|10\rangle}{\sqrt{3}}$ again has a Hermitian coefficient matrix:

$$\frac{1}{\sqrt{3}}\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix} = \left[\frac{1}{\sqrt{1+\Phi^2}}\begin{pmatrix}\Phi & -1\\ 1 & \Phi\end{pmatrix}\right]\left[\frac{1}{\sqrt{3}}\begin{pmatrix}\Phi & 0\\ 0 & 1-\Phi\end{pmatrix}\right]\left[\frac{1}{\sqrt{1+\Phi^2}}\begin{pmatrix}\Phi & 1\\ -1 & \Phi\end{pmatrix}\right]$$

where Φ is the golden ratio $\frac{1+\sqrt{5}}{2}$. Letting $N = \sqrt{1+\Phi^2}$,

$$|\psi_2\rangle = \frac{\Phi}{\sqrt{3}}\left(\frac{\Phi|0\rangle + |1\rangle}{N}\right)^{\otimes 2} + \frac{1-\Phi}{\sqrt{3}}\left(\frac{\Phi|1\rangle - |0\rangle}{N}\right)^{\otimes 2}$$

80. Suppose that $|\psi\rangle = \sum_i \lambda_i |i_A\rangle|i_B\rangle$ and $|\phi\rangle = \sum_i \lambda_i |i'_A\rangle|i'_B\rangle$. Let $U = A_A\left(A_{A'}\right)^*$, where A_A and $A_{A'}$ are square matrices formed by a columnwise arrangement of i_A and i'_A, respectively. Then $A_A = UA_{A'}$. Furthermore, $UU^* = A_A\left(A_{A'}\right)^* A_{A'}A_A^* = A_AA_A^* = I$, so U is unitary.

Similarly, there exists a unitary matrix V such that $B_B = VB_{B'}$. Thus,

$$|\psi\rangle = \sum_i \lambda_i |i_A\rangle|i_B\rangle \tag{142}$$
$$= \sum_i \lambda_i (U|i'_A\rangle) \otimes (V|i'_B\rangle) \tag{143}$$

$$= (U \otimes V) \sum_i \lambda_i |i'_A\rangle |i'_B\rangle \tag{144}$$

$$= (U \otimes V) |\phi\rangle \tag{145}$$

Problems

1. We already showed in Exercise 60 that for a normal $\vec{n} \in \mathbb{R}^3$, $\vec{n} \cdot \vec{\sigma}$ has eigenvalues ± 1 and eigenvectors $|+\rangle$ and $|-\rangle$, whose corresponding projectors are

$$P_+ = |+\rangle \langle +| = \frac{I + \vec{n} \cdot \vec{\sigma}}{2} \tag{146}$$

$$P_- = |-\rangle \langle -| = \frac{I - \vec{n} \cdot \vec{\sigma}}{2} \tag{147}$$

Using the definition of an operator function:

$$f(\theta \vec{n} \cdot \vec{\sigma}) = f\left(\sum_i \theta \lambda_i |i\rangle \langle i|\right) \tag{148}$$

$$= \sum_i f(\theta \lambda_i) |i\rangle \langle i| \tag{149}$$

$$= f(\theta) \frac{I + \vec{n} \cdot \vec{\sigma}}{2} + f(-\theta) \frac{I - \vec{n} \cdot \vec{\sigma}}{2} \tag{150}$$

$$= \frac{f_\theta + f_{-\theta}}{2} I + \frac{f_\theta - f_{-\theta}}{2} \vec{n} \cdot \vec{\sigma} \tag{151}$$

4

Exercises

1. **Eigenvectors of Pauli matrices**: Pauli X:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \left[\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\right] \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \left[\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\right]$$
$$\frac{|0\rangle + |1\rangle}{\sqrt{2}} \Rightarrow (\phi, \theta) = \left(0, \frac{\pi}{2}\right) \Rightarrow (1, 0, 0)$$
$$\frac{|0\rangle - |1\rangle}{\sqrt{2}} \Rightarrow (\phi, \theta) = \left(\pi, \frac{\pi}{2}\right) \Rightarrow (-1, 0, 0)$$

Pauli Y:

$$Y = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} = \left[\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}\right] \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \left[\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}\right]$$

$$
\begin{aligned}
\frac{|0\rangle + i\,|1\rangle}{\sqrt{2}} &\Rightarrow (\phi, \theta) = \left(\frac{\pi}{2}, \frac{\pi}{2}\right) \Rightarrow (0, 1, 0) \\
\frac{|0\rangle - |1\rangle}{\sqrt{2}} &\Rightarrow (\phi, \theta) = \left(-\frac{\pi}{2}, \frac{\pi}{2}\right) \Rightarrow (0, -1, 0)
\end{aligned}
$$

Pauli Z:

$$
Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = IZI^*
$$

$$
\begin{aligned}
|0\rangle &\Rightarrow \theta = 0 \Rightarrow (0, 0, 1) \\
|1\rangle &\Rightarrow \theta = \pi \Rightarrow (0, 0, -1)
\end{aligned}
$$

2.

