Quantum Computation and Quantum Information 10th Anniversary Edition - Unnoficial Solutions

Adonai H. da Silva
adonaih@gmail.com

Chapters: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, Appendices.

1 Introduction and overview

Exercises: 1.1, 1.2.

1.1

If the function is balanced and we select two random inputs the probability of obtaining the same output is

$$\frac{\frac{2^n}{2}-1}{2^n-1} = \frac{2^n-2}{2^n-1} \times \frac{1}{2} < \frac{1}{2},$$

so with two evaluations, it is possible to solve Deutsch-Jozsa's problem with error probability $\epsilon < 1/2$.

1.2

If a device can distinguish between two non-orthogonal states $|\psi\rangle$ and $|\phi\rangle$ then it knows each components' amplitudes and phases, so upon identifying the state it can create a copy of it through some unitary acting upon a standard state $|s\rangle$.

Conversely, if a device can clone the states $|\psi\rangle$ and $|\phi\rangle$ then it can create several copies of each, allowing us to perform several measurements and get information about the amplitudes and phases with arbitrary precision, thus allowing us to completely distinguish them.

2 Introduction to quantum mechanics

Exercises: 2.1, 2.2, 2.3, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 2.11, 2.12, 2.13, 2.14, 2.15, 2.16, 2.17, 2.18, 2.19, 2.20, 2.21, 2.22, 2.23, 2.24, 2.25, 2.26, 2.27, 2.28, 2.29, 2.30, 2.31, 2.32, 2.33, 2.34, 2.35, 2.36, 2.37, 2.38, 2.39, 2.40, 2.41, 2.42, 2.43, 2.44, 2.45, 2.46, 2.47, 2.48, 2.49, 2.50, 2.51, 2.52, 2.53, 2.54, 2.55, 2.56, 2.57, 2.58, 2.59, 2.60, 2.61, 2.62, 2.63, 2.64, 2.65, 2.66, 2.67, 2.68, 2.69, 2.70, 2.71, 2.72, 2.73, 2.74, 2.75, 2.76, 2.77, 2.78, 2.79, 2.80, 2.81, 2.82.

2.1

$$\begin{bmatrix} 1 \\ -1 \end{bmatrix} + \begin{bmatrix} 1 \\ 2 \end{bmatrix} - \begin{bmatrix} 2 \\ 1 \end{bmatrix} = 0.$$

2.2

$$\begin{aligned} A\left|0\right\rangle &= \left|1\right\rangle = 0\left|0\right\rangle + 1\left|1\right\rangle, \\ A\left|1\right\rangle &= \left|0\right\rangle = 1\left|0\right\rangle + 0\left|1\right\rangle. \end{aligned}$$

So writing the basis vectors as

$$\left|0\right\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \left|1\right\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix},$$

we have

$$A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

2.3

$$\begin{aligned} BA\left|v_i\right\rangle &= B\left(\sum_j A_{ji}\left|w_j\right\rangle\right) \\ &= \sum_j A_{ji} B\left|w_j\right\rangle \\ &= \sum_j A_{ji} \sum_k B_{kj}\left|x_k\right\rangle \\ &= \sum_j \sum_k B_{kj} A_{ji}\left|x_k\right\rangle, \end{aligned}$$

but $\sum_j B_{kj}A_{ji}$ is precisely B's k-th row multiplied by A's i-th column (matrix multiplication), thus we have

$$BA\left|v_i\right\rangle = \sum_k (BA)_{ki}\left|x_k\right\rangle.$$

2.4

$$I\left|v_i\right\rangle = \sum_j I_{ji}\left|v_j\right\rangle = \left|v_i\right\rangle,$$

that is, I is such that $I_{ji} = 0$ for $j \neq i$ and $I_{ji} = 1$ for $j = i$, meaning I is represented by the identity matrix.

2.5

For $|v\rangle$ and $|w_i\rangle \in \mathbb{C}^n$, where

$$|v\rangle = (v_1, \cdots, v_n), |w_i\rangle = (w_{i1}, \cdots, w_{in}),$$

we have property (1):

$$\begin{aligned}\left(|v\rangle, \sum_i \lambda_i |w_i\rangle\right) = \left((v_1, \cdots, v_n), \sum_i \lambda_i (w_{i1}, \cdots, w_{in})\right) &= \sum_j v_j^* \sum_i \lambda_i w_{ij} \\ &= \sum_i \lambda_i \sum_j v_j^* w_{ij} \\ &= \sum_i \lambda_i ((v_1, \cdots, v_n), (w_{i1}, \cdots, w_{in})) \\ &= \sum_i \lambda_i (|v\rangle, |w_i\rangle),\end{aligned}$$

property (2):

$$\begin{aligned}(|v\rangle, |w_i\rangle) &= \sum_j v_j^* w_{ij} \\ &= \left(\sum_j w_{ij}^* v_j\right)^* \\ &= (|w_i\rangle, |v\rangle)^*,\end{aligned}$$

and property (3):

$$\begin{aligned}(|v\rangle, |v\rangle) &= \sum_i v_i^* v_i \\ &= \sum_i |v_i|^2 \geq 0.\end{aligned}$$

2.6

Using property (2) we have

$$\left(\sum_i \lambda_i |w_i\rangle, |v\rangle\right) = \left(|v\rangle, \sum_i \lambda_i |w_i\rangle\right)^*,$$

and using properties (1) and (2) yields

$$\begin{aligned}\left(|v\rangle, \sum_i \lambda_i |w_i\rangle\right)^* &= \left(\sum_i \lambda_i (|v\rangle, |w_i\rangle)\right)^* \\ &= \sum_i \lambda_i^* (|w_i\rangle, |v\rangle).\end{aligned}$$

2.7

$$\langle w \,|\, v \rangle = \begin{bmatrix} 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ -1 \end{bmatrix} = 1 - 1 = 0.$$

$$\| |w\rangle \| = \| |v\rangle \| = \sqrt{2},$$

so the normalized forms are given by

$$\frac{|w\rangle}{\| |w\rangle \|} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \frac{|v\rangle}{\| |v\rangle \|} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}.$$

2.8

For $|v_1\rangle$ and $|v_2\rangle$ we have

$$\begin{aligned} \langle v_1 \,|\, v_2 \rangle &= \left(\frac{\langle w_1|}{\| |w_1\rangle \|} \right) \left(\frac{|w_2\rangle \, \langle v_1 \,|\, w_2 \rangle \, |v_1\rangle}{\| |w_2\rangle \|} \right) \\ &= \frac{\langle w_1 \,|\, w_2 \rangle - \langle v_1 \,|\, w_2 \rangle \, \langle w_1 \,|\, v_1 \rangle}{\| |w_1\rangle \| \| |w_2\rangle \|} \\ &= \frac{\langle w_1 \,|\, w_2 \rangle - \frac{\langle w_1 \,|\, w_2 \rangle}{\| |w_1\rangle \|} \| w_1 \|}{\| |w_1\rangle \| \| |w_2\rangle \|} \\ &= 0. \end{aligned}$$

Because it is a structure constructed inductively the same should hold for any $|v_i\rangle$. So by the end of the Gram–Schmidt process we have $\dim(V)$ vectors $|v_i\rangle$ satisfying $\langle v_i \,|\, v_j \rangle = \delta_{ij}$, thus the set $\{|v_i\rangle\}$ is an orthonormal basis for V.

2.9

$$\begin{aligned} I &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = |0\rangle\langle 0| + |1\rangle\langle 1|, \\ X &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = |0\rangle\langle 1| + |1\rangle\langle 0|, \\ Y &= \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = -i\,|0\rangle\langle 1| + i\,|1\rangle\langle 0|, \\ Z &= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1|. \end{aligned}$$

2.10

All matrix elements can be calculated as

$$\langle v_l \,|\, v_j \rangle \, \langle v_k \,|\, v_m \rangle = \delta_{lj} \delta_{km},$$

thus it is an operator whose matrix representation has value 1 at the j'th row and k'th column and 0 everywhere else.

2.11

X : $\det(X - \lambda I) = \lambda^2 - 1 = 0 \quad \Longrightarrow \quad$ eigenvalues $= \{-1, 1\}$.

For eigenvalue 1 :

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix} \quad \Longrightarrow \quad \text{eigenvector} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \left(|0\rangle + |1\rangle \right).$$

For eigenvalue -1 :

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = - \begin{bmatrix} a \\ b \end{bmatrix} \quad \Longrightarrow \quad \text{eigenvector} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{1}{\sqrt{2}} \left(|0\rangle - |1\rangle \right).$$

Y : $\det(Y - \lambda I) = \lambda^2 - 1 = 0 \quad \Longrightarrow \quad$ eigenvalues $= \{-1, 1\}$.

For eigenvalue 1 :

$$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix} \quad \Longrightarrow \quad \text{eigenvector} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ i \end{bmatrix} = \frac{1}{\sqrt{2}} \left(|0\rangle + i\,|1\rangle \right).$$

For eigenvalue -1 :

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = - \begin{bmatrix} a \\ b \end{bmatrix} \quad \Longrightarrow \quad \text{eigenvector} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -i \end{bmatrix} = \frac{1}{\sqrt{2}} \left(|0\rangle - i\,|1\rangle \right).$$

Z : is already diagonal in the computational basis $\quad \Longrightarrow \quad$ eigenvalues $= \{-1, 1\}$.

For eigenvalue 1 :

$$\text{eigenvector} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle .$$

For eigenvalue -1 :

$$\text{eigenvector} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle .$$

2.12

$$\det \begin{bmatrix} 1-\lambda & 0 \\ 1 & 1-\lambda \end{bmatrix} = \lambda^2 - 2\lambda + 1 = 0 \quad \Longrightarrow \quad \text{eigenvalue} = 1 \text{ (degenerate)}.$$

$$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix} \quad \Longrightarrow \quad a + b = b \quad \Longrightarrow \quad \text{eigenvector} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle .$$

And there is no other eigenvector for the degenerate eigenvalue, thus this matrix is not diagonalizable.

2.13

$$\begin{aligned}\left(|a\rangle, \left(|w\rangle\langle v|\right)^\dagger |b\rangle\right) &= \left(\langle v \,|\, a\rangle\, |w\rangle, |b\rangle\right) \\ &= \langle v \,|\, a\rangle^* \left(|w\rangle, |b\rangle\right) \\ &= \langle a \,|\, v\rangle \langle w \,|\, b\rangle \\ &= \left(|a\rangle, \left(|v\rangle\langle w|\right)|b\rangle\right).\end{aligned}$$

2.14

$$\begin{aligned}\left(\left(\sum_i a_i A_i\right)^\dagger |v\rangle, |w\rangle\right) &= \left(|v\rangle, \sum_i a_i A_i |w\rangle\right) \\ &= \sum_i a_i \left(|v\rangle, A_i |w\rangle\right) \\ &= \sum_i a_i \left(A_i^\dagger |v\rangle, |w\rangle\right) \\ &= \left(\sum_i a_i^* A_i^\dagger |v\rangle, |w\rangle\right).\end{aligned}$$

2.15

$$\begin{aligned}\left(\left(A^\dagger\right)^\dagger |v\rangle, |w\rangle\right) &= \left(|v\rangle, A^\dagger |w\rangle\right) \\ &= \left(A^\dagger |w\rangle, |v\rangle\right)^* \\ &= \left(|w\rangle, A |v\rangle\right)^* \\ &= \left(A |v\rangle, |w\rangle\right).\end{aligned}$$

2.16

$$\begin{aligned}P^2 &= \left(\sum_{i=1}^k |i\rangle\langle i|\right)\left(\sum_{j=1}^k |j\rangle\langle j|\right) \\ &= \sum_{i=1}^k \sum_{j=1}^k |i\rangle \langle i \,|\, j\rangle |j\rangle \\ &= \sum_{i=1}^k \sum_{j=1}^k |i\rangle\langle j| \,\delta_{ij} \\ &= \sum_{i=1}^k |i\rangle\langle i| = P.\end{aligned}$$

2.17

Let H be a normal operator. Then there exists an operator M that diagonalizes H to H_d, that is

$$H = M^\dagger H_d M,$$
$$H^\dagger = M^\dagger H_d^\dagger M.$$

If H has real eigenvalues then $H_d^\dagger = H_d$, thus

$$H^\dagger = M^\dagger H_d^\dagger M = M^\dagger H_d M = H.$$

Conversely, if H is Hermitian then $H_d = H_d^\dagger$, which means all eigenvalues are real.

2.18

Let $|v\rangle$ be an eigenvector of U. Then

$$U|v\rangle = \lambda|v\rangle,$$
$$\langle v|U^\dagger = \lambda^*\langle v|.$$

But we must have

$$\langle v\,|\,U^\dagger U\,|\,v\rangle = \lambda^*\lambda\langle v\,|\,v\rangle = \langle v\,|\,v\rangle \quad\Longrightarrow\quad \lambda^*\lambda = 1 \quad\Longrightarrow\quad \lambda = e^{i\theta}.$$

2.19

$$X: X^\dagger = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^\dagger = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^T = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = X$$
$$X^\dagger X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$
$$Y: Y^\dagger = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}^\dagger = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix}^T = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = Y$$
$$Y^\dagger Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$
$$Z: Z^\dagger = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}^\dagger = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}^T = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = Z$$
$$Z^\dagger Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

2.20

$$I = \sum_i |v_i\rangle\langle v_i| = \sum_i |w_i\rangle\langle w_i|.$$

Then A'_{ij} can be written as

$$\begin{aligned} A'_{ij} = \langle v_i \,|\, A \,|\, v_j \rangle &= \sum_k \sum_l \langle v_i \,|\, w_k \rangle \langle w_k \,|\, A \,|\, w_l \rangle \langle w_l \,|\, v_j \rangle \\ &= \sum_k \sum_l \langle v_i \,|\, w_k \rangle A''_{kl} \langle w_l \,|\, v_j \rangle . \end{aligned}$$

If $|v_i\rangle$ and $|w_i\rangle$ are both orthonormal bases then there exists a unitary U such that $|w_i\rangle = U\,|v_i\rangle$, thus

$$A'_{ij} = \sum_k \sum_l U_{ik} A''_{kl} U^\dagger_{lj}.$$

2.21

Let $|v\rangle \in V(\dim = 1)$ be an eigenvector of $M = M^\dagger$ with eigenvalue λ and also element of subspace P. Then

$$\begin{aligned} M &= (P+Q)\, M\, (P+Q) \\ &= PMP + PMQ + QMP + QMQ. \end{aligned}$$

Because M is Hermitian we have that $PMP = \lambda P$ and QMQ are normal and diagonal with respect to an orthonormal basis for the subspaces P and Q respectively. Also

$$\begin{aligned} QMP &= 0, \\ PMQ &= (QMP)^\dagger = 0. \end{aligned}$$

Thus $M = PMP + QMQ$ is diagonal with respect to some orthonormal basis for space V. And by induction, this must be true for higher dimensional Hilbert spaces.

2.22

Let $|v\rangle$ and $|w\rangle$ be two eigenvectors of a Hermitian operator H with different eigenvalues. Then

$$\begin{aligned} H\,|v\rangle &= \alpha\,|v\rangle\,, \\ H\,|w\rangle &= \beta\,|w\rangle\,. \end{aligned}$$

But we must have

$$\langle w \,|\, H \,|\, v \rangle = \alpha \langle w \,|\, v \rangle = \beta \langle w \,|\, v \rangle \quad \Longrightarrow \quad (\alpha - \beta) \langle w \,|\, v \rangle = 0.$$

Since $\alpha \neq \beta$, $|v\rangle$ and $|w\rangle$ must be orthogonal.

2.23

Let $|v\rangle$ be an eigenvector of the projector P. Then

$$P|v\rangle = \lambda|v\rangle,$$
$$P^2|v\rangle = \lambda P|v\rangle = \lambda^2|v\rangle.$$

Since P is a projector, $P = P^2$, thus

$$\lambda = \lambda^2 \quad \Longrightarrow \quad \lambda = 0 \text{ or } 1.$$

2.24

Defining

$$B \coloneqq \frac{A + A^\dagger}{2}, C \coloneqq \frac{A - A^\dagger}{2i},$$

we can write operator A as $A = B + iC$. If A is positive then

$$(|v\rangle, A|v\rangle) = (|v\rangle, B|v\rangle) + i(|v\rangle, C|v\rangle) \geq 0.$$

But that is only possible if $C = 0 \Rightarrow A = A^\dagger$.

2.25

$$A|v\rangle = |w\rangle,$$
$$\langle v|A^\dagger = \langle w|,$$

$$\Longrightarrow \quad \langle v|A^\dagger A|v\rangle = \langle w|w\rangle \geq 0.$$

2.26

$$|\psi\rangle^{\otimes 2} = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) = \frac{|0\rangle|0\rangle + |0\rangle|1\rangle + |1\rangle|0\rangle + |1\rangle|1\rangle}{2}$$
$$= \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix} \otimes \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix} = \frac{1}{2}\begin{bmatrix}1\\1\\1\\1\end{bmatrix},$$

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

$$= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \otimes \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \otimes \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{2\sqrt{2}} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix},$$

2.27

$$X \otimes Z = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix},$$

$$I \otimes X = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix},$$

$$X \otimes I = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}.$$

The last two examples show that the tensor product is non-commutative.

2.28

Let A be represented by an $m \times n$ matrix. Then

$$(A \otimes B)^* = \begin{bmatrix} A_{11}B & \cdots & A_{1n}B \\ \vdots & \ddots & \vdots \\ A_{m1}B & \cdots & A_{mn}B \end{bmatrix}^* = \begin{bmatrix} A_{11}^*B^* & \cdots & A_{1n}^*B^* \\ \vdots & \ddots & \vdots \\ A_{m1}^*B^* & \cdots & A_{mn}^*B^* \end{bmatrix} = A^* \otimes B^*,$$

$$(A \otimes B)^T = \begin{bmatrix} A_{11}B & \cdots & A_{1n}B \\ \vdots & \ddots & \vdots \\ A_{m1}B & \cdots & A_{mn}B \end{bmatrix}^T = \begin{bmatrix} A_{11}B^T & \cdots & A_{m1}B^T \\ \vdots & \ddots & \vdots \\ A_{1n}B^T & \cdots & A_{mn}B^T \end{bmatrix} = A^T \otimes B^T,$$

$$(A \otimes B)^\dagger = ((A \otimes B)^*)^T = (A^* \otimes B^*)^T = (A^*)^T \otimes (B^*)^T = A^\dagger \otimes B^\dagger.$$

2.29

$$(U_1 \otimes U_2)^\dagger (U_1 \otimes U_2) = \left(U_1^\dagger \otimes U_2^\dagger\right)(U_1 \otimes U_2)$$

$$
\begin{aligned}
&= U_1^\dagger U_1 \otimes U_2^\dagger U_2 \\
&= I_1 \otimes I_2
\end{aligned}
$$

2.30

$$
\begin{aligned}
H_1 \otimes H_2 &= H_1^\dagger \otimes H_2^\dagger \\
&= (H_1 \otimes H_2)^\dagger
\end{aligned}
$$

2.31

$$
\begin{aligned}
\left(|v\rangle \otimes |w\rangle, (A \otimes B)\,|v\rangle \otimes |w\rangle\right) &= \left(|v\rangle \otimes |w\rangle, A\,|v\rangle \otimes B\,|w\rangle\right) \\
&= \langle v \,|\, A \,|\, v\rangle \, \langle w \,|\, B \,|\, w\rangle .
\end{aligned}
$$

Since $\langle v \,|\, A \,|\, v\rangle \geq 0$ and $\langle w \,|\, B \,|\, w\rangle \geq 0$ it follows that

$$
\left(|v\rangle \otimes |w\rangle, (A \otimes B)\,|v\rangle \otimes |w\rangle\right) \geq 0.
$$

2.32

$$
\begin{aligned}
(P_1 \otimes P_2)^2 &= (P_1 \otimes P_2)\,(P_1 \otimes P_2) \\
&= P_1^2 \otimes P_2^2 \\
&= P_1 \otimes P_2.
\end{aligned}
$$

2.33

$$
\begin{aligned}
H &= \frac{1}{\sqrt{2}} \big[\, (|0\rangle + |1\rangle)\,\langle 0| + (|0\rangle - |1\rangle)\,\langle 1| \,\big] \\
&= \frac{1}{\sqrt{2}} \left(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|\right) \\
&= \frac{1}{\sqrt{2}} \sum_{x,y=0}^{1} (-1)^{x \cdot y}\, |x\rangle\langle y| .
\end{aligned}
$$

Thus

$$
\begin{aligned}
H^{\otimes n} &= \frac{1}{\sqrt{2}} \sum_{x_1,y_1=0}^{1} (-1)^{x_1 \cdot y_1}\, |x_1\rangle\langle y_1| \otimes \cdots \otimes \frac{1}{\sqrt{2}} \sum_{x_n,y_n=0}^{1} (-1)^{x_n \cdot y_n}\, |x_n\rangle\langle y_n| \\
&= \frac{1}{\sqrt{2^n}} \sum_{x_1,y_1=0}^{1} \cdots \sum_{x_n,y_n=0}^{1} (-1)^{x_1 \cdot y_1} \cdots (-1)^{x_n \cdot y_n}\, |x_1\rangle\langle y_1| \otimes \cdots \otimes |x_n\rangle\langle y_n| .
\end{aligned}
$$

If we define $|x\rangle$ and $|y\rangle$ as the bit sequence states

$$|x\rangle \coloneqq \bigotimes_{i=1}^{n} |x_i\rangle\,,$$
$$|y\rangle \coloneqq \bigotimes_{i=1}^{n} |y_i\rangle\,,$$

and $x \cdot y$ as the bitwise product

$$x \cdot y \coloneqq \bigoplus_{i=1}^{n} x_i \cdot y_i,$$

where $\oplus$ denotes sum modulo-2 (or the XOR logic operation), then we can write

$$H^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x,y} (-1)^{x \cdot y} |x\rangle\langle y|\,.$$

$$\begin{aligned} H^{\otimes 2} = \frac{1}{\sqrt{2^2}} \big[&(-1)^{0\oplus 0} |00\rangle\langle 00| + (-1)^{0\oplus 0} |01\rangle\langle 00| + (-1)^{0\oplus 0} |10\rangle\langle 00| + (-1)^{0\oplus 0} |11\rangle\langle 00| \\ &+(-1)^{0\oplus 0} |00\rangle\langle 01| + (-1)^{0\oplus 1} |01\rangle\langle 01| + (-1)^{0\oplus 0} |10\rangle\langle 01| + (-1)^{0\oplus 1} |11\rangle\langle 01| \\ &+(-1)^{0\oplus 0} |00\rangle\langle 10| + (-1)^{0\oplus 0} |01\rangle\langle 10| + (-1)^{1\oplus 0} |10\rangle\langle 10| + (-1)^{1\oplus 0} |11\rangle\langle 10| \\ &+(-1)^{0\oplus 0} |00\rangle\langle 11| + (-1)^{0\oplus 1} |01\rangle\langle 11| + (-1)^{1\oplus 0} |10\rangle\langle 11| + (-1)^{1\oplus 1} |11\rangle\langle 11| \big] \end{aligned}$$

$$\implies \quad H^{\otimes 2} = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

2.34

$$\det \begin{bmatrix} 4-\lambda & 3 \\ 3 & 4-\lambda \end{bmatrix} = \lambda^2 - 8\lambda + 7 = 0 \quad \implies \quad \text{eigenvalues} = \{1, 7\}.$$

For eigenvalue 1 :

$$\begin{bmatrix} 4 & 3 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix} \quad \implies \quad \text{eigenvector} = |v_1\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$$

For eigenvalue 7 :

$$\begin{bmatrix} 4 & 3 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = 7 \begin{bmatrix} a \\ b \end{bmatrix} \quad \implies \quad \text{eigenvector} = |v_7\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}.$$

So labeling the matrix as M we have

$$\sqrt{M} = \sqrt{1}\,|v_1\rangle\langle v_1| + \sqrt{7}\,|v_7\rangle\langle v_7| = \frac{1}{2}\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} + \frac{\sqrt{7}}{2}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1+\sqrt{7} & -1+\sqrt{7} \\ -1+\sqrt{7} & 1+\sqrt{7} \end{bmatrix},$$

$$\log(M) = \log(1)\,|v_1\rangle\langle v_1| + \log(7)\,|v_7\rangle\langle v_7| = \frac{\log(7)}{2}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}.$$

2.35

$$\begin{aligned}\vec{v}\cdot\vec{\sigma} &= v_1\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} + v_2\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} + v_3\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \\ &= \begin{bmatrix} v_3 & v_1 - iv_2 \\ v_1 + iv_2 & -v_3 \end{bmatrix}.\end{aligned}$$

$$\det(\vec{v}\cdot\vec{\sigma} - \lambda I) = \lambda^2 - \left(v_1^2 + v_2^2 + v_3^2\right) = 0.$$

Since $\vec{v}$ is a unit vector, $v_1^2 + v_2^2 + v_3^2 = 1$ and the eigenvalues are $\{-1, 1\}$. Labeling the respective eigenvectors as $|e_-\rangle$ and $|e_+\rangle$ we have

$$\begin{aligned} I &= |e_+\rangle\langle e_+| + |e_-\rangle\langle e_-|\,, \\ \vec{v}\cdot\vec{\sigma} &= |e_+\rangle\langle e_+| - |e_-\rangle\langle e_-|\,. \end{aligned}$$

$$\begin{aligned}\exp(i\theta\vec{v}\cdot\vec{\sigma}) &= \exp(i\theta)\,|e_+\rangle\langle e_+| + \exp(-i\theta)\,|e_-\rangle\langle e_-| \\ &= \cos(\theta)\,|e_+\rangle\langle e_+| + i\sin(\theta)\,|e_+\rangle\langle e_+| + \cos(\theta)\,|e_-\rangle\langle e_-| - i\sin(\theta)\,|e_-\rangle\langle e_-| \\ &= \cos(\theta)\left(|e_+\rangle\langle e_+| + |e_-\rangle\langle e_-|\right) + i\sin(\theta)\left(|e_+\rangle\langle e_+| - |e_-\rangle\langle e_-|\right) \\ &= \cos(\theta)I + i\sin(\theta)\vec{v}\cdot\vec{\sigma}.\end{aligned}$$

2.36

$$\begin{aligned}\mathrm{tr}(X) &= 0 + 0 = 0, \\ \mathrm{tr}(Y) &= 0 + 0 = 0, \\ \mathrm{tr}(Z) &= 1 + (-1) = 0.\end{aligned}$$

2.37

$$\begin{aligned}\mathrm{tr}(AB) &= \sum_i \langle i\,|\,AB\,|\,i\rangle \\ &= \sum_i \sum_j \langle i\,|\,A\,|\,j\rangle\,\langle j\,|\,B\,|\,i\rangle\end{aligned}$$

$$
\begin{aligned}
&= \sum_i \sum_j \langle j \,|\, B \,|\, i \rangle \langle i \,|\, A \,|\, j \rangle \\
&= \sum_j \langle j \,|\, BA \,|\, j \rangle \\
&= \operatorname{tr}(BA).
\end{aligned}
$$

2.38

$$
\begin{aligned}
\operatorname{tr}(A+B) &= \sum_i \langle i \,|\, (A+B) \,|\, i \rangle \\
&= \sum_i \langle i \,|\, A \,|\, i \rangle + \sum_i \langle i \,|\, B \,|\, i \rangle \\
&= \operatorname{tr}(A) + \operatorname{tr}(B),
\end{aligned}
$$

$$
\begin{aligned}
\operatorname{tr}(zA) &= \sum_i \langle i \,|\, (zA) \,|\, i \rangle \\
&= z \sum_i \langle i \,|\, A \,|\, i \rangle \\
&= z \operatorname{tr}(A).
\end{aligned}
$$

2.39

For linear operators A and B_i acting on V, and $z_i \in \mathbb{C}$, we have property (1):

$$
\begin{aligned}
\left(A, \sum_i z_i B_i \right) = \operatorname{tr}\left(\sum_i z_i A^\dagger B_i \right) &= \sum_i z_i \operatorname{tr}\big(A^\dagger B_i\big) \\
&= \sum_i z_i \left(A, B_i \right),
\end{aligned}
$$

property (2):

$$
\begin{aligned}
(A, B_i) = \operatorname{tr}\big(A^\dagger B_i\big) &= \sum_j \left\langle j \,\middle|\, A^\dagger B_i \,\middle|\, j \right\rangle \\
&= \left(\sum_j \left\langle j \,\middle|\, B_i^\dagger A \,\middle|\, j \right\rangle \right)^* \\
&= \left(\operatorname{tr}\Big(B_i^\dagger A \Big) \right)^* \\
&= (B_i, A)^*,
\end{aligned}
$$

and property (3):

$$
\begin{aligned}
(A, A) = \operatorname{tr}\big(A^\dagger A\big) &= \sum_i \left\langle i \,\middle|\, A^\dagger A \,\middle|\, i \right\rangle \\
&= \sum_i \| A \,|i\rangle \|^2 \geq 0.
\end{aligned}
$$

If $\dim(V) = d$ the transformations $V \to V$ can be represented by $d \times d$ matrices $M \in L_V$, meaning there are d^2 independent parameters necessary to write a transformation matrix, thus $\dim(L_V) = d^2$.

If $|i\rangle$ for $i \in \{1, \cdots, d\}$ is an orthonormal basis for V then the set of d^2 operators $\{|i\rangle\langle j|\}$ for $i, j \in \{1, \cdots, d\}$ forms an orthonormal basis for L_V, because for any i, j, k and l we have

$$\begin{aligned}(|i\rangle\langle j|, |k\rangle\langle l|) = \mathrm{tr}\Big((|i\rangle\langle j|)^\dagger |k\rangle\langle l|\Big) &= \sum_{m=1}^{d} \langle m \,|\, j\rangle \langle i \,|\, k\rangle \langle l \,|\, m\rangle \\ &= \delta_{ik} \sum_{m=1}^{d} \langle l \,|\, m\rangle \langle m \,|\, j\rangle \\ &= \delta_{ik}\delta_{jl}.\end{aligned}$$

2.40

$$\begin{aligned}[X, Y] &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} - \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 2i & 0 \\ 0 & -2i \end{bmatrix} = 2iZ, \\ [Y, Z] &= \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} - \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = \begin{bmatrix} 0 & 2i \\ 2i & 0 \end{bmatrix} = 2iX, \\ [Z, X] &= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} - \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 0 & 2 \\ -2 & 0 \end{bmatrix} = 2iY.\end{aligned}$$

2.41

$$\begin{aligned}\{Y, X\} = \{X, Y\} &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} + \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = 0, \\ \{Z, Y\} = \{Y, Z\} &= \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = 0, \\ \{X, Z\} = \{Z, X\} &= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = 0,\end{aligned}$$

$$\begin{aligned}X^2 &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I, \\ Y^2 &= \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I, \\ Z^2 &= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I.\end{aligned}$$

2.42

$$\begin{aligned} AB &= \frac{1}{2}\left(2AB + BA - BA\right) \\ &= \frac{1}{2}\left(AB - BA + AB + BA\right) \\ &= \frac{[A,B] + \{A,B\}}{2}. \end{aligned}$$

2.43

$$\begin{aligned} \sigma_j \sigma_k = \frac{[\sigma_j, \sigma_k] + \{\sigma_j, \sigma_k\}}{2} &= \frac{2i\sum_{l=1}^{3} \epsilon_{jkl}\sigma_l + 2\delta_{jk} I}{2} \\ &= \delta_{jk} I + i\sum_{l=1}^{3} \epsilon_{jkl}\sigma_l. \end{aligned}$$

2.44

If $[A,B] = \{A,B\} = 0$ and A is invertible, then

$$[A,B] + \{A,B\} = 2AB = 0 \quad \Longrightarrow \quad 2A^{-1}AB = 0 \quad \Longrightarrow \quad B = 0.$$

2.45

$$\begin{aligned} [A,B]^\dagger &= (AB - BA)^\dagger \\ &= B^\dagger A^\dagger - A^\dagger B^\dagger \\ &= \left[B^\dagger, A^\dagger\right]. \end{aligned}$$

2.46

$$\begin{aligned} [A,B] &= AB - BA \\ &= -\left(BA - AB\right) \\ &= -[B,A]. \end{aligned}$$

2.47

$$\begin{aligned} i[A,B] &= iAB - iBA \\ &= \left(-iB^\dagger A^\dagger + iA^\dagger B^\dagger\right)^\dagger \\ &= \left(iAB - iBA\right)^\dagger \\ &= \left(i[A,B]\right)^\dagger. \end{aligned}$$

2.48

$$P = IP = PI,$$
$$U = UI = IU.$$

By the spectral theorem H can be written as

$$H = \sum_i \lambda_i \left|i\right\rangle\!\left\langle i\right|,$$

thus

$$\begin{aligned}
\sqrt{H^\dagger H} = \sqrt{HH^\dagger} = \sqrt{H^2} &= \sqrt{\sum_i \sum_j \lambda_i \lambda_j \left|i\right\rangle \left\langle i \,|\, j\right\rangle \left\langle j\right|} \\
&= \sqrt{\sum_i \lambda_i^2 \left|i\right\rangle\!\left\langle i\right|} \\
&= \sum_i \left|\lambda_i\right| \left|i\right\rangle\!\left\langle i\right| \\
\implies \quad H &= U \sum_i \left|\lambda_i\right| \left|i\right\rangle\!\left\langle i\right| = \sum_i \left|\lambda_i\right| \left|i\right\rangle\!\left\langle i\right| U,
\end{aligned}$$

where $U = H\left(\sqrt{H^2}\right)^{-1}$.

2.49

Let M be a normal matrix, then by the spectral theorem we can write

$$M = \sum_i \lambda_i \left|i\right\rangle\!\left\langle i\right|,$$

thus

$$\begin{aligned}
\sqrt{M^\dagger M} = \sqrt{MM^\dagger} &= \sqrt{\sum_i \sum_j \lambda_i \lambda_j^* \left|i\right\rangle \left\langle i \,|\, j\right\rangle \left\langle j\right|} \\
&= \sqrt{\sum_i \left|\lambda_i\right|^2 \left|i\right\rangle\!\left\langle i\right|} \\
&= \sum \left|\lambda_i\right| \left|i\right\rangle\!\left\langle i\right| \\
\implies \quad M &= U \sum_i \left|\lambda_i\right| \left|i\right\rangle\!\left\langle i\right| = \sum_i \left|\lambda_i\right| \left|i\right\rangle\!\left\langle i\right| U,
\end{aligned}$$

where $U = M\left(\sqrt{M^\dagger M}\right)^{-1}$.

2.50

Labeling the matrix as M we have

$$J^2 = M^\dagger M = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix},$$
$$K^2 = MM^\dagger = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}.$$

$$\det\big(J^2 - \lambda I\big) = \lambda^2 - 3\lambda + 1 = 0 \quad \Longrightarrow \quad \text{eigenvalues} = \frac{3 \pm \sqrt{5}}{2}.$$
$$\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \frac{3 \pm \sqrt{5}}{2} \begin{bmatrix} a \\ b \end{bmatrix} \quad \Longrightarrow \quad \text{eigenvectors} = |j_\pm\rangle = \frac{1}{\sqrt{10 \mp 2\sqrt{5}}} \begin{bmatrix} 2 \\ -1 \pm \sqrt{5} \end{bmatrix}.$$
$$\det\big(K^2 - \lambda I\big) = \lambda^2 - 3\lambda + 1 = 0 \quad \Longrightarrow \quad \text{eigenvalues} = \frac{3 \pm \sqrt{5}}{2}.$$
$$\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \frac{3 \pm \sqrt{5}}{2} \begin{bmatrix} a \\ b \end{bmatrix} \quad \Longrightarrow \quad \text{eigenvectors} = |k_\pm\rangle = \frac{1}{\sqrt{10 \pm 2\sqrt{5}}} \begin{bmatrix} 2 \\ 1 \pm \sqrt{5} \end{bmatrix}.$$

So the left and right positive operators are given by

$$J = \sqrt{\frac{3+\sqrt{5}}{2}}\, |j_+\rangle\langle j_+| + \sqrt{\frac{3-\sqrt{5}}{2}}\, |j_-\rangle\langle j_-| = \frac{1}{\sqrt{5}} \begin{bmatrix} 3 & 1 \\ 1 & 2 \end{bmatrix},$$
$$K = \sqrt{\frac{3+\sqrt{5}}{2}}\, |k_+\rangle\langle k_+| + \sqrt{\frac{3-\sqrt{5}}{2}}\, |k_-\rangle\langle k_-| = \frac{1}{\sqrt{5}} \begin{bmatrix} 2 & 1 \\ 1 & 3 \end{bmatrix},$$

and the unitary is given by

$$U = MJ^{-1} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \frac{1}{\sqrt{5}} \begin{bmatrix} 2 & -1 \\ -1 & 3 \end{bmatrix} = \frac{1}{\sqrt{5}} \begin{bmatrix} 2 & -1 \\ 1 & 2 \end{bmatrix}.$$

2.51

$$H^\dagger H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I.$$

2.52

$$H^2 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I.$$

2.53

$$\det(H - \lambda I) = \lambda^2 - 1 = 0 \quad \Longrightarrow \quad \text{eigenvalues} = \{-1, 1\}.$$

For eigenvalue 1 :

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}a\\ b\end{bmatrix}=\begin{bmatrix}a\\ b\end{bmatrix}\quad\Longrightarrow\quad\text{eigenvector}=\frac{1}{\sqrt{4-2\sqrt{2}}}\begin{bmatrix}1\\ -1+\sqrt{2}\end{bmatrix}$$

For eigenvalue -1 :

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}a\\ b\end{bmatrix}=-\begin{bmatrix}a\\ b\end{bmatrix}\quad\Longrightarrow\quad\text{eigenvector}=\frac{1}{\sqrt{4+2\sqrt{2}}}\begin{bmatrix}1\\ -1-\sqrt{2}\end{bmatrix}.$$

2.54

If $[A,B]=0$ then they share a common eigenbasis $\{|i\rangle\}$, that is

$$A=\sum_i \alpha_i\,|i\rangle\langle i|\,,$$
$$B=\sum_i \beta_i\,|i\rangle\langle i|\,.$$

$$\begin{aligned}\Longrightarrow\quad \exp(A)\exp(B)&=\sum_i \exp(\alpha_i)\,|i\rangle\langle i|\sum_j \exp(\beta_j)\,|j\rangle\langle j|\\ &=\sum_i\sum_j \exp(\alpha_i+\beta_j)\,|i\rangle\,\langle i\,|\,j\rangle\,\langle j|\\ &=\sum_i \exp(\alpha_i+\beta_i)\,|i\rangle\langle i|\\ &=\exp(A+B).\end{aligned}$$

2.55

Considering that the Hamiltonian has a spectral decomposition $\sum_j E_j(t_1,t_2)\,|j\rangle\langle j|$ yields

$$\begin{aligned}U^\dagger(t_1,t_2)U(t_1,t_2)&=\exp\left(\frac{iH(t_1,t_2)}{\hbar}\right)\exp\left(\frac{-iH(t_1,t_2)}{\hbar}\right)\\ &=\sum_j\sum_k \exp\left(\frac{iE_j(t_1,t_2)}{\hbar}\right)\exp\left(\frac{-iE_k(t_1,t_2)}{\hbar}\right)|j\rangle\,\langle j\,|\,k\rangle\,\langle k|\\ &=\sum_j \exp\left(\frac{iE_j(t_1,t_2)-iE_j(t_1,t_2)}{\hbar}\right)|j\rangle\langle j|\\ &=\exp(0)\sum_j |j\rangle\langle j|\\ &=I.\end{aligned}$$

2.56

If U is unitary then it can be written as $\sum_j \exp(i\theta_j)\,|j\rangle\langle j|$, where $\theta_j \in \mathbb{R}$, thus

$$\begin{aligned} K = -i\log(U) &= -i\sum_j \log[\exp(i\theta_j)]\,|j\rangle\langle j| \\ &= -i\sum_j i\theta_j\,|j\rangle\langle j| \\ &= \left(-i\sum_j i\theta_j\,|j\rangle\langle j|\right)^\dagger \\ &= K^\dagger. \end{aligned}$$

2.57

After a measurement is performed over an initial state $|\psi\rangle$, using the operators set $\{L_l\}$, the state is transformed to the one associated with the measurement outcome l, given by

$$|\psi_l\rangle = \frac{L_l\,|\psi\rangle}{\sqrt{\left\langle\psi\right|L_l^\dagger L_l\left|\psi\right\rangle}}.$$

Then, if a measurement is performed over $|\psi_l\rangle$, using the operators set $\{M_m\}$, the final state can be written as

$$\begin{aligned} |\psi_{lm}\rangle = \frac{M_m\,|\psi_l\rangle}{\sqrt{\left\langle\psi_l\right|M_m^\dagger M_m\left|\psi_l\right\rangle}} &= \frac{M_m}{\sqrt{\left(\frac{\langle\psi|L_l^\dagger}{\sqrt{\langle\psi\,|\,L_l^\dagger L_l\,|\,\psi\rangle}}\right)M_m^\dagger M_m\left(\frac{L_l|\psi\rangle}{\sqrt{\langle\psi\,|\,L_l^\dagger L_l\,|\,\psi\rangle}}\right)}}\left(\frac{L_l\,|\psi\rangle}{\sqrt{\left\langle\psi\right|L_l^\dagger L_l\left|\psi\right\rangle}}\right) \\ &= \frac{M_m L_l\,|\psi\rangle}{\sqrt{\left\langle\psi\right|L_l^\dagger M_m^\dagger M_m L_l\left|\psi\right\rangle}}. \end{aligned}$$

Alternatively, if a measurement was to be performed over $|\psi\rangle$, using the operators set $\{N_{lm}\}$, the final state would be

$$\frac{N_{lm}\,|\psi\rangle}{\sqrt{\left\langle\psi\right|N_{lm}^\dagger N_{lm}\left|\psi\right\rangle}} = \frac{M_m L_l\,|\psi\rangle}{\sqrt{\left\langle\psi\right|L_l^\dagger M_m^\dagger M_m L_l\left|\psi\right\rangle}} = |\psi_{lm}\rangle\,.$$

2.58

$$\langle M\rangle = \langle\psi\,|\,M\,|\,\psi\rangle = m\,\langle\psi\,|\,\psi\rangle = m,$$

$$\Delta(M) = \sqrt{\langle M^2\rangle - \langle M\rangle^2} = \sqrt{\langle\psi\,|\,MM\,|\,\psi\rangle - m^2} = \sqrt{m^2 - m^2} = 0.$$

2.59

$$\langle X \rangle = \langle 0 \,|\, X \,|\, 0 \rangle = \langle 0 \,|\, 1 \rangle = 0,$$

$$\Delta(X) = \sqrt{\langle X^2 \rangle - \langle X \rangle^2} = \sqrt{\langle 0 \,|\, I \,|\, 0 \rangle - 0} = \sqrt{1 - 0} = 1$$

2.60

$$\begin{aligned} \vec{v} \cdot \vec{\sigma} &= v_1 \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} + v_2 \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} + v_3 \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \\ &= \begin{bmatrix} v_3 & v_1 - iv_2 \\ v_1 + iv_2 & -v_3 \end{bmatrix}. \end{aligned}$$

$$\det(\vec{v} \cdot \vec{\sigma} - \lambda I) = \lambda^2 - \left(v_1^2 + v_2^2 + v_3^2\right) = 0.$$

Since $\vec{v}$ is a unit vector, $v_1^2 + v_2^2 + v_3^2 = 1$ and the eigenvalues are $\{-1, 1\}$.