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

3.

$$
R_z\left(\frac{\pi}{4}\right) = \begin{pmatrix} \exp\left(-\frac{\pi i}{8}\right) & 0 \\ 0 & \exp\left(\frac{\pi i}{8}\right) \end{pmatrix} = \exp\left(-\frac{\pi i}{8}\right) T
$$

4. Note that $X^2 = Y^2 = Z^2 = I$, $XZ = -ZX$, and $ZXZ = -Z^2X = -X$.

$$
\begin{aligned}
R_z\left(\frac{\pi}{2}\right) R_x\left(\frac{\pi}{2}\right) R_z\left(\frac{\pi}{2}\right) &= \frac{1}{\sqrt{2}^3} (I - iZ)\,(I - iX)\,(I - iZ) \\
&= \frac{1}{\sqrt{2}^3} (I - iZ)\,[I - i\,(X + Z) - XZ] \\
&= \frac{1}{\sqrt{2}^3} [I - i\,(X + Z) - XZ - iZ - XZ - I + iZXZ] \\
&= \frac{1}{\sqrt{2}^3} [-i\,(X + Z) - iZ - iX]
\end{aligned}
$$

$$
\begin{aligned}
&= -\frac{2i}{\sqrt{2}^3}(X+Z) \\
&= -i\frac{X+Z}{\sqrt{2}} \\
&= -iH
\end{aligned}
$$

5. Let $n \in \mathbb{R}^3$ with $\|n\|^2 = 1$ and note that $XY = -YX, XZ = -ZX, YZ = -ZY$.

$$
\begin{aligned}
(n \cdot \sigma)^2 &= \left(\sum_{i \in \{x,y,z\}} n_i \sigma_i \right)^2 \\
&= \sum_{i \in \{x,y,z\}} n_i^2 \sigma_i^2 + \sum_{\substack{i,j \in \{x,y,z\} \\ i \neq j}} n_i n_j \sigma_i \sigma_j \\
&= \sum_{i \in \{x,y,z\}} n_i^2 \sigma_i^2 \\
&= I \sum_{i \in \{x,y,z\}} n_i^2 && \text{since } X^2 = Y^2 = Z^2 = I \\
&= I
\end{aligned}
$$

6. Some identities ($c_\theta = \cos\theta$, and $s_\theta = \sin\theta$):
   (a) $YZ = iX$, $XZ = -iY$, $XY = iZ$.

   (b) $R_i(-a) = c_{\frac{a}{2}} I - i s_{\left(-\frac{a}{2}\right)} \sigma_i = c_{\frac{a}{2}} I + i s_{\frac{a}{2}} \sigma_i = R_i(a)^* = R_i(a)^{-1}$.

   (c) Letting $b = a/2$:
      i.
$$
\begin{aligned}
R_z(a) Z R_z(a)^* &= (c_b I - i s_b Z) Z (c_b I + i s_b Z) \\
&= c_b^2 Z + s_b^2 Z^3 + i c_b s_b Z^2 - i c_b s_b Z^2 \\
&= Z
\end{aligned}
$$

      ii.
$$
\begin{aligned}
R_z(a) X R_z(a)^* &= c_b^2 X + s_b^2 ZXZ + i c_b s_b XZ - i c_b s_b ZX \\
&= \left(c_b^2 - s_b^2\right) X + 2 i c_b s_b XZ
\end{aligned}
$$

$$= c_a X + s_a Y$$

iii.

$$\begin{aligned} R_z(a) Y R_z(a)^* &= c_b^2 Y + s_b^2 ZYZ + ic_b s_b YZ - ic_b s_b ZY \\ &= \left(c_b^2 - s_b^2\right) Y + 2ic_b s_b YZ \\ &= c_a Y - s_a X \end{aligned}$$

iv.

$$\begin{aligned} R_y(a) Z R_y(a)^* &= (c_b I - is_b Y) Z (c_b I + is_b Y) \\ &= c_b^2 Z + s_b^2 YZY + ic_b s_b ZY - ic_b s_b YZ \\ &= \left(c_b^2 - s_b^2\right) Z - 2ic_b s_b YZ \\ &= c_a Z + s_a X \end{aligned}$$

Proposition: Let n be a unit vector of $\mathbb{R}^3$, and $0 \le \theta \le 2\pi$, $0 \le \phi \le \pi$ such that $n = (\sin\phi\cos\theta, \sin\phi\sin\theta, \cos\phi)$. Then,

$$R_n(\omega) = R_{(\theta,\phi)}(\omega) = R_z(\theta) R_y(\phi) R_z(\omega) R_y(-\phi) R_z(-\theta)$$

.

<u>Proof</u>:

$$\begin{aligned} \Omega &= R_y(\phi) R_z(\omega) R_y(\phi)^* \\ &= c_{\frac{\omega}{2}} I - is_{\frac{\omega}{2}} R_y(\phi) Z R_y(\phi)^* \\ &= c_{\frac{\omega}{2}} I - is_{\frac{\omega}{2}} \left[c_\phi Z + s_\phi X\right] \end{aligned}$$

Expanding again:

$$\begin{aligned} R_z(\theta) \Omega R_z(\theta)^* &= c_{\frac{\omega}{2}} I - is_{\frac{\omega}{2}} R_z(\theta) \left[c_\phi Z + s_\phi X\right] R_z(\theta)^* \\ &= c_{\frac{\omega}{2}} I - is_{\frac{\omega}{2}} \left[c_\phi Z + s_\phi R_z(\theta) X R_z(\theta)^*\right] \\ &= c_{\frac{\omega}{2}} I - is_{\frac{\omega}{2}} \left[c_\phi Z + s_\phi (c_\theta X + s_\theta Y)\right] \\ &= c_{\frac{\omega}{2}} I - is_{\frac{\omega}{2}} (n_z Z + n_x X + n_y Y) \\ &= R_n(\omega) \end{aligned}$$

□

By Exercise 2.72, a qubit state $|\psi\rangle$ represented by the Bloch vector λ will have density matrix $\rho = |\psi\rangle\langle\psi| = (I + \lambda \cdot \sigma)/2$.

$$R_z(a) \rho R_z(a)^* = \frac{1}{2}\left(I + R_z(a)(\lambda \cdot \sigma) R_z(a)\right)$$

$$
\begin{aligned}
&= \frac{1}{2}\left[I + \lambda_x\left(c_a X + s_a Y\right) + \lambda_y\left(c_a Y - s_a X\right) + \lambda_z Z\right] \\
&= \frac{1}{2}\left[I + \lambda_x\left(c_a - s_a\right) X + \lambda_y\left(c_a + s_a\right) Y + \lambda_z\right] \\
&= \frac{I + \lambda' \cdot \sigma}{2}
\end{aligned}
$$

So the effect of $R_z(a)$ is to z-rotate λ by a. Similarly, $R_y(a)$ will y-rotate λ by a. Letting $R_{z,\theta} = R_z(\theta)$, the action of $R_n(\omega)$ on λ will be:

$$
\begin{aligned}
\rho' &= R_{(\theta,\phi)}(\omega)\,\rho R_{(\theta,\phi)}(\omega)^* \\
&= R_{z,\theta}\left(R_{y,\phi}\left(R_{z,\omega}\left(R_{y,-\phi}\left(R_{z,-\theta}\rho R_{z,\theta}\right)R_{y,\phi}\right)R_{z,-\omega}\right)R_{y,-\phi}\right)R_{z,-\theta}
\end{aligned}
$$

which is a rotation around n by ω.

7. Since $XY = -YX$, $XYX = -YX^2 = -Y$. Then:

$$
\begin{aligned}
XR_y(\theta)X &= \cos(\theta) I - i\sin(\theta) XYX \\
&= \cos(\theta) I + i\sin(\theta) Y \\
&= \cos(\theta) I - i\sin(-\theta) Y \qquad = R_y(-\theta)
\end{aligned}
$$

8. (a) **Proposition**: I, X, Y, Z form a basis in the space of matrices $\mathbb{C}^{2\times 2}$.

   Proof: In such a space, I, X, Y, Z are linearly independent:

$$
\begin{aligned}
jI + kX + mY + nZ &= 0 \\
\begin{pmatrix} j+n & k-im \\ k+im & j-n \end{pmatrix} &= 0 \\
j+n = 0,\ j-n = 0 &\Rightarrow j = n = 0 \\
k-im = 0,\ k+im = 0 &\Rightarrow k = m = 0
\end{aligned}
$$

   and $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} j+n & k-im \\ k+im & j-n \end{pmatrix} \Rightarrow j = \frac{a+d}{2},\ n = \frac{a-d}{2},\ k = \frac{b+c}{2},\ m = i\frac{b-c}{2}$, so that the coefficients are unique. □

   Next, let $U \in \mathbb{C}^{2\times 2}$ be unitary. By Exercise 2.18 and the spectral theorem,

$$
\begin{aligned}
U &= V\begin{pmatrix} e^{ia} & 0 \\ 0 & e^{ib} \end{pmatrix} V^* \\
&= e^{ic} V\begin{pmatrix} e^{ik} & 0 \\ 0 & e^{-ik} \end{pmatrix} V^* \\
&= e^{ic} V \Lambda V^* \\
&= e^{ic} W
\end{aligned}
$$

where $c = -i\frac{a+b}{2}$ and $k = \frac{a-b}{2}$ so that

$$\mathrm{tr}\,[W] = \mathrm{tr}\,[\Lambda] = e^{ik} + e^{-ik} = 2\cos k \in \mathbb{R}$$

Using the above proposition, $W = wI + n \cdot \sigma$ (where $n \in \mathbb{C}^3$, σ is the usual vector of Pauli matrices, and $w = (\exp(ik) + \exp(-ik))/2 = \cos k$). Since W is also unitary:

$$\begin{aligned} I &= WW^* \\ &= (wI + n \cdot \sigma)(wI + n^* \cdot \sigma) \\ &= w^2 I + (w(n + n^*)) \cdot \sigma + (n \cdot \sigma)(n^* \cdot \sigma) \\ &= w^2 I + (2w\mathrm{Re}\,(n)) \cdot \sigma + \langle n|n\rangle I + \left(n_x n_y^* - n_y n_x^*\right) XY \\ &\qquad + (n_x n_z^* - n_z n_x^*) XZ + \left(n_y n_z^* - n_z n_y^*\right) YZ \end{aligned}$$

which yields the constraints

$$\begin{aligned} \cos^2 k + \langle n|n\rangle &= 1 \\ \mathrm{Re}\,(n)\cos k &= 0 \\ n_x n_y^* &= n_y n_x^* \\ n_y n_z^* &= n_z n_y^* \\ n_x n_z^* &= n_z n_x^* \end{aligned}$$

Letting $n = \left(r_x e^{ix}, r_y e^{iy}, r_z e^{iz}\right)$, the last three constraints become:

$$\begin{aligned} e^{i(x-y)} &= e^{i(y-x)} \Rightarrow x = y \\ e^{i(y-z)} &= e^{i(z-y)} \Rightarrow y = z \\ e^{i(x-z)} &= e^{i(z-x)} \Rightarrow x = z \end{aligned}$$

which means that $n = e^{i\theta} r$, where $r \in \mathbb{R}^3$ and $\theta = x = y = z$.