For eigenvalue 1:

$$\begin{bmatrix} v_3 & v_1 - iv_2 \\ v_1 + iv_2 & -v_3 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix} \quad \Longrightarrow \quad \text{eigenvector} = |e_+\rangle = \frac{1}{\sqrt{2 + 2v_3}} \begin{bmatrix} 1 + v_3 \\ v_1 + iv_2 \end{bmatrix}.$$

For eigenvalue -1:

$$\begin{bmatrix} v_3 & v_1 - iv_2 \\ v_1 + iv_2 & -v_3 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = -\begin{bmatrix} a \\ b \end{bmatrix} \quad \Longrightarrow \quad \text{eigenvector} = |e_-\rangle = \frac{1}{\sqrt{2 - 2v_3}} \begin{bmatrix} 1 - v_3 \\ -v_1 - iv_2 \end{bmatrix}.$$

The projector operators are then given by

$$\begin{aligned} P_+ = |e_+\rangle\langle e_+| &= \frac{1}{\sqrt{2 + 2v_3}} \begin{bmatrix} 1 + v_3 \\ v_1 + iv_2 \end{bmatrix} \frac{1}{\sqrt{2 + 2v_3}} \begin{bmatrix} 1 + v_3 & v_1 - iv_2 \end{bmatrix} \\ &= \frac{1}{2\,(1 + v_3)} \begin{bmatrix} (1 + v_3)^2 & (1 + v_3)\,(v_1 - iv_2) \\ (1 + v_3)\,(v_1 + iv_2) & v_1^2 + v_2^2 \end{bmatrix} \\ &= \frac{1}{2} \begin{bmatrix} 1 + v_3 & v_1 - iv_2 \\ v_1 + iv_2 & 1 - v_3 \end{bmatrix} \\ &= \frac{1}{2} \left(I + \vec{v} \cdot \vec{\sigma}\right) \\ P_- = |e_-\rangle\langle e_-| &= \frac{1}{\sqrt{2 - 2v_3}} \begin{bmatrix} 1 - v_3 \\ -v_1 - iv_2 \end{bmatrix} \frac{1}{\sqrt{2 - 2v_3}} \begin{bmatrix} 1 - v_3 & -v_1 + iv_2 \end{bmatrix} \\ &= \frac{1}{2\,(1 - v_3)} \begin{bmatrix} (1 - v_3)^2 & (1 - v_3)\,(-v_1 + iv_2) \\ (1 - v_3)\,(-v_1 - iv_2) & v_1^2 + v_2^2 \end{bmatrix} \end{aligned}$$

$$= \frac{1}{2}\begin{bmatrix} 1-v_3 & -v_1+iv_2 \\ -v_1-iv_2 & 1+v_3 \end{bmatrix}$$
$$= \frac{1}{2}\left(I - \vec{v}\cdot\vec{\sigma}\right).$$

2.61

$$\begin{aligned} p(1) = \langle 0 \,|\, P_+ \,|\, 0\rangle &= \frac{1}{2}\left(\langle 0 \,|\, I \,|\, 0\rangle + \langle 0 \,|\, \vec{v}\cdot\vec{\sigma} \,|\, 0\rangle\right) \\ &= \frac{1}{2}\left(\langle 0 \,|\, I \,|\, 0\rangle + v_1 \langle 0 \,|\, X \,|\, 0\rangle + v_2 \langle 0 \,|\, Y \,|\, 0\rangle + v_3 \langle 0 \,|\, Z \,|\, 0\rangle\right) \\ &= \frac{1}{2}\left(1 + 0 + 0 + v_3\right) \\ &= \frac{1+v_3}{2}. \end{aligned}$$

$$\begin{aligned} |\psi\rangle = \frac{P_+ \,|0\rangle}{\sqrt{\langle 0 \,|\, P_+ \,|\, 0\rangle}} &= \frac{1}{2}\left(\frac{I\,|0\rangle + v_1 X\,|0\rangle + v_2 Y\,|0\rangle + v_3 Z\,|0\rangle}{\sqrt{\frac{1+v_3}{2}}}\right) \\ &= \frac{(1+v_3)\,|0\rangle + (v_1+iv_2)\,|1\rangle}{\sqrt{2+2v_3}} \\ &= |e_+\rangle\,. \end{aligned}$$

2.62

If the measurement operators P_m and the POVM elements E_m coincide then

$$E_m = P_m^\dagger P_m = P_m \quad \Longrightarrow \quad P_m \text{ are positive operators} \quad \Longrightarrow \quad P_m^\dagger = P_m,$$

thus

$$P_m^\dagger P_m = P_m^2 \quad \Longrightarrow \quad P_m^2 = P_m.$$

2.63

Unitaries U_m rise naturally from the left polar decomposition of operators M_m, given by

$$M_m = U_m \sqrt{M_m^\dagger M_m} = U_m \sqrt{E_m}.$$

2.64

We can use an idea analogous to the Gram-Schmidt process to produce the states

$$|\phi_i\rangle = |\psi_i\rangle - \sum_{j=1\,(j\neq i)}^{m} \frac{\langle \psi_j \,|\, \psi_i\rangle\,|\psi_j\rangle}{\||\psi_j\rangle\|^2},$$

orthogonal to all states $|\psi_j\rangle$ with $j \neq i$. So by choosing

$$E_i = \alpha_i \, |\phi_i\rangle\langle\phi_i| \, , \text{ for } i \in \{1, \cdots, m\} \, , \text{ and } E_{m+1} = I - \sum_{i=1}^{m} E_i,$$

where α_i are constants such that E_{m+1} is a positive operator, then we satisfy the condition $\sum_i E_i = I$, and for any measurement outcome E_i, for $i \in \{1, \cdots, m\}$, Bob knows with certainty that the received state is $|\psi_i\rangle$, because the probability of obtaining E_i upon receiving any other state $|\psi_j\rangle$ is

$$\langle\psi_j \,|\, E_i \,|\, \psi_j\rangle = \alpha_i \, \langle\psi_j \,|\, \phi_i\rangle \, \langle\phi_i|\psi_j\rangle = 0.$$

2.65

In the Hadamard basis $\{|+\rangle \, , |-\rangle\}$ the states are written as

$$\frac{|0\rangle + |1\rangle}{\sqrt{2}} = |+\rangle \, ,$$
$$\frac{|0\rangle - |1\rangle}{\sqrt{2}} = |-\rangle \, .$$

2.66

$$\begin{aligned}
\left(\frac{\langle 00| + \langle 11|}{\sqrt{2}}\right) X_1 Z_2 \left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right) &= \frac{1}{2}\big(\langle 0 \,|\, X_1 \,|\, 0\rangle \, \langle 0 \,|\, Z_2 \,|\, 0\rangle + \langle 0 \,|\, X_1 \,|\, 1\rangle \, \langle 0 \,|\, Z_2 \,|\, 1\rangle \\
&\qquad + \langle 1 \,|\, X_1 \,|\, 0\rangle \, \langle 1 \,|\, Z_2 \,|\, 0\rangle + \langle 1 \,|\, X_1 \,|\, 1\rangle \, \langle 1 \,|\, Z_2 \,|\, 1\rangle \big) \\
&= \frac{1}{2}\big(\langle 0 \,|\, 1\rangle \, \langle 0 \,|\, 0\rangle + \langle 0 \,|\, 0\rangle \, \langle 0 \,|\, 1\rangle + \langle 1 \,|\, 1\rangle \, \langle 1 \,|\, 0\rangle + \langle 1 \,|\, 0\rangle \, \langle 1 \,|\, 1\rangle \big) \\
&= 0.
\end{aligned}$$

2.67

Let $W^\perp$ be the orthogonal complement of the subspace W, then we have $V = W \oplus W^\perp$. Also, consider that $\{|w_i\rangle\}$ and $\left\{|w_i^\perp\rangle\right\}$ are orthonormal basis for the subspaces W and $W^\perp$ respectively. We can define an operator U' given by

$$U' \coloneqq \sum_{i=1}^{\dim(W)} U \, |w_i\rangle\langle w_i| + \sum_{i=1}^{\dim(W^\perp)} \left|w_i^\perp\right\rangle\!\left\langle w_i^\perp\right| .$$

Any vector $|v\rangle \in V$ can be written as

$$|v\rangle = \sum_{i=1}^{\dim(W)} a_i \, |w_i\rangle + \sum_{i=1}^{\dim(W^\perp)} b_i \, |w_i^\perp\rangle \, ,$$

thus

$$\begin{aligned} U' |v\rangle &= \sum_{i=1}^{\dim(W)} \sum_{j=1}^{\dim(W)} a_j U |w_i\rangle \langle w_i | w_j\rangle + \sum_{i=1}^{\dim(W^\perp)} \sum_{i=j}^{\dim(W^\perp)} b_j |w_i^\perp\rangle \left\langle w_i^\perp \middle| w_j^\perp \right\rangle \\ &= \sum_{i=1}^{\dim(W)} a_i U |w_i\rangle + \sum_{i=1}^{\dim(W^\perp)} b_i |w_i^\perp\rangle \quad \in V. \end{aligned}$$

$$\begin{aligned} U'^\dagger U' &= \sum_{i=1}^{\dim(W)} \sum_{j=1}^{\dim(W)} |w_i\rangle \left\langle w_i \middle| U^\dagger U \middle| w_j \right\rangle \langle w_j| + \sum_{i=1}^{\dim(W^\perp)} \sum_{j=1}^{\dim(W^\perp)} |w_i^\perp\rangle \left\langle w_i^\perp \middle| w_j^\perp \right\rangle \langle w_j^\perp| \\ &= \sum_{i=1}^{\dim(W)} |w_i\rangle\langle w_i| + \sum_{i=1}^{\dim(W^\perp)} \left|w_i^\perp\right\rangle\left\langle w_i^\perp\right| \\ &= I. \end{aligned}$$

So we clearly have a unitary operator $U' : V \to V$. Any vector $|w\rangle \in W$ can be written as

$$|w\rangle = \sum_{i=1}^{\dim(W)} c_i |w_i\rangle ,$$

thus

$$\begin{aligned} U' |w\rangle &= \sum_{i=1}^{\dim(W)} \sum_{j=1}^{\dim(W)} c_j U |w_i\rangle \langle w_i | w_j\rangle + \sum_{i=1}^{\dim(W^\perp)} \sum_{j=1}^{\dim(W)} c_j |w_i^\perp\rangle \left\langle w_i^\perp \middle| w_j \right\rangle \\ &= \sum_{i=1}^{\dim(W)} c_i U |w_i\rangle \\ &= U |w\rangle . \end{aligned}$$

Therefore, there exists a unitary operator $U' : V \to V$ which extends U.

2.68

Suppose there are states $|a\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$ and $|b\rangle = \beta_0 |0\rangle + \beta_1 |1\rangle$ such that $|\psi\rangle$ can be written as $|\psi\rangle = |a\rangle |b\rangle$. Then explicitly we have

$$\begin{aligned} |\psi\rangle = (\alpha_0 |0\rangle + \alpha_1 |1\rangle)(\beta_0 |0\rangle + \beta_1 |1\rangle) &= \alpha_0\beta_0 |00\rangle + \alpha_0\beta_1 |01\rangle + \alpha_1\beta_0 |10\rangle + \alpha_1\beta_1 |11\rangle \\ &= \frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle , \end{aligned}$$

but there are no possible combination of values for $\alpha_0, \alpha_1, \beta_0$ and β_1 that satisfies this equality.

2.69

Labeling the Bell states as

$$
\begin{aligned}
|\Phi^+\rangle &= \frac{|00\rangle + |11\rangle}{\sqrt{2}}, \\
|\Phi^-\rangle &= \frac{|00\rangle - |11\rangle}{\sqrt{2}}, \\
|\Psi^+\rangle &= \frac{|01\rangle + |10\rangle}{\sqrt{2}}, \\
|\Psi^-\rangle &= \frac{|01\rangle - |10\rangle}{\sqrt{2}},
\end{aligned}
$$

we have the following relations:

$$
\begin{aligned}
\left\langle \Phi^{\pm} \middle| \Phi^{\pm} \right\rangle &= \frac{\langle 00| \pm \langle 11|}{\sqrt{2}} \frac{|00\rangle \pm |11\rangle}{\sqrt{2}} = \frac{\langle 0\,|\,0\rangle \langle 0\,|\,0\rangle \pm \langle 0\,|\,1\rangle \langle 0\,|\,1\rangle \pm \langle 1\,|\,0\rangle \langle 1\,|\,0\rangle + \langle 1\,|\,1\rangle \langle 1\,|\,1\rangle}{2} = 1, \\
\left\langle \Psi^{\pm} \middle| \Psi^{\pm} \right\rangle &= \frac{\langle 01| \pm \langle 10|}{\sqrt{2}} \frac{|01\rangle \pm |10\rangle}{\sqrt{2}} = \frac{\langle 0\,|\,0\rangle \langle 1\,|\,1\rangle \pm \langle 0\,|\,1\rangle \langle 1\,|\,0\rangle \pm \langle 1\,|\,0\rangle \langle 0\,|\,1\rangle + \langle 1\,|\,1\rangle \langle 0\,|\,0\rangle}{2} = 1, \\
\left\langle \Phi^{\pm} \middle| \Phi^{\mp} \right\rangle &= \frac{\langle 00| \pm \langle 11|}{\sqrt{2}} \frac{|00\rangle \mp |11\rangle}{\sqrt{2}} = \frac{\langle 0\,|\,0\rangle \langle 0\,|\,0\rangle \mp \langle 0\,|\,1\rangle \langle 0\,|\,1\rangle \pm \langle 1\,|\,0\rangle \langle 1\,|\,0\rangle - \langle 1\,|\,1\rangle \langle 1\,|\,1\rangle}{2} = 0, \\
\left\langle \Psi^{\pm} \middle| \Psi^{\mp} \right\rangle &= \frac{\langle 01| \pm \langle 10|}{\sqrt{2}} \frac{|01\rangle \mp |10\rangle}{\sqrt{2}} = \frac{\langle 0\,|\,0\rangle \langle 1\,|\,1\rangle \mp \langle 0\,|\,1\rangle \langle 1\,|\,0\rangle \pm \langle 1\,|\,0\rangle \langle 0\,|\,1\rangle - \langle 1\,|\,1\rangle \langle 0\,|\,0\rangle}{2} = 0, \\
\left\langle \Phi^{\pm} \middle| \Psi^{\pm} \right\rangle &= \frac{\langle 00| \pm \langle 11|}{\sqrt{2}} \frac{|01\rangle \pm |10\rangle}{\sqrt{2}} = \frac{\langle 0\,|\,0\rangle \langle 0\,|\,1\rangle \pm \langle 0\,|\,1\rangle \langle 0\,|\,0\rangle \pm \langle 1\,|\,0\rangle \langle 1\,|\,1\rangle + \langle 1\,|\,1\rangle \langle 1\,|\,0\rangle}{2} = 0, \\
\left\langle \Phi^{\pm} \middle| \Psi^{\mp} \right\rangle &= \frac{\langle 00| \pm \langle 11|}{\sqrt{2}} \frac{|01\rangle \mp |10\rangle}{\sqrt{2}} = \frac{\langle 0\,|\,0\rangle \langle 0\,|\,1\rangle \mp \langle 0\,|\,1\rangle \langle 0\,|\,0\rangle \pm \langle 1\,|\,0\rangle \langle 1\,|\,1\rangle - \langle 1\,|\,1\rangle \langle 1\,|\,0\rangle}{2} = 0.
\end{aligned}
$$

2.70

$$
\begin{aligned}
\left\langle \Phi^{\pm} \middle| E \otimes I \middle| \Phi^{\pm} \right\rangle &= \frac{\langle 0\,|\,E\,|\,0\rangle \langle 0\,|\,0\rangle \pm \langle 0\,|\,E\,|\,1\rangle \langle 0\,|\,1\rangle \pm \langle 1\,|\,E\,|\,0\rangle \langle 1\,|\,0\rangle + \langle 1\,|\,E\,|\,1\rangle \langle 1\,|\,1\rangle}{2} \\
&= \frac{\langle 0\,|\,E\,|\,0\rangle + \langle 1\,|\,E\,|\,1\rangle}{2}, \\
\left\langle \Psi^{\pm} \middle| E \otimes I \middle| \Psi^{\pm} \right\rangle &= \frac{\langle 0\,|\,E\,|\,0\rangle \langle 1\,|\,1\rangle \pm \langle 0\,|\,E\,|\,1\rangle \langle 1\,|\,0\rangle \pm \langle 1\,|\,E\,|\,0\rangle \langle 0\,|\,1\rangle + \langle 1\,|\,E\,|\,1\rangle \langle 0\,|\,0\rangle}{2} \\
&= \frac{\langle 0\,|\,E\,|\,0\rangle + \langle 1\,|\,E\,|\,1\rangle}{2}.
\end{aligned}
$$

So, if Eve intercepts Alice's qubit and performs a measurement using measurement operators $\{M_m\}$ the probability of obtaining outcome m is

$$
\left\langle \psi \middle| M_m^\dagger M_m \middle| \psi \right\rangle = \frac{\left\langle 0 \middle| M_m^\dagger M_m \middle| 0 \right\rangle + \left\langle 1 \middle| M_m^\dagger M_m \middle| 1 \right\rangle}{2}
$$

for all m, independently of the four possible states $|\psi\rangle$. Therefore Eve could not infer anything about the qubit sent by Alice.

2.71

Let $\{|\psi_i\rangle\}$ be an orthonormal basis for which the density operator is diagonal. Then

$$\begin{aligned}
\rho^2 &= \sum_i \sum_j p_i p_j \, |\psi_i\rangle \, \langle\psi_i \,|\, \psi_j\rangle \, \langle\psi_j| \\
&= \sum_i p_i^2 \, |\psi_i\rangle\langle\psi_i| \\
\implies \quad \operatorname{tr}\big(\rho^2\big) &= \sum_j \left\langle \psi_j \,\middle|\, \left(\sum_i p_i^2 \, |\psi_i\rangle\langle\psi_i| \right) \,\middle|\, \psi_j \right\rangle \\
&= \sum_i \sum_j p_i^2 \, \langle\psi_j \,|\, \psi_i\rangle \, \langle\psi_i \,|\, \psi_j\rangle \\
&= \sum_j p_j^2 \leq 1,
\end{aligned}$$

because $\sum_i p_i = 1$ and $p_i \leq 1$ for all i. Equality would only occur if $p_i = 1$ for some i and $p_j = 0$ for all $j \neq i$, that is, a pure state.

2.72

A density operator ρ is positive (hence Hermitian) and has trace equal to one. So for $a, b, c \in \mathbb{R}$, such that $-1 \leq c \leq 1$, we can write ρ as

$$\begin{aligned}
\rho &= \frac{1}{2} \begin{bmatrix} 1+c & a-ib \\ a+ib & 1-c \end{bmatrix} \\
&= \frac{1}{2} \left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} 0 & a \\ a & 0 \end{bmatrix} + \begin{bmatrix} 0 & -ib \\ ib & 0 \end{bmatrix} + \begin{bmatrix} c & 0 \\ 0 & -c \end{bmatrix} \right) \\
&= \frac{I + aX + bY + cZ}{2}.
\end{aligned}$$

We must have $\operatorname{tr}(\rho^2) \leq 1$, thus

$$\begin{aligned}
\operatorname{tr}\big(\rho^2\big) &= \frac{1}{4} \operatorname{tr} \begin{bmatrix} a^2 + b^2 + (1+c)^2 & 2\,(a-ib) \\ 2\,(a+ib) & a^2 + b^2 + (1-c)^2 \end{bmatrix} \\
&= \frac{1}{2} \left(1 + a^2 + b^2 + c^2\right) \quad \implies \quad a^2 + b^2 + c^2 \leq 1.
\end{aligned}$$

So defining the vector $\vec{r} \coloneqq (a, b, c)$, we have $\|\vec{r}\| \leq 1$ and

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

For $\rho = I/2$ we have $\vec{r} = 0$, meaning the null vector. So the state would be represented by the origin in the Bloch sphere.

If ρ is pure then

$$\operatorname{tr}\big(\rho^2\big) = 1 \quad \iff \quad a^2 + b^2 + c^2 = 1 \quad \iff \quad \|\vec{r}\| = 1.$$

For pure states we have $\rho = |\psi\rangle\langle\psi|$, thus we may write

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle,$$

where θ and φ are polar angles of the unit Bloch vector $\vec{r}$, as described in Section 1.2.

2.73

$$\begin{aligned}|\psi\rangle &= \rho\rho^{-1}|\psi\rangle \\ &= \sum_i p_i |\psi_i\rangle \langle\psi_i| \rho^{-1} |\psi\rangle .\end{aligned}$$

Because $|\psi\rangle$ is a state in the support of ρ we may write

$$\begin{aligned}|\psi\rangle &= \sum_j a_j |\psi_j\rangle \\ \implies \quad |\psi\rangle &= \sum_i \sum_j p_i a_j |\psi_i\rangle \langle\psi_i| \rho^{-1} |\psi_j\rangle \\ &= \sum_i p_i \langle\psi_i| \rho^{-1} |\psi_i\rangle a_i |\psi_i\rangle ,\end{aligned}$$

but this equality holds only if

$$p_i = \frac{1}{\langle\psi_i| \rho^{-1} |\psi_i\rangle}.$$

2.74

$$\begin{aligned}\rho^{AB} = (|a\rangle|b\rangle)(\langle a|\langle b|) &= |a\rangle\langle a| \otimes |b\rangle\langle b| \\ \implies \quad \rho^A = \mathrm{tr}_B(\rho^{AB}) &= |a\rangle\langle a| \,\mathrm{tr}(|b\rangle\langle b|) \\ &= |a\rangle\langle a| .\end{aligned}$$

2.75

Labeling the density operators as

$$\begin{aligned}\rho^{\Phi^\pm} = |\Phi^\pm\rangle\langle\Phi^\pm| &= \frac{|00\rangle \pm |11\rangle}{\sqrt{2}} \frac{\langle 00| \pm \langle 11|}{\sqrt{2}} = \frac{|00\rangle\langle 00| \pm |00\rangle\langle 11| \pm |11\rangle\langle 00| + |11\rangle\langle 11|}{2}, \\ \rho^{\Psi^\pm} = |\Psi^\pm\rangle\langle\Psi^\pm| &= \frac{|01\rangle \pm |10\rangle}{\sqrt{2}} \frac{\langle 01| \pm \langle 10|}{\sqrt{2}} = \frac{|01\rangle\langle 01| \pm |01\rangle\langle 10| \pm |10\rangle\langle 01| + |10\rangle\langle 10|}{2},\end{aligned}$$

we have the following relations:

$$\begin{aligned}\rho_1^{\Phi^\pm} = \mathrm{tr}_2\left(\rho^{\Phi^\pm}\right) &= \frac{|0\rangle\langle 0| \,\mathrm{tr}(|0\rangle\langle 0|) \pm |0\rangle\langle 1| \,\mathrm{tr}(|0\rangle\langle 1|) \pm |1\rangle\langle 0| \,\mathrm{tr}(|1\rangle\langle 0|) + |1\rangle\langle 1| \,\mathrm{tr}(|1\rangle\langle 1|)}{2} \\ &= \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} = \frac{I}{2},\end{aligned}$$

$$\begin{aligned}
\rho_2^{\Phi^\pm} = \mathrm{tr}_1\Big(\rho^{\Phi^\pm}\Big) &= \frac{\mathrm{tr}(|0\rangle\langle 0|)\,|0\rangle\langle 0| \pm \mathrm{tr}(|0\rangle\langle 1|)\,|0\rangle\langle 1| \pm \mathrm{tr}(|1\rangle\langle 0|)\,|1\rangle\langle 0| + \mathrm{tr}(|1\rangle\langle 1|)\,|1\rangle\langle 1|}{2} \\
&= \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} = \frac{I}{2}, \\
\rho_1^{\Psi^\pm} = \mathrm{tr}_2\Big(\rho^{\Psi^\pm}\Big) &= \frac{|0\rangle\langle 0|\,\mathrm{tr}(|1\rangle\langle 1|) \pm |0\rangle\langle 1|\,\mathrm{tr}(|1\rangle\langle 0|) \pm |1\rangle\langle 0|\,\mathrm{tr}(|0\rangle\langle 1|) + |1\rangle\langle 1|\,\mathrm{tr}(|0\rangle\langle 0|)}{2} \\
&= \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} = \frac{I}{2}, \\
\rho_2^{\Psi^\pm} = \mathrm{tr}_1\Big(\rho^{\Psi^\pm}\Big) &= \frac{\mathrm{tr}(|0\rangle\langle 0|)\,|1\rangle\langle 1| \pm \mathrm{tr}(|0\rangle\langle 1|)\,|1\rangle\langle 0| \pm \mathrm{tr}(|1\rangle\langle 0|)\,|0\rangle\langle 1| + \mathrm{tr}(|1\rangle\langle 1|)\,|0\rangle\langle 0|}{2} \\
&= \frac{|1\rangle\langle 1| + |0\rangle\langle 0|}{2} = \frac{I}{2}.
\end{aligned}$$

2.76

Let $\dim(A) = m$ and $\dim(B) = n$, and consider that $\{|j\rangle\}$ and $\{|k\rangle\}$ are orthonormal basis for spaces A and B respectively. Then any state $|\psi\rangle \in A \otimes B$ can be written as

$$|\psi\rangle = \sum_{j=1}^{m}\sum_{k=1}^{n} a_{jk}\,|j\rangle\,|k\rangle\,.$$

By the singular value decomposition we have

$$a = u\begin{bmatrix} d \\ 0 \end{bmatrix} v \quad \text{if } m > n \text{ and } a = u\begin{bmatrix} d & 0 \end{bmatrix} v \quad \text{if } m < n,$$

where u is a unitary $m \times m$ matrix, v is a unitary $n \times n$ matrix and d is a diagonal $\min\{m,n\} \times \min\{m,n\}$ matrix. The 0 just indicates that there are $m-n$ rows with null entries in the case where $m > n$ or $n - m$ columns in the case where $m < n$. If $m > n$ then we can write $u = \begin{bmatrix} u_1 & u_2 \end{bmatrix}$ where u_1 is $m \times n$ and u_2 is $m \times (m-n)$, thus

$$a = u_1 dv \quad \Longrightarrow \quad a_{jk} = (u_1)_{ji}\, d_{ii} v_{ik}.$$

Labeling the n column vectors of u_1 as $|i_A\rangle = (u_1)_{ji}\,|j\rangle$, the n row vectors of v as $|i_B\rangle = v_{ik}\,|k\rangle$, and $\lambda_i \coloneqq d_{ii}$ then we may write

$$|\psi\rangle = \sum_{i=1}^{n} \lambda_i\,|i_A\rangle\,|i_B\rangle\,.$$

Equivalently, if $m < n$ then we can write $v = \begin{bmatrix} v_1 \\ v_2 \end{bmatrix}$ where v_1 is $m \times n$ and v_2 is $(n-m) \times n$, thus

$$a = udv_1 \quad \Longrightarrow \quad a_{jk} = u_{ji} d_{ii}\,(v_1)_{ik}\,.$$

Labeling the m column vectors of u as $|i_A\rangle = u_{ji}\,|j\rangle$, the m row vectors of v_1 as $|i_B\rangle = (v_1)_{ik}$, and $\lambda_i \coloneqq d_{ii}$ we also may write

$$|\psi\rangle = \sum_{i=1}^{m} \lambda_i\,|i_A\rangle\,|i_B\rangle\,.$$

2.77

First, notice that if the Schmidt coefficients are non-degenerate then the Schmidt decomposition is unique up to phase. To see that, consider that the Schmidt decomposition of the pure state $|\psi\rangle$ of a composite system $A \otimes B$ is given by

$$|\psi\rangle = \sum_i \lambda_i\,|i_A\rangle\,|i_B\rangle \quad \Longrightarrow \quad \rho = |\psi\rangle\langle\psi| = \sum_i \lambda_i^2\,|i_A\rangle\langle i_A| \otimes |i_B\rangle\langle i_B|\,.$$

So, the eigenvalues of the density operator are given by λ_i^2, and because the Schmidt coefficients are non-negative, all $\sqrt{\lambda_i^2}$ are uniquely defined. Furthermore, if they are all non-degenerate then the states $|i_A\rangle\,|i_B\rangle$ associated with each coefficient are also uniquely defined up to phase. Therefore the Schmidt decomposition is unique up to phase.

Now consider the pure state $|\psi\rangle \in A \otimes B \otimes C$, where A, B and C are one qubit spaces, given by

$$|\psi\rangle = \frac{1}{\sqrt{10}}\big(2\,|0\rangle\,|0\rangle\,|0\rangle + 2\,|1\rangle\,|1\rangle\,|0\rangle + |0\rangle\,|1\rangle\,|1\rangle + |1\rangle\,|0\rangle\,|1\rangle\,\big).$$

This state can be rewritten as

$$\begin{aligned}|\psi\rangle &= \frac{2}{\sqrt{5}}\left(\frac{1}{\sqrt{2}}\,|0\rangle\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle\,|1\rangle\right)|0\rangle + \frac{1}{\sqrt{5}}\left(\frac{1}{\sqrt{2}}\,|0\rangle\,|1\rangle + \frac{1}{\sqrt{2}}\,|1\rangle\,|0\rangle\right)|1\rangle \\ &= \frac{2}{\sqrt{5}}\,|\Phi^+\rangle\,|0\rangle + \frac{1}{\sqrt{5}}\,|\Psi^+\rangle\,|1\rangle\,.\end{aligned}$$

This is a Schmidt decomposition $|\psi\rangle = \lambda_0\,|0_D\rangle\,|0_C\rangle + \lambda_1\,|1_D\rangle\,|1_C\rangle$ considering $D \coloneqq A \otimes B$. Since the Schmidt coefficients are different this decomposition is unique, so $|\psi\rangle$ can be written as a tripartite Schmidt decomposition if and only if $|0_D\rangle$ and $|1_D\rangle$ can be written as $|0_A\rangle\,|0_B\rangle$ and $|1_A\rangle\,|1_B\rangle$ respectively. Since they are Bell states this is impossible, thus $|\psi\rangle$ cannot be written in the form

$$|\psi\rangle = \sum_i \lambda_i\,|i_A\rangle\,|i_B\rangle\,|i_C\rangle\,.$$

2.78

$$|\psi\rangle = \sum_i \lambda_i\,|i_A\rangle\,|i_B\rangle\,.$$

Since $\sum_i \lambda_i^2 = 1$, if $\lambda_j = 1$ for some j then it has Schmidt number 1 and

$$|\psi\rangle = |j_A\rangle\,|j_B\rangle\,.$$

The converse is immediate.

If $|\psi\rangle$ is a product state then

$$\begin{aligned} |\psi\rangle = |\psi_A\rangle\,|\psi_B\rangle \quad &\Longrightarrow \quad \rho = |\psi\rangle\langle\psi| = |\psi_A\rangle\langle\psi_A| \otimes |\psi_B\rangle\langle\psi_B| \\ &\Longrightarrow \quad \rho^A = \mathrm{tr}_B(\rho) = |\psi_A\rangle\langle\psi_A|\,, \\ &\qquad\quad \rho^B = \mathrm{tr}_A(\rho) = |\psi_B\rangle\langle\psi_B|\,. \end{aligned}$$

The converse is immediate.

2.79

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}\,|0\rangle\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle\,|1\rangle\,;$$

$$\frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2} = \frac{|0\rangle + |1\rangle}{\sqrt{2}}\,\frac{|0\rangle + |1\rangle}{\sqrt{2}} = |+\rangle\,|+\rangle\,;$$

For the third state we have

$$\begin{aligned} \frac{|00\rangle + |01\rangle + |10\rangle}{\sqrt{3}} \quad \Longrightarrow \quad \rho = \frac{1}{3}\big[\, &|0\rangle\langle 0| \otimes |0\rangle\langle 0| + |0\rangle\langle 0| \otimes |0\rangle\langle 1| + |0\rangle\langle 1| \otimes |0\rangle\langle 0| \\ &+ |0\rangle\langle 0| \otimes |1\rangle\langle 0| + |0\rangle\langle 0| \otimes |1\rangle\langle 1| + |0\rangle\langle 1| \otimes |1\rangle\langle 0| \\ &+ |1\rangle\langle 0| \otimes |0\rangle\langle 0| + |1\rangle\langle 0| \otimes |0\rangle\langle 1| + |1\rangle\langle 1| \otimes |0\rangle\langle 0|\,\big] \end{aligned}$$

$$\begin{aligned} \Longrightarrow \quad \rho^A = \rho^B = \mathrm{tr}_A(\rho) &= \frac{1}{3}\big(2\,|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1|\,\big) \\ &= \frac{1}{3}\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}. \end{aligned}$$

$$\det\big(\rho^B - \lambda I\big) = \lambda^2 - \lambda + \frac{1}{9} = 0 \quad \Longrightarrow \quad \text{eigenvalues} = \lambda_\pm = \frac{3 \pm \sqrt{5}}{6}.$$

$$\frac{1}{3}\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} a \\ b \end{bmatrix} = \frac{3 \pm \sqrt{5}}{6}\begin{bmatrix} a \\ b \end{bmatrix} \quad \Longrightarrow \quad \text{eigenvectors} = |e_\pm\rangle = \frac{\exp(i\theta_\pm)}{\sqrt{10 \mp 2\sqrt{5}}}\begin{bmatrix} 2 \\ -1 \pm \sqrt{5} \end{bmatrix}.$$

$$\begin{array}{c}\text{Choosing the correct phases} \\ \big(\theta_+ = 0\,;\ \ \theta_- = \frac{\pi}{2}\big)\end{array} \quad \Longrightarrow \quad \frac{|00\rangle + |01\rangle + |10\rangle}{\sqrt{3}} = \sqrt{\lambda_+}\,|e_+\rangle\,|e_+\rangle + \sqrt{\lambda_-}\,|e_-\rangle\,|e_-\rangle\,.$$

2.80

$$|\psi\rangle = \sum_i \lambda_i\,|\psi_i^A\rangle\,|\psi_i^B\rangle\,,$$

$$|\varphi\rangle = \sum_i \lambda_i |\varphi_i^A\rangle |\varphi_i^B\rangle .$$

Let $U : A \to A$ and $V : B \to B$ be unitary transformations such that $U|\varphi_i^A\rangle = |\psi_i^A\rangle$ and $V|\varphi_i^B\rangle = |\psi_i^B\rangle$, then we may write

$$\begin{aligned} |\psi\rangle &= \sum_i \lambda_i U |\varphi_i^A\rangle \otimes V |\varphi_i^B\rangle \\ &= (U \otimes V) \sum_i \lambda_i |\varphi_i^A\rangle |\varphi_i^B\rangle \\ &= (U \otimes V) |\varphi\rangle . \end{aligned}$$

2.81

Consider that the density operator is given by $\rho^A = \sum_i p_i |i_A\rangle\langle i_A|$, then the two purifications can be written as

$$\begin{aligned} |AR_1\rangle &= \sum_i \sqrt{p_i} |i_A\rangle |i_{R_1}\rangle , \\ |AR_2\rangle &= \sum_i \sqrt{p_i} |i_A\rangle |i_{R_2}\rangle . \end{aligned}$$

Let $U_R : R \to R$ be a unitary transformation such that $U_R |i_{R_2}\rangle = |i_{R_1}\rangle$, then we may write

$$\begin{aligned} |AR_1\rangle &= \sum_i \sqrt{p_i} I_A |i_A\rangle \otimes U_R |i_{R_2}\rangle \\ &= (I_A \otimes U_R) \sum_i \sqrt{p_i} |i_A\rangle |i_{R_2}\rangle \\ &= (I_A \otimes U_R) |AR_2\rangle . \end{aligned}$$

2.82

$$\begin{aligned} \mathrm{tr}_R \left[\left(\sum_i \sqrt{p_i} |\psi_i\rangle |i\rangle \right) \left(\sum_j \sqrt{p_j} \langle\psi_j| \langle j| \right) \right] &= \sum_i \sum_j \sqrt{p_i p_j} |\psi_i\rangle\langle\psi_j| \, \mathrm{tr}(|i\rangle\langle j|) \\ &= \sum_i p_i |\psi_i\rangle\langle\psi_i| = \rho. \end{aligned}$$

To measure R in the basis $|i\rangle$ means we are using the set of projective measurement operators $\{I \otimes |i\rangle\langle i|\}$. So, the probability of obtaining outcome i is

$$\begin{aligned} \sum_j \sqrt{p_j} \langle\psi_j| \langle j| \left(I \otimes |i\rangle\langle i| \right) \sum_k \sqrt{p_k} |\psi_k\rangle |k\rangle &= \sum_j \sum_k \sqrt{p_j p_k} \langle\psi_j | I | \psi_k\rangle \langle j | i\rangle \langle i | k\rangle \\ &= \sqrt{p_i p_i} \langle\psi_i | I | \psi_i\rangle = p_i, \end{aligned}$$

and the corresponding post-measurement state of system A is $|\psi_i\rangle$.

Due to the unitary freedom in the ensemble for density matrices there exists an ensemble $\{q_j, |\phi_j\rangle\}$

that generates the same density matrix ρ, with the condition that

$$\sqrt{q_j}\,|\phi_j\rangle = \sum_i u_{ji}\sqrt{p_i}\,|\psi_i\rangle$$

for some unitary matrix u_{ji}. So, considering an orthonormal basis $\{|r_i\rangle\}$ for R, we may write any purification $|AR\rangle$ as

$$\begin{aligned}|AR\rangle &= \sum_j \sqrt{q_j}\,|\phi_j\rangle\,|r_j\rangle \\ &= \sum_j \left(\sum_i u_{ji}\sqrt{p_i}\,|\psi_i\rangle\right) \otimes |r_j\rangle \\ &= \sum_i \sqrt{p_i}\,|\psi_i\rangle \otimes \left(\sum_j u_{ji}\,|r_j\rangle\right).\end{aligned}$$

Now, let $U : R \to R$ be a unitary transformation such that, for all $|r_i\rangle \in R$, we have $U\,|r_i\rangle = \sum_j u_{ji}\,|r_j\rangle \coloneqq |i\rangle$, thus

$$|AR\rangle = \sum_i \sqrt{p_i}\,|\psi_i\rangle\,|i\rangle\,.$$

It is straightforward to see that $\{|i\rangle\}$ is an orthonormal basis for R since

$$\begin{aligned}\langle i\,|\,j\rangle &= \left\langle r_i \,\middle|\, U^\dagger U \,\middle|\, r_j\right\rangle \\ &= \langle r_i\,|\,r_j\rangle \\ &= \delta_{ij},\end{aligned}$$

and we have already shown that, for a purification of this form, if we measure R in the basis $\{|i\rangle\}$, we obtain outcome i with probability p_i, meaning we have post-measurement state $|\psi_i\rangle$ for system A with probability p_i.

3 Introduction to computer science

Exercises: 3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7, 3.8, 3.9, 3.10, 3.11, 3.12, 3.13, 3.14, 3.15, 3.16, 3.17, 3.18, 3.19, 3.20, 3.21, 3.22, 3.23, 3.24, 3.25, 3.26, 3.27, 3.28, 3.29, 3.30, 3.31, 3.32.

3.1

Since Turing machines can be thought of as computing functions from non-negative integers to non-negative integers (or in general, from reals to reals within finite precision), if a process in nature computes a function that consists of a map between different sets, it would not be computable by a Turing machine.

3.2

Considering a Turing machine with m possible internal states q_i, and an alphabet of n possible symbols Γ_j, any program line can be written as

$$\langle q_i, \Gamma_j, q_{i'}, \Gamma_{j'}, s \rangle \, .$$

Now, we map each program line to a string constructed in the following form:

- For each q_i we add the character "S" i times.

- For each Γ_j we add the character "A" j times.

- For $s = -1, 0$ or 1 we add, respectively, the characters "L", "K" or "R".

In the end, considering the program has N lines, it can be entirely mapped to the string

$$\underbrace{\mathrm{S}\cdots\mathrm{S}}_{i_1 \text{ times}}\underbrace{\mathrm{A}\cdots\mathrm{A}}_{j_1 \text{ times}}\underbrace{\mathrm{S}\cdots\mathrm{S}}_{i'_1 \text{ times}}\underbrace{\mathrm{A}\cdots\mathrm{A}}_{j'_1 \text{ times}}\underbrace{\mathrm{I}_1}_{\text{L, K or R}} \cdots \underbrace{\mathrm{S}\cdots\mathrm{S}}_{i_N \text{ times}}\underbrace{\mathrm{A}\cdots\mathrm{A}}_{j_N \text{ times}}\underbrace{\mathrm{S}\cdots\mathrm{S}}_{i'_N \text{ times}}\underbrace{\mathrm{A}\cdots\mathrm{A}}_{j'_N \text{ times}}\underbrace{\mathrm{I}_N}_{\text{L, K or R}} \, .$$

Now we make the character $\rightarrow$ number association

$$\mathrm{S} \rightarrow 0, \ \mathrm{A} \rightarrow 1, \ \mathrm{L} \rightarrow 2, \ \mathrm{K} \rightarrow 3, \ \mathrm{R} \rightarrow 4,$$

and for each character a_i of the string, we use its associated number a_i to calculate $p_i^{a_i}$, where p_i is the i-th prime number. With that, any Turing machine can be uniquely identified with the number

$$\prod_{i=1}^{l} p_i^{a_i},$$

where l denotes the length of the Turing machine's corresponding character string.

3.3

Consider a two-tape Turing machine where the input is written in tape 1 and tape 2 is initially blank. Then we can output, in tape 2, the reversed input number by using

$$\begin{aligned}
&1 : \langle q_s, \triangleright, \triangleright, q_1, \triangleright, \triangleright, +1, +1 \rangle \\
&2 : \langle q_1, 0, b, q_1, 0, b, +1, 0 \rangle \\
&3 : \langle q_1, 1, b, q_1, 1, b, +1, 0 \rangle \\
&4 : \langle q_1, b, b, q_2, b, b, -1, 0 \rangle \\
&5 : \langle q_2, 0, b, q_2, 0, 0, -1, +1 \rangle \\
&6 : \langle q_2, 1, b, q_2, 1, 1, -1, +1 \rangle \\
&7 : \langle q_2, \triangleright, b, q_h, \triangleright, b, 0, 0 \rangle \, .
\end{aligned}$$

3.4

Consider a two-tape Turing machine where the input $x\,b\,y$ is written in tape 1 and tape 2 is initially blank. Then we can output, in tape 2, $x + y \mod 2$ by using

$$
\begin{aligned}
1 &: \langle q_s, \triangleright, \triangleright, q_1, \triangleright, \triangleright, +1, +1\rangle \\
2 &: \langle q_1, 0, b, q_1, 0, 0, +1, 0\rangle \\
3 &: \langle q_1, 1, b, q_1, 1, 1, +1, 0\rangle \\
4 &: \langle q_1, 0, 0, q_1, 0, 0, +1, 0\rangle \\
5 &: \langle q_1, 1, 0, q_1, 1, 1, +1, 0\rangle \\
6 &: \langle q_1, 0, 1, q_1, 0, 0, +1, 0\rangle \\
7 &: \langle q_1, 1, 1, q_1, 1, 1, +1, 0\rangle \\
8 &: \langle q_1, b, 0, q_2, b, 0, +1, 0\rangle \\
9 &: \langle q_1, b, 1, q_2, b, 1, +1, 0\rangle \\
10 &: \langle q_2, 0, 0, q_2, 0, 0, +1, 0\rangle \\
11 &: \langle q_2, 1, 0, q_2, 1, 0, +1, 0\rangle \\
12 &: \langle q_2, 0, 1, q_2, 0, 1, +1, 0\rangle \\
13 &: \langle q_2, 1, 1, q_2, 1, 1, +1, 0\rangle \\
14 &: \langle q_2, b, 0, q_3, b, 0, -1, 0\rangle \\
15 &: \langle q_2, b, 1, q_3, b, 1, -1, 0\rangle \\
16 &: \langle q_3, 0, 0, q_h, 0, 0, 0, 0\rangle \\
17 &: \langle q_3, 1, 0, q_h, 1, 1, 0, 0\rangle \\
18 &: \langle q_3, 0, 1, q_h, 0, 1, 0, 0\rangle \\
19 &: \langle q_3, 1, 1, q_h, 1, 0, 0, 0\rangle\,.
\end{aligned}
$$

3.5

Suppose there exists an algorithm $H_1(\cdot)$ that, upon receiving a Turing machine M as input, yields the result

$$
H_1(M) = \begin{cases} 0 \;\; ; \;\; \text{if } M \text{ doesn't halt for blank input} \\ 1 \;\; ; \;\; \text{if } M \text{ does halt for blank input} \end{cases}.
$$

If $H_1(\cdot)$ exists then we can define another algorithm H_2 that satisfies

$$
H_2 \begin{cases} \text{halts} \;\; ; \;\; \text{if } H_1(H_2) = 0 \\ \text{never halts} \;\; ; \;\; \text{if } H_1(H_2) = 1 \end{cases}.
$$

Now we ask the question: Does H_2 halt for blank input? There are two possible answers:

- H_2 does halt for blank input $\Rightarrow$ $H_1(H_2) = 1$ $\Rightarrow$ H_2 never halts.

- H_2 doesn't halt for blank input $\Rightarrow$ $H_1(H_2) = 0$ $\Rightarrow$ H_2 does halt.

In both cases we have a contradiction, so $H_1(\cdot)$ cannot exist meaning there are no algorithms capable of telling if M halts for blank input or not.

3.6

Suppose there exists an algorithm $H_p(x)$ that computes the probabilistic halting function correctly with probability strictly larger than 1/2. Then we can define an algorithm A that satisfies

$$A \begin{cases} \text{halts} & ; \quad \text{if } H_p(A) = 0 \\ \text{never halts} & ; \quad \text{if } H_p(A) = 1 \end{cases}.$$

Now we ask the question: Does A halt for input A with probability $\geq 1/2$? There are two possible scenarios:

- The answer is "yes":

  $h_p(A) = 1 \;\Rightarrow\; H_p(A) = 1$ with probability $p > 1/2 \;\Rightarrow\; A$ never halts with probability $p > 1/2 \;\Rightarrow\; A$ halts with probability $p < 1/2 \;\Rightarrow\; h_p(A) = 0 \;\Rightarrow$ the answer is "no".

- The answer is "no":

  $h_p(A) = 0 \;\Rightarrow\; H_p(A) = 0$ with probability $p > 1/2 \;\Rightarrow\; A$ halts with probability $p > 1/2 \;\Rightarrow$ $h_p(A) = 1 \;\Rightarrow$ the answer is "yes".

In both cases we have a contradiction, so $H_p(x)$ cannot exist meaning there are no algorithms capable of correctly computing $h_p(x)$ with probability strictly larger than 1/2.

3.7

Yes, it is still undecidable, at least for computing the halting function for Turing machines augmented by the power of calling the oracle. The proof is analogous to the usual proof for the halting problem since one can always define a program for a Turing machine that halts if the oracle returns 0 for its own input and loops forever if the oracle returns 1. An oracle would only allow the computation of the halting function for Turing machines without oracle.

3.8

Denoting AND $\coloneqq \wedge$, NAND $\coloneqq \overline{\wedge}$, NOT $\coloneqq \neg$, OR $\coloneqq \vee$ and XOR $\coloneqq \oplus$ we have:

$$\begin{aligned} 1 \,\overline{\wedge}\, (a \,\overline{\wedge}\, b) &= 1 \,\overline{\wedge}\, \neg\,(a \wedge b) \\ &= \neg\,(1 \wedge \neg\,(a \wedge b)) \\ &= a \wedge b, \end{aligned}$$

$$\begin{aligned} (a \,\overline{\wedge}\, (1 \,\overline{\wedge}\, b)) \,\overline{\wedge}\, (b \,\overline{\wedge}\, (1 \,\overline{\wedge}\, a)) &= (a \,\overline{\wedge}\, \neg\,(1 \wedge b)) \,\overline{\wedge}\, (b \,\overline{\wedge}\, \neg\,(1 \wedge a)) \\ &= \neg\,(a \wedge \neg\,(1 \wedge b)) \,\overline{\wedge}\, \neg\,(b \wedge \neg\,(1 \wedge a)) \\ &= \neg\,(\neg\,(a \wedge \neg\,(1 \wedge b)) \wedge \neg\,(b \wedge \neg\,(1 \wedge a))) \end{aligned}$$

$$
\begin{aligned}
&= \neg\left(\neg\left(a \wedge \neg b\right) \wedge \neg\left(b \wedge \neg a\right)\right) \\
&= \left(a \wedge \neg b\right) \vee \left(b \wedge \neg a\right) \\
&= a \oplus b,
\end{aligned}
$$

$$
\begin{aligned}
1 \mathbin{\overline{\wedge}} a &= \neg\left(1 \wedge a\right) \\
&= \neg a.
\end{aligned}
$$

3.9

If $f(n)$ is $O(g(n))$ then there are constants c and n_0 such that, for $n > n_0$, we have

$$
f(n) \leq cg(n) \quad \Longleftrightarrow \quad \frac{1}{c} f(n) \leq g(n),
$$

for constants $1/c$ and $n_0 \;\Rightarrow\; g(n)$ is $\Omega(f(n))$. The converse is immediate.

If $f(n)$ is $\Theta(g(n))$ then $f(n)$ is both $O(g(n))$ and $\Omega(g(n))$, and using the previous result we have

$$
\begin{aligned}
f(n) \text{ is } O(g(n)) \quad &\Longleftrightarrow \quad g(n) \text{ is } \Omega(f(n)), \\
f(n) \text{ is } \Omega(g(n)) \quad &\Longleftrightarrow \quad g(n) \text{ is } O(f(n)).
\end{aligned}
$$

Thus $f(n)$ is $\Theta(g(n))$ if and only if $g(n)$ is $\Theta(f(n))$.

3.10

$$
g(n) = \sum_{i=0}^{k} a_i n^i \quad \Longrightarrow \quad g(n) \text{ is } O\left(n^k\right),
$$

so for $l \geq k$ we have that $g(n)$ is $O\left(n^l\right)$.

3.11

$$
\begin{aligned}
\frac{\mathrm{d}}{\mathrm{d}n} \log(n) &= n^{-1}, \\
\frac{\mathrm{d}}{\mathrm{d}n} n^k &= k n^{k-1},
\end{aligned}
$$

and for $k > 0$, if we take $c = 1/k$, then for all $n > 1$ we have

$$
n^{-1} \leq ckn^{k-1} \quad \Longrightarrow \quad \log(n) \leq cn^k,
$$

which means that $\log(n)$ is $O\left(n^k\right)$ for $k > 0$.