Suppose that $\cos k = 0$. Then $\langle n|n\rangle = \|r\|^2 = 1$. Thus,

$$\begin{aligned} U &= e^{ic} W \\ &= e^{ic}(\cos(k) I + n \cdot \sigma) \\ &= \frac{e^{ic} e^{i\theta}}{i}(ir \cdot \sigma) \\ &= e^{i\phi} R_r(\pi), \phi = c + \theta - \frac{\pi}{2} \end{aligned}$$

On the other hand, if $\cos k \neq 0$, then $\mathrm{Re}\,(n) = 0$ and

$$n = e^{i\theta} r = (\cos\theta + i\sin\theta) r = i\sin(\theta) r$$

Since $\cos^2 k + \langle n|n \rangle = \cos^2 k + \sin^2 \theta = 1$, it must be that $\theta = k$. Expanding U once more:

$$\begin{aligned} U &= e^{ic} \left(\cos(k) I + i \sin(k) r \right) \\ &= e^{ic} R_r (2k) \end{aligned}$$

(b)

$$\begin{aligned} H &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \\ &= \frac{X+Z}{\sqrt{2}} \\ &= -\frac{1}{i} \left(\cos\left(\frac{\pi}{2}\right) I - i \sin\left(\frac{\pi}{2}\right) n \cdot \sigma \right), n = \frac{1}{\sqrt{2}} (1, 0, 1) \\ &= \exp\left(i \frac{\pi}{2}\right) R_n (\pi) \end{aligned}$$

(c) We want to find a k such that $e^{ik} \left(e^{ic} + e^{-ic} \right) = 1+i$, for some $c \in \mathbb{R}$:

$$\begin{aligned} S &= \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \\ &= \exp\left(i \frac{\pi}{4}\right) \begin{pmatrix} \exp\left(-i \frac{\pi}{4}\right) & 0 \\ 0 & \exp\left(i \frac{\pi}{4}\right) \end{pmatrix} \\ &= \exp\left(i \frac{\pi}{4}\right) \left(\cos\left(\frac{\pi}{4}\right) I - i \sin\left(\frac{\pi}{4}\right) Z \right) \\ &= \exp\left(i \frac{\pi}{4}\right) R_n \left(\frac{\pi}{2}\right), n = (0, 0, 1) \end{aligned}$$

9. Suppose that $U = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{C}^{2\times 2}$ is unitary. Since its column vectors are normal,

$$U = \begin{pmatrix} e^{i\alpha} \cos j & e^{i\beta} \sin k \\ e^{i\gamma} \sin j & e^{i\delta} \cos k \end{pmatrix}$$

Or, factoring out $e^{i\alpha}$ with no loss of generality,

$$U = e^{i\alpha} \begin{pmatrix} \cos j & e^{i\beta} \sin k \\ e^{i\gamma} \sin j & e^{i\delta} \cos k \end{pmatrix}$$

The column vectors are also orthogonal, implying that

$$\begin{pmatrix} a^* & c^* \end{pmatrix} \begin{pmatrix} b \\ d \end{pmatrix} = 0$$

$$
\begin{aligned}
&= e^{i\beta}\cos j \sin k + e^{i\delta - i\gamma}\sin j \cos k \\
&= \cos j \sin k + e^{i\delta + i\gamma - i\beta}\sin j \cos k
\end{aligned}
$$

and

$$
\begin{aligned}
\begin{pmatrix} b^* & d^* \end{pmatrix}\begin{pmatrix} a \\ c \end{pmatrix} &= 0 \\
&= e^{-i\beta}\cos j \sin k + e^{i\gamma - i\delta}\sin j \cos k \\
&= \cos j \sin k + e^{i\beta + i\gamma - i\delta}\sin j \cos k
\end{aligned}
$$

which together imply that $\delta = \gamma + \beta$. Substituting back into the previous equation,

$$
\begin{aligned}
\cos j \sin k + e^{i\beta + i\gamma - i\delta}\sin j \cos k &= \cos j \sin k + \sin j \cos k \\
&= \sin(j + k) \\
&= 0 \\
\implies j &= -k
\end{aligned}
$$

Substituting back into the definition of U and multiplying by a global phase of $\exp\left(-i\frac{\beta+\gamma}{2}\right)$,

$$
\begin{aligned}
U &= e^{-i\frac{\beta+\gamma}{2}} e^{i\alpha}\begin{pmatrix} \cos j & -e^{i\beta}\sin j \\ e^{i\gamma}\sin j & e^{i\delta}\cos j \end{pmatrix} \\
&= e^{-i\frac{\beta+\gamma}{2}}\begin{pmatrix} e^{i\alpha}\cos j & -e^{i\alpha + i\beta}\sin j \\ e^{i\alpha + i\gamma}\sin j & e^{i\alpha + i\beta + i\gamma}\cos j \end{pmatrix} \\
&= \begin{pmatrix} e^{i\alpha - i\frac{\beta}{2} - \frac{\gamma}{2}}\cos j & -e^{i\alpha + i\frac{\beta}{2} - i\frac{\gamma}{2}}\sin j \\ e^{i\alpha - i\frac{\beta}{2} + \frac{\gamma}{2}}\sin j & e^{i\alpha + i\frac{\beta}{2} + \frac{\gamma}{2}}\cos j \end{pmatrix}
\end{aligned}
$$

12. From Exercise 4.08, H will rotate a Bloch vector by around $(1, 0, 1)$ by π. Intuitively, this rotation is equivalent to z-rotating by π and then y-rotating by $\pi/2$. Confirming algebraically:

$$
\begin{aligned}
H &= iR_{\frac{(1,0,1)}{\sqrt{2}}}(\pi) \\
&= iR_z(2\pi)\, R_y\left(\frac{\pi}{2}\right) R_z(\pi) \\
&= iI\left[\frac{1}{\sqrt{2}}(I - iY)\right](-iZ) \\
&= \frac{1}{\sqrt{2}}(Z - iYZ) \\
&= \frac{1}{\sqrt{2}}(Z + X) && \text{since } YZ = iX
\end{aligned}
$$

$$= H$$

So, $H = \exp(\pi i/2) ABC$ where $A = R_y(\pi/4)$, $B = R_y(-\pi/4) R_z(\pi/2)$, and $C = R_z(-\pi/2)$.