3.12

First let us analyse the case $k < 0$. In this case, $n^k = n^{\log n}$ for $n = 1$, and for $n > 1$ we have

$$\begin{aligned}\frac{\mathrm{d}}{\mathrm{d}n} n^k &= kn^{k-1} < 0,\\ \frac{\mathrm{d}}{\mathrm{d}n} n^{\log n} &= 2\log(n) n^{\log n - 1} > 0,\end{aligned}$$

so clearly n^k is $O\big(n^{\log n}\big)$ and $n^{\log n}$ cannot be $O\big(n^k\big)$ for $k < 0$. Now, for $k \geq 0$, $n^k = n^{\log n}$ for $n = e^k$, and for $n > e^k$, that is $n = ce^k$ for some constant $c > 1$, we have

$$\begin{aligned}\left(\frac{\mathrm{d}}{\mathrm{d}n} n^k\right)_{n=ce^k} &= kc^{k-1}e^{k(k-1)},\\ \left(\frac{\mathrm{d}}{\mathrm{d}n} n^{\log n}\right)_{n=ce^k} &= 2\left(\log c + k\right) c^{\log c + k - 1} e^{k(\log c + k - 1)}.\end{aligned}$$

The derivative of $n^{\log n}$ is clearly larger than the derivative of n^k since $\log c > 0$, so n^k is $O\big(n^{\log n}\big)$ and $n^{\log n}$ cannot be $O\big(n^k\big)$ for $k \geq 0$. Therefore n^k is $O\big(n^{\log n}\big)$ for any k but $n^{\log n}$ is never $O\big(n^k\big)$.

3.13

Let us start by taking the logarithm of both functions, that is $\log(c^n) = n \log c$ and $\log\big(n^{\log n}\big) = [\log n]^2$. The derivative of both functions yields

$$\begin{aligned}\frac{\mathrm{d}}{\mathrm{d}n}\left(n \log c\right) &= \log c,\\ \frac{\mathrm{d}}{\mathrm{d}n}\left(\log n\right)^2 &= \frac{2}{n}\log n.\end{aligned}$$

If $c > 1$ then clearly, for some large enough n_0, we have

$$\frac{2}{n}\log n \leq \log c$$

for $n > n_0$ since $\lim_{n\to\infty}[\log(n)/n] = 0$ and $\log c > 0$. Thus

$$[\log n]^2 \leq n \log c \quad\Longleftrightarrow\quad \log\big(n^{\log n}\big) \leq \log(c^n) \quad\Longleftrightarrow\quad n^{\log n} \leq c^n$$

for large enough n, thus $n^{\log n}$ is $O(c^n)$ and c^n cannot be $O\big(n^{\log n}\big)$. From that, it follows that c^n is $\Omega\big(n^{\log n}\big)$ and $n^{\log n}$ cannot be $\Omega(c^n)$.

3.14

If $e(n)$ is $O(f(n))$ and $g(n)$ is $O(h(n))$ there are constants c_1, c_2 and n_0 such that, for $n > n_0$

$$\begin{aligned}e(n) &\leq c_1 f(n),\\ g(n) &\leq c_2 h(n).\end{aligned}$$

Multiplying both inequalities yields

$$e(n)g(n) \leq c_1 c_2 \left[f(n)h(n)\right],$$

which means $e(n)g(n)$ is $O(f(n)h(n))$.

3.15

Every time a compare-and-swap operation is applied, 2 among the $n!$ possible initial orderings will be correct, therefore after k applications we have, at most, 2^k possible initial orderings correctly ordered. So the total number N of required applications for all $n!$ initial orderings is such that

$$2^N = n! \quad \Longrightarrow \quad N = \log(n!).$$

Using Stirling's approximation, for sufficiently large n and some constant c we have

$$N = cn\log n + O(\log n) \quad \Longrightarrow \quad cn\log n \leq N \quad \Longrightarrow \quad N \text{ is } \Omega(n\log n).$$

3.16

**From errata:* $2^n/\log n$ should be $2^n/n$.

Let $f_n(k)$ be a function that computes the number of functions on n inputs that uses, at most, k gates. There are $4 = 2^{2^1}$ possible Boolean functions on one single input, they are: $B_1(x) = 0, B_2(x) = x, B_3(x) = \neg x$ and $B_4(x) = 1$. By induction it is straightforward to conclude that there are 2^{2^n} Boolean functions on n inputs. Thus if all Boolean functions on n inputs can be computed using at most k gates then we must have $f_n(k) \geq 2^{2^n}$. So, if we show that

$$f_n\left(\frac{2^n}{n}\right) < 2^{2^n}$$

it would mean that there exist Boolean functions on n inputs that require more than $2^n/n$ logic gates to compute. We can estimate an upper bound for $f_n(k)$ with a counting argument. For that we suppose all circuits to be composed of binary gates, that is, gates on two bit inputs and one bit output (it is a reasonable supposition since it is possible to build a universal set of logic gates using only binary gates). There are $2^{2^2} = 16$ possible binary gates, and each one's two inputs can be the output of one of the other $k-1$ gates or one of the n inputs, and the output can be used as input by any of the other $k-1$ gates or be part of the final answer, so for the i-th gate we have roughly

$$\begin{aligned} 16k\binom{n+k-1}{2} &= 16k\frac{(n+k-1)!}{2!\,(n+k-3)!} \\ &= 8k\,(n+k-1)\,(n+k-2) \end{aligned}$$

possibilities. Since the label i can be anything from 1 to k we must elevate it to the k-th power, yielding a number of about

$$\left[8k\,(n+k-1)\,(n+k-2)\right]^k$$

possible circuits. But this is clearly an over-count since the labels i are arbitrary, so in order to compensate we divide it by $k!$ giving us a rough estimate

$$\begin{aligned} f_n(k) &\approx \frac{\left[8k\left(n+k-1\right)\left(n+k-2\right)\right]^k}{k!} \\ &\leq \frac{\left[8k\left(n+k\right)^2\right]^k}{k!}. \end{aligned}$$

Using Stirling's approximation we have that $k! \geq (k/e)^k$, thus

$$f_n(k) \leq (8e)^k \left(n+k\right)^{2k}.$$

We shall eventually consider $k = 2^n/n$ so it is safe to assume $n < k$ meaning

$$f_n(k) < (32e)^k \, k^{2k}.$$

Now properly setting $k = 2^n/n$ yields

$$\begin{aligned} f_n\left(\frac{2^n}{n}\right) &< (32e)^{2^n/n} \left(\frac{2^n}{n}\right)^{2\times 2^n/n} \\ &= \left(\frac{32e}{n^2}\right)^{2^n/n} 2^{2^n} 2^{2^n} \\ &< \left(\frac{64e}{n^2}\right)^{2^n} 2^{2^n}. \end{aligned}$$

Notice that for large enough n (in this estimation it would be for $n > 8\sqrt{e} \approx 13$) it is guaranteed that $f_n(2^n/n) < 2^{2^n}$, thus there exist Boolean functions on n inputs that require no less than $2^n/n$ logic gates to compute.

3.17

If the factoring decision problem is in **P** then given a number N we can answer, in polynomial time, if N has a non-trivial factor $p_1 \leq \sqrt{N}$. If the answer is "no" then we solved the problem of finding the prime factors of N in polynomial time (since in this case N is itself a prime). If the answer is "yes" we can then answer, in polynomial time, if N/p_1 has a non-trivial factor $p_2 \leq \sqrt{N/p_1}$, and repeat this process until we obtain "no" as answer. In this case, we will have obtained all prime factors $\{p_1, p_2, \cdots\}$ of N in polynomial time. Therefore, if the factoring decision problem is in **P** then the problem of finding the prime factors of a number is also in **P**.

Conversely, if we can obtain the prime factors $\{p_1, p_2, \cdots\}$ of N in polynomial time, then we could answer if N has a non-trivial factor less than some number in polynomial time, since we could just obtain the answers $\{p_1, p_2, \cdots\}$ in polynomial time. That means if the problem of finding the prime factors of a number is in **P** then the factoring decision problem is also in **P**.

3.18

Clearly $\mathbf{P} \subseteq \mathbf{NP}$. And also, if some $L \in \mathbf{P}$ then its complement $\overline{L}$ must also be in $\mathbf{P}$ since, if it is possible to obtain "yes" for L in a decision problem in polynomial time with a Turing machine M, it is possible to use another Turing machine M' that simulates M and outputs "yes" if M outputs "no" for L, meaning M' would output "yes" for $\overline{L}$ in polynomial time, so it is also true that $\mathbf{P} \subseteq \mathbf{coNP}$. With that, let us suppose that $\mathbf{P} = \mathbf{NP}$, then

- $\forall\, L \in \mathbf{NP}$:

  $L \in \mathbf{P}$, but since $\mathbf{P} \subseteq \mathbf{coNP} \;\Rightarrow\; L \in \mathbf{coNP}$.

- $\forall\, L \in \mathbf{coNP}$:

  $\overline{L} \in \mathbf{NP} \;\Rightarrow\; \overline{L} \in \mathbf{P} \;\Rightarrow\; L \in \mathbf{P} \;\Rightarrow\; L \in \mathbf{NP}$.

We proved that $\mathbf{P} = \mathbf{NP} \;\Rightarrow\; \mathbf{coNP} = \mathbf{NP}$, so the contrapositive must be true, that is, $\mathbf{coNP} \neq \mathbf{NP} \;\Rightarrow\; \mathbf{P} \neq \mathbf{NP}$.

3.19

In order to check if two vertices i and j are connected one must simply start at i and "walk" through the edges until j is reached. In the worst case scenario, one must pass through all the other vertices before reaching j meaning that cn steps are required at most, where c is a constant, thus REACHABILITY is a problem that can be solved in $O(n)$ steps.

In order to check if a graph is connected one must simply run the REACHABILITY problem for j varying from 1 to n with $j \neq i$. In the worst case scenario $cn\,(n-1)$ steps are required meaning this problem can be solved in $O(n^2)$ steps.

3.20

If a vertex is connected to two edges it can be entered and left once, so if it connected to an even number of n edges it can be visited $n/2$ times without the necessity of crossing any edges more than once. And if we start at a vertex connected to an even number of edges then we must also end the walk on it since every time this vertex is visited two of its connecting edges are used meaning there would be one last edge for us to end the walk on it. So if all vertices are connected to an even number of edges it is always possible to start at one point, visit every vertex crossing each edge only once, and then finish where we started, completing a cycle.

This automatically provides an algorithm for finding an Euler cycle: if all vertices are connected to an even number of edges one must simply start at any vertex and visit all the others, always using a different edge, up to the point where we have walked through all the edges once.

3.21

If L_1 is reducible to L_2 then there exists a Turing machine M that receives $x \in L_1$ and outputs $R(x) \in L_2$ in polynomial time, and if L_2 is reducible to L_3 then there is another Turing machine M' that receives $y \in L_2$ and outputs $S(y) \in L_3$ in polynomial time. So we can create a Turing machine

M'' as the composite of M and M', that is, M'' receives $x \in L_1$, simulates M, use $R(x)$ as input for M', simulates M' and then outputs $S(R(x)) \in L_3$ in polynomial time, meaning L_1 is reducible to L_3.

3.22

All other languages of the same complexity class can be reduced to L. If L is reducible to L' then all other languages of the same complexity class can be reduced to L', meaning L' is complete.

3.23

-

3.24

-

3.25

A Turing machine, with l possible internal states and an alphabet of m possible symbols, that belongs in **PSPACE** uses $p(n)$ symbols of information, where n is the number of input symbols and $p(n) = \sum_i^k a_i n^i$. So, there is a total of $lm^{p(n)}$ possible states in which this Turing machine can be. We must assume that the machine halts for at least one of these states and that it doesn't enter in any infinite loop. So in the worst case scenario this machine must go through some multiple of all possible states before halting, meaning a number of steps given by

$$\begin{aligned} clm^{p(n)} &= cl \times 2^{p(n)\log m} \\ &= cl \times 2^{\log m \sum_i^k a_i n^i}, \end{aligned}$$

where c is a constant. Clearly $b \coloneqq cl$ is a constant and all $\alpha_i \coloneqq a_i \log m$ are also constants, so the running time of this machine is

$$b \times 2^{\sum_i^k \alpha_i n^i} = O\Big(2^{n^k}\Big) \quad \Longrightarrow \quad \mathbf{PSPACE} \subseteq \mathbf{EXP}.$$

3.26

Since $\log n \leq cn^k$ for constant $c \geq 1/k$ and $k > 0$ it means that

$$O(\log n) \leq O\big(n^k\big) \quad \Longrightarrow \quad \mathbf{L} \subseteq \mathbf{P}.$$

3.27

In the worst case scenario, a minimal vertex cover may be composed of just one of the two vertices at each step, in other words, it may be that in each step, among all edges touching either α or β, every single one touches α, meaning β would not need to be accounted. If this happens for every step then in the end VC is, at most, double the size of a minimal vertex cover.

3.28

It is obvious that $k \geq 3/4 \Rightarrow L \in \mathbf{BPP}$. For $1/2 < k < 3/4$ the probability of M correctly classifying x (accepting or rejecting it) is not high enough. But we can define a Turing machine M' that simulates M, running it n times for the same input x, and either accepts or rejects x based on the number of "yes" and "no" answers obtained by running M n times. Then the probability that M' will correctly classify x is the probability of having $n_c > n/2$, where n_c is the number of times M correctly classified x. This probability is given by

$$p = \sum_{n_c=\frac{n}{2}+1}^{n} \binom{n}{n_c} k^{n_c}(1-k)^{n-n_c},$$

so we would just need to find n such that $p \geq 3/4$, and that is always possible since $n \to \infty \Rightarrow n_c \to nk$, and because $k > 1/2$ we would have $n_c > n/2$ with probability $p \to 1$, thus $L \in \mathbf{BPP}$.

3.29

Denoting the Fredkin gate as F and considering the input state (a, b, c) we have

- If $c = 0$:

$$F(F(a, b, c)) = F(a, b, c) = (a, b, c).$$

- If $c = 1$:

$$F(F(a, b, c)) = F(b, a, c) = (a, b, c).$$

3.30

For $c = 0$: if both a and b are set to 1 they only collide in the center and close to the end, sending them to a' and b' respectively. If just one of them is set to 1 then they just follow their natural path to a' or b' respectively. And if both are set to 0 nothing happens obviously. So for $c = 0$ we have $F(a, b, 0)$ being correctly executed.

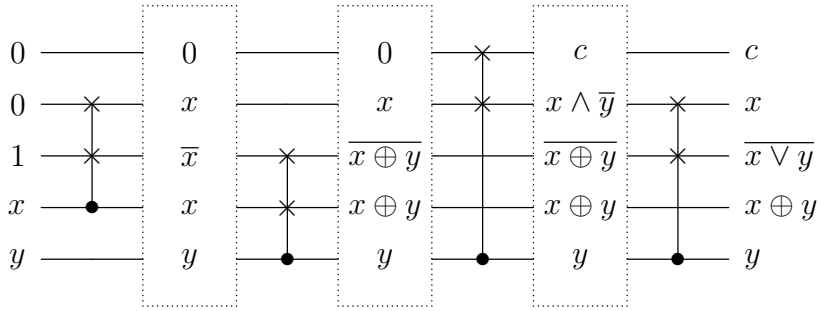
For $c = 1$: if both a and b are set to 1 there are 4 collisions between b and c and 5 collisions between a and b sending a, b and c to a', b' and c' respectively. If just one of them is set to 1 then they collide with c 4 times, ending up in b' or a' respectively, and sending c to c'. And if both are set to 0 c just follows its natural path to c'. So for $c = 1$ we have $F(a, b, 1)$ being correctly executed.

3.31

First, notice that $c = x \wedge y$, and

$$\begin{aligned}
&F(0, 1, x) = (x, \neg x, x)\,, \\
&F(\neg x, x, y) = (\neg\,(x \oplus y)\,, x \oplus y, y)\,, \\
&F(0, x, y) = (x \wedge y, x \wedge \neg y, y)\,, \\
&F(x \wedge \neg y, \neg\,(x \oplus y)\,, y) = (x, \neg\,(x \vee y)\,, y)\,.
\end{aligned}$$

Using these relations we can construct the following circuit, using three ancilla bits:



The boxes between each pair of Fredkin gates are just to indicate the state of each bit after each step. The bits at the end of the circuit can be outputted in the form $(x, y, c, x \oplus y)$ and the garbage bit, that is the one with value $\neg(x \vee y)$, can be discarded. Since we have only used Fredkin gates (and one NOT gate to set the third ancilla bit to 1 at the beginning) this circuit is reversible.

3.32

Simulating Toffoli with Fredkin:

Denoting the Toffoli gate as T, its action with control bits x and y and target bit t is given by $T(x, y, t) = (x, y, t \oplus (x \wedge y))$. We can output $t \oplus (x \wedge y)$ by using

$$F(\neg t, t, x \wedge y) = (\neg(t \oplus (x \wedge y)), t \oplus (x \wedge y), x \wedge y),$$

but first we need to create $\neg t, t$ and $x \wedge y$, and also need to generate the outputs x and y. To create $\neg t$ and t we can use two ancilla bits and apply

$$F(0, 1, t) = (t, \neg t, t).$$

To create $x \wedge y$ and y we can use one ancilla bit and apply

$$F(0, x, y) = (x \wedge y, x \wedge \neg y, y),$$

but if we apply just it we won't be able to get output x since there will be no bits with value x, so first we need to use two more ancilla bits to create a copy of it with

$$F(0, 1, x) = (x, \neg x, x).$$

So with five ancilla bits and four Fredkin gates it is possible to simulate a Toffoli gate.

Simulating Fredkin with Toffoli:

The action of the Fredkin gate with target bits a and b and control bit c is given by $F(a, b, c) = (a \oplus ((a \oplus b) \wedge c), b \oplus ((a \oplus b) \wedge c), c)$. We can output $a \oplus ((a \oplus b) \wedge c)$, $b \oplus ((a \oplus b) \wedge c)$ and c by applying

$$T(a \oplus b, c, a) = (a \oplus b, c, a \oplus ((a \oplus b) \wedge c)),$$
$$T(a \oplus b, c, b) = (a \oplus b, c, b \oplus ((a \oplus b) \wedge c)),$$

but first we need to create $a \oplus b$. For that we can use one ancilla bit and apply

$$T(b, 1, a) = (b, 1, a \oplus b),$$

but if we apply just it we won't be able to apply $T(a \oplus b, c, a)$ since there will be no bits with value a, so first we need to use one more ancilla bit to create a copy of it with

$$T(a, 1, 0) = (a, 1, a).$$

So with two ancilla bits and four Toffoli gates it is possible to simulate a Fredkin gate.

4 Quantum circuits

Exercises: 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10, 4.11, 4.12, 4.13, 4.14, 4.15, 4.16, 4.17, 4.18, 4.19, 4.20, 4.21, 4.22, 4.23, 4.24, 4.25, 4.26, 4.27, 4.28, 4.29, 4.30, 4.31, 4.32, 4.33, 4.34, 4.35, 4.36, 4.37, 4.38, 4.39, 4.40, 4.41, 4.42, 4.43, 4.44, 4.45, 4.46, 4.47, 4.48, 4.49, 4.50, 4.51.

4.1

$$\begin{aligned}
X \text{ : eigenvectors } &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \text{ and } \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\
&= \cos\frac{\pi}{4}|0\rangle + e^{i0}\sin\frac{\pi}{4}|1\rangle \text{ and } \cos\frac{\pi}{4}|0\rangle + e^{i\pi}\sin\frac{\pi}{4}|1\rangle \\
&\Longrightarrow (\theta = \pi/2, \varphi = 0) \text{ and } (\theta = \pi/2, \varphi = \pi) \\
&\Longrightarrow \text{Equator with longitudes } 0^\circ \text{ and } 180^\circ \text{ respectively.}
\end{aligned}$$

$$\begin{aligned}
Y \text{ : eigenvectors } &= \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) \text{ and } \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle) \\
&= \cos\frac{\pi}{4}|0\rangle + e^{i\pi/2}\sin\frac{\pi}{4}|1\rangle \text{ and } \cos\frac{\pi}{4}|0\rangle + e^{-i\pi/2}\sin\frac{\pi}{4}|1\rangle \\
&\Longrightarrow (\theta = \pi/2, \varphi = \pi/2) \text{ and } (\theta = \pi/2, \varphi = -\pi/2) \\
&\Longrightarrow \text{Equator with longitudes } 90^\circ \text{ and } -90^\circ \text{ respectively.}
\end{aligned}$$

$$\begin{aligned}
Z \text{ : eigenvectors } &= |0\rangle \text{ and } |1\rangle \\
&= \cos 0\,|0\rangle + e^{i\varphi}\sin 0\,|1\rangle \text{ and } \cos\frac{\pi}{2}|0\rangle + e^{i\varphi}\sin\frac{\pi}{2}|1\rangle \\
&\Longrightarrow (\theta = 0, \varphi) \text{ and } (\theta = \pi, \varphi) \\
&\Longrightarrow \text{North and south poles respectively.}
\end{aligned}$$

4.2

$$\exp(iAx) = \sum_{j=0}^{\infty} \frac{(iAx)^j}{j!}$$

$$= \sum_{j=0}^{\infty} \frac{(-1)^j (Ax)^{2j}}{(2j)!} + i \sum_{j=0}^{\infty} \frac{(-1)^j (Ax)^{2j+1}}{(2j+1)!}.$$

Since $A^2 = I$ we have $A^{2j} = I$ and $A^{2j+1} = A$, thus

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

From this result, since the Pauli matrices obey $\sigma_j^2 = I$, it follows that

$$\begin{aligned}e^{-i\theta X/2} &= \cos\frac{\theta}{2} I - i \sin\frac{\theta}{2} X, \\ e^{-i\theta Y/2} &= \cos\frac{\theta}{2} I - i \sin\frac{\theta}{2} Y, \\ e^{-i\theta Z/2} &= \cos\frac{\theta}{2} I - i \sin\frac{\theta}{2} Z.\end{aligned}$$

4.3

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

4.4

$$\begin{aligned}H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} &= \begin{bmatrix} \cos\frac{\pi}{4} & \sin\frac{\pi}{4} \\ \sin\frac{\pi}{4} & -\cos\frac{\pi}{4} \end{bmatrix} \\ &= \begin{bmatrix} e^{-i\pi/4} & 0 \\ 0 & e^{i\pi/4} \end{bmatrix} \begin{bmatrix} e^{i\pi/4}\cos\frac{\pi}{4} & e^{i\pi/4}\sin\frac{\pi}{4} \\ e^{-i\pi/4}\sin\frac{\pi}{4} & e^{i3\pi/4}\cos\frac{\pi}{4} \end{bmatrix} \\ &= \begin{bmatrix} e^{-i\pi/4} & 0 \\ 0 & e^{i\pi/4} \end{bmatrix} \begin{bmatrix} e^{i\pi/2}\cos\frac{\pi}{4} & \sin\frac{\pi}{4} \\ \sin\frac{\pi}{4} & e^{i\pi/2}\cos\frac{\pi}{4} \end{bmatrix} \begin{bmatrix} e^{-i\pi/4} & 0 \\ 0 & e^{i\pi/4} \end{bmatrix} \\ &= e^{i\pi/2} \begin{bmatrix} e^{-i\pi/4} & 0 \\ 0 & e^{i\pi/4} \end{bmatrix} \begin{bmatrix} \cos\frac{\pi}{4} & -i\sin\frac{\pi}{4} \\ -i\sin\frac{\pi}{4} & \cos\frac{\pi}{4} \end{bmatrix} \begin{bmatrix} e^{-i\pi/4} & 0 \\ 0 & e^{i\pi/4} \end{bmatrix} \\ &= e^{i\pi/2} R_z(\pi/2) R_x(\pi/2) R_z(\pi/2).\end{aligned}$$

4.5

$$\begin{aligned}(\hat{n}\cdot\vec{\sigma})^2 &= (n_x X + n_y Y + n_z Z)^2 \\ &= n_x^2 X^2 + n_y^2 Y^2 + n_z^2 Z^2 + n_x n_y \{X, Y\} + n_x n_z \{X, Z\} + n_y n_z \{Y, Z\}.\end{aligned}$$

Since all Pauli matrices obey $\sigma_j^2 = I$ and $\{\sigma_j, \sigma_k\} = 0$ we have

$$(\hat{n} \cdot \vec{\sigma})^2 = \left(n_x^2 + n_y^2 + n_z^2\right) I = I.$$

From this result it follows that

$$\exp(-i\theta \hat{n} \cdot \vec{\sigma}/2) = \cos\frac{\theta}{2} I - i \sin\frac{\theta}{2} (\hat{n} \cdot \vec{\sigma}).$$

4.6

First, let us show that the effects of $R_x(\theta)$, $R_y(\theta)$ and $R_z(\theta)$ upon the Bloch vector correspond to rotations of an angle θ around the x, y and z axis respectively. A qubit in the pure state $|\psi\rangle$ whose Bloch vector is $\vec{\lambda}$ has density operator given by

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

Applying $R_z(\theta)$ on $|\psi\rangle$ yields

$$R_z(\theta) \rho R_z^\dagger(\theta) = \frac{I + \lambda_x R_z(\theta) X R_z^\dagger(\theta) + \lambda_x R_z(\theta) Y R_z^\dagger(\theta) + \lambda_z Z}{2}.$$

We can expand the terms

$$\begin{aligned}
R_z(\theta) X R_z^\dagger(\theta) &= \left(\cos\frac{\theta}{2} I - i \sin\frac{\theta}{2} Z\right) X \left(\cos\frac{\theta}{2} I + i \sin\frac{\theta}{2} Z\right) \\
&= \cos\frac{\theta}{2}\cos\frac{\theta}{2} X + i \cos\frac{\theta}{2}\sin\frac{\theta}{2}[X, Z] + \sin\frac{\theta}{2}\sin\frac{\theta}{2} ZXZ \\
&= \left(\cos\frac{\theta}{2}\cos\frac{\theta}{2} - \sin\frac{\theta}{2}\sin\frac{\theta}{2}\right) X + 2\cos\frac{\theta}{2}\sin\frac{\theta}{2} Y \\
&= \cos\theta X + \sin\theta Y, \\
R_z(\theta) Y R_z^\dagger(\theta) &= \left(\cos\frac{\theta}{2} I - i \sin\frac{\theta}{2} Z\right) Y \left(\cos\frac{\theta}{2} I + i \sin\frac{\theta}{2} Z\right) \\
&= \cos\frac{\theta}{2}\cos\frac{\theta}{2} Y + i \cos\frac{\theta}{2}\sin\frac{\theta}{2}[Y, Z] + \sin\frac{\theta}{2}\sin\frac{\theta}{2} ZYZ \\
&= \left(\cos\frac{\theta}{2}\cos\frac{\theta}{2} - \sin\frac{\theta}{2}\sin\frac{\theta}{2}\right) Y - 2\cos\frac{\theta}{2}\sin\frac{\theta}{2} X \\
&= \cos\theta Y - \sin\theta X,
\end{aligned}$$

yielding

$$\begin{aligned}
R_z(\theta) \rho R_z^\dagger(\theta) &= \frac{I + \lambda_x (\cos\theta X + \sin\theta Y) + \lambda_y (\cos\theta Y - \sin\theta X) + \lambda_z Z}{2} \\
&= \frac{I + \vec{\lambda}' \cdot \vec{\sigma}}{2},
\end{aligned}$$

where the new Bloch vector $\vec{\lambda}'$ is given by

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

which is precisely a rotation in 3-dimensional space of an angle θ around the z axis. The process is the same for the $R_x(\theta)$ and $R_y(\theta)$ operators. Now notice that for an arbitrary axis directed by the unit vector $\hat{n} = (\cos\alpha \sin\beta, \sin\alpha \sin\beta, \cos\beta)$ we may write

$$\begin{aligned}R_{\hat{n}}(\theta) &= \cos\frac{\theta}{2} I - i \sin\frac{\theta}{2} (\hat{n} \cdot \vec{\sigma}) \\ &= \cos\frac{\theta}{2} I - i \sin\frac{\theta}{2} (\cos\alpha \sin\beta X + \sin\alpha \sin\beta Y + \cos\beta Z) \\ &= \cos\frac{\theta}{2} I - i \sin\frac{\theta}{2} \cos\beta Z - i \sin\frac{\theta}{2} \sin\beta (\cos\alpha X + \sin\alpha Y) \\ &= R_z(\alpha) \left(\cos\frac{\theta}{2} I - i \sin\frac{\theta}{2} (\cos\beta Z + \sin\beta X) \right) R_z^\dagger(\alpha) \\ &= R_z(\alpha) R_y(\beta) \left(\cos\frac{\theta}{2} I - i \sin\frac{\theta}{2} Z \right) R_y^\dagger(\beta) R_z^\alpha(\alpha) \\ &= R_z(\alpha) R_y(\beta) R_z(\theta) R_y^\dagger(\beta) R_z^\dagger(\alpha),\end{aligned}$$

meaning we can express $R_{\hat{n}}(\theta)$ as a combination of operators R_y and R_z, which were shown to be rotation operators over the Bloch vector, thus $R_{\hat{n}}$ is also a rotation, in particular, around the $\hat{n}$ axis. The physical interpretation is that the operations $R_y^\dagger(\beta) R_z^\dagger(\alpha)$ and $R_z(\alpha) R_y(\beta)$ are just a change in the frame of reference. The Bloch vector is first written in the reference frame where it has the same relative position to the z axis as it had originally with the $\hat{n}$ axis, then the rotation is performed around the z axis and the system is returned to the original frame of reference.

4.7

$$XYX = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix} = -Y.$$

From this result it follows that

$$\begin{aligned}X R_y(\theta) X &= X \left(\cos\frac{\theta}{2} I - i \sin\frac{\theta}{2} Y \right) X \\ &= \cos\frac{\theta}{2} I + i \sin\frac{\theta}{2} Y \\ &= R_y(-\theta).\end{aligned}$$

4.8

We can write any unitary operator as the exponential of some Hermitian operator K as

$$U = \exp(iK),$$

and any Hermitian operator can be expanded as

$$K = \begin{bmatrix} a+d & b-ic \\ b+ic & a-d \end{bmatrix} = aI + bX + cY + dZ.$$

Choosing $a = \alpha$, $b = -n_x\theta/2$, $c = -n_y\theta/2$, and $d = -n_z\theta/2$ such that $n_x^2 + n_y^2 + n_z^2 = 1$ yields

$$\begin{aligned} U &= \exp\left(i\alpha I - i\frac{\theta}{2}\left(n_x X + n_y Y + n_z Z\right)\right) \\ &= \exp(i\alpha I)\exp(-i\theta\hat{n}\cdot\vec{\sigma}/2) \\ &= \exp(i\alpha)R_{\hat{n}}(\theta). \end{aligned}$$

$$\begin{aligned} H = \frac{X+Z}{\sqrt{2}} &= i\left(-i\left[\frac{1}{\sqrt{2}}X + \frac{1}{\sqrt{2}}Z\right]\right) \\ &= \exp(i\pi/2)\left(\cos\frac{\pi}{2}I - i\sin\frac{\pi}{2}\left[\frac{1}{\sqrt{2}}X + 0Y + \frac{1}{\sqrt{2}}Z\right]\right) \\ &= \exp(i\pi/2)R_{\frac{1}{\sqrt{2}}(1,0,1)}(\pi) \\ \implies \alpha = \frac{\pi}{2}, \theta = \pi, \hat{n} &= \frac{1}{\sqrt{2}}(1,0,1). \end{aligned}$$

$$\begin{aligned} S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} &= \exp(i\pi/4)\begin{bmatrix} \exp(-i\pi/4) & 0 \\ 0 & \exp(i\pi/4) \end{bmatrix} \\ &= \exp(i\pi/4)R_z(\pi/2) \\ \implies \alpha = \frac{\pi}{4}, \theta = \frac{\pi}{2}, \hat{n} &= (0,0,1). \end{aligned}$$

4.9

Since any 3-dimensional rotation around an arbitrary axis can be written in terms of the three Euler angles we can write $R_{\hat{n}}(\theta) = R_z(\beta)R_y(\gamma)R_z(\delta)$. And because any unitary operator can be written as $U = \exp(i\alpha)R_{\hat{n}}(\theta)$ we have

$$\begin{aligned} U &= \exp(i\alpha)R_z(\beta)R_y(\gamma)R_z(\delta) \\ &= \exp(i\alpha)\begin{bmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{bmatrix}\begin{bmatrix} \cos\frac{\gamma}{2} & -\sin\frac{\gamma}{2} \\ \sin\frac{\gamma}{2} & \cos\frac{\gamma}{2} \end{bmatrix}\begin{bmatrix} e^{-i\delta/2} & 0 \\ 0 & e^{i\delta/2} \end{bmatrix} \end{aligned}$$

$$= \begin{bmatrix} e^{i(\alpha-\beta/2-\delta/2)}\cos\frac{\gamma}{2} & -e^{i(\alpha-\beta/2+\delta/2)}\sin\frac{\gamma}{2} \\ e^{i(\alpha+\beta/2-\delta/2)}\sin\frac{\gamma}{2} & e^{i(\alpha+\beta/2+\delta/2)}\cos\frac{\gamma}{2} \end{bmatrix}.$$

4.10

It is always possible to find three angles β', γ' and δ' analogous to the usual Euler angles such that $R_z(\beta)R_y(\gamma)R_z(\delta) = R_x(\beta')R_y(\gamma')R_x(\delta')$, thus for some α' we may write

$$\begin{aligned} U &= \exp(i\alpha')R_x(\beta')R_y(\gamma')R_x(\delta') \\ &= \exp(i\alpha') \begin{bmatrix} \cos\frac{\beta'}{2} & -i\sin\frac{\beta'}{2} \\ i\sin\frac{\beta'}{2} & \cos\frac{\beta'}{2} \end{bmatrix} \begin{bmatrix} \cos\frac{\gamma'}{2} & -\sin\frac{\gamma'}{2} \\ \sin\frac{\gamma'}{2} & \cos\frac{\gamma'}{2} \end{bmatrix} \begin{bmatrix} \cos\frac{\delta'}{2} & -i\sin\frac{\delta'}{2} \\ i\sin\frac{\delta'}{2} & \cos\frac{\delta'}{2} \end{bmatrix} \\ &= \begin{bmatrix} A & -B \\ B & A \end{bmatrix}, \end{aligned}$$

where

$$\begin{aligned} A &= e^{i\alpha'}\left[\frac{1}{2}\cos\left(\frac{\beta'-\delta'-\gamma'}{2}\right) + \frac{1}{2}\cos\left(\frac{\beta'-\delta'+\gamma'}{2}\right) - i\sin\left(\frac{\beta'+\delta'}{2}\right)\sin\left(\frac{\gamma'}{2}\right)\right], \\ B &= e^{i\alpha'}\left[\cos\left(\frac{\beta'-\delta'}{2}\right)\sin\left(\frac{\gamma'}{2}\right) + i\cos\left(\frac{\gamma'}{2}\right)\sin\left(\frac{\beta'+\delta'}{2}\right)\right]. \end{aligned}$$

4.11

Writing the operators in terms of Euler angles yields

$$\begin{aligned} R_{\hat{n}}(\beta) &= R_z(\theta_1)R_y(\phi_1)R_z(\psi_1), \\ R_{\hat{m}}(\gamma) &= R_z(\theta_2)R_y(\phi_2)R_z(\psi_2), \\ R_{\hat{n}}(\delta) &= R_z(\theta_3)R_y(\phi_3)R_z(\psi_3), \end{aligned}$$

and considering $\alpha = \alpha_1 + \alpha_2 + \alpha_3$ we have that

$$\begin{aligned} e^{i\alpha}R_{\hat{n}}(\beta)R_{\hat{m}}(\gamma)R_{\hat{n}}(\delta) = &\left[e^{i\alpha_1}R_z(\theta_1)R_y(\phi_1)R_z(\psi_1)\right] \\ &\times \left[e^{i\alpha_2}R_z(\theta_2)R_y(\phi_2)R_z(\psi_2)\right] \\ &\times \left[e^{i\alpha_3}R_z(\theta_3)R_y(\phi_3)R_z(\psi_3)\right]. \end{aligned}$$

According to Theorem 4.1 the three terms between square brackets are unitary operators, and the multiplication of three unitary operators is itself an unitary operator, meaning that for appropriate choice of α, β, γ and δ we may write any unitary as

$$U = e^{i\alpha}R_{\hat{n}}(\beta)R_{\hat{m}}(\gamma)R_{\hat{n}}(\delta).$$

4.12

First let us determine the values of α, β, γ and δ in the Z-Y decomposition through

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} = \begin{bmatrix}e^{i(\alpha-\beta/2-\delta/2)}\cos\frac{\gamma}{2} & -e^{i(\alpha-\beta/2+\delta/2)}\sin\frac{\gamma}{2}\\ e^{i(\alpha+\beta/2-\delta/2)}\sin\frac{\gamma}{2} & e^{i(\alpha+\beta/2+\delta/2)}\cos\frac{\gamma}{2}\end{bmatrix}$$
$$\implies \alpha = \frac{\pi}{2}, \beta = 0, \gamma = \frac{\pi}{2}, \delta = \pi.$$

Therefore the operators are given by

$$A = R_z(0)R_y(\pi/4) = \begin{bmatrix}\cos\frac{\pi}{8} & -\sin\frac{\pi}{8}\\ \sin\frac{\pi}{8} & \cos\frac{\pi}{8}\end{bmatrix},$$
$$B = R_y(-\pi/4)R_z(-\pi/2) = \begin{bmatrix}e^{i\pi/4}\cos\frac{\pi}{8} & e^{-i\pi/4}\sin\frac{\pi}{8}\\ -e^{i\pi/4}\sin\frac{\pi}{8} & e^{-i\pi/4}\cos\frac{\pi}{8}\end{bmatrix},$$
$$C = R_z(\pi/2) = \begin{bmatrix}e^{-i\pi/4} & 0\\ 0 & e^{i\pi/4}\end{bmatrix}.$$

4.13

$$\begin{aligned}HXH &= \frac{(X+Z)}{\sqrt{2}}X\frac{(X+Z)}{\sqrt{2}}\\ &= \frac{1}{2}(XXX + XXZ + ZXX + ZXZ)\\ &= \frac{1}{2}(X + Z + Z - X)\\ &= Z.\end{aligned}$$

$$\begin{aligned}HYH &= \frac{(X+Z)}{\sqrt{2}}Y\frac{(X+Z)}{\sqrt{2}}\\ &= \frac{1}{2}(XYX + XYZ + ZYX + ZYZ)\\ &= \frac{1}{2}(-Y + iI - iI - Y)\\ &= -Y.\end{aligned}$$

$$\begin{aligned}HZH &= \frac{(X+Z)}{\sqrt{2}}Z\frac{(X+Z)}{\sqrt{2}}\\ &= \frac{1}{2}(XZX + XZZ + ZZX + ZZZ)\\ &= \frac{1}{2}(-Z + X + X + Z)\\ &= X.\end{aligned}$$

4.14

$$\begin{aligned} T &= \exp(i\pi/8) R_z(\pi/4) \\ &= \exp(i\pi/8) \left(\cos\frac{\pi}{8} I - i \sin\frac{\pi}{8} Z \right), \end{aligned}$$

thus

$$\begin{aligned} HTH &= \exp(i\pi/8) \left(\cos\frac{\pi}{8} I - i \sin\frac{\pi}{8} HZH \right) \\ &= \exp(i\pi/8) \left(\cos\frac{\pi}{8} I - i \sin\frac{\pi}{8} X \right) \\ &= \exp(i\pi/8) R_x(\pi/4). \end{aligned}$$

4.15

$$\begin{aligned} R_{\hat{n}_2}(\beta_2) R_{\hat{n}_1}(\beta_1) &= \exp\left(-i\frac{\beta_2}{2} \hat{n}_2 \cdot \vec{\sigma} \right) \exp\left(-i\frac{\beta_1}{2} \hat{n}_1 \cdot \vec{\sigma} \right) \\ &= \left(c_2 I - i s_2 \hat{n}_2 \cdot \vec{\sigma} \right) \left(c_1 I - i s_1 \hat{n}_1 \cdot \vec{\sigma} \right) \\ &= c_1 c_2 I - i \left(c_2 s_1 \hat{n}_1 + c_1 s_2 \hat{n}_2 \right) \cdot \vec{\sigma} - s_1 s_2 \left(\hat{n}_1 \cdot \vec{\sigma} \right) \left(\hat{n}_2 \cdot \vec{\sigma} \right). \end{aligned}$$

The last term can be expanded to

$$\begin{aligned} \left(\hat{n}_1 \cdot \vec{\sigma} \right) \left(\hat{n}_2 \cdot \vec{\sigma} \right) &= \left(n_{1x} X + n_{1y} Y + n_{1z} Z \right) \left(n_{2x} X + n_{2y} Y + n_{2z} Z \right) \\ &= n_{1x} n_{2x} X^2 + n_{1y} n_{2y} Y^2 + n_{1y} n_{2y} Y^2 \\ &\quad + n_{1x} n_{2y} XY + n_{2x} n_{1y} YX + n_{1x} n_{2z} XZ + n_{2x} n_{1z} ZX + n_{1y} n_{2z} YZ + n_{2y} n_{1z} ZY \\ &= \left(n_{1x} n_{2x} + n_{1y} n_{2y} + n_{1z} n_{2z} \right) I \\ &\quad + \left(n_{1x} n_{2y} - n_{2x} n_{1y} \right) iZ - \left(n_{1x} n_{2z} - n_{2x} n_{1z} \right) iY + \left(n_{1y} n_{2z} - n_{2y} n_{1z} \right) iX \\ &= \left(\hat{n}_1 \cdot \hat{n}_2 \right) I + i \left(\hat{n}_1 \times \hat{n}_2 \right) \cdot \vec{\sigma}. \end{aligned}$$

Substituting it back into the equality yields

$$\begin{aligned} R_{\hat{n}_2}(\beta_2) R_{\hat{n}_1}(\beta_1) &= \left(c_1 c_2 - s_1 s_2 \, \hat{n}_1 \cdot \hat{n}_2 \right) I - i \left(c_2 s_1 \hat{n}_1 + c_1 s_2 \hat{n}_2 - s_1 s_2 \, \hat{n}_2 \times \hat{n}_1 \right) \cdot \vec{\sigma} \\ &= c_{12} I - i s_{12} \hat{n}_{12} \cdot \vec{\sigma} \\ &= R_{\hat{n}_{12}}(\beta_{12}). \end{aligned}$$

For $\beta_1 = \beta_2$ and $\hat{n}_1 = \hat{z}$ we have

$$c_{12} = c^2 - s^2 \, \hat{z} \cdot \hat{n}_2,$$

$$\begin{aligned} s_{12} \hat{n}_{12} &= cs\hat{z} + cs\hat{n}_2 - s^2 \, \hat{n}_2 \times \hat{z} \\ &= sc \left(\hat{z} + \hat{n}_2 \right) - s^2 \, \hat{n}_2 \times \hat{z}. \end{aligned}$$

4.16

The operators shown in the circuits can be written, respectively, as

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

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

4.17

Since $HZH = X$ we have that a CNOT gate is equivalent to a controlled-(HZH) gate, that is

$$C(HZH) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 0 & 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 0 & 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = CX$$

4.18

Taking two generic states $|\psi\rangle = a_0 |0\rangle + a_1 |1\rangle$ and $|\phi\rangle = b_0 |0\rangle + b_1 |1\rangle$ we have the joint state

$$|\psi\rangle \otimes |\phi\rangle = a_0 b_0 |0\rangle \otimes |0\rangle + a_0 b_1 |0\rangle \otimes |1\rangle + a_1 b_0 |1\rangle \otimes |0\rangle + a_1 b_1 |1\rangle \otimes |1\rangle .$$

Applying $CZ_{(1,2)}$ and $CZ_{(2,1)}$ over the joint state, where the first index is the control qubit and the second one the target, yields

$$\begin{aligned} CZ_{(1,2)} |\psi\rangle \otimes |\phi\rangle &= a_0 b_0 |0\rangle \otimes |0\rangle + a_0 b_1 |0\rangle \otimes |1\rangle + a_1 b_0 |1\rangle \otimes |0\rangle - a_1 b_1 |1\rangle \otimes |1\rangle , \\ CZ_{(2,1)} |\psi\rangle \otimes |\phi\rangle &= a_0 b_0 |0\rangle \otimes |0\rangle + a_0 b_1 |0\rangle \otimes |1\rangle + a_1 b_0 |1\rangle \otimes |0\rangle - a_1 b_1 |1\rangle \otimes |1\rangle . \end{aligned}$$

4.19

Considering a generic joint state $|\psi\rangle \otimes |\phi\rangle = (a_0 |0\rangle + a_1 |1\rangle) \otimes (b_0 |0\rangle + b_1 |1\rangle)$, the density operator and the action of CNOT upon it are given, respectively, by

$$\rho = |\psi\rangle\langle\psi| \otimes |\phi\rangle\langle\phi| = \begin{bmatrix} |a_0|^2 & a_0 a_1^* \\ a_0^* a_1 & |a_1|^2 \end{bmatrix} \otimes \begin{bmatrix} |b_0|^2 & b_0 b_1^* \\ b_0^* b_1 & |b_1|^2 \end{bmatrix}$$

$$= \begin{bmatrix} |a_0|^2|b_0|^2 & |a_0|^2 b_0 b_1^* & a_0 a_1^* |b_0|^2 & a_0 a_1^* b_0 b_1^* \\ |a_0|^2 b_0^* b_1 & |a_0|^2 |b_1|^2 & a_0 a_1^* b_0^* b_1 & a_0 a_1^* |b_1|^2 \\ a_0^* a_1 |b_0|^2 & a_0^* a_1 b_0 b_1^* & |a_1|^2 |b_0|^2 & |a_1|^2 b_0 b_1^* \\ a_0^* a_1 b_0^* b_1 & a_0^* a_1 |b_1|^2 & |a_1|^2 b_0^* b_1 & |a_1|^2 |b_1|^2 \end{bmatrix},$$

$$(CX)\,\rho\,(CX)^\dagger = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} |a_0|^2|b_0|^2 & |a_0|^2 b_0 b_1^* & a_0 a_1^* |b_0|^2 & a_0 a_1^* b_0 b_1^* \\ |a_0|^2 b_0^* b_1 & |a_0|^2 |b_1|^2 & a_0 a_1^* b_0^* b_1 & a_0 a_1^* |b_1|^2 \\ a_0^* a_1 |b_0|^2 & a_0^* a_1 b_0 b_1^* & |a_1|^2 |b_0|^2 & |a_1|^2 b_0 b_1^* \\ a_0^* a_1 b_0^* b_1 & a_0^* a_1 |b_1|^2 & |a_1|^2 b_0^* b_1 & |a_1|^2 |b_1|^2 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$
$$= \begin{bmatrix} |a_0|^2|b_0|^2 & |a_0|^2 b_0 b_1^* & a_0 a_1^* b_0 b_1^* & a_0 a_1^* |b_0|^2 \\ |a_0|^2 b_0^* b_1 & |a_0|^2 |b_1|^2 & a_0 a_1^* |b_1|^2 & a_0 a_1^* b_0^* b_1 \\ a_0^* a_1 b_0^* b_1 & a_0^* a_1 |b_1|^2 & |a_1|^2 |b_1|^2 & |a_1|^2 b_0^* b_1 \\ a_0^* a_1 |b_0|^2 & a_0^* a_1 b_0 b_1^* & |a_1|^2 b_0 b_1^* & |a_1|^2 |b_0|^2 \end{bmatrix},$$

which is a permutation between the third and fourth columns, and third and fourth rows.