13. Using the identities from exercises 4.05 and 4.06:

$$\begin{aligned} HXH &= \frac{1}{2}(X+Z) X (X+Z) \\ &= \frac{1}{2}\left(X^3 + ZXZ + X^2 Z + ZX^2\right) \\ &= \frac{1}{2}(X - X + 2Z) \\ &= Z \end{aligned}$$

And since $ZYX = -YZX = YXZ = -XYZ$:

$$HYH = \frac{1}{2}(XYX + ZYZ + ZYX + XYZ) = \frac{1}{2} \cdot -2Y = -Y$$

and

$$HZH = \frac{1}{2}\left(XZX + Z^3 + Z^2 X + XZ^2\right) = \frac{1}{2} \cdot 2X = X$$

14. Since $T = \exp(i\pi/8) R_z(\pi/8)$ and noting that $H^2 = I$,

$$\begin{aligned} HTH &= \exp\left(\frac{i\pi}{8}\right) H (\cos I - i \sin Z) H \\ &= \exp\left(\frac{i\pi}{8}\right) (\cos I - i \sin HZH) \\ &= \exp\left(\frac{i\pi}{8}\right) (\cos I - i \sin X) \\ &= \exp\left(\frac{i\pi}{8}\right) R_x\left(\frac{\pi}{8}\right) \end{aligned}$$

15. **Setup**: Let $m, n \in \mathbb{R}^3$, $\|m\| = \|n\| = 1$. Using the identities in 4.06:

$$\begin{aligned} (m \cdot \sigma)(n \cdot \sigma) &= (m_x X + m_y Y + m_z Z)(n_x X + n_y Y + n_z Z) \\ &= (m \cdot n) I + (m_y n_z - m_z n_y) YZ + (m_z n_x - m_x n_z) ZX \\ &\quad + (m_x n_y - m_y n_z) XY \\ &= (m \cdot n) I + i (m_y n_z - m_z n_y) X + i (m_z n_x - m_x n_z) Y \\ &\quad + i (m_x n_y - m_y n_z) Z \\ &= (m \cdot n) I + i (m \times n) \cdot \sigma \end{aligned}$$

(a) Letting $c_i = \cos(\beta_i/2)$ and $s_i = \sin(\beta_i/2)$, the composition C of two qubit rotations becomes:

$$\begin{aligned}
C &= R_{n_2}(\beta_2) R_{n_1}(\beta_1) \\
&= [c_2 I - i s_2 (n_2 \cdot \sigma)] [c_1 I - i s_1 (n_1 \cdot \sigma)] \\
&= c_1 c_2 I - s_1 s_2 [(n_2 \cdot n_1) I + i (n_2 \times n_1) \cdot \sigma] \\
&\qquad - i [c_1 s_2 (n_2 \cdot \sigma) + s_1 c_2 (n_1 \cdot \sigma)] \\
&= [c_1 c_2 - s_1 s_2 (n_2 \cdot n_1)] I - i [s_1 s_2 (n_2 \times n_1) + c_1 s_2 n_2 + s_1 c_2 n_1] \cdot \sigma
\end{aligned}$$

Thus, $C = R_{n_{12}}(\beta_{12})$, where $\cos(\beta_{12}/2) = c_1 c_2 - s_1 s_2 (n_2 \cdot n_1)$ and $\sin(\beta_{12}/2)\, n_{12} = s_1 s_2 (n_2 \times n_1) + c_1 s_2 n_2 + s_1 c_2 n_1$.

(b) If $\beta_1 = \beta_2$ and $n_1 = z$, then $c_1 = c_2 = c$, $s_1 = s_2 = s$, $\cos(\beta_{12}/2) = c^2 - s^2 (n_2 \cdot z)$, and $\sin(\beta_{12}/2)\, n_{12} = s^2 (n_2 \times z) + sc\,(n_2 + n_1)$.

16. The circuit

```
--- [H] ---
-----------
```

is

$$I \otimes H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}$$

while

```
-----------
--- [H] ---
```

is

$$H \otimes I = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}$$

17.
```
--- [H] --- [Z] --- [H] ---
             |
-------------+-------------
```

When the lower qubit is $|0\rangle$, the upper qubit remains unchanged since $H^2 = I$. When it is $|1\rangle$, the upper is flipped, since $HZH = X$.

18. ```
--- [Z] ---
      |
-----+-----
```

has mapping: $|0\rangle|i\rangle \mapsto |0\rangle|i\rangle$, $|10\rangle \mapsto |10\rangle$, $|11\rangle \mapsto -|11\rangle$. On the other hand,