4.20

The circuit in the image can be written as

$$(H \otimes H)\, CX_{(1,2)}\, (H \otimes H) = \frac{1}{4} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$
$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} = CX_{(2,1)}.$$

$$\begin{aligned} CX_{(1,2)} |+\rangle |+\rangle &= (H \otimes H)\, (H \otimes H)\, CX_{(1,2)}\, (H \otimes H) |0\rangle |0\rangle \\ &= (H \otimes H)\, CX_{(2,1)} |0\rangle |0\rangle \\ &= (H \otimes H) |0\rangle |0\rangle \\ &= |+\rangle |+\rangle, \\ CX_{(1,2)} |-\rangle |+\rangle &= (H \otimes H)\, (H \otimes H)\, CX_{(1,2)}\, (H \otimes H) |1\rangle |0\rangle \\ &= (H \otimes H)\, CX_{(2,1)} |1\rangle |0\rangle \\ &= (H \otimes H) |1\rangle |0\rangle \\ &= |-\rangle |+\rangle, \\ CX_{(1,2)} |+\rangle |-\rangle &= (H \otimes H)\, (H \otimes H)\, CX_{(1,2)}\, (H \otimes H) |0\rangle |1\rangle \\ &= (H \otimes H)\, CX_{(2,1)} |0\rangle |1\rangle \\ &= (H \otimes H) |1\rangle |1\rangle \end{aligned}$$

$$
\begin{aligned}
&= |-\rangle\,|-\rangle\,,\\
CX_{(1,2)}\,|-\rangle\,|-\rangle &= (H\otimes H)\,(H\otimes H)\,CX_{(1,2)}\,(H\otimes H)\,|1\rangle\,|1\rangle\\
&= (H\otimes H)\,CX_{(2,1)}\,|1\rangle\,|1\rangle\\
&= (H\otimes H)\,|0\rangle\,|1\rangle\\
&= |+\rangle\,|-\rangle\,.
\end{aligned}
$$

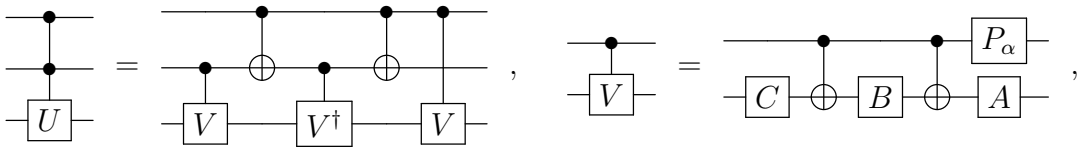
4.21

Considering the initial state as a (normalized) superposition of all four possibilities for the control qubits c_1 and c_2 with the target qubit t, given by $|\Psi\rangle = (|0\rangle\,|0\rangle + |0\rangle\,|1\rangle + |1\rangle\,|0\rangle + |1\rangle\,|1\rangle)\,|\psi\rangle$, we have

$$
\begin{aligned}
|\Psi\rangle &\xrightarrow{CV_{(c_2,t)}} |0\rangle\,|0\rangle\,|\psi\rangle + |0\rangle\,|1\rangle\,\Big(V\,|\psi\rangle\Big) + |1\rangle\,|0\rangle\,|\psi\rangle + |1\rangle\,|1\rangle\,\Big(V\,|\psi\rangle\Big)\\
&\xrightarrow{CX_{(c_1,c_2)}} |0\rangle\,|0\rangle\,|\psi\rangle + |0\rangle\,|1\rangle\,\Big(V\,|\psi\rangle\Big) + |1\rangle\,|1\rangle\,|\psi\rangle + |1\rangle\,|0\rangle\,\Big(V\,|\psi\rangle\Big)\\
&\xrightarrow{CV^\dagger_{(c_2,t)}} \Big(|0\rangle\,|0\rangle + |0\rangle\,|1\rangle\Big)\,|\psi\rangle + |1\rangle\,|1\rangle\,\Big(V^\dagger\,|\psi\rangle\Big) + |1\rangle\,|0\rangle\,\Big(V\,|\psi\rangle\Big)\\
&\xrightarrow{CX_{(c_2,c_1)}} \Big(|0\rangle\,|0\rangle + |0\rangle\,|1\rangle\Big)\,|\psi\rangle + |1\rangle\,|0\rangle\,\Big(V^\dagger\,|\psi\rangle\Big) + |1\rangle\,|1\rangle\,\Big(V\,|\psi\rangle\Big)\\
&\xrightarrow{CV_{(c_1,t)}} \Big(|0\rangle\,|0\rangle + |0\rangle\,|1\rangle + |1\rangle\,|0\rangle\Big)\,|\psi\rangle + |1\rangle\,|1\rangle\,\Big(V^2\,|\psi\rangle\Big)\\
&= \Big(|0\rangle\,|0\rangle + |0\rangle\,|1\rangle + |1\rangle\,|0\rangle\Big)\,|\psi\rangle + |1\rangle\,|1\rangle\,\Big(U\,|\psi\rangle\Big) = C^2(U)\,|\Psi\rangle\,.
\end{aligned}
$$

4.22

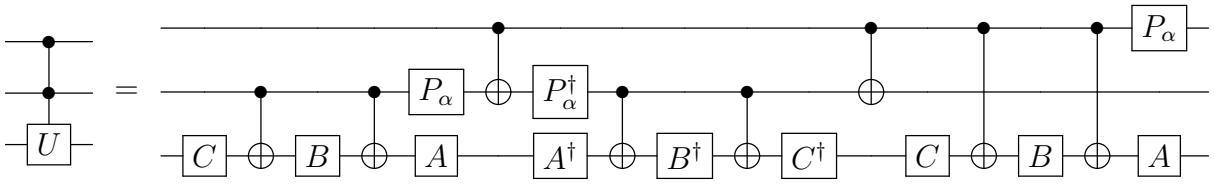
We have the following relations:

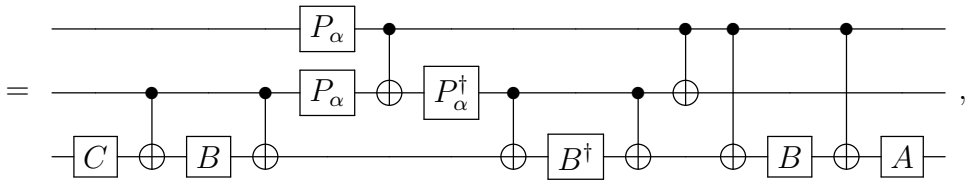


where P_α denotes the phase gate given by

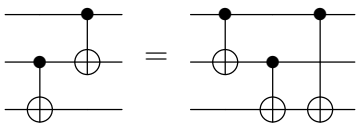
$$
P_\alpha = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{bmatrix}.
$$

Using the second relation we can decompose $C^2(U)$ as

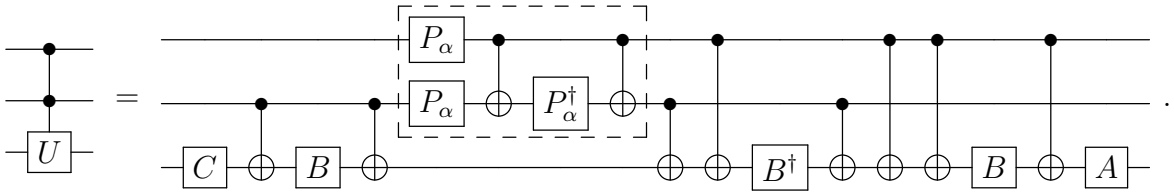




and using the fact that



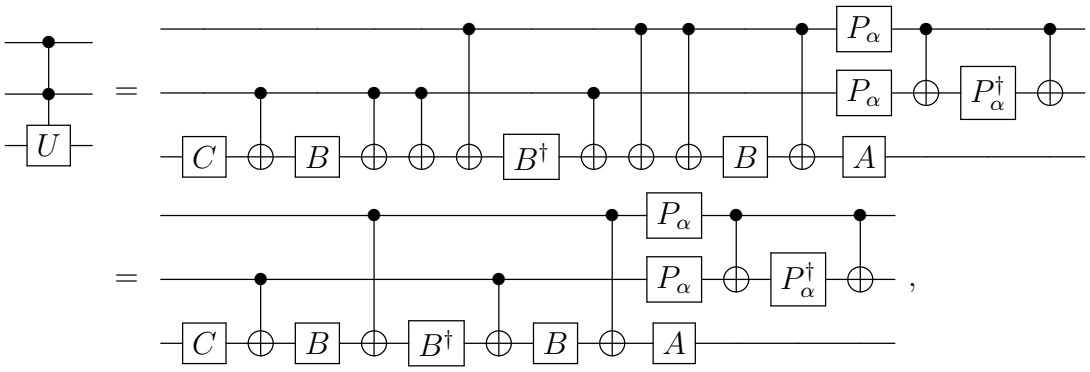
we can write the sixth CNOT gate before the fourth and fifth ones as



Notice that the operator inside the box, given by

$$CX_{(c_1,c_2)}\left(I\otimes P_\alpha^\dagger\right)CX_{(c_1,c_2)}\left(P_\alpha\otimes P_\alpha\right)=\begin{bmatrix}I & 0\\ 0 & X\end{bmatrix}\begin{bmatrix}I & 0\\ 0 & P_\alpha^\dagger\end{bmatrix}\begin{bmatrix}I & 0\\ 0 & X\end{bmatrix}\begin{bmatrix}P_\alpha & 0\\ 0 & e^{i\alpha}P_\alpha\end{bmatrix}$$
$$=\begin{bmatrix}P_\alpha & 0\\ 0 & e^{i\alpha}XP_\alpha^\dagger XP_\alpha\end{bmatrix},$$

is diagonal and can, therefore, be written in any part of the circuit since it involves only the two control qubits, thus

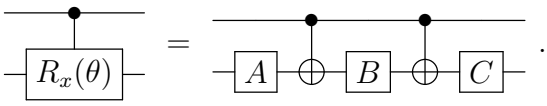


4.23

For the $R_x(\theta)$ gate we have

$$R_x(\theta)=\begin{bmatrix}\cos\frac{\theta}{2} & -i\sin\frac{\theta}{2}\\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2}\end{bmatrix}=\begin{bmatrix}e^{i(\alpha-\beta/2-\delta/2)}\cos\frac{\gamma}{2} & -e^{i(\alpha-\beta/2+\delta/2)}\sin\frac{\gamma}{2}\\ e^{i(\alpha+\beta/2-\delta/2)}\sin\frac{\gamma}{2} & e^{i(\alpha+\beta/2+\delta/2)}\cos\frac{\gamma}{2}\end{bmatrix}$$
$$\implies \alpha=0,\beta=-\frac{\pi}{2},\gamma=\theta,\delta=\frac{\pi}{2},$$

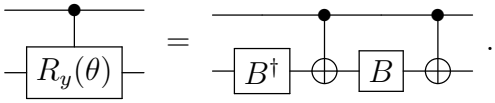
meaning that with the operators $A = R_z(-\pi/2)R_y(\theta/2), B = R_y(-\theta/2)$ and $C = R_z(\pi/2)$ we can write $R_x(\theta) = AXBXC$, and thus create the circuit



It is impossible to reduce the number of single qubit gates to two for general θ since that would require the possibility of writing $R_x(\theta) = e^{i\omega}XD^\dagger XD$ for some operator D and phase ω, which is equivalent to $D^\dagger XD = R_x(\theta+\pi)$ up to a global phase that would be corrected by ω. But it is a fact that $(D^\dagger XD)^2 = I$, and that implies $(R_x(\theta+\pi))^2 = R_x(2\theta) = I$, which is only true for $\theta = 0$ or π. On the other hand, for the $R_y(\theta)$ gate we can write

$$\begin{aligned}
R_y(\theta) &= R_y(\theta/2)R_y(\theta/2) \\
&= \left(\cos\frac{\theta}{4}I - i\sin\frac{\theta}{4}Y\right)R_y(\theta/2) \\
&= \left(\cos\frac{\theta}{4}I + i\sin\frac{\theta}{4}XYX\right)R_y(\theta/2) \\
&= X\left(\cos\frac{\theta}{4}I + i\sin\frac{\theta}{4}Y\right)XR_y(\theta/2) \\
&= XR_y(-\theta/2)XR_y(\theta/2),
\end{aligned}$$

meaning that, using the operator B defined above, we can create the circuit



4.24

Considering the initial state as a (normalized) superposition of all four possibilities for the control qubits c_1 and c_2 with the target qubit t, given by $|\Psi\rangle = (|0\rangle|0\rangle + |0\rangle|1\rangle + |1\rangle|0\rangle + |1\rangle|1\rangle)|\psi\rangle$, we have

$$\begin{aligned}
|\Psi\rangle &\xrightarrow{I\otimes I\otimes H} \Big(|0\rangle|0\rangle + |0\rangle|1\rangle + |1\rangle|0\rangle + |1\rangle|1\rangle\Big)H|\psi\rangle \\
&\xrightarrow{CX_{(c_2,t)}} |0\rangle|0\rangle\Big(H|\psi\rangle\Big) + |0\rangle|1\rangle\Big(XH|\psi\rangle\Big) + |1\rangle|0\rangle\Big(H|\psi\rangle\Big) + |1\rangle|1\rangle\Big(XH|\psi\rangle\Big) \\
&\xrightarrow{I\otimes I\otimes T^\dagger} |0\rangle|0\rangle\Big(T^\dagger H|\psi\rangle\Big) + |0\rangle|1\rangle\Big(T^\dagger XH|\psi\rangle\Big) + |1\rangle|0\rangle\Big(T^\dagger H|\psi\rangle\Big) + |1\rangle|1\rangle\Big(T^\dagger XH|\psi\rangle\Big) \\
&\xrightarrow{CX_{(c_1,t)}} |0\rangle|0\rangle\Big(T^\dagger H|\psi\rangle\Big) + |0\rangle|1\rangle\Big(T^\dagger XH|\psi\rangle\Big) + |1\rangle|0\rangle\Big(XT^\dagger H|\psi\rangle\Big) \\
&\qquad + |1\rangle|1\rangle\Big(XT^\dagger XH|\psi\rangle\Big) \\
&\xrightarrow{I\otimes I\otimes T} |0\rangle|0\rangle\Big(H|\psi\rangle\Big) + |0\rangle|1\rangle\Big(XH|\psi\rangle\Big) + |1\rangle|0\rangle\Big(TXT^\dagger H|\psi\rangle\Big) \\
&\qquad + |1\rangle|1\rangle\Big(TXT^\dagger XH|\psi\rangle\Big) \\
&\xrightarrow{CX_{(c_2,t)}} \Big(|0\rangle|0\rangle + |0\rangle|1\rangle\Big)H|\psi\rangle + |1\rangle|0\rangle\Big(TXT^\dagger H|\psi\rangle\Big) + |1\rangle|1\rangle\Big(XTXT^\dagger XH|\psi\rangle\Big)
\end{aligned}$$

$$
\begin{aligned}
&\xrightarrow{I\otimes I\otimes T^\dagger}\Big(|0\rangle|0\rangle+|0\rangle|1\rangle\Big)T^\dagger H|\psi\rangle+|1\rangle|0\rangle\Big(XT^\dagger H|\psi\rangle\Big)+|1\rangle|1\rangle\Big(T^\dagger XTXT^\dagger XH|\psi\rangle\Big)\\
&\xrightarrow{CX_{(c_1,t)}}\Big(|0\rangle|0\rangle+|0\rangle|1\rangle+|1\rangle|0\rangle\Big)T^\dagger H|\psi\rangle+|1\rangle|1\rangle\Big(XT^\dagger XTXT^\dagger XH|\psi\rangle\Big)\\
&\xrightarrow{I\otimes T^\dagger\otimes T}\Big(|0\rangle|0\rangle+e^{-i\pi/4}|0\rangle|1\rangle+|1\rangle|0\rangle\Big)H|\psi\rangle+e^{-i\pi/4}|1\rangle|1\rangle\Big(\left(TXT^\dagger X\right)^2H|\psi\rangle\Big)\\
&\xrightarrow{CX_{(c_1,c_2)}\otimes H}\Big(|0\rangle|0\rangle+e^{-i\pi/4}|0\rangle|1\rangle+|1\rangle|1\rangle\Big)|\psi\rangle+e^{-i\pi/4}|1\rangle|0\rangle\Big(H\left(TXT^\dagger X\right)^2H|\psi\rangle\Big)\\
&\xrightarrow{I\otimes T^\dagger\otimes I}\Big(|0\rangle|0\rangle+e^{-i\pi/2}|0\rangle|1\rangle+e^{-i\pi/4}|1\rangle|1\rangle\Big)|\psi\rangle+e^{-i\pi/4}|1\rangle|0\rangle\Big(H\left(TXT^\dagger X\right)^2H|\psi\rangle\Big)\\
&\xrightarrow{CX_{(c_1,c_2)}}\Big(|0\rangle|0\rangle+e^{-i\pi/2}|0\rangle|1\rangle+e^{-i\pi/4}|1\rangle|0\rangle\Big)|\psi\rangle+e^{-i\pi/4}|1\rangle|1\rangle\Big(H\left(TXT^\dagger X\right)^2H|\psi\rangle\Big)\\
&\xrightarrow{T\otimes S\otimes I}\Big(|0\rangle|0\rangle+|0\rangle|1\rangle+|1\rangle|0\rangle\Big)|\psi\rangle+i|1\rangle|1\rangle\Big(H\left(TXT^\dagger X\right)^2H|\psi\rangle\Big).
\end{aligned}
$$

But expanding the operator acting on the last term yields

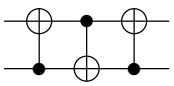
$$
\begin{aligned}
TXT^\dagger X &= R_z(\pi/4)XR_z(-\pi/4)X\\
&= R_z(\pi/2)\\
\implies \quad iH\left(TXT^\dagger X\right)^2H &= iHR_z(\pi)H\\
&= iR_x(\pi)\\
&= X,
\end{aligned}
$$

thus the action of the circuit is effectively

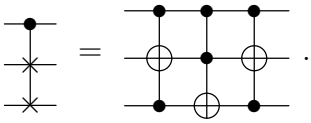
$$
|\Psi\rangle\longrightarrow\Big(|0\rangle|0\rangle+|0\rangle|1\rangle+|1\rangle|0\rangle\Big)|\psi\rangle+|1\rangle|1\rangle\Big(X|\psi\rangle\Big)=CCX|\Psi\rangle.
$$

4.25

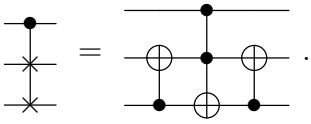
It is a fact that the SWAP gate can be built with CNOT gates as



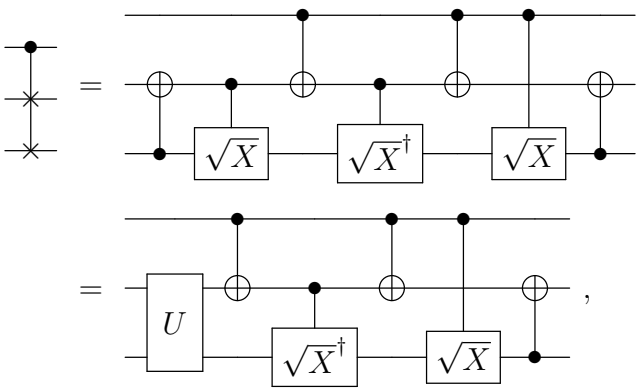
thus a controlled-SWAP gate can be written as



We have that $\text{CNOT}^2 = I \otimes I$, so we can just eliminate the second control from the first and third Toffoli gates because, for the $|0\rangle$ component of the controlled-SWAP's control bit, the action of the circuit will be only the first and third CNOTs, which will cancel each other, and for the $|1\rangle$ component, the SWAP operation will be performed naturally. So

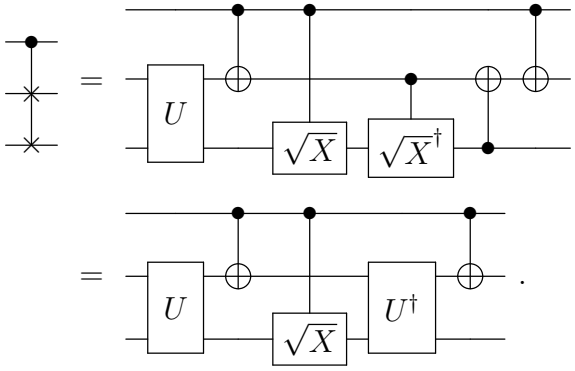


Decomposing the Toffoli gate using only two-qubit gates yields



where we have defined the two-qubit gate $U \coloneqq C\sqrt{X}_{(t_1,t_2)}CX_{(t_2,t_1)}$.

The $\sqrt{X}$ gate commutes with the two previous gates and the last two CNOT gates also commutes, meaning we can write



4.26

Considering the initial state as a (normalized) superposition of all four possibilities for the control qubits c_1 and c_2 with the target qubit t, given by $|\Psi\rangle = (|0\rangle|0\rangle + |0\rangle|1\rangle + |1\rangle|0\rangle + |1\rangle|1\rangle)|\psi\rangle$, we have

$$
\begin{aligned}
|\Psi\rangle &\xrightarrow{I\otimes I\otimes R_y(\theta)} \Big(|0\rangle|0\rangle + |0\rangle|1\rangle + |1\rangle|0\rangle + |1\rangle|1\rangle\Big) R_y(\theta)|\psi\rangle \\
&\xrightarrow{CX_{(c_2,t)}} |0\rangle|0\rangle\Big(R_y(\theta)|\psi\rangle\Big) + |0\rangle|1\rangle\Big(XR_y(\theta)|\psi\rangle\Big) + |1\rangle|0\rangle\Big(R_y(\theta)|\psi\rangle\Big) \\
&\qquad + |1\rangle|1\rangle\Big(XR_y(\theta)|\psi\rangle\Big) \\
&\xrightarrow{I\otimes I\otimes R_y(\theta)} |0\rangle|0\rangle\Big(R_y(2\theta)|\psi\rangle\Big) + |0\rangle|1\rangle\Big(R_y(\theta)XR_y(\theta)|\psi\rangle\Big) + |1\rangle|0\rangle\Big(R_y(2\theta)|\psi\rangle\Big) \\
&\qquad + |1\rangle|1\rangle\Big(R_y(\theta)XR_y(\theta)|\psi\rangle\Big) \\
&\xrightarrow{CX_{(c_1,t)}} |0\rangle|0\rangle\Big(R_y(2\theta)|\psi\rangle\Big) + |0\rangle|1\rangle\Big(R_y(\theta)XR_y(\theta)|\psi\rangle\Big) + |1\rangle|0\rangle\Big(XR_y(2\theta)|\psi\rangle\Big) \\
&\qquad + |1\rangle|1\rangle\Big((XR_y(\theta))^2|\psi\rangle\Big) \\
&\xrightarrow{I\otimes I\otimes R_y(-\theta)} |0\rangle|0\rangle\Big(R_y(\theta)|\psi\rangle\Big) + |0\rangle|1\rangle\Big(XR_y(\theta)|\psi\rangle\Big) + |1\rangle|0\rangle\Big(R_y(-\theta)XR_y(2\theta)|\psi\rangle\Big) \\
&\qquad + |1\rangle|1\rangle\Big(R_y(-\theta)(XR_y(\theta))^2|\psi\rangle\Big)
\end{aligned}
$$

$$
\begin{aligned}
\xrightarrow{CX_{(c_2,t)}} & \Big(|0\rangle |0\rangle + |0\rangle |1\rangle \Big) R_y(\theta) |\psi\rangle + |1\rangle |0\rangle \Big(R_y(-\theta) X R_y(2\theta) |\psi\rangle \Big) \\
& + |1\rangle |1\rangle \Big(X R_y(-\theta) \left(X R_y(\theta)\right)^2 |\psi\rangle \Big) \\
\xrightarrow{I\otimes I\otimes R_y(-\theta)} & \Big(|0\rangle |0\rangle + |0\rangle |1\rangle \Big) |\psi\rangle + |1\rangle |0\rangle \Big(R_y(-2\theta) X R_y(2\theta) |\psi\rangle \Big) \\
& + |1\rangle |1\rangle \Big(R_y(-\theta) X R_y(-\theta) \left(X R_y(\theta)\right)^2 |\psi\rangle \Big).
\end{aligned}
$$

Setting $\theta = \pi/4$ we have, for the remaining operators:

$$
\begin{aligned}
R_y(-\pi/2) X R_y(\pi/2) &= X X R_y(-\pi/2) X R_y(\pi/2) \\
&= X R_y(\pi) \\
&= Z,
\end{aligned}
$$

$$
\begin{aligned}
R_y(-\pi/4) X R_y(-\pi/4) \left(X R_y(\pi/4)\right)^2 &= \Big(R_y(-\pi/4) X R_y(-\pi/4) \Big) X \Big(R_y(\pi/4) X R_y(\pi/4) \Big) \\
&= \Big(X R_y(0) \Big) X \Big(X R_y(0) \Big) \\
&= X.
\end{aligned}
$$

Thus the action of the circuit is effectively

$$
|\Psi\rangle \longrightarrow \Big(|0\rangle |0\rangle + |0\rangle |1\rangle \Big) |\psi\rangle + |1\rangle |0\rangle \Big(Z |\psi\rangle \Big) + |1\rangle |1\rangle \Big(X |\psi\rangle \Big),
$$

that is, the Toffoli gate with the addition of a relative phase π to $|\Psi\rangle$'s $|1\rangle |0\rangle |1\rangle$ component.

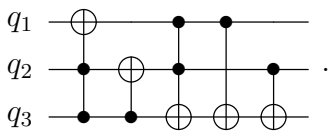
4.27

The transformation consists of the following permutations:

$$
\begin{aligned}
|0\rangle |0\rangle |0\rangle &\longrightarrow |0\rangle |0\rangle |0\rangle , \\
|0\rangle |0\rangle |1\rangle &\longrightarrow |0\rangle |1\rangle |0\rangle , \\
|0\rangle |1\rangle |0\rangle &\longrightarrow |0\rangle |1\rangle |1\rangle , \\
|0\rangle |1\rangle |1\rangle &\longrightarrow |1\rangle |0\rangle |0\rangle , \\
|1\rangle |0\rangle |0\rangle &\longrightarrow |1\rangle |0\rangle |1\rangle , \\
|1\rangle |0\rangle |1\rangle &\longrightarrow |1\rangle |1\rangle |0\rangle , \\
|1\rangle |1\rangle |0\rangle &\longrightarrow |1\rangle |1\rangle |1\rangle , \\
|1\rangle |1\rangle |1\rangle &\longrightarrow |0\rangle |0\rangle |1\rangle .
\end{aligned}
$$

If we treat each component of the three-qubit state as a binary number, the action is effectively $+1$ mod 8 ($+2$ for $|1\rangle |1\rangle |1\rangle$), with the exception of the $|0\rangle |0\rangle |0\rangle$ component, which is left invariant. Notice that the first qubit, q_1, flips when both the second and third ones are set to $|1\rangle$, the second qubit, q_2, flips when the third one is set to $|1\rangle$ and the third qubit, q_3, always flips except when the

first and second ones both end up as $|0\rangle$. So we can construct the circuit



4.28

-

4.29

-

4.30

-

4.31

Considering a generic state $|\psi\rangle = (a_0 |0\rangle + a_1 |1\rangle) \otimes (b_0 |0\rangle + b_1 |1\rangle)$ we have:

$$\begin{aligned} CX_1C |\psi\rangle &= CX_1\Big(a_0b_0 |0\rangle |0\rangle + a_0b_1 |0\rangle |1\rangle + a_1b_0 |1\rangle |1\rangle + a_1b_1 |1\rangle |0\rangle\Big) \\ &= C\Big(a_0b_0 |1\rangle |0\rangle + a_0b_1 |1\rangle |1\rangle + a_1b_0 |0\rangle |1\rangle + a_1b_1 |0\rangle |0\rangle\Big) \\ &= a_0b_0 |1\rangle |1\rangle + a_0b_1 |1\rangle |0\rangle + a_1b_0 |0\rangle |1\rangle + a_1b_1 |0\rangle |0\rangle \\ &= X_1X_2 |\psi\rangle , \end{aligned}$$

$$\begin{aligned} CY_1C |\psi\rangle &= CY_1\Big(a_0b_0 |0\rangle |0\rangle + a_0b_1 |0\rangle |1\rangle + a_1b_0 |1\rangle |1\rangle + a_1b_1 |1\rangle |0\rangle\Big) \\ &= iC\Big(a_0b_0 |1\rangle |0\rangle + a_0b_1 |1\rangle |1\rangle - a_1b_0 |0\rangle |1\rangle - a_1b_1 |0\rangle |0\rangle\Big) \\ &= i\Big(a_0b_0 |1\rangle |1\rangle + a_0b_1 |1\rangle |0\rangle - a_1b_0 |0\rangle |1\rangle - a_1b_1 |0\rangle |0\rangle\Big) \\ &= Y_1X_2 |\psi\rangle , \end{aligned}$$

$$\begin{aligned} CZ_1C |\psi\rangle &= CZ_1\Big(a_0b_0 |0\rangle |0\rangle + a_0b_1 |0\rangle |1\rangle + a_1b_0 |1\rangle |1\rangle + a_1b_1 |1\rangle |0\rangle\Big) \\ &= C\Big(a_0b_0 |0\rangle |0\rangle + a_0b_1 |0\rangle |1\rangle - a_1b_0 |1\rangle |1\rangle - a_1b_1 |1\rangle |0\rangle\Big) \\ &= a_0b_0 |0\rangle |0\rangle + a_0b_1 |0\rangle |1\rangle - a_1b_0 |1\rangle |0\rangle - a_1b_1 |1\rangle |1\rangle \\ &= Z_1 |\psi\rangle , \end{aligned}$$

$$\begin{aligned} CX_2C |\psi\rangle &= CX_2\Big(a_0b_0 |0\rangle |0\rangle + a_0b_1 |0\rangle |1\rangle + a_1b_0 |1\rangle |1\rangle + a_1b_1 |1\rangle |0\rangle\Big) \\ &= C\Big(a_0b_0 |0\rangle |1\rangle + a_0b_1 |0\rangle |0\rangle + a_1b_0 |1\rangle |0\rangle + a_1b_1 |1\rangle |1\rangle\Big) \\ &= a_0b_0 |0\rangle |1\rangle + a_0b_1 |0\rangle |0\rangle + a_1b_0 |1\rangle |1\rangle + a_1b_1 |1\rangle |0\rangle \end{aligned}$$

$$= X_2 |\psi\rangle ,$$

$$\begin{aligned} CY_2C |\psi\rangle &= CY_2\Big(a_0b_0 |0\rangle |0\rangle + a_0b_1 |0\rangle |1\rangle + a_1b_0 |1\rangle |1\rangle + a_1b_1 |1\rangle |0\rangle \Big) \\ &= iC\Big(a_0b_0 |0\rangle |1\rangle - a_0b_1 |0\rangle |0\rangle - a_1b_0 |1\rangle |0\rangle + a_1b_1 |1\rangle |1\rangle \Big) \\ &= i\Big(a_0b_0 |0\rangle |1\rangle - a_0b_1 |0\rangle |0\rangle - a_1b_0 |1\rangle |1\rangle + a_1b_1 |1\rangle |0\rangle \Big) \\ &= Z_1Y_2 |\psi\rangle , \end{aligned}$$

$$\begin{aligned} CZ_2C |\psi\rangle &= CZ_2\Big(a_0b_0 |0\rangle |0\rangle + a_0b_1 |0\rangle |1\rangle + a_1b_0 |1\rangle |1\rangle + a_1b_1 |1\rangle |0\rangle \Big) \\ &= C\Big(a_0b_0 |0\rangle |0\rangle - a_0b_1 |0\rangle |1\rangle - a_1b_0 |1\rangle |1\rangle + a_1b_1 |1\rangle |0\rangle \Big) \\ &= a_0b_0 |0\rangle |0\rangle - a_0b_1 |0\rangle |1\rangle - a_1b_0 |1\rangle |0\rangle + a_1b_1 |1\rangle |1\rangle \\ &= Z_1Z_2 |\psi\rangle , \end{aligned}$$

$$\begin{aligned} R_{z,1}(\theta)C |\psi\rangle &= R_{z,1}(\theta)\Big(a_0b_0 |0\rangle |0\rangle + a_0b_1 |0\rangle |1\rangle + a_1b_0 |1\rangle |1\rangle + a_1b_1 |1\rangle |0\rangle \Big) \\ &= e^{-i\theta/2}a_0b_0 |0\rangle |0\rangle + e^{-i\theta/2}a_0b_1 |0\rangle |1\rangle + e^{i\theta/2}a_1b_0 |1\rangle |1\rangle + e^{i\theta/2}a_1b_1 |1\rangle |0\rangle \\ &= CR_{z,1}(\theta) |\psi\rangle , \end{aligned}$$

$$\begin{aligned} R_{x,2}(\theta)C |\psi\rangle &= R_{x,2}(\theta)\Big(a_0b_0 |0\rangle |0\rangle + a_0b_1 |0\rangle |1\rangle + a_1b_0 |1\rangle |1\rangle + a_1b_1 |1\rangle |0\rangle \Big) \\ &= a_0b_0 |0\rangle \left(\cos\frac{\theta}{2} |0\rangle - i\sin\frac{\theta}{2} |1\rangle\right) + a_0b_1 |0\rangle \left(\cos\frac{\theta}{2} |1\rangle - i\sin\frac{\theta}{2} |0\rangle\right) \\ &\quad + a_1b_0 |1\rangle \left(\cos\frac{\theta}{2} |1\rangle - i\sin\frac{\theta}{2} |0\rangle\right) + a_1b_1 |1\rangle \left(\cos\frac{\theta}{2} |0\rangle - i\sin\frac{\theta}{2} |1\rangle\right) \\ &= a_0 \left(b_0\cos\frac{\theta}{2} - ib_1\sin\frac{\theta}{2}\right) |0\rangle |0\rangle + a_0 \left(b_1\cos\frac{\theta}{2} - ib_0\sin\frac{\theta}{2}\right) |0\rangle |1\rangle \\ &\quad + a_1 \left(b_0\cos\frac{\theta}{2} - ib_1\sin\frac{\theta}{2}\right) |1\rangle |1\rangle + a_1 \left(b_1\cos\frac{\theta}{2} - ib_0\sin\frac{\theta}{2}\right) |1\rangle |0\rangle \\ &= CR_{x,2}(\theta) |\psi\rangle . \end{aligned}$$

4.32

Let us consider the first qubit initially in state $\rho_1 = |\psi\rangle\langle\psi|$ and the second one initially in $\rho_2 = |\phi\rangle\langle\phi|$. After a projective measurement is performed on the second qubit, its state becomes

$$\begin{aligned} \rho_2' &= \sum_{i=0}^{1} p(i) |i\rangle\langle i| \\ &= \sum_{i=0}^{1} \mathrm{tr}(P_i |\phi\rangle\langle\phi| P_i) \frac{P_i |\phi\rangle\langle\phi| P_i}{\mathrm{tr}(P_i |\phi\rangle\langle\phi| P_i)} \\ &= \sum_{i=0}^{1} P_i |\phi\rangle\langle\phi| P_i, \end{aligned}$$

while for the first qubit we have $\rho_1' = \rho_1$. Thus the post-measurement density operator of the entire system is given by

$$\begin{aligned}\rho' = \rho_1' \otimes \rho_2' &= \sum_{i=0}^{1} |\psi\rangle\langle\psi| \otimes P_i \, |\phi\rangle\langle\phi| \, P_i \\ &= \sum_{i=0}^{1} (I \otimes P_i) \, \rho \, (I \otimes P_i) \\ &= P_0 \rho P_0 + P_1 \rho P_1,\end{aligned}$$

where the projectors are to be understood as acting on the second qubit only.

$$\begin{aligned}\mathrm{tr}_2(\rho') &= \sum_{i=0}^{1} |\psi\rangle\langle\psi| \, \mathrm{tr}_2 \left(P_i \, |\phi\rangle\langle\phi| \, P_i\right) \\ &= \sum_{i=0}^{1} \sum_{j=0}^{1} |\psi\rangle\langle\psi| \, \langle j \,|\, i\rangle \, \langle i \,|\, \phi\rangle \, \langle \phi \,|\, i\rangle \, \langle i \,|\, j\rangle \\ &= \sum_{j=0}^{1} |\psi\rangle\langle\psi| \, \langle j \,|\, \phi\rangle \, \langle \phi \,|\, j\rangle = \mathrm{tr}_2(\rho).\end{aligned}$$

4.33

Considering a generic two-qubit state written in the Bell basis $|\psi\rangle = a_+ \, |\Phi^+\rangle + b_+ \, |\Psi^+\rangle + a_- \, |\Phi^-\rangle + b_- \, |\Psi^-\rangle$, the circuit performs

$$\begin{aligned}|\psi\rangle &\xrightarrow{CX_{(1,2)}} a_+ \left(\frac{|0\rangle \, |0\rangle + |1\rangle \, |0\rangle}{\sqrt{2}}\right) + b_+ \left(\frac{|0\rangle \, |1\rangle + |1\rangle \, |1\rangle}{\sqrt{2}}\right) + a_- \left(\frac{|0\rangle \, |0\rangle - |1\rangle \, |0\rangle}{\sqrt{2}}\right) \\ &\qquad + b_- \left(\frac{|0\rangle \, |1\rangle - |1\rangle \, |1\rangle}{\sqrt{2}}\right) \\ &\xrightarrow{H \otimes I} a_+ \, |0\rangle \, |0\rangle + b_+ \, |0\rangle \, |1\rangle + a_- \, |1\rangle \, |0\rangle + b_- \, |1\rangle \, |1\rangle \, ,\end{aligned}$$

and after the measurements in the computational basis we obtain

$$\begin{aligned}&|0\rangle \, |0\rangle \quad \text{with probability } |a_+|^2, \\ &|0\rangle \, |1\rangle \quad \text{with probability } |b_+|^2, \\ &|1\rangle \, |0\rangle \quad \text{with probability } |a_-|^2, \\ &|1\rangle \, |1\rangle \quad \text{with probability } |b_-|^2.\end{aligned}$$

These are the same probabilities of obtaining $|\Phi^+\rangle$, $|\Psi^+\rangle$, $|\Phi^-\rangle$ and $|\Psi^-\rangle$ respectively if we had performed the measurement directly using the Bell projectors. So effectively, the circuit is a measurement in the Bell basis, meaning that obtaining $|0\rangle \, |0\rangle$ is equivalent to obtaining $|\Phi^+\rangle$, $|0\rangle \, |1\rangle$ is equivalent to $|\Psi^+\rangle$, $|1\rangle \, |0\rangle$ is equivalent to $|\Phi^-\rangle$ and $|1\rangle \, |1\rangle$ is equivalent to $|\Psi^-\rangle$.

4.34

Let us consider that $U|\psi_+\rangle = |\psi_+\rangle$ and $U|\psi_-\rangle = -|\psi_-\rangle$ are the two eigenvalue relations for operator U. Now, if we consider a generic two-qubit state given by $|\Psi\rangle = |0\rangle|\psi_{\text{in}}\rangle = |0\rangle(a|\psi_+\rangle + b|\psi_-\rangle)$ the circuit performs

$$\begin{aligned}
|\Psi\rangle &\xrightarrow{H\otimes I} \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)(a|\psi_+\rangle + b|\psi_-\rangle) \\
&\xrightarrow{CU_{(1,2)}} |0\rangle\left(\frac{a|\psi_+\rangle + b|\psi_-\rangle}{\sqrt{2}}\right) + |1\rangle\left(\frac{a|\psi_+\rangle - b|\psi_-\rangle}{\sqrt{2}}\right) \\
&\xrightarrow{H\otimes I} a|0\rangle|\psi_+\rangle + b|1\rangle|\psi_-\rangle\,.
\end{aligned}$$

After measuring the first qubit we have

$$\begin{aligned}
&|0\rangle \quad \text{with probability } |a|^2, \\
&|1\rangle \quad \text{with probability } |b|^2,
\end{aligned}$$

and because this is an entangled state, if we obtain $|0\rangle$ then the second qubit is in state $|\psi_+\rangle$, meaning the result for observable U is $+1$, and if we obtain $|1\rangle$ then the second qubit is in state $|\psi_-\rangle$, meaning the result for observable U is -1. Thus this circuit implements a measurement of U.

4.35

Considering the initial state as a generic superposition, given by $|\Psi\rangle = (a|0\rangle + b|1\rangle)|\psi\rangle$, we have, for the left-hand side

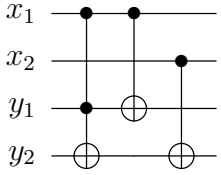
$$\begin{aligned}
|\Psi\rangle &\xrightarrow{CU_{(c,t)}} a|0\rangle|\psi\rangle + b|1\rangle\Big(U|\psi\rangle\Big) \\
&\xrightarrow{\text{meas.}} \begin{cases} |0\rangle|\psi\rangle & \text{with probability } |a|^2 \\ |1\rangle\big(U|\psi\rangle\big) & \text{with probability } |b|^2 \end{cases},
\end{aligned}$$

and for the right-hand side

$$\begin{aligned}
|\Psi\rangle &\xrightarrow{\text{meas.}} \begin{cases} |0\rangle|\psi\rangle & \text{with probability } |a|^2 \\ |1\rangle|\psi\rangle & \text{with probability } |b|^2 \end{cases} \\
&\xrightarrow{CU_{(c,t)}} \begin{cases} |0\rangle|\psi\rangle & \text{with probability } |a|^2 \\ |1\rangle\big(U|\psi\rangle\big) & \text{with probability } |b|^2 \end{cases}.
\end{aligned}$$

4.36

Index 1 indicates the least significant bit and 2 indicates the most significant bit:



4.37

Labeling the transform as T we have

$$U_1T = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix}$$

$$= \frac{1}{2} \begin{bmatrix} \sqrt{2} & \frac{1+i}{\sqrt{2}} & 0 & \frac{1-i}{\sqrt{2}} \\ 0 & \frac{1-i}{\sqrt{2}} & \sqrt{2} & \frac{1+i}{\sqrt{2}} \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix},$$

$$U_2U_1T = \begin{bmatrix} \sqrt{\frac{2}{3}} & 0 & \frac{1}{\sqrt{3}} & 0 \\ 0 & 1 & 0 & 0 \\ \frac{1}{\sqrt{3}} & 0 & -\sqrt{\frac{2}{3}} & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \frac{1}{2} \begin{bmatrix} \sqrt{2} & \frac{1+i}{\sqrt{2}} & 0 & \frac{1-i}{\sqrt{2}} \\ 0 & \frac{1-i}{\sqrt{2}} & \sqrt{2} & \frac{1+i}{\sqrt{2}} \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix}$$

$$= \frac{1}{2} \begin{bmatrix} \sqrt{3} & \frac{i}{\sqrt{3}} & \frac{1}{\sqrt{3}} & -\frac{i}{\sqrt{3}} \\ 0 & \frac{1-i}{\sqrt{2}} & \sqrt{2} & \frac{1+i}{\sqrt{2}} \\ 0 & \frac{3+i}{\sqrt{6}} & -\sqrt{\frac{2}{3}} & \frac{3-i}{\sqrt{6}} \\ 1 & -i & -1 & i \end{bmatrix},$$

$$U_3U_2U_1T = \begin{bmatrix} \frac{\sqrt{3}}{2} & 0 & 0 & \frac{1}{2} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \frac{1}{2} & 0 & 0 & -\frac{\sqrt{3}}{2} \end{bmatrix} \frac{1}{2} \begin{bmatrix} \sqrt{3} & \frac{i}{\sqrt{3}} & \frac{1}{\sqrt{3}} & -\frac{i}{\sqrt{3}} \\ 0 & \frac{1-i}{\sqrt{2}} & \sqrt{2} & \frac{1+i}{\sqrt{2}} \\ 0 & \frac{3+i}{\sqrt{6}} & -\sqrt{\frac{2}{3}} & \frac{3-i}{\sqrt{6}} \\ 1 & -i & -1 & i \end{bmatrix}$$

$$= \frac{1}{2} \begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & \frac{1-i}{\sqrt{2}} & \sqrt{2} & \frac{1+i}{\sqrt{2}} \\ 0 & \frac{3+i}{\sqrt{6}} & -\sqrt{\frac{2}{3}} & \frac{3-i}{\sqrt{6}} \\ 0 & \frac{2i}{\sqrt{3}} & \frac{2}{\sqrt{3}} & -\frac{2i}{\sqrt{3}} \end{bmatrix},$$

$$U_4U_3U_2U_1T = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{\sqrt{3}(1+i)}{4} & \frac{3-i}{4} & 0 \\ 0 & \frac{3+i}{4} & -\frac{\sqrt{3}(1-i)}{4} & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \frac{1}{2} \begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & \frac{1-i}{\sqrt{2}} & \sqrt{2} & \frac{1+i}{\sqrt{2}} \\ 0 & \frac{3+i}{\sqrt{6}} & -\sqrt{\frac{2}{3}} & \frac{3-i}{\sqrt{6}} \\ 0 & \frac{2i}{\sqrt{3}} & \frac{2}{\sqrt{3}} & -\frac{2i}{\sqrt{3}} \end{bmatrix}$$

$$= \frac{1}{2} \begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 2\sqrt{\frac{2}{3}} & i\sqrt{\frac{2}{3}} & \sqrt{\frac{2}{3}} \\ 0 & 0 & \sqrt{2} & i\sqrt{2} \\ 0 & \frac{2i}{\sqrt{3}} & \frac{2}{\sqrt{3}} & -\frac{2i}{\sqrt{3}} \end{bmatrix},$$

$$U_5U_4U_3U_2U_1T = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \sqrt{\frac{2}{3}} & 0 & -\frac{i}{\sqrt{3}} \\ 0 & 0 & 1 & 0 \\ 0 & \frac{i}{\sqrt{3}} & 0 & -\sqrt{\frac{2}{3}} \end{bmatrix} \frac{1}{2} \begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 2\sqrt{\frac{2}{3}} & i\sqrt{\frac{2}{3}} & \sqrt{\frac{2}{3}} \\ 0 & 0 & \sqrt{2} & i\sqrt{2} \\ 0 & \frac{2i}{\sqrt{3}} & \frac{2}{\sqrt{3}} & -\frac{2i}{\sqrt{3}} \end{bmatrix}$$
$$= \frac{1}{2} \begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & \sqrt{2} & i\sqrt{2} \\ 0 & 0 & -\sqrt{2} & i\sqrt{2} \end{bmatrix},$$
$$U_6U_5U_4U_3U_2U_1T = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ 0 & 0 & -\frac{i}{\sqrt{2}} & -\frac{i}{\sqrt{2}} \end{bmatrix} \frac{1}{2} \begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & \sqrt{2} & i\sqrt{2} \\ 0 & 0 & -\sqrt{2} & i\sqrt{2} \end{bmatrix}$$
$$= I.$$

4.38

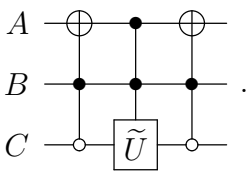
Any $d \times d$ unitary matrix whose first column does not contain a zero will require at least $d-1$ two-level unitary matrices. The reason is that one two-level unitary matrix is required in order to turn one entry of the first column to zero, and there are $d-1$ entries in the first column that needs to be eliminated, meaning at least $d-1$ two-level unitary matrices are required for the decomposition.

4.39

The transformation acts on states $|0\rangle|1\rangle|0\rangle$ and $|1\rangle|1\rangle|1\rangle$, and a Gray code connecting them is

$$\begin{matrix} A & B & C \\ 0 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{matrix}.$$

So a circuit that implements the transformation is



.

4.40

$$E(R_{\hat{n}}(\alpha), R_{\hat{n}}(\alpha+\beta)) = \max_{|\psi\rangle} \|(R_{\hat{n}}(\alpha) - R_{\hat{n}}(\alpha+\beta))|\psi\rangle\|$$
$$= \max_{|\psi\rangle} \|R_{\hat{n}}(\alpha)(I - R_{\hat{n}}(\beta))|\psi\rangle\|$$

$$
\begin{aligned}
&= \max_{|\psi\rangle} \sqrt{\left\langle \psi \,\middle|\, \left(I - R^\dagger_{\hat{n}}(\beta)\right) R^\dagger_{\hat{n}}(\alpha) R_{\hat{n}}(\alpha) \left(I - R_{\hat{n}}(\beta)\right) \,\middle|\, \psi \right\rangle} \\
&= \max_{|\psi\rangle} \sqrt{\left\langle \psi \,\middle|\, \left(2I - R^\dagger_{\hat{n}}(\beta) - R_{\hat{n}}(\beta)\right) \,\middle|\, \psi \right\rangle} \\
&= \max_{|\psi\rangle} \sqrt{2 - \left\langle \psi \,\middle|\, \left(e^{i\frac{\beta}{2}\hat{n}\cdot\vec{\sigma}} + e^{-i\frac{\beta}{2}\hat{n}\cdot\vec{\sigma}}\right) \,\middle|\, \psi \right\rangle}.
\end{aligned}
$$

The operator in the last terms can be rewritten as

$$
\begin{aligned}
e^{i\frac{\beta}{2}\hat{n}\cdot\vec{\sigma}} + e^{-i\frac{\beta}{2}\hat{n}\cdot\vec{\sigma}} &= \cos\frac{\beta}{2} I - i \sin\frac{\beta}{2} \hat{n}\cdot\vec{\sigma} + \cos\frac{\beta}{2} I + i\sin\frac{\beta}{2}\hat{n}\cdot\vec{\sigma} \\
&= 2\cos\frac{\beta}{2} I,
\end{aligned}
$$

and the result therefore does not depend on $|\psi\rangle$. Thus

$$
\begin{aligned}
E(R_{\hat{n}}(\alpha), R_{\hat{n}}(\alpha+\beta)) &= \sqrt{2 - 2\cos\frac{\beta}{2}} \\
&= \sqrt{2 - e^{i\beta/2} - e^{-i\beta/2}} \\
&= \sqrt{\left(1 - e^{i\beta/2}\right)\left(1 - e^{-i\beta/2}\right)} \\
&= |1 - \exp(i\beta/2)|.
\end{aligned}
$$

Given a tolerance $\epsilon > 0$ we can always find β such that $3|1 - \exp(i\beta/2)| < \epsilon$, and once an appropriate β is calculated we can always approximate $R_{\hat{n}}(\theta)^n \approx R_{\hat{n}}(\alpha+\beta)$ with arbitrary accuracy for some integer n, justifying Equation (4.76).

4.41

The action of the circuit is

$$
\begin{aligned}
|0\rangle|0\rangle|\psi\rangle &\xrightarrow{H\otimes H\otimes I} \frac{1}{2}\Big(|0\rangle|0\rangle + |0\rangle|1\rangle + |1\rangle|0\rangle + |1\rangle|1\rangle\Big)|\psi\rangle \\
&\xrightarrow{CCX} \frac{1}{2}\Big(|0\rangle|0\rangle + |0\rangle|1\rangle + |1\rangle|0\rangle\Big)|\psi\rangle + \frac{1}{2}|1\rangle|1\rangle\Big(X|\psi\rangle\Big) \\
&\xrightarrow{I\otimes I\otimes S} \frac{1}{2}\Big(|0\rangle|0\rangle + |0\rangle|1\rangle + |1\rangle|0\rangle\Big)S|\psi\rangle + \frac{1}{2}|1\rangle|1\rangle\Big(SX|\psi\rangle\Big) \\
&\xrightarrow{CCX} \frac{1}{2}\Big(|0\rangle|0\rangle + |0\rangle|1\rangle + |1\rangle|0\rangle\Big)S|\psi\rangle + \frac{1}{2}|1\rangle|1\rangle\Big(XSX|\psi\rangle\Big) \\
&\xrightarrow{H\otimes H\otimes I} \frac{1}{4}\Big(|0\rangle|0\rangle\big(3S + XSX\big)|\psi\rangle + |0\rangle|1\rangle\big(S - XSX\big)|\psi\rangle + |1\rangle|0\rangle\big(S - XSX\big)|\psi\rangle \\
&\qquad + |1\rangle|1\rangle\big(-S + XSX\big)|\psi\rangle\Big),
\end{aligned}
$$

meaning that, after the measurement, if we obtain $|0\rangle|0\rangle$ then

$$
\begin{aligned}
3S + XSX &= 3\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} + \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \\
&= \sqrt{10}\begin{bmatrix} \frac{3+i}{\sqrt{10}} & 0 \\ 0 & \frac{1+3i}{\sqrt{10}} \end{bmatrix}
\end{aligned}
$$

is applied to the third qubit. We can rewrite this operator as

$$\begin{aligned} 3S + XSX &= \sqrt{10}e^{i\phi} \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix} \\ &\implies \phi = \frac{1}{4}, \theta = \arccos\frac{3}{5} \\ &\implies \sqrt{10}e^{i\pi/4}R_z(\theta) \end{aligned}$$

that is, $R_z(\theta)$ is applied to the third qubit up to a global phase. Meanwhile, if we obtain any other result then the applied operator is

$$\begin{aligned} \pm(S - XSX) &= \pm\left(\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} - \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\right) \\ &= \pm\sqrt{2}\begin{bmatrix} \frac{1-i}{\sqrt{2}} & 0 \\ 0 & -\frac{1-i}{\sqrt{2}} \end{bmatrix} \\ &= \pm\sqrt{2}e^{-i\pi/4}Z, \end{aligned}$$

that is, Z up to a global phase. The probability of obtaining $|0\rangle|0\rangle$ is

$$\left|\frac{\sqrt{10}e^{i\pi/4}}{4}\right|^2 \langle 0|0\rangle\langle 0|0\rangle\left\langle\psi\middle|R_z^\dagger(\theta)R_z(\theta)\middle|\psi\right\rangle = \frac{5}{8}.$$

After the measurement is performed the result can be $|0\rangle|0\rangle(R_z(\theta)|\psi\rangle)$, $|0\rangle|1\rangle(Z|\psi\rangle)$, $|1\rangle|0\rangle(Z|\psi\rangle)$ or $|1\rangle|1\rangle(Z|\psi\rangle)$, so in order to guarantee that $R_z(\theta)$ is applied to the third qubit we must simply apply Z to the third qubit and X (remember that $X = HZH$) to any ancilla qubits that end up in state $|1\rangle$, and apply the same circuit again until we get $|0\rangle|0\rangle$ as result. The probability of not obtaining $|0\rangle|0\rangle$ after n repetitions of the circuit is $(3/8)^n$, which approaches zero for large n.

4.42

If θ is a rational multiple of 2π then it can be written as

$$\theta = \frac{a}{m} \times 2\pi,$$

where $a \in \mathbb{Z}$ and m is some positive integer. Thus

$$\begin{aligned} e^{i\theta m} = e^{ia\times 2\pi} = 1 \quad &\implies \quad \frac{(3+4i)^m}{5^m} = 1 \\ &\implies \quad (3+4i)^m = 5^m. \end{aligned}$$

We have that $(3+4i)^2 = -7+24i \equiv 3+4i \pmod 5$. By induction, it follows that $(3+4i)^m \equiv 3+4i \pmod 5$ for all integer $m > 0$, meaning there is no m that satisfies $(3+4i)^m = 5^m$, therefore θ must be an irrational multiple of 2π.

4.43

We can write any unitary as

$$U = R_z(\beta)R_x(\gamma)R_z(\delta),$$

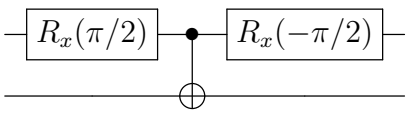
and analogously to the proof that Hadamard, phase, CNOT and $\pi/8$ form an universal set of gates, we have that it is possible to approximate any rotation $R_z(\alpha)$ with arbitrary precision as $R_z(\theta)^n$ for some integer n. Besides, notice that the circuit in Figure 4.17 can be used to perform $R_x(\theta)$ if we apply a Hadamard gate to the third qubit at the beggining and end of the circuit. So using only Hadamard, phase, CNOT and Toffoli gates we can perform any unitary

$$U = R_z(\theta)^{n_1}R_x(\theta)^{n_2}R_z(\theta)^{n_3}$$

for integers n_1, n_2 and n_3, meaning they form a set of universal gates.

4.44

We can approximate any rotation $R_x(\theta)$ with arbitrary precision as $R_x(\pi\alpha)^n$ for some integer n and irrational α. So, with gate G and ancilla qubits set to $|1\rangle$, we can generate $R_x(\theta)$, CNOT and Toffoli gates up to global phases. So from an initial two-qubit state $|0\rangle\,|0\rangle$ we may apply the circuit



,

with arbitrary precision, obtaining the transformation

$$\begin{aligned}
|0\rangle\,|0\rangle &\xrightarrow{R_x\otimes I} \frac{|0\rangle\,|0\rangle - i\,|1\rangle\,|0\rangle}{\sqrt{2}} \\
&\xrightarrow{CX} \frac{|0\rangle\,|0\rangle - i\,|1\rangle\,|1\rangle}{\sqrt{2}} \\
&\xrightarrow{R_x^\dagger\otimes I} \frac{|0\rangle\,|0\rangle + i\,|1\rangle\,|0\rangle + |0\rangle\,|1\rangle - i\,|1\rangle\,|1\rangle}{2} \\
&= \frac{1}{\sqrt{2}}\Big(\,|0\rangle\,|+\rangle + i\,|1\rangle\,|-\rangle\,\Big).
\end{aligned}$$

If we measure the first qubit, the second one is left in either the state $|+\rangle$ or $|-\rangle$, meaning we can indirectly perform Hadamard gates, and since $HR_x(\theta)H = R_z(\theta)$, we can perform any rotations $R_z(\theta)$. Thus we are able to reproduce any one-qubit gate as well as CNOT and Toffoli gates with arbitrary precision, so G is an universal gate.

4.45

H, S, CNOT and Toffoli gates, in matricial representation, all consist of matrices with complex integer entries. Any unitary U involving n qubits is represented by an $SU(2^n)$ matrix, meaning it is represented by a $2^n \times 2^n$ matrix, and since it is constructed with a tensor product of the four gates, all of its entries are also complex integers. And lastly, all four gates only contains 1, -1 and i, the

exception is the Hadamard gate, which is multiplied by $1/\sqrt{2} = 2^{-1/2}$. Thus if k Hadamard gates are necessary to create U, then it will have the form $2^{-k/2}M$, where M is a $2^n \times 2^n$ matrix with complex integer entries. And since it is possible to build the Toffoli gate using H, CNOT and the $\pi/8$ gate, this result should hold if we replace the Toffoli gate by the $\pi/8$ gate.

4.46

For one qubit, we need two real numbers to describe its amplitudes, that is

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle .$$

For n qubits we naturally need 2^n real numbers, so the $2^n \times 2^n$ density matrix will have $2^{2n} = 4^n$ independent real numbers. Lastly, we need to consider the normalization condition, that is, $\mathrm{tr}(\rho) = 1$, and this will account for $4^n - 1$ independent real numbers.

4.47

Let us start with the simplest case of $L = 2$, then

$$\begin{aligned} e^{-iHt} &= e^{-i(H_1+H_2)t} \\ &= \sum_{j=0}^{\infty} \frac{(-i)^j (H_1+H_2)^j t^j}{j!}. \end{aligned}$$

If $[H_1, H_2] = 0$, then we have

$$(H_1+H_2)^j = \sum_{k=0}^{j} \frac{j!}{k!(j-k)!} H_1^k H_2^{j-k}.$$

Substituting this result yields

$$\begin{aligned} e^{-iHt} &= \sum_{j=0}^{\infty}(-i)^j t^j \sum_{k=0}^{j} \frac{H_1^k}{k!}\frac{H_2^{j-k}}{(j-k)!} \\ &= \sum_{j=0}^{\infty}\sum_{k=0}^{j} \frac{(-i)^k H_1^k t^k}{k!}\frac{(-i)^{j-k} H_2^{j-k} t^{j-k}}{(j-k)!}. \end{aligned}$$

Since j runs from 0 to ∞, k also varies from 0 to ∞, as well as the difference $j - k \equiv l$, so we may rewrite this result as

$$\begin{aligned} e^{-iHt} &= \sum_{k=0}^{\infty}\sum_{l=0}^{\infty} \frac{(-i)^k H_1^k t^k}{k!}\frac{(-i)^l H_2^l t^l}{l!} \\ &= e^{-iH_1 t} e^{-iH_2 t}. \end{aligned}$$

If we make the replacement $H_1 + H_2 \to \sum_k^L H_k$ such that $[H_j, H_k]\ \forall\ j$ and k, this result should still hold by induction. Thus

$$e^{-iHt} = e^{-iH_1 t} e^{-iH_2 t} \cdots e^{-iH_L t}.$$

4.48

If all H_k involves at most c of the total n qubits, then there is roughly $n!/(n-c)! \leq n^c$ different possible H_k, meaning L is $O(n^c)$, that is, a polynomial in n.

4.49

$$\begin{aligned}
e^{(A+B)\Delta t} &= I + (A+B)\Delta t + \frac{(A+B)^2}{2!}\Delta t^2 + O\big(\Delta t^3\big) \\
&= \left[I + A\Delta t + \frac{A^2}{2!}\Delta t^2\right]\left[I + B\Delta t + \frac{B^2}{2!}\Delta t^2\right]\left[I - \frac{[A,B]}{2}\Delta t^2\right] + O\left(\Delta t^3\right) \\
&= \left[e^{A\Delta t} + O\big(\Delta t^3\big)\right]\left[e^{B\Delta t} + O\big(\Delta t^3\big)\right]\left[e^{-\frac{1}{2}[A,B]\Delta t^2} + O\big(\Delta t^4\big)\right] + O\big(\Delta t^3\big) \\
&= e^{A\Delta t} e^{B\Delta t} e^{-\frac{1}{2}[A,B]\Delta t^2} + O\big(\Delta t^3\big),
\end{aligned}$$

this is, Equation (4.105). Now, for Equation (4.103) we have

$$\begin{aligned}
e^{i(A+B)\Delta t} &= I + i(A+B)\Delta t + O\big(\Delta t^2\big) \\
&= [I + iA\Delta t]\,[I + iB\Delta t] + O\big(\Delta t^2\big) \\
&= \left[e^{iA\Delta t} + O\big(\Delta t^2\big)\right]\left[e^{iB\Delta t} + O\big(\Delta t^2\big)\right] + O(\Delta t^2) \\
&= e^{iA\Delta t} e^{iB\Delta t} + O\big(\Delta t^2\big).
\end{aligned}$$

And for Equation (4.104) we have

$$\begin{aligned}
e^{i(A+B)\Delta t} &= I + i(A+B)\Delta t + \frac{i^2(A+B)^2}{2!}\Delta t^2 + O\big(\Delta t^3\big) \\
&= \left[I + \frac{iA}{2}\Delta t + \frac{\frac{i^2A^2}{4}}{2!}\Delta t^2\right]\left[I + iB\Delta t + \frac{i^2B^2}{2!}\Delta t^2\right]\left[I + \frac{iA}{2}\Delta t + \frac{\frac{i^2A^2}{4}}{2!}\Delta t^2\right] + O\big(\Delta t^3\big) \\
&= \left[e^{iA\Delta t/2} + O\big(\Delta t^3\big)\right]\left[e^{iB\Delta t} + O\big(\Delta t^3\big)\right]\left[e^{iA\Delta t/2} + O\big(\Delta t^3\big)\right] + O\big(\Delta t^3\big) \\
&= e^{iA\Delta t/2} e^{iB\Delta t} e^{iA\Delta t/2} + O\big(\Delta t^3\big).
\end{aligned}$$

4.50

Multiplying both terms inside the square brackets yields

$$U_{\Delta t} = e^{-iH_1\Delta t} \cdots e^{-iH_{L-1}\Delta t} e^{-2iH_L\Delta t} e^{-iH_{L-1}\Delta t} \cdots e^{-iH_1\Delta t}.$$

Now we use the fact that

$$e^{-iH_{L-1}\Delta t} e^{-2iH_L\Delta t} e^{-iH_{L-1}\Delta t} = e^{-2i(H_L + H_{L-1})} + O\big(\Delta t^3\big)$$

$$\implies \quad U_{\Delta t} = e^{-iH_1\Delta t}\cdots e^{-iH_{L-2}\Delta t}\left[e^{-2i(H_L+H_{L-1})} + O\big(\Delta t^3\big)\right] e^{-iH_{L-2}\Delta t}\cdots e^{-iH_1\Delta t}.$$

If we apply this relation until we reach H_1, we get the result

$$\begin{aligned} U_{\Delta t} &= e^{-2i\sum_k^L H_k\Delta t} + O\big(\Delta t^3\big) \\ &= e^{-2iH\Delta t} + O\big(\Delta t^3\big). \end{aligned}$$

The error has an upper limit given by

$$E\big(U_{\Delta t}^m, e^{-2miH\Delta t}\big) \leq mE\big(U_{\Delta t}, e^{-2iH\Delta t}\big).$$

From the result obtained above we know that $E\big(U_{\Delta t}, e^{-2iH\Delta t}\big)$ is $O(\Delta t^3)$, that is, there is some constant α such that $E\big(U_{\Delta t}, e^{-2iH\Delta t}\big) = \alpha\Delta t^3$, meaning that

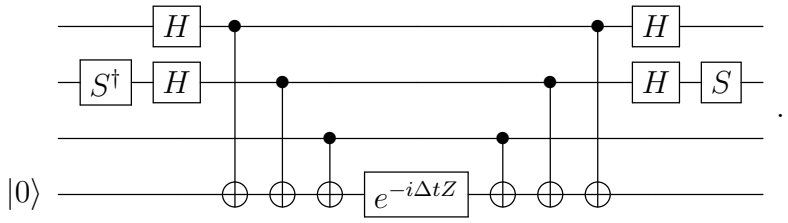
$$E\big(U_{\Delta t}^m, e^{-2miH\Delta t}\big) \leq m\alpha\Delta t^3.$$

4.51

Using the fact that $X = HZH$ and $Y = S^\dagger XS$, the Hamiltonian can be rewritten as

$$\begin{aligned} H &= H_1Z_1H_1 \otimes S_2^\dagger H_2Z_2H_2S_2 \otimes Z_3 \\ &= \Big(H_1 \otimes S_2^\dagger H_2 \otimes I_3\Big)\Big(Z_1 \otimes Z_2 \otimes Z_3\Big)\Big(H_1 \otimes H_2S_2 \otimes I_3\Big). \end{aligned}$$

That is, if we apply the H, $S^\dagger$ and S gates to the first and second qubits at the beginning and end of the circuit, the effective Hamiltonian that must be implemented is the $Z_1 \otimes Z_2 \otimes Z_3$. Thus, a possible circuit to implement the Hamiltonian H is



5 The quantum Fourier transform and its applications

Exercises: 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7, 5.8, 5.9, 5.10, 5.11, 5.12, 5.13, 5.14, 5.15, 5.16, 5.17, 5.18, 5.19, 5.20, 5.21, 5.22, 5.23, 5.24, 5.25, 5.26, 5.27, 5.28, 5.29.

5.1

The transformation is unitary if and only if the resulting states $|j\rangle$ are such that $\langle j'|j\rangle = \delta_{jj'}$.

$$\langle j'|j\rangle = \left(\frac{1}{\sqrt{N}}\sum_{k=0}^{N-1} e^{-2\pi ij'k/N}\langle k|\right)\left(\frac{1}{\sqrt{N}}\sum_{l=0}^{N-1} e^{2\pi ijl/N}|l\rangle\right)$$

$$= \frac{1}{N} \sum_{k=0}^{N-1} \sum_{l=0}^{N-1} e^{2\pi i(jl-j'k)/N} \langle k|l\rangle$$
$$= \frac{1}{N} \sum_{k=0}^{N-1} e^{2\pi ik(j-j')/N} = \delta_{jj'}.$$

5.2

$$|00\cdots0\rangle \longrightarrow \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{2\pi i(k\times0)/2^n} |k\rangle$$
$$= \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} |k\rangle ,$$

where k inside the *ket* should be written in its binary representation.

5.3

In order to calculate one y_k we need to execute 2^n sum operations, and since there are 2^n different y_k, roughly $2^n \times 2^n = \Theta(2^{2n})$ arithmetic operations are necessary in order to perform the Fourier transform on a classical computer.

The quantum Fourier transform could be calculated more efficiently using the binary fractions, represented by the coefficients $0.j_l j_{l+1} \cdots j_m$. According to Equation (5.4), we need the coefficients from $0.j_n$ up to $0.j_1 j_2 \cdot j_n$. We can calculate them through the iteration

$$\begin{aligned} 0.j_n &= \frac{j_n}{2}, \\ 0.j_{n-1}j_n &= \frac{j_{n-1}}{2} + \frac{0.j_n}{2}, \\ &\vdots \\ 0.j_1 j_2 \cdots j_n &= \frac{j_1}{2} + \frac{0.j_2 \cdots j_n}{2}. \end{aligned}$$

There are n coefficients and $n-1$ steps, at each step we divide by 2 and add a term, meaning there are two arithmetic operations per step, so we need roughly $2(n-1)$ operations to calculate one of the 2^n different $|j_1, \cdots, j_n\rangle$, resulting in $2(n-1) \times 2^n$ operations, that is, $\Theta(n2^n)$.

5.4

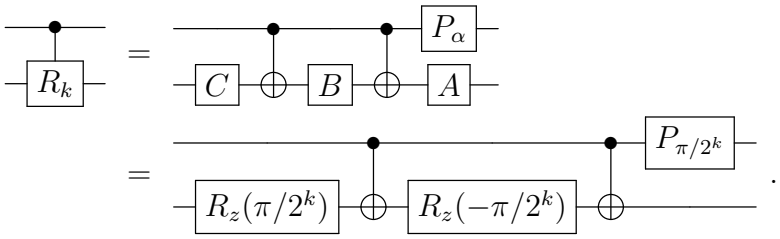
We must find A, B, C and α such that $R_k = e^{i\alpha} AXBXC$ and $ABC = I$ (see Exercise 4.12).

$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix} = \begin{bmatrix} e^{i(\alpha-\beta/2-\delta/2)} \cos\frac{\gamma}{2} & -e^{i(\alpha-\beta/2+\delta/2)} \sin\frac{\gamma}{2} \\ e^{i(\alpha+\beta/2-\delta/2)} \sin\frac{\gamma}{2} & e^{i(\alpha+\beta/2+\delta/2)} \cos\frac{\gamma}{2} \end{bmatrix}$$
$$\Longrightarrow \alpha = \frac{\pi}{2^k}, \beta = 0, \gamma = 0, \delta = \frac{\pi}{2^{k-1}}.$$

Therefore the operators are given by

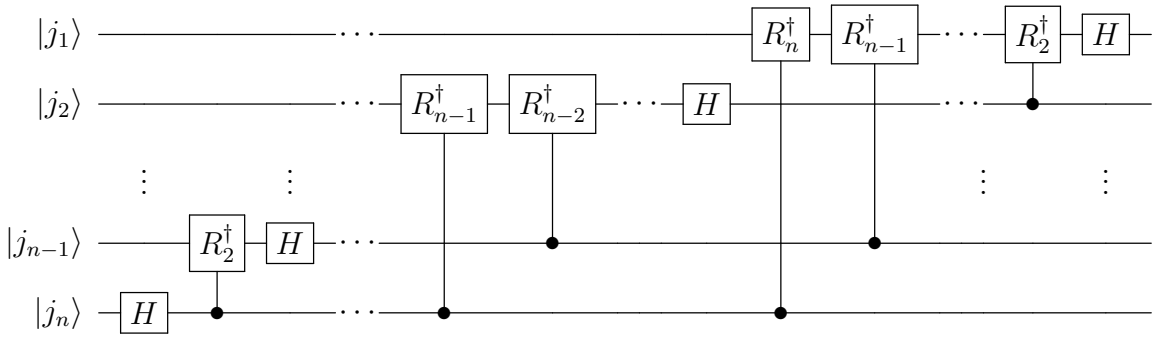
$$
\begin{aligned}
A &= R_z(\beta)R_y(\gamma/2) = I, \\
B &= R_y(-\gamma/2)R_z(-(\delta+\beta)/2) = R_z(-\pi/2^k), \\
C &= R_z((\delta-\beta)/2) = R_z(\pi/2^k).
\end{aligned}
$$

And the controlled-R_k gate can thus be decomposed as (see Exercise 4.22)



5.5

It is just the inverse circuit of the one shown in Figure 5.1. So omitting the SWAP gates at the start of the circuit, for simplicity, we have



5.6

We can decompose the quantum Fourier transform on n qubits into N gates, where N scales as $\Theta(n^2)$. We are then considering that $U = \prod_{j=1}^{N} U_j$ and $V = \prod_{j=1}^{N} V_j$. The application of each V_j contributes roughly to an error of $E(U_j, V_j)$ that scales as $\Theta(1/p(n))$. This means that there are constants α and β such that $N = \alpha n^2$ and $E(U_j, V_j) = \beta/p(n)$. The error associated with the quantum Fourier transform has a rough upper limit given by

$$
E(U, V) \leq NE(U_j, V_j) = \alpha\beta\frac{n^2}{p(n)},
$$

meaning that $E(U, V)$ scales as $\Theta(n^2/p(n))$.

5.7

For an arbitrary state $|j\rangle$, we may write it as $|j_0, \cdots, j_{t-1}\rangle$, where each j_k is either 0 or 1. The sequence of controlled-U operations consists in applying the controlled-U^{2^k} using the qubit in state $|j_{t-1-k}\rangle$ as control, from $k = 0$ to $k = t - 1$. With that, each operation is effectively an unitary

$U^{j_{t-1-k}2^k}$ being applied on $|u\rangle$. So the action of the circuit is

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

But $\sum_{l=0}^{t-1} j_l 2^{t-1-l}$ is precisely the number j decomposed as a sum of its binary digits multiplied by the correspondent powers of two, thus the action of the circuit is effectively

$$|j\rangle\,|u\rangle \longrightarrow |j\rangle\,U^j\,|u\rangle\,.$$

5.8

If the final state is $\sum_u c_u\,|\widetilde{\varphi_u}\rangle\,|u\rangle$ then the probability of measuring $\widetilde{\varphi_u}$, such that $\widetilde{\varphi_u}$ is close to φ to an accuracy of n bits, that is, $e = 2^{t-n} - 1$, is given by

$$P = |c_u|^2 p(|\widetilde{\varphi_u} - \varphi| > e),$$

where $p(|\widetilde{\varphi_u} - \varphi| > e)$ is the probability that, given that $\widetilde{\varphi_u}$ was measured, it is a value sufficiently close to φ. Since the probability that the condition is not satisfied is upper bounded by $1/(2(e-1))$, the probability of success is such that

$$\begin{aligned} p(|\widetilde{\varphi_u} - \varphi| > e) &\geq 1 - \frac{1}{2(e-1)} \\ &= 1 - \frac{1}{2(2^{t-n}-2)}. \end{aligned}$$

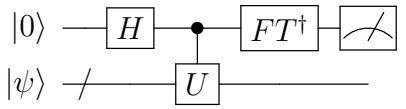
By choosing t according to Equation (5.35) we have

$$\begin{aligned} p(|\widetilde{\varphi_u} - \varphi| > e) &\geq 1 - \frac{1}{2\left(2^{\lceil \log\left(2+\frac{1}{2\epsilon}\right)\rceil} - 2\right)} \\ &\geq 1 - \frac{1}{2\left(2 + \frac{1}{2\epsilon} - 2\right)} \\ &= 1 - \epsilon \end{aligned}$$

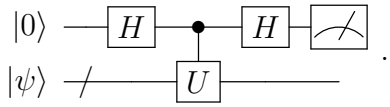
$$\implies \quad P \geq |c_u|^2(1-\epsilon).$$

5.9

Since there are only two possible eigenvalues: ± 1, only one ancilla qubit initialized to $|0\rangle$ is necessary. So the phase estimation algorithm applied to this problem should read



The quantum Fourier transform (as well as its inverse) of a single qubit is just a Hadamard gate, so the circuit is just



This is the exact same circuit as that of Exercise 4.34. If the classical register reads 0 then $|\psi\rangle$ collapsed to the eigenspace associated with eigenvalue +1 and, on the other hand, if it reads 1 then it collapsed to the other eigenspace.

5.10

$$\begin{aligned}
5^1 &= 5 \equiv 5 \pmod{21},\\
5^2 &= 25 \equiv 4 \pmod{21},\\
5^3 &= 125 \equiv 20 \pmod{21},\\
5^4 &= 625 \equiv 16 \pmod{21},\\
5^5 &= 3125 \equiv 17 \pmod{21},\\
5^6 &= 15625 \equiv 1 \pmod{21}.
\end{aligned}$$

5.11

Let us consider the list $\left\{x^0, x^1, \cdots, x^N\right\}$ modulo N. There are at most N different integers in this list, but it contains $N+1$ elements, therefore, at least one of these numbers must appear twice in the list. This means that we always have two numbers a and b, satisfying $a < b$ and $b \leq N$, such that $x^b \equiv x^a \pmod{N}$. Which implies

$$x^{b-a} \equiv 1 \pmod{N}.$$

So the order of x modulo N is some number r such that $r \leq b - a$, and since both, a and b, satisfy $a < N$ and $b \leq N$, we must have $r \leq N$.

5.12

Since U is effectively the identity operator for $N \leq y \leq 2^L - 1$, it is obviously unitary for this case. Now, for $0 \leq y \leq N-1$, U is unitary if and only if $\left\langle y' \middle| U^\dagger U \middle| y \right\rangle = \delta_{yy'}$.

$$\left\langle y' \middle| U^\dagger U \middle| y \right\rangle = \langle xy' \pmod{N} \,|\, xy \pmod{N} \rangle .$$

Since x is co-prime to N then there is an inverse x^{-1} such that $xx^{-1} \equiv 1 \pmod{N}$. This means that $xy \pmod{N} \equiv xy$ and $xy' \pmod{N} \equiv xy'$. Thus

$$\left\langle y' \middle| U^\dagger U \middle| y \right\rangle = \langle xy' \,|\, xy \rangle = \delta_{yy'}.$$

5.13

$$\begin{aligned}\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|u_s\rangle &= \frac{1}{r}\sum_{s=0}^{r-1}\sum_{k=0}^{r-1}\exp\left(-\frac{2\pi isk}{r}\right)|x^k \pmod N\rangle \\ &= \frac{1}{r}\sum_{k=0}^{r-1} r\delta_{k0}\,|x^k \pmod N\rangle \\ &= |x^0 \pmod N\rangle = |1\rangle\,.\end{aligned}$$

Or equivalently

$$\begin{aligned}\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}\exp\left(\frac{2\pi isk}{r}\right)|u_s\rangle &= \frac{1}{r}\sum_{s=0}^{r-1}\sum_{l=0}^{r-1}\exp\left(\frac{2\pi is(k-l)}{r}\right)|x^l \pmod N\rangle \\ &= \sum_{l=0}^{r-1}\delta_{kl}\,|x^l \pmod N\rangle \\ &= |x^k \pmod N\rangle\,.\end{aligned}$$

5.14

If we initialize the second register in the state $|0\rangle$ we get

$$\begin{aligned}V|j\rangle|0\rangle &= |j\rangle|0 + x^j \pmod N\rangle \\ &= |j\rangle|x^j \pmod N\rangle\,.\end{aligned}$$

This is the same result we would get if we had used U^j and initialized the second register in the state $|1\rangle$. **Incomplete...**

5.15

We may write x and y as the product of their prime factors, that is

$$\begin{aligned}x &= q_1^{m_1}q_2^{m2}\cdots, \\ y &= q_1^{n_1}q_2^{n_2}\cdots,\end{aligned}$$

where q_i is the i-th prime number. The lcm and gcd of both can be calculated, respectively, as

$$\begin{aligned}\mathrm{lcm}(x,y) &= \prod_i q_i^{\max\{m_i,n_i\}}, \\ \gcd(x,y) &= \prod_i q_i^{\min\{m_i,n_i\}}.\end{aligned}$$

Multiplying both quantities gives us

$$\mathrm{lcm}(x,y)\times\gcd(x,y) = \prod_i q_i^{\max\{m_i,n_i\}}\times q_i^{\min\{m_i,n_i\}}$$

$$= \prod_i q_i^{\max\{m_i,n_i\}+\min\{m_i,n_i\}}.$$

But for all i, it is a fact that $\max\{m_i, n_i\} + \min\{m_i, n_i\} = m_i + n_i$, thus

$$\begin{aligned}\operatorname{lcm}(x,y) \times \gcd(x,y) &= \prod_i q_i^{m_i+n_i} \\ &= q_1^{m_1+n_1} q_2^{m_2+n_2} \cdots \\ &= (q_1^{m_1} q_2^{m_2} \cdots)\,(q_1^{n_1} q_2^{n_2} \cdots) \\ &= xy\end{aligned}$$

$$\implies \quad \operatorname{lcm}(x,y) = \frac{xy}{\gcd(x,y)}.$$

The gcd can be computed using Euclid's algorithm. This algorithm involves operations that are no harder than arithmetic multiplication, which can be calculated at a cost of $O(L^2)$ for two L bit numbers, thus the lcm can be computed in $O(L^2)$ operations.

5.16

$$\int_x^{x+1} \frac{1}{y^2}\,\mathrm{d}y = \frac{1}{x^2+x}.$$

It is a fact that $x^2 \geq 2x$ for $x \geq 2$, thus using this condition we have

$$\frac{1}{x^2+x} = \frac{2}{2x^2+2x} \geq \frac{2}{2x^2+x^2} = \frac{2}{3x^2} \quad \implies \quad \int_x^{x+1} \frac{1}{y^2}\,\mathrm{d}y \geq \frac{2}{3x^2} \quad \text{for } x \geq 2.$$

From this result we conclude that

$$\frac{1}{x^2} \leq \frac{3}{2}\int_x^{x+1} \frac{1}{y^2}\,\mathrm{d}y.$$

If we denote the i-th prime number as q_i then this relation is still valid if we substitute x by any prime number since the smallest prime is 2. That is, for all i it is true that

$$\frac{1}{q_i^2} \leq \frac{3}{2}\int_{q_i}^{q_i+1} \frac{1}{y^2}\,\mathrm{d}y \leq \frac{3}{2}\int_{q_i}^{q_{i+1}} \frac{1}{y^2}\,\mathrm{d}y,$$

where in the last inequality we used the fact that $q_{i+1} \geq q_i + 1$ for all prime numbers. Now we must simply sum for all primes on both sides, that is

$$\begin{aligned}\frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{5^2} + \cdots &\leq \frac{3}{2}\left(\int_2^3 \frac{1}{y^2}\,\mathrm{d}y + \int_3^5 \frac{1}{y^2}\,\mathrm{d}y + \int_5^7 \frac{1}{y^2}\,\mathrm{d}y + \cdots\right) \\ &\Downarrow \\ \sum_q \frac{1}{q^2} &\leq \frac{3}{2}\int_2^\infty \frac{1}{y^2}\,\mathrm{d}y = \frac{3}{4}.\end{aligned}$$

Now, since

$$1 - \sum_q p(q|s_1')p(q|s_2') \geq 1 - \sum_q \frac{1}{q^2},$$

and $\sum_q 1/q^2 \leq 3/4$, Equation (5.58) follows immediately, that is

$$1 - \sum_q p(q|s_1')p(q|s_2') \geq 1 - \frac{3}{4} = \frac{1}{4}.$$

5.17

(1) If $a > 1$ is ℓ bits long, then a^b will be, at most, $b\ell$ bits long. And since $a^b = N$, which is L bits long, we have $b\ell = L$ and thus $b \leq L$.

(2) **Incomplete...**

5.18

$N = 91$ is not even, so the first step would not return 2, and knowing that 91 is composed of different primes (a little bit of cheating) we can safely say that the second step would return *false*. In step 3 we choose 4, co-prime to 91, then we have

$$\begin{aligned}
4^1 &= 4 \equiv 4 \pmod{91},\\
4^2 &= 16 \equiv 16 \pmod{91},\\
4^3 &= 64 \equiv 64 \pmod{91},\\
4^4 &= 256 \equiv 74 \pmod{91},\\
4^5 &= 1024 \equiv 23 \pmod{91},\\
4^6 &= 4096 \equiv 1 \pmod{91}.
\end{aligned}$$

So we have that $r = 6$ is the order of 4 modulo 91. Now

$$x^{r/2} = 4^3 = 64 \pmod{91} \neq -1 \pmod{91},$$

and as the last step we calculate $\gcd(64 - 1, 91) = 7$, which is indeed a prime factor of 91 since its prime factorization is $91 = 7 \times 13$.

5.19

For the order-finding subroutine to be required, the number must not have 2 as a prime factor, and it must have at least two different prime numbers in its decomposition. So the smallest such number must be the product of the two first primes next to 2, that is $3 \times 5 = 15$.

5.20

**From errata:* $\sqrt{N/r}$ should be N/r.

Since $f(x+r) = f(x)$ we may rewrite

$$\begin{aligned}\hat{f}(\ell) &= \frac{1}{\sqrt{N}} \sum_{k\in\{0,r,\cdots,N-r\}} e^{-2\pi i\ell k/N} f(0) + \cdots + \frac{1}{\sqrt{N}} \sum_{k\in\{r-1,2r-1,\cdots,N-1\}} e^{-2\pi i\ell k/N} f(r-1) \\ &= \frac{1}{\sqrt{N}} \sum_{k\in\{0,r,\cdots,N-r\}} e^{-2\pi i\ell k/N} \left[f(0) + e^{-2\pi i\ell/N} f(1) + \cdots + e^{-2\pi i\ell(r-1)} f(r-1)\right].\end{aligned}$$

To relate this result to Equation (5.63) let us first denote the functions as states, that is, $\hat{f}(\ell) \to |\hat{f}(\ell)\rangle$ and $f(x) \to |f(x)\rangle$. We also have to use the fact that

$$\sum_{k\in\{0,r,\cdots,N-r\}} e^{-2\pi i\ell k/N} = \begin{cases} N/r & ; \text{ if } \ell \text{ is an integer multiple of } N/r \\ 1 & ; \text{ otherwise} \end{cases}.$$

Thus

$$\begin{aligned}|\hat{f}(\ell)\rangle &= \frac{1}{\sqrt{N}} \frac{N}{r} \left[|f(0)\rangle + e^{-2\pi i\ell/N} f(1) + \cdots + e^{-2\pi i\ell(r-1)/N} |f(r-1)\rangle\right] \\ &= \frac{\sqrt{N}}{r} \sum_{x=0}^{r-1} e^{-2\pi i\ell x/N} |f(x)\rangle.\end{aligned}$$

Considering that N is an integer multiple of the period r, the result coincides with Equation (5.63) if we take the case where the proportion relation is just $N = r$.

5.21

(1) Applying U_y to the states $|\hat{f}(\ell)\rangle$ yields

$$\begin{aligned}U_y |\hat{f}(\ell)\rangle &= \frac{1}{\sqrt{r}} \sum_{x=0}^{r-1} e^{-2\pi i\ell x/r} U_y |f(x)\rangle \\ &= \frac{1}{\sqrt{r}} \sum_{x=0}^{r-1} e^{-2\pi i\ell x/r} |f(x+y)\rangle.\end{aligned}$$

Now, if $x+y < r$ then we may just call it $x' \coloneqq x+y$, otherwise, we may also write it as $x+y = x'+\alpha r$, where α is some positive integer, so in any case, we can always use $f(x+y) \to f(x')$ and perform the variable substitution $x \to x' - y$, yielding

$$\begin{aligned}U_y |\hat{f}(\ell)\rangle &= \frac{1}{\sqrt{r}} \sum_{x'=y}^{r+y-1} e^{-2\pi i\ell(x'-y)/r} |f(x')\rangle \\ &= e^{2\pi i\ell y/r} \frac{1}{\sqrt{r}} \sum_{x'=y}^{r+y-1} e^{-2\pi i\ell x'/r} |f(x')\rangle.\end{aligned}$$

Because of the periodicity of $f(x)$, the terms for $x' > r-1$ will be the same as terms for $0 \le x' < y$ and therefore

$$\begin{aligned} U_y \left|\hat{f}(\ell)\right\rangle &= e^{2\pi i \ell y/r} \frac{1}{\sqrt{r}} \sum_{x'=0}^{r-1} e^{-2\pi i \ell x'/r} \left|f(x')\right\rangle \\ &= e^{2\pi i \ell y/r} \left|\hat{f}(\ell)\right\rangle . \end{aligned}$$

(2) U_y will just add an immaterial phase, that will not affect the probability of measurement outcomes. Explicitly we have

$$\begin{aligned} U_y \left|f(x_0)\right\rangle &= \frac{1}{\sqrt{r}} \sum_{\ell=0}^{r-1} e^{2\pi i x_0 \ell/r} U_y \left|\hat{f}(\ell)\right\rangle \\ &= \frac{1}{\sqrt{r}} \sum_{\ell=0}^{r-1} e^{2\pi i (x_0+y) \ell/r} U_y \left|\hat{f}(\ell)\right\rangle . \end{aligned}$$

In the period-finding protocol, in step 3, if we were to apply U_y instead of U we would obtain

$$\frac{e^{2\pi i \ell y/r}}{\sqrt{r 2^t}} \sum_{\ell=0}^{r-1} \sum_{x=0}^{2^t-1} e^{2\pi i \ell x/r} \left|x\right\rangle \left|\hat{f}(\ell)\right\rangle ,$$

and after the $QFT^\dagger$ we would have

$$\frac{1}{\sqrt{r}} \sum_{\ell=0}^{r-1} e^{2\pi i \ell y/r} \left|\widetilde{\ell/r}\right\rangle \left|\hat{f}(\ell)\right\rangle .$$

The overall phase does not affect the outcome probabilities, so U_y can be used to realize the black box, which is just as good as U.

5.22

*It seems there is an $1/r$ factor missing in the first equality and an extra $1/\sqrt{r}$ in the second one.

The first step is simply the Fourier transform on two variables:

$$\begin{aligned} \left|\hat{f}(\ell_1, \ell_2)\right\rangle &= \sum_{x_1=0}^{r-1} \sum_{x_2=0}^{r-1} \frac{1}{\sqrt{r}} e^{-2\pi i \ell_1 x_1/r} \frac{1}{\sqrt{r}} e^{-2\pi i \ell_2 x_2/r} \left|f(x_1, x_2)\right\rangle \\ &= \frac{1}{r} \sum_{x_1=0}^{r-1} \sum_{x_2=0}^{r-1} e^{-2\pi i (\ell_1 x_1 + \ell_2 x_2)/r} \left|f(x_1, x_2)\right\rangle . \end{aligned}$$

Now we use the periodicity property of the function, that is $f(x_1, x_2) = f(0, x_2 + s x_1)$, and get

$$\left|\hat{f}(\ell_1, \ell_2)\right\rangle = \frac{1}{r} \sum_{x_1=0}^{r-1} \sum_{x_2=0}^{r-1} e^{-2\pi i (\ell_1 x_1 + \ell_2 x_2)/r} \left|f(0, x_2 + s x_1)\right\rangle .$$

Making the variable substitution $x_2 \to j - sx_1$ yields

$$\begin{aligned}|\hat{f}(\ell_1,\ell_2)\rangle &= \frac{1}{r}\sum_{x_1=0}^{r-1}\sum_{j=sx_1}^{r-1+sx_1} e^{-2\pi i(\ell_1 x_1+\ell_2 j-\ell_2 s x_1)/r}\,|f(0,j)\rangle \\ &= \frac{1}{r}\sum_{x_1=0}^{r-1} e^{-2\pi i(\ell_1/s-\ell_2)sx_1/r}\sum_{j=sx_1}^{r-1+sx_1} e^{-2\pi i\ell_2 j/r}\,|f(0,j)\rangle\,.\end{aligned}$$

The first sum results in r, and because of the periodicity of $f(x_1,x_2)$, the terms for $j > r-1$ will be the same as terms for $0 \le j < sx_1$, so the result is

$$|\hat{f}(\ell_1,\ell_2)\rangle = \sum_{j=0}^{r-1} e^{-2\pi i\ell_2 j/r}\,|f(0,j)\rangle$$

5.23

*Just like in the last exercise, we should remove the $1/\sqrt{r}$ factor from Equation (4.70). Also, there should not be a minus sign in the exponential.

$$\frac{1}{r}\sum_{\ell_1=0}^{r-1}\sum_{\ell_2=0}^{r-1} e^{2\pi i(\ell_1 x_1+\ell_2 x_2)/r}\,|\hat{f}(\ell_2,\ell_2)\rangle = \frac{1}{r}\sum_{\ell_1=0}^{r-1}\sum_{\ell_2=0}^{r-1}\sum_{j=0}^{r-1} e^{2\pi i(\ell_1 x_1+\ell_2 x_2-\ell_2 j)/r}\,|f(0,j)\rangle\,.$$

Using the constraint that $\ell_1/s - \ell_2$ is an integer multiple of r we may write $\ell_1 = s(\alpha r + \ell_2)$, where α is an integer. Substituting in the relation yields

$$\begin{aligned}\frac{1}{r}\sum_{\ell_1=0}^{r-1}\sum_{\ell_2=0}^{r-1} e^{2\pi i(\ell_1 x_1+\ell_2 x_2)/r}\,|\hat{f}(\ell_2,\ell_2)\rangle &= \frac{1}{r}\sum_{\ell_2=0}^{r-1}\sum_{j=0}^{r-1} e^{2\pi i(s\alpha r x_1+s\ell_2 x_1+\ell_2 x_2-\ell_2 j)/r}\,|f(0,j)\rangle \\ &= \frac{1}{r}e^{2\pi i s\alpha r x_1}\sum_{\ell_2=0}^{r-1}\sum_{j=0}^{r-1} e^{2\pi i(sx_1+x_2-j)\ell_2/r}\,|f(0,j)\rangle\,.\end{aligned}$$

In this expression, $e^{2\pi i s\alpha r x_1}$ is just an immaterial global phase, and the sum over ℓ_2 can be identified with a Kronecker delta as $\frac{1}{r}\sum_{\ell_2=0}^{r-1} e^{2\pi i(sx_1+x_2-j)\ell_2/r} = \delta_{j,sx_1+x_2}$, thus

$$\begin{aligned}\frac{1}{r}\sum_{\ell_1=0}^{r-1}\sum_{\ell_2=0}^{r-1} e^{2\pi i(\ell_1 x_1+\ell_2 x_2)/r}\,|\hat{f}(\ell_2,\ell_2)\rangle &= \sum_{j=0}^{r-1}\delta_{j,sx_1+x_2}\,|f(0,j)\rangle \\ &= |f(0,sx_1+x_2)\rangle \\ &= |f(x_1,x_2)\rangle\,.\end{aligned}$$

5.24

Applying the continued fractions algorithm to the first and second registers we can obtain, respectively, fractions $a_1/b_1 \approx \widetilde{s\ell_2/r}$ and $a_2/b_2 \approx \widetilde{\ell_2/r}$, so computing $(a_1 b_2)/(b_1 a_2)$ results in s.

5.25

-

5.26

-

5.27

-

5.28

-

5.29

-

6 Quantum search algorithms

Exercises: 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 6.10, 6.11, 6.12, 6.13, 6.14, 6.15, 6.16, 6.17, 6.18, 6.19, 6.20.