```
-----+-----
      |
--- [Z] ---
```

has mapping: $|i\rangle|0\rangle \mapsto |i\rangle|0\rangle$, $|01\rangle \mapsto |01\rangle$, $|11\rangle \mapsto -|11\rangle$. Since the mappings are identical, their matrices will be the same as well.

19. Let $|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$ and

$$I \otimes X^c = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Then $|\phi\rangle = (I \otimes X^c)|\psi\rangle = a|00\rangle + b|01\rangle + d|10\rangle + c|11\rangle$ and its density matrix is:

$$|\phi\rangle\langle\phi| = \begin{pmatrix} aa^* & ab^* & ad^* & ac^* \\ ba^* & bb^* & bd^* & bc^* \\ ca^* & cb^* & cd^* & cc^* \\ da^* & db^* & dd^* & dc^* \end{pmatrix}$$

which is simply a permutation of

$$|\psi\rangle\langle\psi| = \begin{pmatrix} aa^* & ab^* & ac^* & ad^* \\ ba^* & bb^* & bc^* & bd^* \\ ca^* & cb^* & cc^* & cd^* \\ da^* & db^* & dc^* & dd^* \end{pmatrix}$$

20. Letting $I \otimes X^c$ denote controlled-NOT conditioned on the first qubit, the left circuit diagram is:

$$\begin{aligned} J &= (H \otimes H)(I \otimes X^c)(H \otimes H) \\ &= \frac{1}{2}(H \otimes H)\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \\ &= \frac{1}{4}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \end{pmatrix} \end{aligned}$$
```

$$
\begin{aligned}
&= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \\
&= X^c \otimes I
\end{aligned}
$$

which is the right diagram.

Let $B : |0,1\rangle \mapsto |\pm\rangle$ where $B = H$. Under the $|\pm\rangle$ basis, the operation $X^c \otimes I$ becomes:

$$
\begin{aligned}
L &= (B \otimes B)\, J\, (B \otimes B)^{-1} \\
&= (B \otimes B)\, J\, (B \otimes B) \\
&= (H \otimes H)\, (X^c \otimes I)\, (H \otimes H) \\
&= I \otimes X^c
\end{aligned}
$$

In other words, CNOT conditioned on the second qubit in the $|0,1\rangle$ basis is equivalent to CNOT conditioned on the first qubit in the $|\pm\rangle$ basis.

22.

23. Let $U = R_x(\theta)$. In the Bloch space, this is a rotation around the x-axis by θ which, intuitively, is equivalent to:

$$
R_x(\theta) = R_z\left(-\frac{\pi}{2}\right) R_y(\theta)\, R_z\left(\frac{\pi}{2}\right)
$$

Using the ABC theorem:

```
----------------+--------------------+-----------------------------
                |                    |
--[R_z(pi/2)]--[X]--[R_y(-theta/2)]--[X]--[R_z(-pi/2) R_y(theta/2)]--
```

Now let $U = R_y(\theta) = R_z(0)\, R_y(\theta)\, R_z(0)$. Under the ABC theorem, $C = I$:

```
---+--------------------+------------------
   |                    |
--[X]--[R_y(-theta/2)]--[X]--[R_y(theta/2)]--
```

32. Equation 4.40 follows from equation 2.152. Namely,

$$
\begin{aligned}
\rho' &= \sum_m M_m \rho M_m^* && \text{equation 2.152} \\
&= P_0 \rho P_0^* + P_1 \rho P_1^*
\end{aligned}
$$

$$= P_0 \rho P_0 + P_1 \rho P_1 \qquad \text{since } P_r^2 = P_r$$

where $P_r = I \otimes |i\rangle \langle i|$ and the observable is $I \otimes Z = P_0 - P_1$.

Suppose $\rho = \sum_i p_i |\psi_i\rangle \langle \psi_i|$, where

$$|\psi_i\rangle = \frac{1}{\sqrt{N_i}} \sum_{j=0}^{N_i-1} |a_{i,j}\rangle |b_{i,j}\rangle$$

Then,

$$\begin{aligned}
P_r \rho P_r &= P_r \left[\sum_i p_i \frac{1}{N_i} \left(\sum_{j,k}^{N_i-1} |a_{i,j}\rangle \langle a_{i,k}| \otimes |b_{i,j}\rangle \langle b_{i,k}| \right) \right] P_r \\
&= \sum_i \frac{p_i}{N_i} \left(\sum_{j,k}^{N_i-1} |a_{i,j}\rangle \langle a_{i,k}| \otimes |r\rangle \langle r|b_{i,j}\rangle \langle b_{i,k}|r\rangle \langle r| \right)
\end{aligned}$$

Partial trace $\mathrm{tr}_2 [\rho']$:

$$\begin{aligned}
\mathrm{tr}_2 [\rho'] &= \mathrm{tr}_2 [P_0 \rho P_0] + \mathrm{tr}_2 [P_1 \rho P_1] \\
&= \sum_i \frac{p_i}{N_i} \left(\sum_{j,k}^{N_i-1} |a_{i,j}\rangle \langle a_{i,k}| \, \mathrm{tr} [|0\rangle \langle 0|b_{i,j}\rangle \langle b_{i,k}|0\rangle \langle 0|] \right) \\
&\quad + \sum_i \frac{p_i}{N_i} \left(\sum_{j,k}^{N_i-1} |a_{i,j}\rangle \langle a_{i,k}| \, \mathrm{tr} [|1\rangle \langle 1|b_{i,j}\rangle \langle b_{i,k}|1\rangle \langle 1|] \right) \\
&= \sum_i \frac{p_i}{N_i} \left(\sum_{j,k}^{N_i-1} \langle b_{i,k}|0\rangle \langle 0|b_{i,j}\rangle |a_{i,j}\rangle \langle a_{i,k}| + \langle b_{i,k}|1\rangle \langle 1|b_{i,j}\rangle |a_{i,j}\rangle \langle a_{i,k}| \right) \\
&= \sum_i \frac{p_i}{N_i} \left(\sum_{j,k}^{N_i-1} \langle b_{i,k}| \left(|0\rangle \langle 0| + |1\rangle \langle 1| \right) |b_{i,j}\rangle |a_{i,j}\rangle \langle a_{i,k}| \right) \\
&= \sum_i \frac{p_i}{N_i} \left(\sum_{j,k}^{N_i-1} \langle b_{i,k}|b_{i,j}\rangle |a_{i,j}\rangle \langle a_{i,k}| \right) \\
&= \sum_i \frac{p_i}{N_i} \left(\sum_{j,k}^{N_i-1} \mathrm{tr} [|b_{i,j}\rangle \langle b_{i,k}|] |a_{i,j}\rangle \langle a_{i,k}| \right) \\
&= \sum_i \frac{p_i}{N_i} \left(\sum_{j,k}^{N_i-1} \mathrm{tr}_2 [|a_{i,j}\rangle \langle a_{i,k}| \otimes |b_{i,j}\rangle \langle b_{i,k}|] \right) \\
&= \mathrm{tr}_2 [\rho]
\end{aligned}$$