6.1

The operator consists in adding a phase -1 to all states except $|0\rangle$, therefore it has the form

$$\begin{aligned} |0\rangle\langle 0| - \sum_{x=1}^{N-1} |x\rangle\langle x| &= 2\,|0\rangle\langle 0| - \sum_{x=0}^{N-1} |x\rangle\langle x| \\ &= 2\,|0\rangle\langle 0| - I. \end{aligned}$$

6.2

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

6.3

The choice $\sin\theta = 2\sqrt{M(N-M)}/N$ is compatible with Equation (6.10) since

$$\sin\theta = 2\sin\frac{\theta}{2}\cos\frac{\theta}{2} \quad \Longrightarrow \quad \sin\frac{\theta}{2} = \sqrt{\frac{M}{N}} \text{ and } \cos\frac{\theta}{2} = \sqrt{\frac{N-M}{N}},$$

so we may indeed write the initial state $|\psi\rangle$ as

$$|\psi\rangle = \cos\frac{\theta}{2}|\alpha\rangle + \sin\frac{\theta}{2}|\beta\rangle.$$

Now we must only show that, defining G as in Equation (6.13), we can get the state $\cos\frac{3\theta}{2}|\alpha\rangle + \sin\frac{3\theta}{2}|\alpha\rangle|\beta\rangle$, as can be directly verified

$$G|\psi\rangle = \begin{bmatrix}\cos\theta & -\sin\theta \\ \sin\theta & \cos\theta\end{bmatrix}\begin{bmatrix}\cos\frac{\theta}{2} \\ \sin\frac{\theta}{2}\end{bmatrix} = \begin{bmatrix}\cos\theta\cos\frac{\theta}{2} - \sin\theta\sin\frac{\theta}{2} \\ \sin\theta\cos\frac{\theta}{2} + \cos\theta\sin\frac{\theta}{2}\end{bmatrix} = \begin{bmatrix}\cos\frac{3\theta}{2} \\ \sin\frac{3\theta}{2}\end{bmatrix}.$$

6.4

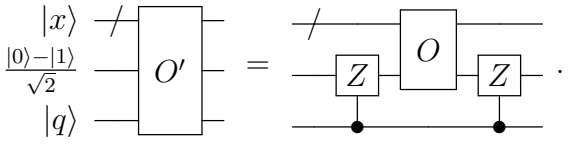
If $1 < M < N/2$ then by the end of step 3 we will have a state which is approximatelly given by

$$\frac{1}{\sqrt{M}}\sum_{j=0}^{M-1}|x_j\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right],$$

that is, a linear combination of the possible solutions $\{|x_0\rangle, \cdots, |x_{M-1}\rangle\}$, each with equal probability of being measured in step 4. So the only difference is that we would need to run the algorithm several times. After the algorithm is executed M times we have a probability of around $M!/M^M$ of having obtained all solutions x_j.

6.5

Notice that if instead of $|x\rangle(|0\rangle - |1\rangle)/\sqrt{2}$ we use $|x\rangle(|0\rangle + |1\rangle)/\sqrt{2}$ then the oracle will not do anything to the state, independently of x being a solution or not. So we may just apply a Z gate, conditioned to qubit $|q\rangle$, to the oracle qubit before and after calling the oracle O, that is



6.6

Considering that the two qubits are in a (normalized) superposition of all four possible states, given by $|\Psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$, the action of the circuit is

$$\begin{aligned}|\Psi\rangle &\xrightarrow{X\otimes X} a|11\rangle + b|10\rangle + c|01\rangle + d|00\rangle \\ &\xrightarrow{I\otimes H} a\frac{|10\rangle - |11\rangle}{\sqrt{2}} + b\frac{|10\rangle + |11\rangle}{\sqrt{2}} + c\frac{|00\rangle - |01\rangle}{\sqrt{2}} + d\frac{|00\rangle + |01\rangle}{\sqrt{2}}\end{aligned}$$

$$
\begin{aligned}
&\xrightarrow{CX_{(1,2)}} a\frac{|11\rangle - |10\rangle}{\sqrt{2}} + b\frac{|11\rangle + |10\rangle}{\sqrt{2}} + c\frac{|00\rangle - |01\rangle}{\sqrt{2}} + d\frac{|00\rangle + |01\rangle}{\sqrt{2}} \\
&\xrightarrow{I\otimes H} -a\,|11\rangle + b\,|10\rangle + c\,|01\rangle + d\,|00\rangle \\
&\xrightarrow{X\otimes X} -a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle \\
&\qquad = (-1)\Big(a\,|00\rangle - b\,|01\rangle - c\,|10\rangle - d\,|11\rangle\Big) \\
&\qquad = (-1)\Big(2a\,|00\rangle - |\Psi\rangle\Big) \\
&\qquad = (-1)\Big(2\,|00\rangle\langle 00| - I\Big)\,|\Psi\rangle\,.
\end{aligned}
$$

6.7

*It seems the phase gates should be with $-i\Delta t$ instead of $i\Delta t$.

First let us write the operations $\exp(-i\,|x\rangle\langle x|\,\Delta t)$ and $\exp(-i\,|\psi\rangle\langle\psi|\,\Delta t)$ explicitly:

$$
\begin{aligned}
\exp(-i\,|x\rangle\langle x|\,\Delta t) &= I + \sum_{j=1}^{\infty} \frac{(-i\Delta t)^j}{j!}\,|x\rangle\langle x| \\
&= I - |x\rangle\langle x| + \sum_{j=0}^{\infty} \frac{(-i\Delta t)^j}{j!}\,|x\rangle\langle x| \\
&= |y\rangle\langle y| + e^{-i\Delta t}\,|x\rangle\langle x|\,,
\end{aligned}
$$

$$
\begin{aligned}
\exp(-i\,|\psi\rangle\langle\psi|\,\Delta t) &= I + \sum_{j=1}^{\infty} \frac{(-i\Delta t)^j}{j!}\,|\psi\rangle\langle\psi| \\
&= I - |\psi\rangle\langle\psi| + \sum_{j=0}^{\infty} \frac{(-i\Delta t)^j}{j!}\,|\psi\rangle\langle\psi| \\
&= I + \left(e^{-i\Delta t} - 1\right)|\psi\rangle\langle\psi|\,.
\end{aligned}
$$

Now we can verify that the circuit in Figure 6.4 acts as

$$
\begin{aligned}
|y\rangle\,|0\rangle &= \Big(\,|x\rangle\langle x| + |y\rangle\langle y|\,\Big)\,|y\rangle\,|0\rangle \\
&= \langle x|y\rangle\,|x\rangle\,|0\rangle + |y\rangle\,|0\rangle \\
&\xrightarrow{\text{Oracle}} \langle x|y\rangle\,|x\rangle\,|1\rangle + |y\rangle\,|0\rangle \\
&\xrightarrow{I^{\otimes n}\otimes P_{-\Delta t}} e^{-i\Delta t}\,\langle x|y\rangle\,|x\rangle\,|1\rangle + |y\rangle\,|0\rangle \\
&\xrightarrow{\text{Oracle}} e^{-i\Delta t}\,\langle x|y\rangle\,|x\rangle\,|0\rangle + |y\rangle\,|0\rangle \\
&= \Big(\,|y\rangle\langle y| + e^{-i\Delta t}\,|x\rangle\langle x|\,\Big)\,|y\rangle\,|0\rangle\,,
\end{aligned}
$$

and the circuit in Figure 6.5 performs

$$
|y\rangle\,|0\rangle = \left(\sum_{j=0}^{N} |j\rangle\langle j|\,\right)|y\rangle\,|0\rangle
$$

$$
\begin{aligned}
&= \sum_{j=0}^{N-1} \langle j|y\rangle \, |j\rangle \, |0\rangle \\
&\xrightarrow{H^{\otimes n}\otimes I} \sum_{j=0}^{N-1} \langle j|y\rangle \, H^{\otimes n} \, |j\rangle \, |0\rangle \\
&= \left(\sum_{j=0}^{N-1} \langle j|y\rangle \, H^{\otimes n} \, |j\rangle - \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \langle j|y\rangle \, |0\rangle \right) |0\rangle + \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \langle j|y\rangle \, |0\rangle \, |0\rangle \\
&\xrightarrow{C^n X_{(\neg 1,2)}\otimes I} \left(\sum_{j=0}^{N-1} \langle j|y\rangle \, H^{\otimes n} \, |j\rangle - \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \langle j|y\rangle \, |0\rangle \right) |0\rangle + \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \langle j|y\rangle \, |0\rangle \, |1\rangle \\
&\xrightarrow{I^{\otimes n}\otimes P_{-\Delta t}} \left(\sum_{j=0}^{N-1} \langle j|y\rangle \, H^{\otimes n} \, |j\rangle - \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \langle j|y\rangle \, |0\rangle \right) |0\rangle + \frac{e^{-i\Delta t}}{\sqrt{N}} \sum_{j=0}^{N-1} \langle j|y\rangle \, |0\rangle \, |1\rangle \\
&\xrightarrow{C^n X_{(\neg 1,2)}\otimes I} \left(\sum_{j=0}^{N-1} \langle j|y\rangle \, H^{\otimes n} \, |j\rangle - \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \langle j|y\rangle \, |0\rangle \right) |0\rangle + \frac{e^{-i\Delta t}}{\sqrt{N}} \sum_{j=0}^{N-1} \langle j|y\rangle \, |0\rangle \, |0\rangle \\
&\xrightarrow{H^{\otimes n}\otimes I} \left(\sum_{j=0}^{N-1} \langle j|y\rangle \, |j\rangle - \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \langle j|y\rangle \, \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} |k\rangle \right) |0\rangle + \frac{e^{-i\Delta t}}{\sqrt{N}} \sum_{j=0}^{N-1} \langle j|y\rangle \, \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} |k\rangle \, |0\rangle \\
&= \left(\sum_{j=0}^{N-1} |j\rangle\langle j| - |\psi\rangle\langle\psi| \right) |y\rangle \, |0\rangle + \left(e^{-i\Delta t} \, |\psi\rangle\langle\psi| \right) |y\rangle \, |0\rangle \\
&= \Big[I + \left(e^{-i\Delta t} - 1 \right) |\psi\rangle\langle\psi| \Big] \, |y\rangle \, |0\rangle
\end{aligned}
$$

6.8

If we have accuracy of $O(\Delta t^r)$ for each step the cumulative error is given by $O\Big(\Delta t^r \sqrt{N}/\Delta t\Big) = O\Big(\Delta t^{r-1}\sqrt{N}\Big)$. We need the error to be $O(1)$ in order to simulate H with high accuracy, that is

$$
\Delta t^{r-1}\sqrt{N} = 1 \quad \Longrightarrow \quad \Delta t = \left(\frac{1}{\sqrt{N}} \right)^{1/(r-1)} = N^{-1/2(r-1)}.
$$

Therefore the number of required oracle calls is

$$
O\Big(\sqrt{N}/\Delta t\Big) = O\big(N^{1/2} N^{1/2(r-1)}\big) = O\big(N^{r/2(r-1)}\big).
$$

6.9

$$
U(\Delta t) = \exp\Big[-i\Delta t\Big(I + \vec{\psi}\cdot\vec{\sigma}\Big)/2\Big] \exp\Big[-i\Delta t\Big(I + \hat{z}\cdot\vec{\sigma}\Big)/2\Big].
$$

Let us expand each exponential explicitly, and for notation simplicity, let us define the quantities $c \coloneqq \cos(\Delta t/2)$ and $s \coloneqq \sin(\Delta t/2)$. The first exponential yields

$$
\begin{aligned}
\exp\Big[-i\Delta t\Big(I + \vec{\psi}\cdot\vec{\sigma}\Big)/2\Big] &= \exp\left[-i\frac{\Delta t}{2} I\right] \exp\left[-i\frac{\Delta t}{2}\vec{\psi}\cdot\vec{\sigma}\right] \\
&= (c - is)\, I \left(cI - is\vec{\psi}\cdot\vec{\sigma} \right)
\end{aligned}
$$

$$= c^2 I - s^2 \vec{\psi}\cdot\vec{\sigma} - ics\left(I + \vec{\psi}\cdot\vec{\sigma}\right),$$

and the second one yields

$$\begin{aligned}\exp\Big[-i\Delta t\Big(I + \hat{z}\cdot\vec{\sigma}\Big)/2\Big] &= \exp\left[-i\frac{\Delta t}{2}I\right]\exp\left[-i\frac{\Delta t}{2}\hat{z}\cdot\vec{\sigma}\right] \\ &= (c - is)\, I\,(cI - is\hat{z}\cdot\vec{\sigma}) \\ &= c^2 I - s^2\hat{z}\cdot\vec{\sigma} - ics\,(I + \hat{z}\cdot\vec{\sigma}).\end{aligned}$$

Substituting both results in the expression for $U(\Delta t)$ we obtain

$$\begin{aligned}U(\Delta t) &= \Big[c^2 I - s^2\vec{\psi}\cdot\vec{\sigma} - icsI - ics\vec{\psi}\cdot\vec{\sigma}\Big]\Big[c^2 I - s^2\hat{z}\cdot\vec{\sigma} - icsI - ics\hat{z}\cdot\vec{\sigma}\Big] \\ &= \left[c^2 - 2ics - s^2\right]\Big(c^2 I - s^2\Big(\vec{\psi}\cdot\vec{\sigma}\Big)\Big(\hat{z}\cdot\vec{\sigma}\Big)\Big) - ics\left[c^2 - 2ics - s^2\right]\Big(\vec{\psi} + \hat{z}\Big)\cdot\vec{\sigma}.\end{aligned}$$

Now we use the fact that (see Exercise 4.15)

$$\Big(\vec{\psi}\cdot\vec{\sigma}\Big)\Big(\hat{z}\cdot\vec{\sigma}\Big) = \Big(\vec{\psi}\cdot\hat{z}\Big)\, I + i\Big(\vec{\psi}\times\hat{z}\Big)\cdot\vec{\sigma}.$$

Substituting it in the expression for $U(\Delta t)$ yields

$$\begin{aligned}U(\Delta t) &= \left[c^2 - 2ics - s^2\right]\Big(c^2 I - s^2\Big(\vec{\psi}\cdot\hat{z}\Big)I - is^2\Big(\vec{\psi}\times\hat{z}\Big)\cdot\vec{\sigma}\Big) - ics\left[c^2 - 2ics - s^2\right]\Big(\vec{\psi} + \hat{z}\Big)\cdot\vec{\sigma} \\ &= \left[c^2 - 2ics - s^2\right]\Big(c^2 - s^2\Big(\vec{\psi}\cdot\hat{z}\Big)\Big)\, I + \left[c^2 - 2ics - s^2\right](-2is)\left(s\frac{\vec{\psi}\times\hat{z}}{2} + c\frac{\vec{\psi} + \hat{z}}{2}\right)\cdot\vec{\sigma}.\end{aligned}$$

Now notice that the term

$$\left[c^2 - 2ics - s^2\right] = \left[c - is\right]^2 = \exp(-i\Delta t),$$

multiplying all terms is just a global phase factor and can therefore be eliminated from the expression, and what is left is the result shown in Equation (6.25)

$$\begin{aligned}& U(\Delta t) = \Big(c^2 - s^2\Big(\vec{\psi}\cdot\hat{z}\Big)\Big)\, I - 2is\left(c\frac{\vec{\psi} + \hat{z}}{2} + s\frac{\vec{\psi}\times\hat{z}}{2}\right)\cdot\vec{\sigma} \\ \Longrightarrow\quad & U(\Delta t) = \left(\cos^2\left(\frac{\Delta t}{2}\right) - \sin^2\left(\frac{\Delta t}{2}\right)\vec{\psi}\cdot\hat{z}\right) I \\ & \qquad - 2i\sin\left(\frac{\Delta t}{2}\right)\left(\cos\left(\frac{\Delta t}{2}\right)\frac{\vec{\psi} + \hat{z}}{2} + \sin\left(\frac{\Delta t}{2}\right)\frac{\vec{\psi}\times\hat{z}}{2}\right)\cdot\vec{\sigma}.\end{aligned}$$

6.10

-

6.11

We may write a Hamiltonian analog the one shown in Equation (6.18), that is

$$H = |\chi\rangle\langle\chi| + |\psi\rangle\langle\psi|\,,$$

where we define the state $|\chi\rangle$ as

$$|\chi\rangle \coloneqq \frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} |x_j\rangle\,.$$

Just like the process for the case of a single solution, if we choose $|\psi\rangle = \sum_{j=0}^{N-1} |x_j\rangle / \sqrt{N}$ then this Hamiltonian can be used to rotate the state $|\psi\rangle$ to the state $|\chi\rangle$, that is, we are sending our state to a superposition of solution states that, when measured, will give us one of the M possible solutions. As for the simulation of such Hamiltonian, we can simulate the Hamiltonians $H_1 = |\chi\rangle\langle\chi|$ and $H_2 = |\psi\rangle\langle\psi|$ for time increments Δt, just like it was done for the case of a single solution.

6.12

(1) The evolution associated with this Hamiltonian is $\exp(-iHt)$. If we restrict ourselves to the space spanned by $|x\rangle$ and $|\psi\rangle$ we can write $|\psi\rangle = \alpha\,|x\rangle + \beta\,|y\rangle$, where $\{|x\rangle\,, |y\rangle\}$ is an orthonormal basis for this space, and therefore

$$H = \begin{bmatrix} \alpha & \beta \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} \alpha & 0 \\ \beta & 0 \end{bmatrix} = \begin{bmatrix} 2\alpha & \beta \\ \beta & 0 \end{bmatrix} = \alpha(I + Z) + \beta X.$$

The evolution is then given by

$$\begin{aligned} \exp(-iHt) &= \exp(-i\alpha t I) \exp(-it\,(\beta X + \alpha Z)) \\ &= e^{-i\alpha t} I\,[\cos(t) I - i \sin(t)\,(\beta X + \alpha Z)]\,. \end{aligned}$$

The global phase factor $e^{-i\alpha t}$ can be ignored. Now applying this evolution to $|\psi\rangle$ yields

$$\begin{aligned} \exp(-iHt)\,|\psi\rangle &= \cos(t)\,|\psi\rangle - i \sin(t)\,(\beta X + \alpha Z)\,|\psi\rangle \\ &= \cos(t)\,|\psi\rangle - i \sin(t)\,|x\rangle\,. \end{aligned}$$

As one can notice, this evolution takes the state $|\psi\rangle$ to the state $|x\rangle$ in a time interval $t = \pi/2$, which is a constant, so it takes time $O(1)$ to be performed.

(2) **Incomplete...**

6.13

Let us denote $\mathbf{E}(S)$ as the expectation of S, then we have

$$\Delta S = \sqrt{\mathbf{E}(S^2) - \mathbf{E}(S)^2}.$$

S is just the mean of the list $\{X_1, \cdots, X_k\}$, that we denote $\overline{X} \coloneqq \sum_j X_j/k$, multiplied by a constant N. If we use the fact that $\mathbf{E}(cx) = c\mathbf{E}(x)$ for constant c we have that

$$\begin{aligned}\Delta S &= \sqrt{N^2\mathbf{E}\Big(\overline{X}^2\Big) - N^2\mathbf{E}\big(\overline{X}\big)^2} \\ &= N\sqrt{\mathbf{E}\Big(\overline{X}^2\Big) - \mathbf{E}\big(\overline{X}\big)^2}.\end{aligned}$$

Each X_j has probability M/N of being 1 so $\mathbf{E}(X_j) = M/N$, and since $X_j^2 = X_j$ for all j it is a fact that $\mathbf{E}(X_j^2) = \mathbf{E}(X_j)$. The necessary expected values can then be calculated as

$$\begin{aligned}\mathbf{E}\Big(\overline{X}^2\Big) &= \mathbf{E}\left(\frac{1}{k^2}\sum_{j,l} X_j X_l\right) \\ &= \frac{1}{k^2}\left(\sum_{j\neq l}\mathbf{E}(X_jX_l) + \sum_j \mathbf{E}(X_j^2)\right) \\ &= \frac{1}{k^2}\left(\sum_{j\neq l}\mathbf{E}(X_j)\mathbf{E}(X_l) + \sum_j \mathbf{E}(X_j)\right) \\ &= \frac{1}{k^2}\left(k(k-1)\frac{M^2}{N^2} + k\frac{M}{N}\right) \\ &= \frac{M}{kN} - \frac{M^2}{kN^2} + \frac{M^2}{N^2},\end{aligned}$$

$$\begin{aligned}\mathbf{E}\big(\overline{X}\big)^2 &= \mathbf{E}\left(\frac{1}{k}\sum_j X_j\right)\mathbf{E}\left(\frac{1}{k}\sum_l X_l\right) \\ &= \frac{1}{k^2}\sum_{j,l}\mathbf{E}(X_j)\mathbf{E}(X_l) = \frac{M^2}{N^2}.\end{aligned}$$

Substituting yields

$$\begin{aligned}\Delta S &= N\sqrt{\frac{M}{kN} - \frac{M^2}{kN^2} + \frac{M^2}{N^2} - \frac{M^2}{N^2}} \\ &= \sqrt{\frac{M(N-M)}{k}}.\end{aligned}$$

Now, in order to obtain M within an accuracy $\sqrt{M}$ with probability 3/4 we need that $\Delta S \leq \alpha\sqrt{M}$ for some constant α. But this can only happen if $k \geq (N-M)/\alpha^2$ which means k must be $\Omega(N)$.

6.14

We consider that all N elements have probability M/N of being a solution, that is an uniform distribution. So the average of a sample of such set of elements is the best estimate we can have for M/N and hence M. In other words, $N \times \sum_j X_j/k$ where all the X_j are sampled uniformly and independently, is the best estimate we can make for M. And since the algorithm based upon it that guesses M correctly within accuracy $\sqrt{M}$ requires $\Omega(N)$ oracle calls, any other classical algorithm

will require at least the same number of calls.

6.15

$$\begin{aligned}\sum_x \|\psi - x\|^2 &\geq \|\psi\|^2 + \sum_x \|x\|^2 - 2\sum_x \|\psi\|\|x\| \\ &= 1 + N - 2\sum_x \|\psi\|\|x\|.\end{aligned}$$

Cauchy-Schwarz inequality gives us $\sum_x \|\psi\|\|x\| \leq \sqrt{\|\psi\|^2}\sqrt{\sum_x \|x\|^2} = \sqrt{N}$. Substituting we get

$$\begin{aligned}\sum_x \|\psi - x\|^2 &\geq 1 + N - 2\sqrt{N} \\ &\geq 2N - 2\sqrt{N}.\end{aligned}$$

6.16

In this case, instead of $|\langle x|\psi_k^x\rangle|^2 \geq 1/2$, we suppose $\sum_x |\langle x|\psi_k^x\rangle|^2/N \geq 1/2 \Rightarrow \sum_x |\langle x|\psi_k^x\rangle|^2 \geq N/2$. Without loss of generality, we may choose $\langle x|\psi_k^x\rangle = |\langle x|\psi_k^x\rangle|$, so

$$\sum_x \|\psi_k^x - x\|^2 = 2N - 2\sum_x |\langle x|\psi_k^x\rangle|.$$

Since $0 \leq |\langle x|\psi_k^x\rangle| \leq 1$ for all x, we clearly have $\sum_x |\langle x|\psi_k^x\rangle|^2 \leq \sum_x |\langle x|\psi_k^x\rangle|$, so

$$\sum_x \|\psi_k^x - x\|^2 \leq 2N - 2\frac{N}{2} = N.$$

So the only difference between this case and the one where we impose that $|\langle x|\psi_k^x\rangle|^2 \geq 1/2$, is that, instead of having $E_k \leq (2-\sqrt{2})N$, we have $E_k \leq N$. Now, if E_k is still $O(N)$ then D_k is still $O(N)$ which means k is still $O(\sqrt{N})$, meaning $O(\sqrt{N})$ oracle calls are still required.

6.17

If the objective is to detect only one solution among the M possible ones, then the average time to do so is the same as finding the only solution of a N/M search space. Therefore it would take $O(\sqrt{N/M})$ oracle applications to find a solution.

6.18

Suppose there are two distinct minimum degree polynomials $p_1(X)$ and $p_2(X)$ representing some Boolean function $F(X)$. If they are distinct there is at least one number $X_0 \in \{0,1\}^n$ such that $p_1(X_0) - p_2(X_0) \neq 0$, but if they both represent $F(X)$ it is also true that $p_1(X_0) = p_2(X_0) = F(X_0)$, meaning $p_1(X_0) - p_2(X_0) = 0$, which is a contradiction. So the minimum degree polynomial representing $F(X)$ is unique.

6.19

The OR operation should return 1 if at least one of the X_i equals 1, and return 0 only if all X_i equal 0. It is straightforward to conclude that the function

$$P(X) = 1 - \prod_{i=0}^{N-1} (1 - X_i)$$

only returns 0 if $\prod_{i=0}^{N-1}(1 - X_i) = 1$, which in turn can only happen if all X_i equal 0. So this is a representation of OR.

6.20

-

7 Quantum computers: physical realization

Exercises: 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9, 7.10, 7.11, 7.12, 7.13, 7.14, 7.15, 7.16, 7.17, 7.18, 7.19, 7.20, 7.21, 7.22, 7.23, 7.24, 7.25, 7.26, 7.27, 7.28, 7.29, 7.30, 7.31, 7.32, 7.33, 7.34, 7.35, 7.36, 7.37, 7.38, 7.39, 7.40, 7.41, 7.42, 7.43, 7.44, 7.45, 7.46, 7.47, 7.48, 7.49, 7.50, 7.51, 7.52.

7.1

$$\begin{aligned} a^\dagger a &= \frac{1}{2m\hbar\omega} (m\omega x - ip)(m\omega x + ip) \\ &= \frac{1}{2m\hbar\omega} \left(p^2 + m^2\omega^2 x^2 + im\omega[x,p]\right) \\ &= \frac{1}{2m\hbar\omega} \left(p^2 + m^2\omega^2 x^2 - \hbar m\omega\right) \\ &= \frac{1}{\hbar\omega} \left(\frac{p^2}{2m} + \frac{1}{2}m\omega^2 x^2\right) - \frac{1}{2} \\ &= \frac{H}{\hbar\omega} - \frac{1}{2}. \end{aligned}$$

7.2

$$\begin{aligned} \left[a, a^\dagger\right] &= aa^\dagger - a^\dagger a \\ &= \frac{H}{\hbar\omega} + \frac{1}{2} - \left(\frac{H}{\hbar\omega} - \frac{1}{2}\right) = 1. \end{aligned}$$

7.3

$$\begin{aligned} [H, a] &= \left(\hbar\omega a^\dagger a + \frac{1}{2}\right) a - a \left(\hbar\omega a^\dagger a + \frac{1}{2}\right) \\ &= \hbar\omega a^\dagger aa - \hbar\omega aa^\dagger a \end{aligned}$$

$$= \hbar\omega\big[a^\dagger, a\big]a = -\hbar\omega a.$$

From this result we see that $[[H,a],a] = 0$. So considering that $H|\psi\rangle = E|\psi\rangle$ with the energy satisfying $E \geq n\hbar\omega$ we may write

$$\begin{aligned} Ha^n|\psi\rangle &= (aH + [H,a])\,a^{n-1}|\psi\rangle \\ &= \left(a^2H + 2[H,a]a\right)a^{n-2}|\psi\rangle \\ &\vdots \\ &= \left(a^nH + n[H,a]a^{n-1}\right)|\psi\rangle \\ &= (E - n\hbar\omega)\,a^n|\psi\rangle\,. \end{aligned}$$

So the state $a^n|\psi\rangle$ is an eigenstate of H with eigenvalue $E - n\hbar\omega$.

7.4

$$\begin{aligned} |n\rangle &= \frac{a^\dagger}{\sqrt{n}}|n-1\rangle \\ &= \frac{\left(a^\dagger\right)^2}{\sqrt{n(n-1)}}|n-2\rangle \\ &\vdots \\ &= \frac{\left(a^\dagger\right)^n}{\sqrt{n!}}|0\rangle\,. \end{aligned}$$

7.5

From Equation (7.12) we have

$$a|n\rangle = \sqrt{n}\,|n-1\rangle\,.$$

Then using Equation (7.11) we obtain

$$\begin{aligned} a^\dagger a|n\rangle &= \sqrt{n}a^\dagger|n-1\rangle \\ &= \sqrt{n}\sqrt{(n-1)+1}\,|(n-1)+1\rangle \\ &= n|n\rangle\,, \end{aligned}$$

which is consistent with Equation (7.10). Besides, since $\langle n|n\rangle = 1$ we expect that $\langle n|H|n\rangle$ will result in the energy E_n associated with the state $|n\rangle$, and using Equation (7.10) we verify that

$$\begin{aligned} \langle n|H|n\rangle &= \hbar\omega\,\langle n|a^\dagger a|n\rangle + \frac{1}{2}\langle n|n\rangle \\ &= n\hbar\omega + \frac{1}{2} = E_n. \end{aligned}$$

7.6

$$\begin{aligned} a\,|\alpha\rangle &= e^{-|\alpha|^2/2}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}a\,|n\rangle \\ &= e^{-|\alpha|^2/2}\sum_{n=1}^{\infty}\frac{\alpha^n}{\sqrt{n!}}\sqrt{n}\,|n-1\rangle\,. \end{aligned}$$

Now we make the variable substitution $n-1\to m$, yielding

$$\begin{aligned} a\,|\alpha\rangle &= e^{-|\alpha|^2/2}\sum_{m=0}^{\infty}\frac{\alpha^{m+1}}{\sqrt{(m+1)!}}\sqrt{m+1}\,|m\rangle \\ &= \alpha e^{-|\alpha|^2/2}\sum_{m=0}^{\infty}\frac{\alpha^m}{\sqrt{m!}}\,|m\rangle = \alpha\,|\alpha\rangle\,. \end{aligned}$$

So the coherent state is an eigenstate of the photon annihilation operator with eigenvalue α.

7.7

Let us consider a generic state $|\psi_{\text{in}}\rangle = c_0\,|01\rangle + c_1\,|10\rangle$. The circuit applies a phase shift of π on the $|01\rangle$ component meaning we obtain $|\psi_{\text{out}}\rangle = e^{i\pi}c_0\,|01\rangle + c_1\,|10\rangle$. In column vector representation we have Equation (7.23), that is

$$|\psi_{\text{out}}\rangle = \begin{bmatrix} e^{i\pi}c_0 \\ c_1 \end{bmatrix} = \begin{bmatrix} e^{i\pi} & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} c_0 \\ c_1 \end{bmatrix} = \begin{bmatrix} e^{i\pi} & 0 \\ 0 & 1 \end{bmatrix}|\psi_{\text{in}}\rangle$$

7.8

$$\begin{aligned} P\,|\alpha\rangle &= e^{-|\alpha|^2/2}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}P\,|n\rangle \\ &= e^{-|\alpha|^2/2}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}e^{in\Delta}\,|n\rangle \\ &= e^{-|\alpha|^2/2}\sum_{n=0}^{\infty}\frac{(\alpha e^{i\Delta})^n}{\sqrt{n!}}\,|n\rangle \\ &= |\alpha e^{i\Delta}\rangle\,. \end{aligned}$$

7.9

*It seems there are some inconsistencies in this subsection. Considering B as given by Equation (7.25), $|01\rangle = a^\dagger\,|00\rangle$ and $|10\rangle = b^\dagger\,|00\rangle$ we should have $B\,|01\rangle = \cos\theta\,|01\rangle - \sin\theta\,|10\rangle$ and $B\,|10\rangle = \sin\theta\,|01\rangle + \cos\theta\,|10\rangle$.

Let us consider a generic state $|\psi\rangle = c_0\,|01\rangle + c_1\,|10\rangle$, the action of the circuit is

$$|\psi\rangle \xrightarrow{B} c_0\frac{|01\rangle - |10\rangle}{\sqrt{2}} + c_1\frac{|01\rangle + |10\rangle}{\sqrt{2}}$$

$$\xrightarrow{P_\pi|01\rangle} c_0\frac{-|01\rangle-|10\rangle}{\sqrt{2}}+c_1\frac{-|01\rangle+|10\rangle}{\sqrt{2}}$$
$$=-c_0\frac{|01\rangle+|10\rangle}{\sqrt{2}}-c_1\frac{|01\rangle-|10\rangle}{\sqrt{2}}.$$

This is indeed a Hadamard gate with an overall phase of π.

7.10

The action of the first circuit is basically $B^\dagger B$, and since B is unitary this is obviously the identity operation. For the second circuit we may consider a generic state $|\psi\rangle = c_0|01\rangle + c_1|10\rangle$

$$\begin{aligned}
|\psi\rangle &\xrightarrow{B} c_0\frac{|01\rangle-|10\rangle}{\sqrt{2}}+c_1\frac{|01\rangle+|10\rangle}{\sqrt{2}}\\
&\xrightarrow{P_\varphi|01\rangle} c_0\frac{e^{i\varphi}|01\rangle-|10\rangle}{\sqrt{2}}+c_1\frac{e^{i\varphi}|01\rangle+|10\rangle}{\sqrt{2}}\\
&=e^{i\varphi}\frac{c_0+c_1}{\sqrt{2}}|01\rangle+\frac{-c_0+c_1}{\sqrt{2}}|10\rangle\\
&\xrightarrow{B^\dagger} e^{i\varphi}\frac{c_0+c_1}{\sqrt{2}}\left(\frac{|01\rangle+|10\rangle}{\sqrt{2}}\right)+\frac{-c_0+c_1}{\sqrt{2}}\left(\frac{-|01\rangle+|10\rangle}{\sqrt{2}}\right)\\
&=\frac{c_0(e^{i\varphi}+1)+c_1(e^{i\varphi}-1)}{2}|01\rangle+\frac{c_0(e^{i\varphi}-1)+c_1(e^{i\varphi}+1)}{2}|10\rangle.
\end{aligned}$$

So in terms of rotations, the circuit performs

$$\frac{1}{2}\begin{bmatrix}e^{i\varphi}+1 & e^{i\varphi}-1\\ e^{i\varphi}-1 & e^{i\varphi}+1\end{bmatrix}\begin{bmatrix}c_0\\c_1\end{bmatrix}=e^{i\varphi/2}\begin{bmatrix}\cos\frac{\varphi}{2} & i\sin\frac{\varphi}{2}\\ i\sin\frac{\varphi}{2} & \cos\frac{\varphi}{2}\end{bmatrix}\begin{bmatrix}c_0\\c_1\end{bmatrix}=e^{i\varphi/2}R_x(\varphi)|\psi\rangle.$$

7.11

$$\begin{aligned}
B|2,0\rangle &= B\frac{b^\dagger}{\sqrt{2}}|1,0\rangle\\
&=\frac{1}{\sqrt{2}}Bb^\dagger B^\dagger B|1,0\rangle\\
&=\frac{1}{\sqrt{2}}\left(\frac{b^\dagger+a^\dagger}{\sqrt{2}}\right)\left(\frac{|01\rangle+|10\rangle}{\sqrt{2}}\right)\\
&=\frac{1}{\sqrt{2}}|1,1\rangle+\frac{1}{2}\Big(|0,2\rangle+|2,0\rangle\Big)
\end{aligned}$$

7.12

$$\begin{aligned}
B|\alpha\rangle|\beta\rangle &= e^{-\left(|\alpha|^2+|\beta|^2\right)/2}\sum_{m=0}^{\infty}\sum_{n=0}^{\infty}\frac{\alpha^m\beta^n}{\sqrt{m!n!}}B|n,m\rangle\\
&=e^{-\left(|\alpha|^2+|\beta|^2\right)/2}\sum_{m=0}^{\infty}\sum_{n=0}^{\infty}\frac{\alpha^m\beta^n}{\sqrt{m!n!}}B\frac{(a^\dagger)^m}{\sqrt{m!}}\frac{(b^\dagger)^n}{\sqrt{n!}}|0,0\rangle\\
&=e^{-\left(|\alpha|^2+|\beta|^2\right)/2}B\exp\left(\alpha a^\dagger+\beta b^\dagger\right)|0,0\rangle
\end{aligned}$$

We have that $Ba^\dagger B^\dagger = a^\dagger \cos\theta - b^\dagger \sin\theta$ and $Bb^\dagger B^\dagger = b^\dagger \cos\theta + a^\dagger \sin\theta$, therefore

$$\begin{aligned}
B\left|\alpha\right\rangle\left|\beta\right\rangle &= e^{-\left(|\alpha|^2+|\beta|^2\right)/2} B \exp\left(\alpha a^\dagger + \beta b^\dagger\right) B^\dagger B \left|0,0\right\rangle \\
&= e^{-\left(|\alpha|^2+|\beta|^2\right)/2} \exp\left(\alpha(a^\dagger\cos\theta - b^\dagger\sin\theta) + \beta(b^\dagger\cos\theta + a^\dagger\sin\theta)\right)\left|0,0\right\rangle \\
&= e^{-\left(|\alpha|^2+|\beta|^2\right)/2} \exp\left((\alpha\cos\theta + \beta\sin\theta)a^\dagger + (\beta\cos\theta - \alpha\sin\theta)b^\dagger\right)\left|0,0\right\rangle \\
&= e^{-\left(|\alpha|^2+|\beta|^2\right)/2} \sum_{m=0}^{\infty}\sum_{n=0}^{\infty} \frac{(\alpha\cos\theta+\beta\sin\theta)^m(\beta\cos\theta-\alpha\sin\theta)^n}{\sqrt{m!n!}} \frac{(a^\dagger)^m}{\sqrt{m!}} \frac{(b^\dagger)^n}{\sqrt{n!}} \left|0,0\right\rangle \\
&= e^{-\left(|\alpha|^2+|\beta|^2\right)/2} \sum_{m=0}^{\infty}\sum_{n=0}^{\infty} \frac{(\alpha\cos\theta+\beta\sin\theta)^m(\beta\cos\theta-\alpha\sin\theta)^n}{\sqrt{m!n!}} \left|n,m\right\rangle \\
&= \left|\alpha\cos\theta + \beta\sin\theta\right\rangle\left|\beta\cos\theta - \alpha\sin\theta\right\rangle .
\end{aligned}$$

7.13

-

7.14

$$\begin{aligned}
K\left|\alpha\right\rangle\left|n\right\rangle &= e^{-|\alpha|^2/2} \sum_{m=0}^{\infty} \frac{\alpha^m}{\sqrt{m!}} e^{i\chi L a^\dagger a b^\dagger b} \left|m\right\rangle\left|n\right\rangle \\
&= e^{-|\alpha|^2/2} \sum_{m=0}^{\infty} \frac{\alpha^m}{\sqrt{m!}} \sum_{j=0}^{\infty} \frac{(i\chi L)^j}{j!} (a^\dagger a)^j \left|m\right\rangle (b^\dagger b)\left|n\right\rangle \\
&= e^{-|\alpha|^2/2} \sum_{m=0}^{\infty} \frac{\alpha^m}{\sqrt{m!}} \sum_{j=0}^{\infty} \frac{(i\chi Lnm)^j}{j!} \left|m\right\rangle\left|n\right\rangle \\
&= e^{-|\alpha|^2/2} \sum_{m=0}^{\infty} \frac{\left(\alpha e^{i\chi Ln}\right)^m}{\sqrt{m!}} \left|m\right\rangle\left|n\right\rangle \\
&= \left|\alpha e^{i\chi Ln}\right\rangle\left|n\right\rangle .
\end{aligned}$$

Now this result implies that for two coherent states $\left|\alpha\right\rangle$ and $\left|\beta\right\rangle$ we have

$$\begin{aligned}
K\left|\alpha\right\rangle\left|\beta\right\rangle &= e^{-|\beta|^2/2} \sum_{m=0}^{\infty} \frac{\beta^m}{\sqrt{m!}} K\left|\alpha\right\rangle\left|m\right\rangle \\
&= e^{-|\beta|^2/2} \sum_{m=0}^{\infty} \frac{\beta^m}{\sqrt{m!}} \left|\alpha e^{i\chi Lm}\right\rangle\left|m\right\rangle .
\end{aligned}$$

Therefore ρ_a can be calculated as

$$\begin{aligned}
\rho_a &= \mathrm{Tr}_b\left[e^{-|\beta|^2} \sum_{m=0}^{\infty}\sum_{m'=0}^{\infty} \frac{\beta^m\beta^{*m'}}{\sqrt{m!m'!}} \left|\alpha e^{i\chi Lm}\right\rangle\left\langle\alpha e^{i\chi Lm'}\right| \otimes \left|m\right\rangle\left\langle m'\right|\right] \\
&= e^{-|\beta|^2} \sum_{m=0}^{\infty}\sum_{m'=0}^{\infty} \frac{\beta^m\beta^{*m'}}{\sqrt{m!m'!}} \left|\alpha e^{i\chi Lm}\right\rangle\left\langle\alpha e^{i\chi Lm'}\right| \sum_{j=0}^{\infty} \left\langle j|m\right\rangle \left\langle m'|j\right\rangle
\end{aligned}$$

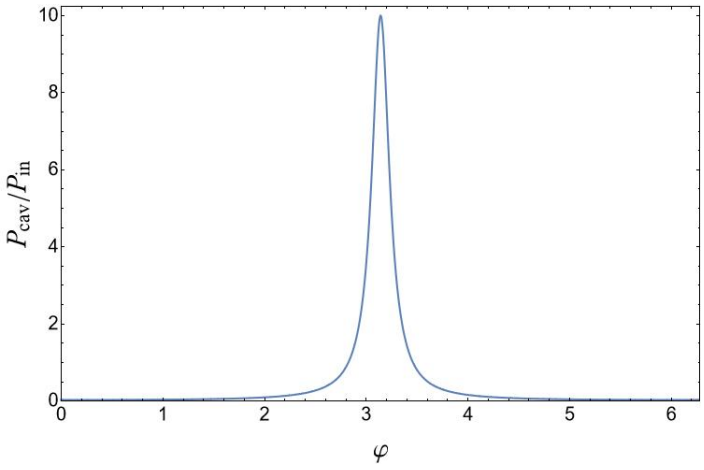
$$= e^{-|\beta|^2} \sum_{m=0}^{\infty} \frac{|\beta|^{2m}}{m!} \left|\alpha e^{i\chi Lm}\right\rangle\!\left\langle \alpha e^{i\chi Lm}\right| .$$

The terms for $m = |\beta|^2 - 2$, $m = |\beta|^2 - 1$, $m = |\beta|^2$ and $m = |\beta|^2 + 1$ have, respectively, amplitudes

$$\begin{aligned}
A_{-2} &= e^{-|\beta|^2} \frac{|\beta|^{2|\beta|^2-4}}{(|\beta|^2-2)!} = e^{-|\beta^2|} \frac{|\beta|^{2|\beta|^2}}{|\beta|^2!} \frac{|\beta|^4 - |\beta|^2}{|\beta|^4}, \\
A_{-1} &= e^{-|\beta|^2} \frac{|\beta|^{2|\beta|^2-2}}{(|\beta|^2-1)!} = e^{-|\beta^2|} \frac{|\beta|^{2|\beta|^2}}{|\beta|^2!} \frac{|\beta|^2}{|\beta|^2}, \\
A_0 &= e^{-|\beta^2|} \frac{|\beta|^{2|\beta|^2}}{|\beta|^2!}, \\
A_{+1} &= e^{-|\beta^2|} \frac{|\beta|^{2|\beta|^2+2}}{(|\beta|^2+1)!} = e^{-|\beta^2|} \frac{|\beta|^{2|\beta|^2}}{|\beta|^2!} \frac{|\beta|^2}{|\beta|^2+1}.
\end{aligned}$$

We see that $A_{-1} = A_0$ but clearly $A_0 > A_{-2}$ and $A_0 > A_{+1}$. By induction, it is clear that these relations are still valid for all $0 \leq m \leq |\beta|^2 - 2$ and $m \geq |\beta|^2 + 1$ since the amplitude for $m = 0$ is $e^{-|\beta|^2} < A_0$ and the amplitude vanishes for $m \to \infty$. Therefore the main contribution to the sum is for $m = |\beta|^2$.

7.15



The peak occurs for $\varphi = \pi$, which is the same as considering $d = \pi c/\omega$.

7.16

We have that

$$\int Y^*_{l_1 m_1} Y_{1m} Y_{l_2 m_2} \, \mathrm{d}\Omega = C \int P_{l_1 m_1}(\cos\theta) P_{1m}(\cos\theta) P_{l_2 m_2}(\cos\theta) e^{i(m_2 - m_1)\varphi} e^{im\varphi} \, \mathrm{d}\Omega,$$

where C is some constant depending on the orbital angular momenta and their components. First let us analyze the condition for $m_2 - m_1$. Since $m = \pm 1$, if $m_2 - m_1 \neq \pm 1$ we will have a term proportional to $e^{\pm in\varphi}$ where n is an integer. Since the φ dependence is in this term exclusively

the integral will vanish when integrated over $\varphi \in [0, 2\pi]$, therefore we must have $m_2 - m_1 = \pm 1$. **Incomplete...**

7.17

For $\omega = \delta = 0$ the Hamiltonian is given by $H = g\left(a^\dagger \sigma_- + a\sigma_+\right)$, so

$$\begin{aligned} H\left|\chi_n\right\rangle &= g\frac{1}{\sqrt{2}}\left[a^\dagger\sigma_-\left|n,1\right\rangle + a\sigma_+\left|n,1\right\rangle + a^\dagger\sigma_-\left|n+1,0\right\rangle + a\sigma_+\left|n+1,0\right\rangle\right] \\ &= g\frac{1}{\sqrt{2}}\left[\sqrt{n+1}\left|n+1,0\right\rangle + \sqrt{n+1}\left|n,1\right\rangle\right] \\ &= g\sqrt{n+1}\frac{1}{\sqrt{2}}\left[\left|n,1\right\rangle + \left|n+1,0\right\rangle\right] = g\sqrt{n+1}\left|\chi_n\right\rangle, \end{aligned}$$

$$\begin{aligned} H\left|\overline{\chi}_n\right\rangle &= g\frac{1}{\sqrt{2}}\left[a^\dagger\sigma_-\left|n,1\right\rangle + a\sigma_+\left|n,1\right\rangle - a^\dagger\sigma_-\left|n+1,0\right\rangle - a\sigma_+\left|n+1,0\right\rangle\right] \\ &= g\frac{1}{\sqrt{2}}\left[\sqrt{n+1}\left|n+1,0\right\rangle - \sqrt{n+1}\left|n,1\right\rangle\right] \\ &= -g\sqrt{n+1}\frac{1}{\sqrt{2}}\left[\left|n,1\right\rangle + \left|n+1,0\right\rangle\right] = -g\sqrt{n+1}\left|\chi_n\right\rangle. \end{aligned}$$

7.18

*Sine and cossine are exchanged in Equation (7.78). Apparently the basis state order should be $|00\rangle$, $|10\rangle$ and $|01\rangle$ instead of $|00\rangle$, $|01\rangle$ and $|10\rangle$. And the Hamiltonian should not be multiplied by -1 in Equation (7.76).

Let us divide the Hamiltonian in two parts: one associated with the subspace spanned by $|00\rangle$ and other with the one spanned by $|01\rangle$ and $|10\rangle$. For the subspace spanned by $|00\rangle$ the Hamiltonian is just $H_1 = \delta\left|00\right\rangle\!\left\langle 00\right|$, so immediately we have

$$\begin{aligned} U_1 &= e^{-iH_1 t} \\ &= e^{-i\delta t}\left|00\right\rangle\!\left\langle 00\right|. \end{aligned}$$

For the second subspace we may write the Hamiltonian as $H_2 = gX + \delta Z$, or equivalently $H_2 = \vec{n}\cdot\vec{\sigma}$ for $\vec{n} = (g, 0, \delta)$, so

$$\begin{aligned} U_2 &= e^{-iH_2 t} \\ &= \cos(|\vec{n}|t)I - i\hat{n}\cdot\vec{\sigma}\sin(|\vec{n}|t) \\ &= \cos\left(\sqrt{g^2+\delta^2}t\right)I - i\frac{gX+\delta Z}{\sqrt{g^2+\delta^2}}\sin\left(\sqrt{g^2+\delta^2}t\right). \end{aligned}$$

Now we identify the Rabi frequency $\Omega = \sqrt{g^2+\delta^2}$ and use the fact that $I = \left|10\right\rangle\!\left\langle 10\right| + \left|01\right\rangle\!\left\langle 01\right|$ (I denotes the identity only in this subspace), $X = \left|10\right\rangle\!\left\langle 01\right| + \left|01\right\rangle\!\left\langle 10\right|$ and $Z = \left|10\right\rangle\!\left\langle 10\right| - \left|01\right\rangle\!\left\langle 01\right|$ to

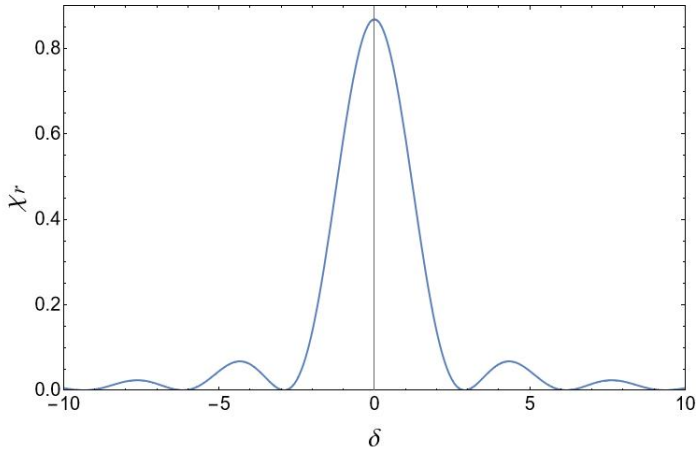
rewrite

$$U_2 = \cos\Omega t\Big(\,|10\rangle\langle 10| + |01\rangle\langle 01|\,\Big) - i\frac{g}{\Omega}\sin\Omega t\Big(\,|10\rangle\langle 01| + |01\rangle\langle 10|\,\Big) - i\frac{\delta}{\Omega}\sin\Omega t\Big(\,|10\rangle\langle 10| - |01\rangle\langle 01|\,\Big)$$
$$= \left(\cos\Omega t - i\frac{\delta}{\Omega}\sin\Omega t\right)|10\rangle\langle 10| + \left(\cos\Omega t + i\frac{\delta}{\Omega}\sin\Omega t\right)|01\rangle\langle 01| - i\frac{g}{\Omega}\sin\Omega t\Big(\,|10\rangle\langle 01| + |01\rangle\langle 10|\,\Big).$$

Adding the solutions of both subspaces we obtain Equation (7.77)

$$U = e^{-i\delta t}\,|00\rangle\langle 00| + \left(\cos\Omega t + i\frac{\delta}{\Omega}\sin\Omega t\right)|01\rangle\langle 01| + \left(\cos\Omega t - i\frac{\delta}{\Omega}\sin\Omega t\right)|10\rangle\langle 10|$$
$$- i\frac{g}{\Omega}\sin\Omega t\Big(\,|01\rangle\langle 10| + |10\rangle\langle 01|\,\Big).$$

7.19



The oscillations are due to the dependency over a squared sine of the Rabi frequency, a quantity that also depends on the detuning δ.

7.20

Taking only the matrix elements in which the atom stays in the ground state gives us

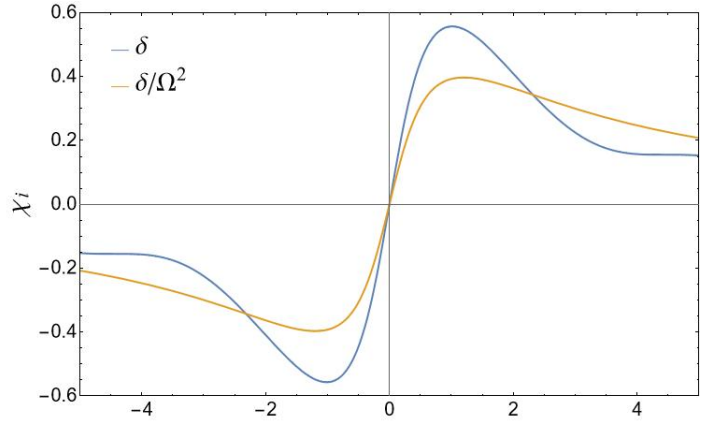
$$U' = e^{-i\delta t}\,|00\rangle\langle 00| + \left(\cos\Omega t - i\frac{\delta}{\Omega}\sin\Omega t\right)|10\rangle\langle 10|\,.$$

Tracing over the atom space and multiplying everything by a global phase $e^{i\delta t}$ yields

$$\mathrm{Tr}_{\mathrm{atom}}[U'] = |0\rangle\langle 0| + e^{i\delta t}\left(\cos\Omega t - i\frac{\delta}{\Omega}\sin\Omega t\right)|1\rangle\langle 1|\,.$$

The phase shift is the difference in the argument of the amplitudes between states $|0\rangle\langle 0|$ and $|1\rangle\langle 1|$

$$\chi_i = \arg\left[e^{i\delta t}\left(\cos\Omega t - i\frac{\delta}{\Omega}\sin\Omega t\right)\right].$$



7.21

Since H is diagonal for H_0, H_1 and H_2 we have that

$$e^{iHt} = \begin{bmatrix} e^{iH_0t} & 0 & 0 \\ 0 & e^{iH_1t} & 0 \\ 0 & 0 & e^{iH_2t}. \end{bmatrix}$$

Now, since H_0 acts only over the subspace panned by $|000\rangle$ we have that $e^{iH_0t} = e^{-i\delta t}\,|000\rangle\langle 000|$. H_1 can be divided in two parts, one that acts over the subspace spanned by $|100\rangle$ and $|001\rangle$ and other over the subspace spanned by $|010\rangle$ and $|002\rangle$. So we may write

$$\begin{aligned} H_1^{(1)} &= g_a\Big(\,|100\rangle\langle 001| + |001\rangle\langle 100|\,\Big) - \delta\Big(\,|100\rangle\langle 100| - |001\rangle\langle 001|\,\Big) \\ &= g_a X - \delta Z, \end{aligned}$$

$$\begin{aligned} H_1^{(2)} &= g_b\Big(\,|010\rangle\langle 002| + |002\rangle\langle 010|\,\Big) - \delta\Big(\,|010\rangle\langle 010| - |002\rangle\langle 002|\,\Big) \\ &= g_b X - \delta Z. \end{aligned}$$

Exponentiation of these two "sub-Hamiltonians" yields respectively (see Exercise 7.18)

$$\begin{aligned} U_1^{(1)} = &\left(\cos\Omega_a t - i\frac{\delta}{\Omega_a}\sin\Omega_a t\right)|100\rangle\langle 100| + \left(\cos\Omega_a t + i\frac{\delta}{\Omega_a}\sin\Omega_a t\right)|001\rangle\langle 001| \\ &+ i\frac{g_a}{\Omega_a}\Big(\,|001\rangle\langle 100| + |100\rangle\langle 001|\,\Big), \end{aligned}$$

$$\begin{aligned} U_1^{(2)} = &\left(\cos\Omega_b t - i\frac{\delta}{\Omega_b}\sin\Omega_b t\right)|010\rangle\langle 010| + \left(\cos\Omega_a t + i\frac{\delta}{\Omega_a}\sin\Omega_a t\right)|002\rangle\langle 002| \\ &+ i\frac{g_a}{\Omega_a}\Big(\,|010\rangle\langle 002| + |002\rangle\langle 010|\,\Big), \end{aligned}$$

where we have defined $\Omega_a \coloneqq \sqrt{g_a^2 + \delta^2}$ and $\Omega_b \coloneqq \sqrt{g_b^2 + \delta^2}$. From these results we can calculate φ_a and φ_b as

$$\begin{aligned}\varphi_a &= \arg\left[\cos\Omega_a t - i\frac{\delta}{\Omega_a}\sin\Omega_a t\right] - \arg\left[e^{-i\delta t}\right] \\ &= \arg\left[e^{i\delta t}\left(\cos\Omega_a t - i\frac{\delta}{\Omega_a}\sin\Omega_a t\right)\right],\end{aligned}$$

$$\begin{aligned}\varphi_b &= \arg\left[\cos\Omega_b t - i\frac{\delta}{\Omega_b}\sin\Omega_b t\right] - \arg\left[e^{-i\delta t}\right] \\ &= \arg\left[e^{i\delta t}\left(\cos\Omega_b t - i\frac{\delta}{\Omega_b}\sin\Omega_b t\right)\right].\end{aligned}$$

Finally, for H_2 we are only interested in the terms proportional to $|110\rangle\langle 110|$, which corresponds to the topmost and leftmost entry of H_2. We can verify that

$$H_2^2 = \begin{bmatrix}\Omega'^2 & 0 & 0 \\ 0 & \Omega_a^2 & g_a g_b \\ 0 & g_a g_b & \Omega_b^2\end{bmatrix} \quad\Longrightarrow\quad H_2^3 = \begin{bmatrix}-\delta\Omega'^2 & \cdots \\ \vdots & \ddots\end{bmatrix}.$$

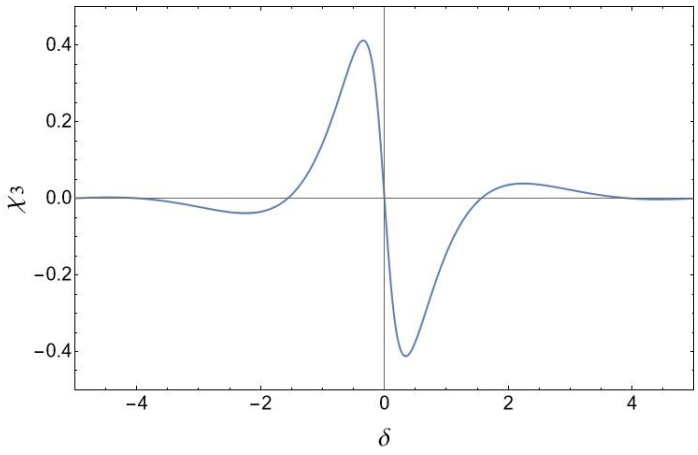
So by induction, caring only for the subspace spanned by $|110\rangle$, we conclude that

$$\begin{aligned}U_2 &= \sum_{j=0}^{\infty}\frac{(it)^j}{j!}H_2^j \\ &= \left(\sum_{k=0}^{\infty}\frac{(it)^{2k}}{(2k)!}\Omega'^{2k} - \delta\sum_{k=0}^{\infty}\frac{(it)^{2k+1}}{(2k+1)!}\Omega'^{2k}\right)|110\rangle\langle 110| + \cdots \\ &= \left(\sum_{k=0}^{\infty}\frac{(-1)^k}{(2k)!}(\Omega' t)^{2k} - i\frac{\delta}{\Omega'}\sum_{k=0}^{\infty}\frac{(-1)^k}{(2k+1)!}(\Omega' t)^{2k+1}\right)|110\rangle\langle 110| + \cdots \\ &= \left(\cos\Omega' t - i\frac{\delta}{\Omega'}\sin\Omega' t\right)|110\rangle\langle 110| + \cdots.\end{aligned}$$

From this result we finally obtain

$$\begin{aligned}\varphi_{ab} &= \arg\left[\cos\Omega' t - i\frac{\delta}{\Omega'}\sin\Omega' t\right] - \arg\left[e^{-i\delta t}\right] \\ &= \arg\left[e^{i\delta t}\left(\cos\Omega' t - i\frac{\delta}{\Omega'}\sin\Omega' t\right)\right].\end{aligned}$$

We can compute the Kerr phase shift as $\chi_3 = \varphi_{ab} - \varphi_a - \varphi_b$. The graph shows the Kerr phase shift as a function of the detuning for $g_a = g_b = 1$ and $t = 0.98$.

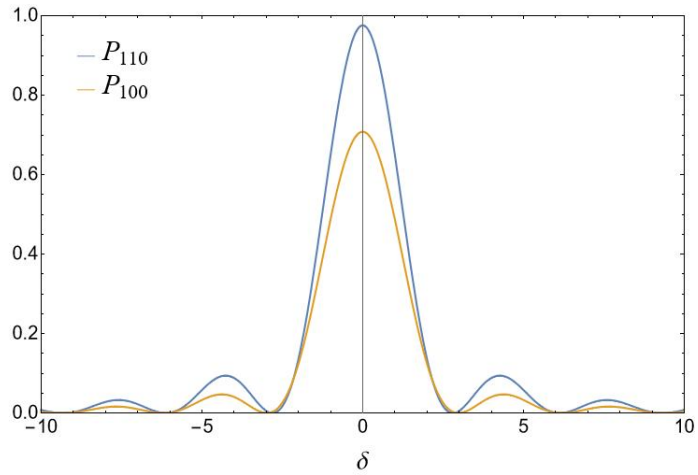


7.22

$$\begin{aligned} P_{110} \coloneqq 1 - \langle 110|U|110\rangle &= 1 - \left|\cos\Omega' t - i\frac{\delta}{\Omega'}\sin\Omega' t\right|^2 \\ &= 1 - \cos^2(\Omega' t) - \frac{\delta^2}{\Omega'^2}\sin^2(\Omega' t) \\ &= \left(1 - \frac{\delta^2}{\delta^2 + g_a^2 + g_b^2}\right)\sin^2\left(\sqrt{\delta^2 + g_a^2 + g_b^2}\,t\right), \end{aligned}$$

$$\begin{aligned} P_{100} \coloneqq 1 - \langle 100|U|100\rangle &= 1 - \left|\cos\Omega_a t - i\frac{\delta}{\Omega_a}\sin\Omega_a t\right|^2 \\ &= 1 - \cos^2(\Omega_a t) - \frac{\delta^2}{\Omega_a^2}\sin^2(\Omega_a t) \\ &= \left(1 - \frac{\delta^2}{\delta^2 + g_a^2}\right)\sin^2\left(\sqrt{\delta^2 + g_a^2}\,t\right). \end{aligned}$$

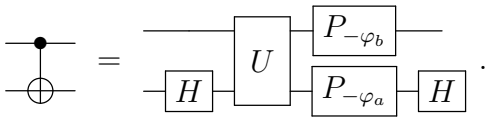
The graph shows P_{110} and P_{100} as function of the detuning for $g_a = g_b = 1$ and $t = 0.98$.



7.23

Notice that for $\varphi_a = \varphi_b = 0$ and $\Delta = \pi$, Equation (7.87) becomes precisely a controlled-Z gate. And since $HZH = X$ it is possible to implement a CNOT gate. If φ_a and φ_b are arbitrary we must

only apply inverse phase shifts to the individual qubits. In terms of quantum circuit, if we denote the two-qubit unitary operation in Equation (7.87) as U we would have



We can verify that for a generic initial state $|\psi\rangle = c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle$ and $\Delta = \pi$ the action of the circuit is

$$
\begin{aligned}
|\psi\rangle &\xrightarrow{I\otimes H} c_{00}\frac{|00\rangle + |01\rangle}{\sqrt{2}} + c_{01}\frac{|00\rangle - |01\rangle}{\sqrt{2}} + c_{10}\frac{|10\rangle + |11\rangle}{\sqrt{2}} + c_{11}\frac{|10\rangle - |11\rangle}{\sqrt{2}} \\
&\xrightarrow{U} c_{00}\frac{|00\rangle + e^{i\varphi_a}|01\rangle}{\sqrt{2}} + c_{01}\frac{|00\rangle - e^{i\varphi_a}|01\rangle}{\sqrt{2}} + c_{10}\frac{e^{i\varphi_b}|10\rangle + e^{i(\varphi_a+\varphi_b+\pi)}|11\rangle}{\sqrt{2}} \\
&\qquad + c_{11}\frac{e^{i\varphi_b}|10\rangle - e^{i(\varphi_a+\varphi_b+\pi)}|11\rangle}{\sqrt{2}} \\
&\xrightarrow{P_{-\varphi_b}\otimes P_{-\varphi a}} c_{00}\frac{|00\rangle + |01\rangle}{\sqrt{2}} + c_{01}\frac{|00\rangle - |01\rangle}{\sqrt{2}} + c_{10}\frac{|10\rangle + e^{i\pi}|11\rangle}{\sqrt{2}} + c_{11}\frac{|10\rangle - e^{i\pi}|11\rangle}{\sqrt{2}} \\
&\qquad = c_{00}\frac{|00\rangle + |01\rangle}{\sqrt{2}} + c_{01}\frac{|00\rangle - |01\rangle}{\sqrt{2}} + c_{10}\frac{|10\rangle - |11\rangle}{\sqrt{2}} + c_{11}\frac{|10\rangle + |11\rangle}{\sqrt{2}} \\
&\xrightarrow{I\otimes H} c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|11\rangle + c_{11}|10\rangle \\
&\qquad = CX|\psi\rangle\,.
\end{aligned}
$$

7.24

$$
\begin{aligned}
\mu_N B &\approx 5\times 10^{-27}\ [\mathrm{J/T}] \times 10\ [\mathrm{T}] = 5\times 10^{-26}\ \mathrm{J}, \\
k_{\mathrm{B}}T &\approx 1.4\times 10^{-23}\ [\mathrm{J/K}] \times 300\ [\mathrm{K}] = 4.2\times 10^{-21}\ \mathrm{J}.
\end{aligned}
$$

The thermal energy is around 10^5 times bigger than the nuclear spin energy.

7.25

Using σ_i to denote X, Y or Z for $i = 1, 2$ or 3 respectively we have

$$
\begin{aligned}
[j_i, j_k] &= \frac{1}{4}[\sigma_{i,1} + \sigma_{i,2}, \sigma_{k,1} + \sigma_{k,2}] \\
&= \frac{1}{4}[\sigma_{i,1}, \sigma_{k,1}] + \frac{1}{4}[\sigma_{i,2}, \sigma_{k,2}].
\end{aligned}
$$

Now we use the fact that $[\sigma_i, \sigma_k] = 2i\epsilon_{ikl}\sigma_l$ (see Exercise 2.40) to obtain

$$
\begin{aligned}
[j_i, j_k] &= \frac{2i}{4}\epsilon_{ikl}(\sigma_{l,1} + \sigma_{l,2}) \\
&= i\epsilon_{ikl}j_l.
\end{aligned}
$$

7.26

We should see the operators as $\sigma_{i,1} = \sigma_i \otimes I$ and $\sigma_{i,2} = I \otimes \sigma_i$, where I is the 2×2 identity matrix. Technically, the eigenvalue associated with j_z is $-m_j$. If we want that to be m_j then we need to use a convention where Z is such that $Z|0\rangle = -|0\rangle$ and $Z|1\rangle = |1\rangle$, or in other words, we should multiply Z by -1. So in the $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ basis we have

$$X_1 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, \quad X_2 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$$Y_1 = \begin{bmatrix} 0 & 0 & -i & 0 \\ 0 & 0 & 0 & -i \\ i & 0 & 0 & 0 \\ 0 & i & 0 & 0 \end{bmatrix}, \quad Y_2 = \begin{bmatrix} 0 & -i & 0 & 0 \\ i & 0 & 0 & 0 \\ 0 & 0 & 0 & -i \\ 0 & 0 & i & 0 \end{bmatrix}$$

$$Z_1 = \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad Z_2 = \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

and hence obtain

$$\begin{aligned} J^2 &= \frac{1}{4}\left((X_1 + X_2)^2 + (Y_1 + Y_2)^2 + (Z_1 + Z_2)^2\right) \\ &= \frac{1}{4}\begin{bmatrix} 2 & 0 & 0 & 2 \\ 0 & 2 & 2 & 0 \\ 0 & 2 & 2 & 0 \\ 2 & 0 & 0 & 2 \end{bmatrix} + \frac{1}{4}\begin{bmatrix} 2 & 0 & 0 & -2 \\ 0 & 2 & 2 & 0 \\ 0 & 2 & 2 & 0 \\ -2 & 0 & 0 & 2 \end{bmatrix} + \frac{1}{4}\begin{bmatrix} 4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 4 \end{bmatrix} = \begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix}, \end{aligned}$$

$$\begin{aligned} J_z &= \frac{1}{2}(Z_1 + Z_2) \\ &= \frac{1}{2}\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} + \frac{1}{2}\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} = \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \end{aligned}$$

Now to rewrite these results in the $\{|0,0\rangle_J, |1,-1\rangle_J, |1,0\rangle_J, |1,1\rangle_J\}$ basis we need the change of basis matrix. It can be obtained directly from the relations

$$|00\rangle = |1,-1\rangle_J \ , \quad |01\rangle = \frac{|0,0\rangle_J + |1,0\rangle_J}{\sqrt{2}} \ , \quad |10\rangle = \frac{-|0,0\rangle_J + |1,0\rangle_J}{\sqrt{2}} \ , \quad |11\rangle = |1,1\rangle_J \, ,$$

which gives us

$$M = \begin{bmatrix} 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ 1 & 0 & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

So finally, the operators J^2 and j_z written in the $\{|0,0\rangle_J, |1,-1\rangle_J, |1,0\rangle_J, |1,1\rangle_J\}$ are

$$MJ^2M^\dagger = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix}, \quad Mj_zM^\dagger = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

7.27

*It seems the states $|1/2,1/2\rangle_k$ and $|1/2,-1/2\rangle_k$, for $k = 1$ and 2, are exchanged.

Treating the operators as $\sigma_{i,1} = \sigma_i \otimes I \otimes I$, $\sigma_{i,2} = I \otimes \sigma_i \otimes I$ and $\sigma_{i,3} = I \otimes I \otimes \sigma_i$, where I is the 2×2 identity matrix, and using the same convention for Z as in Ex. 7.26 we have

$$J^2 = \frac{1}{4}\left((X_1+X_2+X_3)^2 + (Y_1+Y_2+Y_3)^2 + (Z_1+Z_2+Z_3)^2\right) = \frac{1}{4}\begin{bmatrix} 15 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 7 & 4 & 0 & 4 & 0 & 0 & 0 \\ 0 & 4 & 7 & 0 & 4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 7 & 0 & 4 & 4 & 0 \\ 0 & 4 & 4 & 0 & 7 & 0 & 0 & 0 \\ 0 & 0 & 0 & 4 & 0 & 7 & 4 & 0 \\ 0 & 0 & 0 & 4 & 0 & 4 & 7 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 15 \end{bmatrix},$$

$$j_z = \frac{1}{2}(Z_1+Z_2+Z_3) = \frac{1}{2}\begin{bmatrix} -3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 \end{bmatrix}.$$

These results are written in the $\{|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle\}$ basis. From

Equations (7.98) to (7.105) we see that the inverse change of basis matrix is given by

$$M^{-1} = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{3}} & 0 & 0 & -\frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{6}} \\ 0 & 0 & \frac{1}{\sqrt{3}} & 0 & 0 & 0 & 0 & -\frac{2}{\sqrt{6}} \\ 0 & \frac{1}{\sqrt{3}} & 0 & 0 & -\frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{6}} & 0 \\ 0 & 0 & \frac{1}{\sqrt{3}} & 0 & 0 & \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{6}} \\ 0 & \frac{1}{\sqrt{3}} & 0 & 0 & 0 & 0 & \frac{2}{\sqrt{6}} & 0 \\ 0 & \frac{1}{\sqrt{3}} & 0 & 0 & \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{6}} & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

The order of states we are using in the coupled angular momenta basis is $\{|3/2, 3/2\rangle,\ |3/2, 1/2\rangle,\ |3/2, -1/2\rangle,\ |3/2, -3/2\rangle,\ |1/2, 1/2\rangle_1,\ |1/2, -1/2\rangle_1,\ |1/2, 1/2\rangle_2,\ |1/2, -1/2\rangle_2\}$, which is the order the states are written from Equations (7.98) to (7.105). So finally, the J^2 and j_z operators written in the coupled basis are given by

$$MJ^2M^\dagger = \begin{bmatrix} \frac{15}{4} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{15}{4} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{15}{4} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{15}{4} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{3}{4} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \frac{3}{4} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{3}{4} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{3}{4} \end{bmatrix}, \quad Mj_zM^\dagger = \begin{bmatrix} \frac{3}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -\frac{1}{2} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -\frac{3}{2} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -\frac{1}{2} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -\frac{1}{2} \end{bmatrix}.$$

7.28

$$[i_x, i_y] = \begin{bmatrix} -\frac{3i}{2} & 0 & 0 & 0 \\ 0 & -\frac{i}{2} & 0 & 0 \\ 0 & 0 & \frac{i}{2} & 0 \\ 0 & 0 & 0 & \frac{3i}{2} \end{bmatrix} = ii_z,$$

$$[i_y, i_z] = \begin{bmatrix} 0 & i\frac{\sqrt{3}}{2} & 0 & 0 \\ i\frac{\sqrt{3}}{2} & 0 & i & 0 \\ 0 & i & 0 & i\frac{\sqrt{3}}{2} \\ 0 & 0 & i\frac{\sqrt{3}}{2} & 0 \end{bmatrix} = ii_x,$$

$$[i_z, i_x] = \begin{bmatrix} 0 & -\frac{\sqrt{3}}{2} & 0 & 0 \\ \frac{\sqrt{3}}{2} & 0 & -1 & 0 \\ 0 & 1 & 0 & -\frac{\sqrt{3}}{2} \\ 0 & 0 & \frac{\sqrt{3}}{2} & 0 \end{bmatrix} = ii_y.$$

That is, we can write the commutation rules in the compact form $[i_j, i_k] = i\epsilon_{jkl} i_l$, which corresponds to the $SU(2)$ commutation rules.

$$F^2 = \begin{bmatrix} 3 & 0 & 0 & \sqrt{3} & 0 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 4 & 0 & 0 & 2 & 0 & 0 \\ \sqrt{3} & 0 & 0 & 5 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 5 & 0 & 0 & \sqrt{3} \\ 0 & 0 & 2 & 0 & 0 & 4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 6 & 0 \\ 0 & 0 & 0 & 0 & \sqrt{3} & 0 & 0 & 3 \end{bmatrix}, \quad f_z = \begin{bmatrix} -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Diagonalizing F^2 and rearranging the diagonal terms in f_z for it to be consistent with F^2 yields

$$F^2 = \begin{bmatrix} 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 6 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 6 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \end{bmatrix}, \quad f_z = \begin{bmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{bmatrix}.$$

7.29

*The squared sine in p_{decay} should contain an $(\omega - \omega_0)$ instead of $(\omega - \omega_0)^2$.

$$\begin{aligned} \frac{1}{(2\pi c)^3}\frac{8\pi}{3}\int_0^\infty \omega^2 p_{\text{decay}}\,\mathrm{d}\omega &= \frac{1}{(2\pi c)^3}\frac{8\pi}{3}\int_0^\infty \omega^2 \frac{\omega_0^2}{2\hbar\omega\epsilon_0 c^2}|\langle 0|\vec{\mu}|1\rangle|^2 \frac{4\sin^2\left[\frac{t}{2}(\omega-\omega_0)\right]}{(\omega-\omega_0)^2}\,\mathrm{d}\omega \\ &= \frac{2\omega_0^2|\langle 0|\vec{\mu}|1\rangle|^2}{3\pi^2\hbar\epsilon_0 c^5}\int_0^\infty \frac{\omega}{(\omega-\omega_0)^2}\sin^2\left[\frac{t}{2}(\omega-\omega_0)\right]\mathrm{d}\omega. \end{aligned}$$

Let us now focus on the remainder integral, which we will call $\mathcal{I}$. Making the variable substitution $\omega - \omega_0 \equiv x$ yields

$$\begin{aligned} \mathcal{I} &= \int_{-\omega_0}^\infty \frac{x+\omega_0}{x^2}\sin^2\left[\frac{t}{2}x\right]\mathrm{d}x \\ &= \int_{-\omega_0}^\infty \frac{1}{x}\sin^2\left[\frac{t}{2}x\right]\mathrm{d}x + \omega_0\int_{-\omega_0}^\infty \frac{1}{x^2}\sin^2\left[\frac{t}{2}x\right]\mathrm{d}x. \end{aligned}$$

Now, since in general we have $\omega_0 \gg 0$ we can make an approximation where we extend the lower limit of $\mathcal{I}$ to $-\infty$. The first integral contains an odd function and thus vanishes when integrated from $-\infty$ to ∞, so the result is

$$\mathcal{I} \approx \omega_0\int_{-\infty}^\infty \frac{1}{x^2}\sin^2\left[\frac{t}{2}x\right]\mathrm{d}x = \omega_0\frac{t}{2}\pi.$$

Now we can obtain γ_{rad} with

$$\gamma_{\text{rad}} = \frac{2\omega_0^2 |\langle 0|\vec{\mu}|1\rangle|^2}{3\pi^2\hbar\epsilon_0 c^5}\frac{\mathrm{d}\mathcal{I}}{\mathrm{d}t} = \frac{\omega_0^3 |\langle 0|\vec{\mu}|1\rangle|^2}{3\pi\hbar\epsilon_0 c^5}.$$

7.30

$$\gamma_{\text{rad}}^{\text{ed}} \approx \frac{8\pi^3 q^2 a_0^2 \times 10^{45}}{3\pi\hbar\epsilon_0 c^3} \approx 7.5 \times 10^7 \text{ s}^{-1}.$$

Or in terms of lifetime, we can say the electron remains in the excited state for about 10^{-8} seconds.

7.31

Up to an immaterial global phase we have

$$\begin{aligned} R_x(\pi)R_y(\pi/2) &= \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix} \\ &= -i \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \\ &= e^{-i\pi/2} H. \end{aligned}$$

7.32

Considering a generic state $|\psi\rangle = c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle$, where the first entry is the phonon state and the second one the ion's internal state, the circuit performs the transformation

$$\begin{aligned} |\psi\rangle &\xrightarrow{I\otimes R_y(\pi/2)} c_{00}\frac{|00\rangle + |01\rangle}{\sqrt{2}} + c_{01}\frac{-|00\rangle + |01\rangle}{\sqrt{2}} + c_{10}\frac{|10\rangle + |11\rangle}{\sqrt{2}} + c_{11}\frac{-|10\rangle + |11\rangle}{\sqrt{2}} \\ &\xrightarrow{CZ} c_{00}\frac{|00\rangle + |01\rangle}{\sqrt{2}} + c_{01}\frac{-|00\rangle + |01\rangle}{\sqrt{2}} + c_{10}\frac{|10\rangle - |11\rangle}{\sqrt{2}} + c_{11}\frac{-|10\rangle - |11\rangle}{\sqrt{2}} \\ &\xrightarrow{I\otimes R_y(-\pi/2)} c_{00}|00\rangle + c_{01}|01\rangle - c_{10}|11\rangle - c_{11}|10\rangle, \end{aligned}$$

which is a CNOT gate with a relative phase of π over the components where the phonon state is $|1\rangle$.

7.33

We can invert the relation, that is, $|\chi(t)\rangle = e^{-i\omega Zt/2}|\varphi(t)\rangle$, and so the Schrödinger equation becomes

$$\begin{gathered} i\partial_t\left(e^{-i\omega Zt/2}|\varphi(t)\rangle\right) = He^{-i\omega Zt/2}|\varphi(t)\rangle \\ \downarrow \\ \frac{\omega}{2}Ze^{-i\omega Zt/2}|\varphi(t)\rangle + ie^{-i\omega Zt/2}\partial_t|\varphi(t)\rangle = He^{-i\omega Zt/2}|\varphi(t)\rangle. \end{gathered}$$

Multiplying both sides, through the left, by $e^{i\omega Zt/2}$ yields Equation (7.129)

$$\begin{aligned}\frac{\omega}{2}Z\left|\varphi(t)\right\rangle + i\partial_t\left|\varphi(t)\right\rangle &= e^{i\omega Zt/2}He^{-i\omega Zt/2}\left|\varphi(t)\right\rangle \\ &\downarrow \\ i\partial_t\left|\varphi(t)\right\rangle &= \left[e^{i\omega Zt/2}He^{-i\omega Zt/2} - \frac{\omega}{2}Z\right]\left|\varphi(t)\right\rangle.\end{aligned}$$

The Hamiltonian that gives rise to Equation (7.135) has the form $\widetilde{\omega}Z/2$ for some frequency $\widetilde{\omega}$. Notice that if we have $\omega = \omega_0$ then defining the states $\left|\psi(t)\right\rangle$, such that $\left|\chi(t)\right\rangle = e^{-i\widetilde{\omega}Zt/2}\left|\psi(t)\right\rangle$, we obtain the following Schrödinger equation:

$$i\partial_t\left|\psi(t)\right\rangle = \left[e^{i\widetilde{\omega}Zt/2}He^{-i\widetilde{\omega}Zt/2} - \frac{\omega_0}{2}Z\right]\left|\psi(t)\right\rangle.$$

Using Equation (7.130), the rotating frame Hamiltonian becomes

$$\begin{aligned}e^{i\widetilde{\omega}Zt/2}He^{-i\widetilde{\omega}Zt/2} - \frac{\omega_0}{2}Z &= g\left((X\cos\widetilde{\omega}t - Y\sin\widetilde{\omega}t)\cos\omega_0 t + (Y\cos\widetilde{\omega}t + X\sin\widetilde{\omega}t)\sin\omega_0 t\right) \\ &= gX\left(\cos\widetilde{\omega}t\cos\omega_0 t + \sin\widetilde{\omega}t\sin\omega_0 t\right) + gY\left(\cos\widetilde{\omega}t\sin\omega_0 t - \sin\widetilde{\omega}t\cos\omega_0 t\right) \\ &= g\cos[(\omega_0 - \widetilde{\omega})\,t]X + g\sin[(\omega_0 - \widetilde{\omega})\,t]Y.\end{aligned}$$

If we define $g_1(t) \coloneqq g\cos[(\widetilde{\omega} - \omega_0)\,t]$ and $g_2(t) \coloneqq g\sin[(\widetilde{\omega} - \omega_0)\,t]$ we obtain the rotating frame Hamiltonian of Equation (7.135). Notice that for $\widetilde{\omega} = \omega$ we obtain the rotating frame Hamiltonian of Equation (7.131), which is just gX at the resonance $\omega = \omega_0$.

7.34

The precession frequency is given by $\omega = \mu_N g_p B/\hbar$, where μ_N is the nuclear Bohr magneton and g_p is the proton g-factor. So we have

$$\omega = \frac{\mu_N g_p}{\hbar}B \approx 3.16 \times 10^9 \text{ rad} \cdot \text{s}^{-1}.$$

If we want a $\pi/2$ rotation to be accomplished in 10 microseconds we want the period to be $T = 40$ microseconds, meaning $\omega = 2\pi/T \approx 1.57 \times 10^5$ rad $\cdot$ s^{-1}, hence

$$\begin{aligned}B \approx \frac{1.57 \times 10^5 \times \hbar}{\mu_N g_p} &\approx 5.87 \times 10^{-4} \text{ T} \\ &= 5.87 \text{ G}.\end{aligned}$$

7.35

We may express the unit vector as $\hat{n} = (s_\theta c_\varphi, s_\theta s_\varphi, c_\theta)$, where we are using s and c to denote, respectively, the sine and cosine functions. Let us also denote the pauli vectors as $\vec{\sigma}_j = (X_j, Y_j, Z_j)$. So the spherical average of $H^{\text{D}}_{1,2}$ is proportional to

$$\int H^{\text{D}}_{1,2}\,\text{d}\Omega = \frac{\gamma_1\gamma_2\hbar}{4r^3}\left[\vec{\sigma}_1 \cdot \vec{\sigma}_2 \int_0^{2\pi}\int_0^{\pi} s_\theta\,\text{d}\theta\text{d}\varphi\right.$$

$$- 3 \int_0^{2\pi} \int_0^{\pi} \left(X_1 s_\theta c_\varphi + Y_1 s_\theta s_\varphi + Z_1 c_\theta\right) \left(X_2 s_\theta c_\varphi + Y_2 s_\theta s_\varphi + Z_2 c_\theta\right) s_\theta \, \mathrm{d}\theta \mathrm{d}\varphi \Bigg] .$$

The first integral yields 4π. For the second integral, notice that for all terms, with the exception of the ones proportional to X_1X_2, Y_1Y_2 and Z_1Z_2, the integral on φ will be either s_φ, c_φ or $s_\varphi c_\varphi$. All these integrals vanish for the interval $[0, 2\pi]$. We are left only with the integral

$$\begin{aligned} \int_0^{2\pi} \int_0^{\pi} \left(X_1X_2 s_\theta^3 c_\varphi^2 + Y_1Y_2 s_\theta^3 s_\varphi^2 + Z_1Z_2 s_\theta c_\theta^2\right) \mathrm{d}\theta \mathrm{d}\varphi &= \frac{4\pi}{3} \left(X_1X_2 + Y_1Y_2 + Z_1Z_2\right) \\ &= \frac{4\pi}{3} \vec{\sigma}_1 \cdot \vec{\sigma}_2. \end{aligned}$$

We this result, we conclude that

$$\int H_{1,2}^{\mathrm{D}} \, \mathrm{d}\Omega = \frac{\gamma_1\gamma_2\hbar}{4r^3} \left[4\pi \vec{\sigma}_1 \cdot \vec{\sigma}_2 - 3\frac{4\pi}{3} \vec{\sigma}_1 \cdot \vec{\sigma}_2\right] = 0.$$

7.36

-

7.37

-

7.38

$$R_{x1}^2 = \cos\frac{\pi}{2} I - i \sin\frac{\pi}{2} X_1 = -iX_1 \quad \text{and} \quad e^{-iaZ_1 t} = \cos(at) I - i \sin(at) Z_1,$$

therefore

$$\begin{aligned} R_{x1}^2 e^{-iaZ_1 t} R_{x1}^2 &= (-iX_1) \left(\cos(at) I - i \sin(at) Z_1\right) (-iX_1) \\ &= -\cos(at) I + i \sin(at) X_1 Z_1 X_1 \\ &= -\cos(at) - i \sin(at) Z_1 \\ &= -e^{iaZ_1 t}. \end{aligned}$$

Since the negative sign is just a global phase, it can be ignored.

7.39

Let U be a unitary operator such that

$$U H^{\mathrm{sys}} U^\dagger = Z \quad \Longrightarrow \quad U^\dagger Z U = H^{\mathrm{sys}}.$$

So we may have

$$U^\dagger R_x^2 e^{-iZt} R_x^2 U = U^\dagger R_x^2 U U^\dagger e^{-iZt} U U^\dagger R_x^2 U$$

$$= \left(U^\dagger R_x^2 U\right) e^{-iH^{\text{sys}}t} \left(U^\dagger R_x^2 U\right).$$

But this same quantity equals

$$\begin{aligned} U^\dagger R_x^2 e^{-iZ_1 t} R_x^2 U &= U^\dagger e^{iZt} U \\ &= e^{iH_{\text{sys}}t}. \end{aligned}$$

Therefore we have the relation

$$\left(U^\dagger R_x^2 U\right) e^{-iH^{\text{sys}}t} \left(U^\dagger R_x^2 U\right) = e^{iH_{\text{sys}}t},$$

which is a refocus evolution under the general Hamiltonian H^{sys}, meaning pulses of the form $U^\dagger R_x^2 U$ can be used for that.

7.40

-

7.41

-

7.42

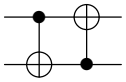
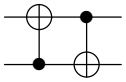
To exchange the positions of c and d we perform

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

and then, to exchange the positions of b and c we apply

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

and the resulting matrix is ρ_2. We first used the gate $CX_{(1,2)}$ and then $CX_{(2,1)}$, therefore, on the left we have the composition $P = CX_{(2,1)}CX_{(1,2)}$ and on the right $P^\dagger = CX_{(1,2)}CX_{(2,1)}$, meaning

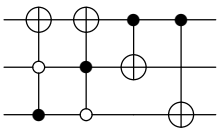
$P =$  and $P^\dagger =$  .

7.43

The initial density operator must be sandwiched with three permutation operators. The three permutations are independent and therefore there is more than one possibility. One of them is, looking at the diagonal, to permutate the 2nd with the 6th entry, the 3rd with the 7th, and the 5th with the 8th.

$$P_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}, P_2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}, P_3 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}.$$

P_1 sends the state $|001\rangle$ to $|101\rangle$ and vice-versa, P_2 sends the state $|010\rangle$ to $|110\rangle$ and vice-versa, and P_3 sends the state $|100\rangle$ to $|111\rangle$. A possible permutation is then given by $P = P_3P_2P_1$, which can be identified with the circuit

$P =$  .

7.44

-

7.45

-

7.46

-

7.47

*The two-qubit operator should be $\exp(iH/8\hbar J)$, or alternatively, the Hamiltonian should be $H = (\pi/4)\hbar J Z_1 Z_2$.