33. Let the state of the two-qubit system be:

$$|\psi\rangle = \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}, \quad a, b, c, d \in \mathbb{C}$$

After the $C_0(X)$ and H_0, the state will be:

$$\begin{aligned}
|\psi'\rangle &= (H \otimes I) \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} |\psi\rangle \\
&= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix} \begin{pmatrix} a \\ b \\ d \\ c \end{pmatrix} \\
&= \frac{1}{\sqrt{2}} \begin{pmatrix} a+d \\ b+c \\ a-d \\ b-c \end{pmatrix}
\end{aligned}$$

Measuring both qubits in the computational basis will project $|\psi'\rangle$ onto its components:

$$|\psi'\rangle \xrightarrow{|00\rangle\langle 00|} \frac{1}{\sqrt{2}} \begin{pmatrix} a+d \\ 0 \\ 0 \\ 0 \end{pmatrix} \qquad \text{with probability } \frac{|a+d|^2}{2}$$

$$|\psi'\rangle \xrightarrow{|01\rangle\langle 01|} \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ b+c \\ 0 \\ 0 \end{pmatrix} \qquad \text{with probability } \frac{|b+c|^2}{2}$$

$$|\psi'\rangle \xrightarrow{|10\rangle\langle 10|} \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 0 \\ a-d \\ 0 \end{pmatrix} \qquad \text{with probability } \frac{|a-d|^2}{2}$$

$$|\psi'\rangle \xrightarrow{|11\rangle\langle 11|} \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 0 \\ 0 \\ b-c \end{pmatrix} \qquad \text{with probability } \frac{|b-c|^2}{2}$$

On the other hand, consider the Bell states:

$$|\beta_0\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

$$|\beta_1\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$

$$|\beta_2\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$

$$|\beta_3\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

Letting $E_m = |\beta_m\rangle \langle\beta_m|$, we have $\sum_m E_m = I$ since the $|\beta_m\rangle$ form an orthonormal basis over the Hermitian space of two qubits.

In other words, the E_m form a POVM for the measurement operators:

$$M_0 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$M_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$M_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$M_3 = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

where $E_m = M_m^* M_m$.

Measuring $|\psi\rangle$ directly in this basis results in:

$$|\psi\rangle \xrightarrow{M_0} \frac{1}{\sqrt{2}} \begin{pmatrix} a+d \\ 0 \\ 0 \\ 0 \end{pmatrix} \qquad \text{with probability } \frac{|a+d|^2}{2}$$

$$|\psi\rangle \xrightarrow{M_1} \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ b+c \\ 0 \\ 0 \end{pmatrix} \qquad \text{with probability } \frac{|b+c|^2}{2}$$

$$|\psi\rangle \xrightarrow{M_2} \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 0 \\ a-d \\ 0 \end{pmatrix} \qquad \text{with probability } \frac{|a-d|^2}{2}$$

$$|\psi\rangle \xrightarrow{M_3} \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 0 \\ 0 \\ b-c \end{pmatrix} \qquad \text{with probability } \frac{|b-c|^2}{2}$$

34. The circuit input is $|0\rangle |\psi\rangle$. After the first Hadamard gate:

$$|0\rangle |\psi\rangle \xrightarrow{H \otimes I} \frac{(|0\rangle + |1\rangle) |\psi\rangle}{\sqrt{2}}$$

After the U conditioned on the first qubit:

$$\frac{(|0\rangle + |1\rangle) |\psi\rangle}{\sqrt{2}} \xrightarrow{C^0(U)} \frac{|0\rangle |\psi\rangle + |1\rangle U |\psi\rangle}{\sqrt{2}}$$

After the second Hadamard:

$$\begin{aligned} \frac{|0\rangle |\psi\rangle + |1\rangle U |\psi\rangle}{\sqrt{2}} \xrightarrow{H \otimes I} & \frac{\frac{|0\rangle + |1\rangle}{\sqrt{2}} |\psi\rangle + \frac{|0\rangle - |1\rangle}{\sqrt{@}} U |\psi\rangle}{\sqrt{2}} \\ &= \frac{|0\rangle (|\psi\rangle + U |\psi\rangle) + |1\rangle (|\psi\rangle - U |\psi\rangle)}{2} \\ &= \frac{|0\rangle (I + U) |\psi\rangle + |1\rangle (I - U) |\psi\rangle}{2} \\ &= |\psi'\rangle \end{aligned}$$

The only possible observable is $\sigma_z \otimes I = |0\rangle \langle 0| \otimes I - |1\rangle \langle 1| \otimes I = P_0 - P_1$ since the measurement is taken in the computational basis on only on the first qubit, and the expected measurement outcomes are ± 1.

The probability of outcome $+1$ is:

$$\begin{aligned} \Pr(+1) &= \langle \psi' | P_0 | \psi' \rangle \\ &= \frac{\langle 0| \langle \psi| (I + U^*) + \langle 1| \langle \psi| (I - U^*)}{2} \frac{|0\rangle (I + U) |\psi\rangle}{2} \\ &= \frac{\langle \psi | I + U^* + U + I | \psi \rangle}{4} \\ &= \frac{\langle \psi | I + U | \psi \rangle}{2} \\ &= \frac{1 + \langle \psi | U | \psi \rangle}{2} \end{aligned}$$

Since U is both Hermitian and unitary, without loss of generality let $U = |a\rangle \langle a| - |b\rangle \langle b|$ where $|a\rangle$ and $|b\rangle$ form an orthonormal basis. Thus,

$$\Pr(+1) = \frac{1 + \langle \psi | U | \psi \rangle}{2}$$

$$
\begin{aligned}
&= \frac{1 + |\langle\psi|a\rangle|^2 - |\langle\psi|b\rangle|^2}{2} \\
&= \frac{|\langle\psi|a\rangle|^2 + |\langle\psi|b\rangle|^2 + |\langle\psi|a\rangle|^2 - |\langle\psi|b\rangle|^2}{2} \\
&= |\langle\psi|a\rangle|^2
\end{aligned}
$$

So the probability of getting $+1$ from measuring the first qubit is exactly equal to getting $+1$ when measuring $|\psi\rangle$ in the U basis.

Similarly, the probability of -1 is:

$$
\begin{aligned}
\Pr(-1) &= \langle\psi'|P_1|\psi'\rangle \\
&= \frac{\langle 0| \langle\psi| (I + U^*) + \langle 1| \langle\psi| (I - U^*)}{2} \frac{|1\rangle (I - U) |\psi\rangle}{2} \\
&= \frac{\langle\psi|2I - 2U|\psi\rangle}{4} \\
&= \frac{1 - \langle\psi|U|\psi\rangle}{2} \\
&= \frac{|\langle\psi|a\rangle|^2 + |\langle\psi|b\rangle|^2 - |\langle\psi|a\rangle|^2 + |\langle\psi|b\rangle|^2}{2} \\
&= |\langle\psi|b\rangle|^2
\end{aligned}
$$

36. Quantum AND-gate using Toffoli:

```
a --+-- a
    |
b --+-- b
    |
0 -[X]- a && b
```

OR-gate using Toffoli and X:

```
a --[X]--+--[X]-- a
         |
b --[X]--+--[X]-- b
         |
1 ------[X]------ !(!a && !b) == a || b
```

A XOR-gate is equivalent to a controlled-X gate:

```
a --+-- a
    |
b -[X]- a ^ b
```

Half-adder:

```
a --+--+-- a
    |  |
```

```
b --+-[X]- a ^ b
    |
0 -[X]---- a && b == carry
```

Full-adder:

```
a --+--+----------------- a
    |  |
b --+-[X]-+--+----------- a ^ b
    |     |  |
0 -[X]----------[X]-+-[X]- a && b
          |  |      |
c --------+-[X]---------- a ^ b ^ c  <===
          |         |
0 -------[X]----[X]-+-[X]- (a ^ b) && c
                    |
1 ----------------[X]---- ((a ^ b) && c) || (a && b) == carry'  <===
```

where the input rungs are a, b, c representing the first two input and carry bits, respectively; and the output rungs of interest are $a \oplus b \oplus c$ and the carry bit.

With the half- and full-adders, the two-bit adder becomes:

```
x_1 -----------[    ]-- carry
y_1 -----------[ FA ]-- x_1 ^ y_1 ^ (x_0 && y_0)
x_0 ---[ HA ]--[    ]
y_0 ---[    ]---------- x_0 ^ y_0
```

5

Exercises

1. Let $Q : \mathbb{C}^N \to \mathbb{C}^N$ be the quantum Fourier transform, where $Q_{jk} = z^{jk}/\sqrt{N}$ and $z = \exp(2\pi i/N)$.

$$
\begin{aligned}
(Q^*Q)_{jk} &= \sum_{m=0}^{N-1} Q^*_{jm} Q_{mk} \\
&= \frac{1}{N} \sum_{m=0}^{N-1} \left(z^{jm}\right)^* z^{mk} \\
&= \frac{1}{N} \sum_{m=0}^{N-1} \left[(z^*)^j z^k\right]^m
\end{aligned}
$$

$$= \frac{1}{N}\begin{cases} N & j = k \\ \sum_{m=0}^{N-1}\left(z^{k-j}\right)^m & j < k \\ \sum_{m=0}^{N-1}\left[\left(z^*\right)^{j-k}\right]^m & j > k \end{cases} \quad \text{since } zz^* = 1$$

$$= \frac{1}{N}\begin{cases} N & j = k \\ \frac{\left(z^{k-j}\right)^N - 1}{z-1} & j < k \\ \frac{\left[\left(z^*\right)^{j-k}\right]^N - 1}{z-1} & j > k \end{cases} \quad \text{sum of geometric series}$$

$$= \begin{cases} 1 & j = k \\ \frac{1^{k-j}-1}{z-1} & j < k \\ \frac{1^{j-k}-1}{z-1} & j > k \end{cases}$$

$$= \delta_{jk}$$

Thus, $Q^*Q = I$ and Q is unitary.

2. Letting $\text{bin}\,(k)$ denote the binary representation of k,

$$|\underbrace{00\ldots 0}_{n \text{ qubits}}\rangle \mapsto \left(\frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1}\exp\left(\frac{2\pi ijk}{N}\right)|k\rangle\right)\Bigg|_{j=0} = \frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1}|\text{bin}\,(k)\rangle$$