Denoting the two-qubit operator as τ, the action of the circuit is $R_{y2}\tau R_{x2}$. Writing each quantum

gate in their matrix representations we have

$$R_{y2} = \exp[-i(\pi/4)I \otimes Y] = \frac{1}{\sqrt{2}} I \otimes I - \frac{i}{\sqrt{2}} I \otimes Y = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & -1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 1 & 1 \end{bmatrix},$$

$$\tau = \exp[i(\pi/4)Z \otimes Z] = \frac{1}{\sqrt{2}} I \otimes I + \frac{i}{\sqrt{2}} Z \otimes Z = \frac{1}{\sqrt{2}} \begin{bmatrix} 1+i & 0 & 0 & 0 \\ 0 & 1-i & 0 & 0 \\ 0 & 0 & 1-i & 0 \\ 0 & 0 & 0 & 1+i \end{bmatrix},$$

$$R_{x2} = \exp[-i(\pi/4)I \otimes X] = \frac{1}{\sqrt{2}} I \otimes I - \frac{i}{\sqrt{2}} I \otimes X = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & -i & 0 & 0 \\ -i & 1 & 0 & 0 \\ 0 & 0 & 1 & -i \\ 0 & 0 & -i & 1 \end{bmatrix}.$$

Multiplication of the three matrix yields

$$R_{y2}\tau R_{x2} = \frac{1}{2\sqrt{2}} \begin{bmatrix} 2+2i & 0 & 0 & 0 \\ 0 & 2-2i & 0 & 0 \\ 0 & 0 & 0 & -2-2i \\ 0 & 0 & 2-2i & 0 \end{bmatrix} = \begin{bmatrix} e^{i\pi/4} & 0 & 0 & 0 \\ 0 & e^{-i\pi/4} & 0 & 0 \\ 0 & 0 & 0 & -e^{i\pi/4} \\ 0 & 0 & e^{-i\pi/4} & 0 \end{bmatrix},$$

which is a CNOT gate with extra relative phases between the two components, meaning it correctly executes the CNOT gate only over classical states. In order to correct the relative phases we can apply $R_{z2} = \exp[-i(\pi/4)I \otimes Z]$. The result is

$$R_{z2}R_{y2}\tau R_{x2} = \begin{bmatrix} e^{-i\pi/4} & 0 & 0 & 0 \\ 0 & e^{i\pi/4} & 0 & 0 \\ 0 & 0 & e^{-i\pi/4} & 0 \\ 0 & 0 & 0 & e^{i\pi/4} \end{bmatrix} \begin{bmatrix} e^{i\pi/4} & 0 & 0 & 0 \\ 0 & e^{-i\pi/4} & 0 & 0 \\ 0 & 0 & 0 & -e^{i\pi/4} \\ 0 & 0 & e^{-i\pi/4} & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{bmatrix},$$

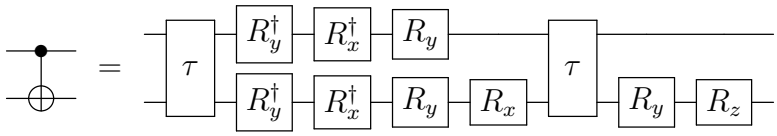
And as it can bee seen, the component $|11\rangle$ still gets a relative phase flip. It is impossible to correct it using only R_z rotations. We need a CZ gate to correct the phase of the $|11\rangle$ right at the beginning. But notice that, up to global phase, CZ corresponds exactly to the operator O shown in Eq. (7.170), which is given by

$$O = R_{y1}R_{x1}^{\dagger}R_{y1}^{\dagger}R_{y2}R_{x2}^{\dagger}R_{y2}^{\dagger}\tau.$$

So a possible quantum circuit for executing the correct CNOT gate would be

$$R_{z2}R_{y2}\tau R_{x2}R_{y1}R_{x1}^{\dagger}R_{y1}^{\dagger}R_{y2}R_{x2}^{\dagger}R_{y2}^{\dagger}\tau,$$

meaning



7.48

$$R_{y2}\tau R_{x2}R_{x1} = \begin{bmatrix} \frac{1+i}{\sqrt{2}} & 0 & 0 & 0 \\ 0 & \frac{1-i}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & 0 & -\frac{1+i}{\sqrt{2}} \\ 0 & 0 & \frac{1-i}{\sqrt{2}} & 0 \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & -\frac{i}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & 0 & -\frac{i}{\sqrt{2}} \\ -\frac{i}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} & 0 \\ 0 & -\frac{i}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} \frac{1+i}{2} & 0 & \frac{1-i}{2} & 0 \\ 0 & \frac{1-i}{2} & 0 & -\frac{1+i}{2} \\ 0 & \frac{-1+i}{2} & 0 & -\frac{1+i}{2} \\ -\frac{1+i}{2} & 0 & \frac{1-i}{2} & 0 \end{bmatrix}$$

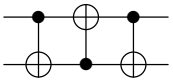
From this result one sees that, if the initial state is given by $|00\rangle$, the final state will be

$$\begin{bmatrix} \frac{1+i}{2} & 0 & \frac{1-i}{2} & 0 \\ 0 & \frac{1-i}{2} & 0 & -\frac{1+i}{2} \\ 0 & \frac{-1+i}{2} & 0 & -\frac{1+i}{2} \\ -\frac{1+i}{2} & 0 & \frac{1-i}{2} & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{1-i}{2} \\ 0 \\ 0 \\ -\frac{1-i}{2} \end{bmatrix} = e^{-i\pi/4}\frac{|00\rangle - |11\rangle}{\sqrt{2}}.$$

7.49

It is a fact that

$$\text{SWAP} = \quad .$$



So let us name the first circuit of Figure 7.19 C_2. And let us define C_1 as the equivalent circuit but with the R_x and R_y rotations applied to the top qubit. Although C_2 yields the wrong relative phases, it is direct to verify that applying $C_1C_2C_1$ corrects all relative phases, yielding the SWAP gate.

$$\begin{aligned} C_2C_1C_2 &= \begin{bmatrix} e^{i\frac{\pi}{4}} & 0 & 0 & 0 \\ 0 & e^{-i\frac{\pi}{4}} & 0 & 0 \\ 0 & 0 & 0 & -e^{i\frac{\pi}{4}} \\ 0 & 0 & e^{-i\frac{\pi}{4}} & 0 \end{bmatrix} \begin{bmatrix} e^{i\frac{\pi}{4}} & 0 & 0 & 0 \\ 0 & 0 & 0 & -e^{i\frac{\pi}{4}} \\ 0 & 0 & e^{-i\frac{\pi}{4}} & 0 \\ 0 & e^{-i\frac{\pi}{4}} & 0 & 0 \end{bmatrix} \begin{bmatrix} e^{i\frac{\pi}{4}} & 0 & 0 & 0 \\ 0 & e^{-i\frac{\pi}{4}} & 0 & 0 \\ 0 & 0 & 0 & -e^{i\frac{\pi}{4}} \\ 0 & 0 & e^{-i\frac{\pi}{4}} & 0 \end{bmatrix} \\ &= \begin{bmatrix} e^{i\frac{\pi}{4}} & 0 & 0 & 0 \\ 0 & e^{-i\frac{\pi}{4}} & 0 & 0 \\ 0 & 0 & 0 & -e^{i\frac{\pi}{4}} \\ 0 & 0 & e^{-i\frac{\pi}{4}} & 0 \end{bmatrix} \begin{bmatrix} e^{i\frac{\pi}{2}} & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & e^{-i\frac{\pi}{2}} & 0 & 0 \end{bmatrix} \\ &= \begin{bmatrix} e^{i\frac{3\pi}{4}} & 0 & 0 & 0 \\ 0 & 0 & e^{i\frac{3\pi}{4}} & 0 \\ 0 & e^{i\frac{3\pi}{4}} & 0 & 0 \\ 0 & 0 & 0 & e^{i\frac{3\pi}{4}} \end{bmatrix} = e^{i3\pi/4}\text{SWAP}. \end{aligned}$$

7.50

Considering the order $|00\rangle$, $|10\rangle$, $|01\rangle$ and $|11\rangle$ we need, for the $x_0 = 0, 1, 2$ cases, the minus sign to be, respectively, on the first, third, and second element of the diagonal. For the $x_0 = 3$ case we know that the oracle can be written as $O_3 = R_{y1}R_{x1}^\dagger R_{y1}^\dagger R_{y2}R_{x2}^\dagger R_{y2}^\dagger \tau$. Breaking this expression into parts we have that

$$R_{y1}R_{x1}^\dagger R_{y1}^\dagger = \begin{bmatrix} e^{-i\pi/4} & 0 & 0 & 0 \\ 0 & e^{-i\pi/4} & 0 & 0 \\ 0 & 0 & e^{i\pi/4} & 0 \\ 0 & 0 & 0 & e^{i\pi/4} \end{bmatrix} \quad \text{and} \quad R_{y2}R_{x2}^\dagger R_{y2}^\dagger = \begin{bmatrix} e^{-i\pi/4} & 0 & 0 & 0 \\ 0 & e^{i\pi/4} & 0 & 0 \\ 0 & 0 & e^{-i\pi/4} & 0 \\ 0 & 0 & 0 & e^{i\pi/4} \end{bmatrix}$$

Through direct verification we obtain

$$R_{y1}R_{x1}^\dagger R_{y1}^\dagger \left(R_{y2}R_{x2}^\dagger R_{y2}^\dagger\right)^\dagger \tau = \begin{bmatrix} e^{i\pi/4} & 0 & 0 & 0 \\ 0 & e^{-i\pi/4} & 0 & 0 \\ 0 & 0 & e^{i\pi/4} & 0 \\ 0 & 0 & 0 & e^{i\pi/4} \end{bmatrix} = e^{i\frac{\pi}{4}} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad (x_0 = 2),$$

$$\left(R_{y1}R_{x1}^\dagger R_{y1}^\dagger\right)^\dagger R_{y2}R_{x2}^\dagger R_{y2}^\dagger \tau = \begin{bmatrix} e^{i\pi/4} & 0 & 0 & 0 \\ 0 & e^{i\pi/4} & 0 & 0 \\ 0 & 0 & e^{-i3\pi/4} & 0 \\ 0 & 0 & 0 & e^{i\pi/4} \end{bmatrix} = e^{i\frac{\pi}{4}} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad (x_0 = 1),$$

$$\left(R_{y1}R_{x1}^\dagger R_{y1}^\dagger\right)^\dagger \left(R_{y2}R_{x2}^\dagger R_{y2}^\dagger\right)^\dagger \tau = \begin{bmatrix} e^{i3\pi/4} & 0 & 0 & 0 \\ 0 & e^{-i\pi/4} & 0 & 0 \\ 0 & 0 & e^{-i\pi/4} & 0 \\ 0 & 0 & 0 & e^{-i\pi/4} \end{bmatrix} = e^{-i\frac{\pi}{4}} \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad (x_0 = 0),$$

therefore

$$\begin{aligned} O_2 &= R_{y1}R_{x1}^\dagger R_{y1}^\dagger R_{y2}R_{x2}R_{y2}^\dagger \tau, \\ O_1 &= R_{y1}R_{x1}R_{y1}^\dagger R_{y2}R_{x2}^\dagger R_{y2}^\dagger \tau, \\ O_0 &= R_{y1}R_{x1}R_{y1}^\dagger R_{y2}R_{x2}R_{y2}^\dagger \tau. \end{aligned}$$

7.51

Using the results of the previous exercise as well as the fact that $H^{\otimes 2} = R_{x1}^2 R_{y1}^\dagger R_{x2}^2 R_{y2}^\dagger$ and $P = R_{y1}R_{x1}R_{y1}^\dagger R_{y2}R_{x2}R_{y2}^\dagger \tau$, and that rotations on different qubits commute, we have:

$$\begin{aligned} G &= H^{\otimes 2} P H^{\otimes 2} O_3 \\ &= R_{x1}^2 R_{y1}^\dagger R_{x2}^2 R_{y2}^\dagger R_{y1}R_{x1}R_{y1}^\dagger R_{y2}R_{x2}R_{y2}^\dagger \tau R_{x1}^2 R_{y1}^\dagger R_{x2}^2 R_{y2}^\dagger R_{y1}R_{x1}^\dagger R_{y1}^\dagger R_{y2}R_{x2}^\dagger R_{y2}^\dagger \tau \end{aligned}$$

$$= \left(R_{x1}^2 R_{y1}^\dagger R_{y1} R_{x1} R_{y1}^\dagger\right)\left(R_{x2}^2 R_{y2}^\dagger R_{y2} R_{x2} R_{y2}^\dagger\right)\tau\left(R_{x1}^2 R_{y1}^\dagger R_{y1} R_{x1}^\dagger R_{y1}^\dagger\right)\left(R_{x2}^2 R_{y2}^\dagger R_{y2} R_{x2}^\dagger R_{y2}^\dagger\right)\tau$$
$$= \left(R_{x1}^3 R_{y1}^\dagger\right)\left(R_{x2}^3 R_{y2}^\dagger\right)\tau\left(R_{x1} R_{y1}^\dagger\right)\left(R_{x2} R_{y2}^\dagger\right)\tau$$
$$= R_{x1}^\dagger R_{y1}^\dagger R_{x2}^\dagger R_{y2}^\dagger \tau R_{x1} R_{y1}^\dagger R_{x2} R_{y2}^\dagger \tau \quad (x_0 = 3)$$

$$\begin{aligned} G &= H^{\otimes 2} P H^{\otimes 2} O_1 \\ &= H^{\otimes 2} P R_{x1}^2 R_{y1}^\dagger R_{x2}^2 R_{y2}^\dagger R_{y1} R_{x1}^\dagger R_{y1}^\dagger R_{y2} R_{x2} R_{y2}^\dagger \tau \\ &= H^{\otimes 2} P \left(R_{x1}^2 R_{y1}^\dagger R_{y1} R_{x1}^\dagger R_{y1}^\dagger\right)\left(R_{x2}^2 R_{y2}^\dagger R_{y2} R_{x2} R_{y2}^\dagger\right)\tau \\ &= H^{\otimes 2} P \left(R_{x1} R_{y1}^\dagger\right)\left(R_{x2}^3 R_{y2}^\dagger\right)\tau \\ &= R_{x1}^\dagger R_{y1}^\dagger R_{x2}^\dagger R_{y2}^\dagger \tau R_{x1} R_{y1}^\dagger R_{x2}^\dagger R_{y2}^\dagger \tau \quad (x_0 = 2) \end{aligned}$$

$$\begin{aligned} G &= H^{\otimes 2} P H^{\otimes 2} O_2 \\ &= H^{\otimes 2} P R_{x1}^2 R_{y1}^\dagger R_{x2}^2 R_{y2}^\dagger R_{y1} R_{x1} R_{y1}^\dagger R_{y2} R_{x2}^\dagger R_{y2}^\dagger \tau \\ &= H^{\otimes 2} P \left(R_{x1}^2 R_{y1}^\dagger R_{y1} R_{x1} R_{y1}^\dagger\right)\left(R_{x2}^2 R_{y2}^\dagger R_{y2} R_{x2}^\dagger R_{y2}^\dagger\right)\tau \\ &= H^{\otimes 2} P \left(R_{x1}^3 R_{y1}^\dagger\right)\left(R_{x2} R_{y2}^\dagger\right)\tau \\ &= R_{x1}^\dagger R_{y1}^\dagger R_{x2}^\dagger R_{y2}^\dagger \tau R_{x1}^\dagger R_{y1}^\dagger R_{x2} R_{y2}^\dagger \tau \quad (x_0 = 1) \end{aligned}$$

$$\begin{aligned} G &= H^{\otimes 2} P H^{\otimes 2} O_0 \\ &= H^{\otimes 2} P R_{x1}^2 R_{y1}^\dagger R_{x2}^2 R_{y2}^\dagger R_{y1} R_{x1} R_{y1}^\dagger R_{y2} R_{x2} R_{y2}^\dagger \tau \\ &= H^{\otimes 2} P \left(R_{x1}^2 R_{y1}^\dagger R_{y1} R_{x1} R_{y1}^\dagger\right)\left(R_{x2}^2 R_{y2}^\dagger R_{y2} R_{x2} R_{y2}^\dagger\right)\tau \\ &= H^{\otimes 2} P \left(R_{x1}^3 R_{y1}^\dagger\right)\left(R_{x2}^3 R_{y2}^\dagger\right)\tau \\ &= R_{x1}^\dagger R_{y1}^\dagger R_{x2}^\dagger R_{y2}^\dagger \tau R_{x1}^\dagger R_{y1}^\dagger R_{x2}^\dagger R_{y2}^\dagger \tau \quad (x_0 = 0) \end{aligned}$$

7.52

-

8 Quantum noise and quantum operations

Exercises: 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9, 8.10, 8.11, 8.12, 8.13, 8.14, 8.15, 8.16, 8.17, 8.18, 8.19, 8.20, 8.21, 8.22, 8.23, 8.24, 8.25, 8.26, 8.27, 8.28, 8.29, 8.30, 8.31, 8.32, 8.33, 8.34, 8.35.

8.1

A unitary operator acting on a pure state results in a pure state, that is, $|\psi\rangle \to U|\psi\rangle \equiv |\phi\rangle$. Therefore, if initially we have $\rho = |\psi\rangle\langle\psi|$, then after the process we have

$$\mathcal{E}(\rho) = |\phi\rangle\langle\phi| = \big(U|\psi\rangle\big)\big(\langle\psi|U^\dagger\big) = U|\psi\rangle\langle\psi|U^\dagger = U\rho U^\dagger.$$

8.2

For an initial state $|\psi^j\rangle$, the state immediately after measurement, associated with the measurement outcome m, is given by

$$|\psi_m\rangle = \frac{M_m|\psi^j\rangle}{\sqrt{p(m)}}.$$

Considering density operators, initially we may have any general state $\rho = \sum_j p_j|\psi^j\rangle\langle\psi^j|$. So the final state is obtained considering all possible pure initial states $|\psi^j\rangle$, which occur with probability p_j, that could result in measurement outcome m. It is given by

$$\sum_j p_j \frac{M_m|\psi^j\rangle\langle\psi^j|M_m^\dagger}{p(m)} = \frac{M_m\left(\sum_j p_j|\psi^j\rangle\langle\psi^j|\right)M_m^\dagger}{p(m)} = \frac{M_m\rho M_m^\dagger}{p(m)} = \frac{\mathcal{E}_m(\rho)}{p(m)}.$$

The probability of obtaining the measurement result m is $p(m) = \sum_j p_j\langle\psi^j|M_m M_m^\dagger|\psi^j\rangle$. If we consider a basis $\{|\phi_k\rangle\}$ we may write

$$\begin{aligned}
p(m) &= \sum_j\sum_k p_j\left\langle\psi^j\,\middle|\,M_m^\dagger\,\middle|\,\phi_k\right\rangle\left\langle\phi_k\,\middle|\,M_m\,\middle|\,\psi^j\right\rangle \\
&= \sum_k\sum_j p_j\left\langle\phi_k\,\middle|\,M_m\,\middle|\,\psi^j\right\rangle\left\langle\psi^j\,\middle|\,M_m^\dagger\,\middle|\,\phi_k\right\rangle \\
&= \sum_k \langle\phi_k|\,\mathcal{E}_m(\rho)\,|\phi_k\rangle \\
&= \mathrm{tr}(\mathcal{E}_m(\rho)),
\end{aligned}$$

and the final state is $\mathcal{E}_m(\rho)/\mathrm{tr}(\mathcal{E}_m(\rho))$.

8.3

The resulting state can be written as

$$\mathcal{E}(\rho) = \mathrm{tr}_{AD}\Big(U\Big[\rho\otimes|0\rangle\langle 0|\Big]U^\dagger\Big),$$

where $\rho \in AB$, $|0\rangle\langle 0| \in CD$ and U acts on states living in $ABCD$. Let $\{|\phi_k\rangle\}$ be a basis for subspace AD. Then we can write

$$\mathcal{E}(\rho) = \sum_k \left\langle\phi_k\,\middle|\,U\Big[\rho\otimes|0\rangle\langle 0|\Big]U^\dagger\,\middle|\,\phi_k\right\rangle$$

$$= \sum_k \langle \phi_k | U | 0 \rangle \, \rho \, \langle 0 \,|\, U^\dagger \,|\, \phi_k \rangle \, .$$

Here we can identify the linear operators $E_k \equiv \langle \phi_k \,|\, U \,|\, 0 \rangle$ such that the map $\mathcal{E}(\rho)$ can be written as

$$\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger .$$

These operators are such that

$$\sum_k E_k^\dagger E_k = \sum_k \langle 0 \,|\, U^\dagger \,|\, \phi_k \rangle \, \langle \phi_k \,|\, U \,|\, 0 \rangle \, .$$

Since the $|\phi_k\rangle$ form a complete basis for subspace AD we have that $\sum_k |\phi_k\rangle\langle\phi_k| = I$ and therefore $\sum_k E_k^\dagger E_k = I$.

8.4

$$\begin{aligned} E_0 &= \langle 0 \,|\, (P_0 \otimes I + P_1 \otimes X) \,|\, 0 \rangle \\ &= P_0 \, \langle 0 \,|\, 0 \rangle + P_1 \, \langle 0 \,|\, 1 \rangle \\ &= P_0, \end{aligned}$$

$$\begin{aligned} E_1 &= \langle 1 \,|\, (P_0 \otimes I + P_1 \otimes X) \,|\, 0 \rangle \\ &= P_0 \, \langle 1 \,|\, 0 \rangle + P_1 \, \langle 1 \,|\, 1 \rangle \\ &= P_1. \end{aligned}$$

Therefore

$$\mathcal{E}(\rho) = P_0 \rho P_0 + P_1 \rho P_1.$$

8.5

$$\begin{aligned} E_0 &= \left\langle 0 \,\middle|\, \left(\frac{X}{\sqrt{2}} \otimes I + \frac{Y}{\sqrt{2}} \otimes X \right) \,\middle|\, 0 \right\rangle \\ &= \frac{X}{\sqrt{2}} \, \langle 0 \,|\, 0 \rangle + \frac{Y}{\sqrt{2}} \, \langle 0 \,|\, 1 \rangle \\ &= \frac{X}{\sqrt{2}}, \end{aligned}$$

$$\begin{aligned} E_1 &= \left\langle 1 \,\middle|\, \left(\frac{X}{\sqrt{2}} \otimes I + \frac{Y}{\sqrt{2}} \otimes X \right) \,\middle|\, 0 \right\rangle \\ &= \frac{X}{\sqrt{2}} \, \langle 1 \,|\, 0 \rangle + \frac{Y}{\sqrt{2}} \, \langle 1 \,|\, 1 \rangle \end{aligned}$$

$$= \frac{Y}{\sqrt{2}}.$$

Therefore

$$\mathcal{E}(\rho) = \frac{1}{2}\left(X\rho X + Y\rho Y\right).$$

8.6

For $\mathcal{E}$ and $\mathcal{F}$ acting on the same space, we consider a principal system A with Hilbert space $\mathscr{H}$ and an environment system B with Hilbert space $\mathscr{H}_{\text{env}}$. Then, for $\rho \in \mathscr{H}$, $\rho_{\text{env}} = \sum_j p_j \left|e_j\right\rangle\!\left\langle e_j\right| \in \mathscr{H}_{\text{env}}$, and unitaries $U_{\mathcal{E}}$ and $U_{\mathcal{F}}$ acting on states of $\mathscr{H} \otimes \mathscr{H}_{\text{env}}$, $\mathcal{E}$ and F can be written as

$$\mathcal{E}(\rho) = \text{tr}_B\Big(U_{\mathcal{E}}\rho \otimes \rho_{\text{env}} U_{\mathcal{E}}^\dagger\Big),$$
$$\mathcal{F}(\rho) = \text{tr}_B\Big(U_{\mathcal{F}}\rho \otimes \rho_{\text{env}} U_{\mathcal{F}}^\dagger\Big).$$

In the operation-sum representation they are given by

$$\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger,$$
$$\mathcal{F}(\rho) = \sum_k F_k \rho F_k^\dagger,$$

where $E_k \equiv \sum_j \sqrt{p_j}\left\langle e_k\right|U_{\mathcal{E}}\left|e_j\right\rangle$ and $F_k \equiv \sum_j \sqrt{p_j}\left\langle e_k\right|U_{\mathcal{F}}\left|e_j\right\rangle$. A composition $\mathcal{F}\circ\mathcal{E}(\rho) \equiv \mathcal{F}(\mathcal{E}(\rho))$ of the operations will be given by

$$\begin{aligned}\mathcal{F}(\mathcal{E}(\rho)) &= \sum_k F_k \mathcal{E}(\rho) F_k^\dagger \\ &= \sum_k \sum_l F_k E_l \rho E_l^\dagger F_k^\dagger \\ &= \sum_{k,l} F_k E_l \rho \left(F_k E_l\right)^\dagger.\end{aligned}$$

Here we can identify linear operators $G_{kl} \equiv F_k E_l$ such that the composition can be written as

$$\mathcal{F}(\mathcal{E}(\rho)) = \sum_{k,l} G_{kl}\rho G_{kl}^\dagger,$$

meaning the composition is also a quantum operation.

For $\mathcal{E}$ and $\mathcal{F}$ acting on different spaces we must consider a system $A^{\mathcal{E}} \otimes B^{\mathcal{E}}$ with Hilbert space $\mathscr{H}^{\mathcal{E}} \otimes \mathscr{H}_{\text{env}}^{\mathcal{E}}$ for $\mathcal{E}$ and another system $A^{\mathcal{F}} \otimes B^{\mathcal{F}}$ with Hilbert space $\mathscr{H}^{\mathcal{F}} \otimes \mathscr{H}_{\text{env}}^{\mathcal{F}}$ for $\mathcal{F}$. The operations have the same form as before with the difference that now each part belongs to its own space. We can naturally construct the spaces $\mathscr{H} \equiv \mathscr{H}^{\mathcal{E}} \otimes \mathscr{H}^{\mathcal{F}}$ and $\mathscr{H}_{\text{env}} \equiv \mathscr{H}_{\text{env}}^{\mathcal{E}} \otimes \mathscr{H}_{\text{env}}^{\mathcal{F}}$ and consider the unitary $U \equiv U_{\mathcal{E}} \otimes U_{\mathcal{F}}$ acting on states of $\mathscr{H} \otimes \mathscr{H}_{\text{env}}$. If we define the quantum operation given by

$$\mathcal{G}(\rho) = \text{tr}_{B^{\mathcal{E}}\otimes B^{\mathcal{F}}}\big(U\rho \otimes \rho_{\text{env}} U^\dagger\big),$$

for $\rho \in \mathscr{H}$ and $\rho_{\text{env}} = \rho_{\text{env}}^{\mathcal{E}} \otimes \rho_{\text{env}}^{\mathcal{F}} \in \mathscr{H}_{\text{env}}$, we see that it can be explicitly written as

$$\begin{aligned}
\mathcal{G}(\rho) &= \text{tr}_{B^{\mathcal{F}}}\Big(\text{tr}_{B^{\mathcal{E}}}\Big([U_{\mathcal{E}} \otimes U_{\mathcal{F}}]\left[\rho \otimes \rho_{\text{env}}^{\mathcal{E}} \otimes \rho_{\text{env}}^{\mathcal{F}}\right]\left[U_{\mathcal{E}}^{\dagger} \otimes U_{\mathcal{F}}^{\dagger}\right]\Big)\Big) \\
&= \text{tr}_{B^{\mathcal{F}}}\Big(U_{\mathcal{F}}\text{tr}_{B^{\mathcal{E}}}\Big(U_{\mathcal{E}}\left[\rho \otimes \rho_{\text{env}}^{\mathcal{E}}\right]U_{\mathcal{E}}^{\dagger}\Big) \otimes \rho_{\text{env}}^{\mathcal{F}}U_{\mathcal{F}}^{\dagger}\Big) \\
&= \text{tr}_{B^{\mathcal{F}}}\Big(U_{\mathcal{F}}\mathcal{E}(\rho) \otimes \rho_{\text{env}}^{\mathcal{F}}U_{\mathcal{F}}^{\dagger}\Big) \\
&= \mathcal{F}(\mathcal{E}(\rho)),
\end{aligned}$$

where the unitaries are implicitly understood as $U_{\mathcal{E}} \equiv U_{\mathcal{E}} \otimes I$ and $U_{\mathcal{F}} \equiv I \otimes U_{\mathcal{F}}$. This result shows that the composition of quantum operations acting on different spaces is also a quantum operation.

8.7

After applying a unitary U to the entire system and doing a general measurement with operators M_m, which results in measurement outcome m, the entire system is left on state

$$\frac{M_m U\rho \otimes \sigma U^{\dagger}M_m^{\dagger}}{p(m)} = \frac{M_m U\rho \otimes \sum_j q_j \left|e_j\right\rangle\!\left\langle e_j\right| U^{\dagger}M_m^{\dagger}}{p(m)},$$

where we are considering a basis $\{|e_j\rangle\}$ for the environment such that the initial state σ is diagonal. By tracing it over the environment we get the normalized quantum operation $\mathcal{E}_m(\rho)$ acting on the principal system, that is

$$\frac{\mathcal{E}_m(\rho)}{p(m)} = \frac{\text{tr}_E\Big(M_m U\rho \otimes \sum_j q_j \left|e_j\right\rangle\!\left\langle e_j\right| U^{\dagger}M_m^{\dagger}\Big)}{p(m)} = \frac{\sum_{j,k} q_j \left\langle e_k \,\middle|\, M_m U\rho \otimes \left|e_j\right\rangle\!\left\langle e_j\right| U^{\dagger}M_m^{\dagger} \,\middle|\, e_k\right\rangle}{p(m)}.$$

Now it is possible to identify the linear operators $E_{jk} \equiv \sqrt{q_j}\left\langle e_k \,\middle|\, M_m U \,\middle|\, e_j\right\rangle$ such that we can write $\mathcal{E}_m(\rho) = \sum_{j,k} E_{jk}\rho E_{jk}^{\dagger}$. The probability of obtaining measurement outcome m will be given by

$$\begin{aligned}
p(m) &= \text{tr}\big(M_m^{\dagger}M_m U\rho \otimes \sigma U^{\dagger}\big] \\
&= \text{tr}\left(M_m U\rho \otimes \sigma U^{\dagger}M_m^{\dagger}\sum_k \left|e_k\right\rangle\!\left\langle e_k\right|\right) \\
&= \text{tr}\left(\sum_k \left\langle e_k \,\middle|\, M_m U\rho \otimes \sigma U^{\dagger}M_m^{\dagger} \,\middle|\, e_k\right\rangle\right) \\
&= \text{tr}\big(\text{tr}_E\big(M_m U\rho \otimes \sigma U^{\dagger}M_m^{\dagger}\big)\big) \\
&= \text{tr}(\mathcal{E}_m(\rho)).
\end{aligned}$$

8.8

By following the exact same procedure as the trace-preserving case with the addition of operator $E_{\infty} \neq 0$, such that, $\sum_k E_k^{\dagger}E_k + E_{\infty}^{\dagger}E_{\infty} = I$, we will have that $\sum_k E_k^{\dagger}E_k \leq I$, which characterizes a non-trace-preserving quantum operation.

8.9

Applying U and then measuring with operators P_m in sequence will give the measurement outcome m with probability

$$\begin{aligned}
p(m) &= \mathrm{tr}\big(P_m^\dagger P_m U\rho\otimes|e_0\rangle\langle e_0|\,U^\dagger\big)\\
&= \mathrm{tr}\left(\sum_k |m,k\rangle\langle m,k| \sum_{m',m'',k',k''} E_{m'k'}\rho\otimes|m',k'\rangle\langle m'',k''|\,E_{m''k''}^\dagger\right)\\
&= \mathrm{tr}\left(\sum_{m',m'',k,k',k''} \langle m,k\,|\,m',k'\rangle\, E_{m'k'}\rho E_{m''k''}^\dagger\,\langle m'',k''\,|\,m,k\rangle\right)\\
&= \mathrm{tr}\left(\sum_k E_{mk}\rho E_{mk}^\dagger\right)\\
&= \mathrm{tr}(\mathcal{E}_m(\rho)).
\end{aligned}$$

The principal system, after the process, will therefore be in the state

$$\frac{\mathrm{tr}_E\big(P_m U\rho\otimes|e_0\rangle\langle e_0|\,U^\dagger P_m^\dagger\big)}{p(m)} = \frac{\mathcal{E}_m(\rho)}{\mathrm{tr}(\mathcal{E}_m(\rho))}.$$

8.10

Let $\{|l\rangle\}$ be a basis for the d-dimentional Hilbert space and let $\{E_1,\cdots,E_n\}$, for $n>d^2$, be the set of elements for the operator-sum representation of $\mathcal{E}$. Then we can define an $n\times n$ matrix W such that its entries are given by $W_{jk}\equiv\mathrm{tr}(E_j^\dagger E_k)$, which can be explicitly written as

$$\begin{aligned}
W_{jk} &= \sum_{l=1}^{d}\left\langle l\,\middle|\,E_j^\dagger E_k\,\middle|\,l\right\rangle\\
&= \sum_{l=1}^{d}\sum_{m=1}^{d}\left\langle l\,\middle|\,E_j^\dagger\,\middle|\,m\right\rangle\langle m\,|\,E_k\,|\,l\rangle\,.
\end{aligned}$$

W is clearly hermitian since

$$W_{jk} = \sum_{l=1}^{d}\left\langle l\,\middle|\,E_j^\dagger E_k\,\middle|\,l\right\rangle = \sum_{l=1}^{d}\left\langle l\,\middle|\,E_k^\dagger E_j\,\middle|\,l\right\rangle^\dagger = W_{kj}^*.$$

Furthermore, since there are d independent $|l\rangle$ and d independent $|m\rangle$ there are at most d^2 independent terms $\langle m\,|\,E_k\,|\,l\rangle$. This means that any entry belonging in a row or column in W beyond d^2 can be written as a linear combination of, at most, the first d^2 rows and columns, that is, for any integer $a>0$, we have that

$$W_{(d^2+a)k} = \sum_{j=1}^{d^2} b_j W_{jk} \quad\text{and}\quad W_{j(d^2+a)} = \sum_{k=1}^{d^2} c_k W_{jk},$$

meaning $\text{rank}(W) \equiv r \leq d^2$. Since W has rank $r \leq d^2$ and is Hermitian, there exists an $n \times n$ unitary matrix u such that $D \equiv uWu^\dagger$ is diagonal with $r \leq d^2$ non-zero entries. The entries of D are given by $D_{lm} = \delta_{lm}\lambda_m$. Therefore, the relation between W and D can be written as

$$\begin{aligned}\delta_{lm}\lambda_m &= \sum_{j,k=1}^{n} u_{lj} W_{jk} u^*_{km} \\ &= \sum_{j,k=1}^{n} \text{tr}\Big(u_{lj} E_j^\dagger E_k u^*_{km}\Big)\end{aligned}$$

$$\implies \quad \lambda_l = \sum_{j,k=1}^{n} \text{tr}\Big(u_{lj} E_j^\dagger E_k u^*_{kl}\Big).$$

Then, by defining a set of n operators $F_j = \sum_{k=1}^{n} E_k u^*_{kj}$ we have

$$\lambda_l = \text{tr}\Big(F_l^\dagger F_l\Big) = \sum_{p=1}^{d} \Big\langle p \Big| F_l^\dagger F_l \Big| p \Big\rangle = \sum_{p=1}^{d}\sum_{q=1}^{d} \Big\langle p \Big| F_l^\dagger \Big| q \Big\rangle \langle q \,|\, F_l \,|\, p\rangle = \sum_{p,q=1}^{d} |\langle p \,|\, F_l \,|\, q\rangle|^2,$$

and since $\lambda_l = 0$ for $l > r$, it follows that $\sum_{p,q=1}^{d} \langle p \,|\, F_l \,|\, q\rangle = 0$ for $l > r$, and because this must hold for any arbitrary choice of basis, we have that $F_l = 0$ for $l > r$. Since the operators F_j and E_k are related by a unitary transformation then, by Theorem 8.2, we can write

$$\mathcal{E}(\rho) = \sum_{j=1}^{r} F_j \rho F_j^\dagger.$$

8.11

Let $\{|j\rangle\}$ be a basis for the d-dimentional Hilbert space and $\{|j'\rangle\}$ be a basis for the d'-dimentional one. We can write the elements of the operator-sum representation as

$$E_k = \sum_{j=1}^{d}\sum_{j'=1}^{d'} |j'\rangle\langle j'| \, E_k \, |j\rangle\langle j| = \sum_{j=1}^{d}\sum_{j'=1}^{d'} \langle j' \,|\, E_k \,|\, j\rangle \, |j'\rangle\langle j| \,.$$

Since there are d independent $|j\rangle$ and d' independent $|j'\rangle$, there are $r \leq dd'$ independent $\langle j' \,|\, E_k \,|\, j\rangle$, meaning that for $k > r$ it holds

$$\langle j' \,|\, E_k \,|\, j\rangle = \sum_{l=1}^{r} c_l \, \langle j' \,|\, E_l \,|\, j\rangle \,.$$

This is the same as saying that, in a basis where the matrix $\text{tr}\Big(E_j^\dagger E_k\Big)$ is diagonal, there are $r \leq dd'$ non-zero eigenvalues. Then in such basis, for $k > r$ we have

$$0 = \text{tr}\Big(E_k^\dagger E_k\Big) = \sum_{l=1}^{d} \Big\langle l \Big| E_k^\dagger E_k \Big| l \Big\rangle = \sum_{l=1}^{d}\sum_{l'=1}^{d'} \Big\langle l \Big| E_k^\dagger \Big| l' \Big\rangle \langle l' \,|\, E_k \,|\, l\rangle = \sum_{l=1}^{d}\sum_{l'=1}^{d'} |\langle l' \,|\, E_k \,|\, l\rangle|^2,$$

and since it must hold for any choice of basis for the two Hilbert spaces, it follows that $E_k = 0$ for $k > r$ and the quantum operation can be described by

$$\mathcal{E}(\rho) = \sum_{k=1}^{r} E_k \rho E_k^\dagger.$$

8.12

All orthogonal matrices are such that $\det(O) = \pm 1$. The subgroup of orthogonal matrices whose determinant is -1 do not include the identity matrix. Since the set of possible matrices O must include the identity matrix, for when M is symmetric, it follows that $\det(O) = 1$.

8.13

From theorem 4.1, any unitary operator can be written as $U = e^{i\alpha} R_z(\theta) R_y(\phi) R_z(\psi)$, which corresponds to active rotations of the Bloch vector. Alternatively, it can be interpreted as passive rotations of the Bloch sphere.

8.14

M is a real matrix and thus, can have a negative determinant. We have that $\det(M) = \det(OS) = \det(O)\det(S) = \det(S)$, and therefore $\det(S)$ can be negative.

8.15

Just like the measurement in the $\{|0\rangle, |1\rangle\}$ basis (or equivalently, the phase-flip channel with $p = 1/2$), where the entire Bloch sphere collapses on the Z axis, a measurement in the $\{|+\rangle, |-\rangle\}$ causes the Bloch sphere to collapse on the X axis. To see this explicitly let us consider an initial state $\rho = (I + \vec{r} \cdot \vec{\sigma})/2$, where $\vec{r} = \{r_x, r_y, r_z\}$ with $\|\vec{r}\| \leq 1$, and $\vec{\sigma} = \{X, Y, Z\}$. The evolved state will be

$$\begin{aligned}
\mathcal{E}(\rho) &= \frac{1}{2} |+\rangle\langle+| (I + r_x X + r_y Y + r_z Z) |+\rangle\langle+| + \frac{1}{2} |-\rangle\langle-| (I + r_x X + r_y Y + r_z Z) |-\rangle\langle-| \\
&= \frac{1}{2} (1 + r_x + 0 + 0) |+\rangle\langle+| + \frac{1}{2} (1 - r_x + 0 + 0) |-\rangle\langle-| \\
&= \frac{1 + r_x}{4} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} + \frac{1 - r_x}{4} \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} \\
&= \frac{1}{2} \begin{bmatrix} 1 & r_x \\ r_x & 1 \end{bmatrix} = \frac{I + r_x X}{2}.
\end{aligned}$$

That is, the Bloch vector is given by $\{r_x, 0, 0\}$, meaning the Bloch sphere collapsed on the X axis.

8.16

Consider $\mathcal{E}_0(\rho) = |0\rangle\langle 0| \rho |0\rangle\langle 0|$, that is, a quantum operation that describes the outcome $|0\rangle$ for a measurement in the computational basis. This cannot be seen as a deformation of the Bloch sphere.

To see this, consider an initial state $|\psi\rangle = a|0\rangle + b|1\rangle$. The action of the quantum operation yields

$$\begin{aligned}\mathcal{E}_0(\rho) &= \frac{1}{2}|0\rangle\langle 0|\left(|a|^2|0\rangle\langle 0| + ab^*|0\rangle\langle 1| + a^*b|1\rangle\langle 0| + |b|^2|1\rangle\langle 1|\right)|0\rangle\langle 0| \\ &= \frac{|a|^2}{2}|0\rangle\langle 0| = \begin{bmatrix}|a|^2 & 0\\ 0 & 0\end{bmatrix}.\end{aligned}$$

Since this is not a density operator for general a it cannot be associated with a Bloch sphere.

8.17

$$\begin{aligned}\mathcal{E}(I) &= \frac{I + XIX + YIY + ZIZ}{4} = \frac{I + I + I + I}{4} = I, \\ \mathcal{E}(X) &= \frac{X + XXX + YXY + ZXZ}{4} = \frac{X + X - X - X}{4} = 0, \\ \mathcal{E}(Y) &= \frac{Y + XXX + YYY + ZYZ}{4} = \frac{Y - Y + Y - Y}{4} = 0, \\ \mathcal{E}(Z) &= \frac{Z + XZX + YZY + ZZZ}{4} = \frac{Z - Z - Z + Z}{4} = 0.\end{aligned}$$

Any density operator can be written as $\rho = (I + \vec{r}\cdot\vec{\sigma})/2$ for $\vec{r} = \{r_x, r_y, r_z\}$, with $\|\vec{r}\| \leq 1$, and $\vec{\sigma} = \{X, Y, Z\}$, thus

$$\mathcal{E}(\rho) = \frac{1}{2}\mathcal{E}(I) + \frac{r_x}{2}\mathcal{E}(X) + \frac{r_y}{2}\mathcal{E}(Y) + \frac{r_z}{2}\mathcal{E}(Z) = \frac{I}{2}.$$

Therefore, using the definition of $\mathcal{E}(\rho)$, we have that

$$\frac{I}{2} = \frac{\rho + X\rho X + Y\rho Y + Z\rho Z}{4}.$$

8.18

Let $\{|j\rangle\}$ be a basis for the d-dimensional Hilbert space such that ρ is diagonal, that is,

$$\rho = \sum_{j=1}^{d} q_j |j\rangle\langle j| \quad \Longrightarrow \quad \mathrm{tr}\left(\rho^k\right) = \sum_{j=1}^{k} q_j^k.$$

This trace satisfies $1/d^{k-1} \leq \mathrm{tr}\left(\rho^k\right) \leq 1$. Now let $\mathcal{E}(\rho) \equiv \sigma$, then

$$\begin{aligned}\sigma &= \frac{pI}{d} + (1-p)\rho \\ &= \frac{p}{d}\sum_{j=1}^{k}|j\rangle\langle j| + (1-p)\sum_{j=1}^{k} q_j|j\rangle\langle j| \\ &= \sum_{j=1}^{k}\left[p\left(\frac{1}{d} - q_j\right) + q_j\right]|j\rangle\langle j|\end{aligned}$$

$$\implies \quad \operatorname{tr}\left(\sigma^k\right) = \sum_{j=1}^{k} \left[p\left(\frac{1}{d} - q_j\right) + q_j \right]^k .$$

Notice that treating the term inside square brackets as a function of p, its derivative is constant and equal to $1/d - q_j$, meaning its extreme values always occur for $p = 0$ and $p = 1$. Therefore $\operatorname{tr}\left(\sigma^k\right)$ is bounded by the cases $p = 0$ and $p = 1$. Calculating each case yields

$$\text{for } p = 0: \quad \operatorname{tr}\left(\sigma^k\right) = \sum_{j=1}^{k} q_j^k = \operatorname{tr}\left(\rho^k\right)$$

$$\text{for } p = 1: \quad \operatorname{tr}\left(\sigma^k\right) = \sum_{j=1}^{k} \frac{1}{d^k} = \frac{1}{d^{k-1}} \leq \operatorname{tr}\left(\rho^k\right).$$

Therefore $\operatorname{tr}\left(\sigma^k\right) \leq \operatorname{tr}\left(\rho^k\right)$, with equality holding if $p = 0$ or if ρ is the maximum mixed state.

8.19

If ρ is a density operator it always holds that $\operatorname{tr}(\rho) = 1$. So similarly to the qubit case, we can write the identity matrix in terms of ρ as

$$\frac{I}{d} = \frac{I}{d}\operatorname{tr}(\rho) = \frac{1}{d}\sum_{j=1}^{d} |j\rangle\langle j| \sum_{k=1}^{d} \langle k\,|\,\rho\,|\,k\rangle = \frac{1}{d}\sum_{j=1}^{d}\sum_{k=1}^{d} |j\rangle\langle k|\,\rho\,|k\rangle\langle j|\,.$$

Substituting it in the depolarizing quantum operation yields

$$\begin{aligned}\mathcal{E}(\rho) &= \frac{p}{d}\sum_{j=1}^{d}\sum_{k=1}^{d} |j\rangle\langle k|\,\rho\,|k\rangle\langle j| + (1-p)\rho \\ &= \sum_{j,k=1}^{d} \left(\sqrt{\frac{p}{d}}\,|j\rangle\langle k|\right)\rho\left(\sqrt{\frac{p}{d}}\,|k\rangle\langle j|\right) + \sqrt{1-p}I\rho\sqrt{1-p}I.\end{aligned}$$

Now we can identify $E_0 \equiv \sqrt{1-p}I$ and $E_{jk} \equiv \sqrt{p/d}\,|j\rangle\langle k|$, for j and k ranging from 1 to d, as a set of elements for the operator-sum representation of the generalized depolarizing channel.

8.20

Let the principal system start at state $\rho_{\text{in}} \equiv \sum_i p_i\,|\psi_i\rangle\langle\psi_i|$, with $|\psi_i\rangle = \alpha_i\,|0\rangle + \beta_i\,|1\rangle$, meaning the total state is $\rho = \sum_i p_i\,(\alpha_i\,|00\rangle + \beta_i\,|10\rangle)\,(\alpha_i^*\,\langle 00| + \beta_i^*\,\langle 10|)$. Then the action of the circuit will be

$$\begin{aligned}\rho &\xrightarrow{CR_y(\theta)_{(1,2)}} \sum_i p_i \left(\alpha_i\,|00\rangle + \beta_i \cos\frac{\theta}{2}\,|10\rangle + \beta_i \sin\frac{\theta}{2}\,|11\rangle\right)\left(\alpha_i^*\,\langle 00| + \beta_i^* \cos\frac{\theta}{2}\,\langle 10| + \beta_i^* \sin\frac{\theta}{2}\,\langle 11|\right) \\ &\xrightarrow{CX_{(2,1)}} \sum_i p_i \left(\alpha_i\,|00\rangle + \beta_i \cos\frac{\theta}{2}\,|10\rangle + \beta_i \sin\frac{\theta}{2}\,|01\rangle\right)\left(\alpha_i^*\,\langle 00| + \beta_i^* \cos\frac{\theta}{2}\,\langle 10| + \beta_i^* \sin\frac{\theta}{2}\,\langle 01|\right).\end{aligned}$$

We may call this state ρ'. Then, a measurement of the environment is made, which yields

$$\rho_{\text{out}} = \operatorname{tr}_{\text{env}}(\rho')$$

$$
\begin{aligned}
&= \sum_i p_i \left[\left(\alpha_i |0\rangle + \beta_i \cos\frac{\theta}{2} |1\rangle \right) \left(\alpha_i^* \langle 0| + \beta_i^* \cos\frac{\theta}{2} \langle 1| \right) + \left(\beta_i \sin\frac{\theta}{2} |0\rangle \right) \left(\beta_i^* \sin\frac{\theta}{2} \langle 0| \right) \right] \\
&= \sum_i p_i \left[\left(|\alpha_i|^2 + |\beta_i|^2 \sin^2\frac{\theta}{2} \right) |0\rangle\langle 0| + \alpha_i \beta_i^* \cos\frac{\theta}{2} |0\rangle\langle 1| + \alpha_i^* \beta_i \cos\frac{\theta}{2} |1\rangle\langle 0| + |\beta_i|^2 \cos^2\frac{\theta}{2} |1\rangle\langle 1| \right] \\
&= \sum_i p_i \begin{bmatrix} |\alpha_i|^2 + |\beta_i|^2 \sin^2\frac{\theta}{2} & \alpha_i \beta_i^* \cos\frac{\theta}{2} \\ \alpha_i^* \beta_i \cos\frac{\theta}{2} & |\beta_i|^2 \cos^2\frac{\theta}{2} \end{bmatrix}.
\end{aligned}
$$

Applying the amplitude damping channel to the same initial state yields

$$
\begin{aligned}
\mathcal{E}_{\mathrm{AD}}(\rho_{\mathrm{in}}) &= E_0 \rho_{\mathrm{in}} E_0^\dagger + E_1 \rho_{\mathrm{in}} E_1^\dagger \\
&= \sum_i p_i \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{bmatrix} \begin{bmatrix} |\alpha_i|^2 & \alpha_i \beta_i^* \\ \alpha_i^* \beta_i & |\beta_i|^2 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{bmatrix} + \sum_i p_i \begin{bmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{bmatrix} \begin{bmatrix} |\alpha_i|^2 & \alpha_i \beta_i^* \\ \alpha_i^* \beta_i & |\beta_i|^2 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ \sqrt{\gamma} & 0 \end{bmatrix} \\
&= \sum_i p_i \begin{bmatrix} |\alpha_i|^2 + |\beta_i|^2 \gamma & \alpha_i \beta_i^* \sqrt{1-\gamma} \\ \alpha_i^* \beta_i \sqrt{1-\gamma} & |\beta_i|^2 (1-\gamma) \end{bmatrix}.
\end{aligned}
$$

From this result we see that setting $\sin^2\frac{\theta}{2} = \gamma$, both quantities coincide.

8.21

In general, if $\{|m\rangle\}$ is a basis for the principal system then E_k can be written as

$$
E_k = \langle k_b | U | 0_b \rangle \equiv \sum_{m,n} \langle m, k_b | U | n, 0_b \rangle |m\rangle\langle n| ,
$$

and considering the basis $\{|m\rangle\}$ as the eigenstates of $a^\dagger a$, we have

$$
\begin{aligned}
E_k &= \sum_{m,n} \left\langle m, k_b \left| U \frac{\left(a^\dagger\right)^n}{\sqrt{n!}} \right| 0, 0_b \right\rangle |m\rangle\langle n| \\
&= \sum_{m,n} \frac{1}{\sqrt{n!}} \left\langle m, k_b \left| U \left(a^\dagger\right)^n \right| 0, 0_b \right\rangle |m\rangle\langle n| .
\end{aligned}
$$

Notice that we may write $U\left(a^\dagger\right)^n = U\left(a^\dagger U^\dagger U\right)^n = \left(U a^\dagger U^\dagger\right)^n U$, thus

$$
E_k = \sum_{m,n} \frac{1}{\sqrt{n!}} \left\langle m, k_b \left| \left(U a^\dagger U^\dagger\right)^n U \right| 0, 0_b \right\rangle |m\rangle\langle n| .
$$

The unitary operator is given by

$$
U = \exp\left[-i\chi \left(a^\dagger b + a b^\dagger\right) \Delta t\right] = \sum_{n=0}^{\infty} \frac{(-i\chi\Delta t)^n}{n!} \left(a^\dagger b + a b^\dagger\right)^n .
$$

Given that $a|0\rangle = 0$ and $b|0_b\rangle = 0$, it follows that, when acting on the vacuum state of both modes, the unitary operator yields $U|0, 0_b\rangle = |0, 0_b\rangle$, and we get

$$
E_k = \sum_{m,n} \frac{1}{\sqrt{n!}} \left\langle m, k_b \left| \left(U a^\dagger U^\dagger\right)^n \right| 0, 0_b \right\rangle |m\rangle\langle n| .
$$

The physical interpretation is, of course, that since it is the vacuum state, there are no particles to be created or annihilated in any mode, and the state remains at the vacuum. Using the Baker-Campbell-Hausdorff formula, we obtain

$$Ua^\dagger U^\dagger = \sum_{j=0}^{\infty} \frac{(-i\chi\Delta t)^j}{j!} C_j,$$

where $C_0 \equiv a^\dagger$ and $C_j \equiv \left[a^\dagger b + ab^\dagger, C_{j-1}\right]$. From this recursive relation we calculate

$$\begin{aligned} C_1 &= \left[a^\dagger b + ab^\dagger, a^\dagger\right] = \left[a, a^\dagger\right] b^\dagger = b^\dagger, \\ C_2 &= \left[a^\dagger b + ab^\dagger, b^\dagger\right] = a^\dagger \left[b, b^\dagger\right] = a^\dagger, \end{aligned}$$

that is,

$$C_j = \begin{cases} a^\dagger & \text{for even } j; \\ b^\dagger & \text{for odd } j. \end{cases}$$

Substituting yields

$$\begin{aligned} Ua^\dagger U^\dagger &= \sum_{j=0}^{\infty} \frac{(-i\chi\Delta t)^{2j}}{(2j)!} a^\dagger + \sum_{j=0}^{\infty} \frac{(-i\chi\Delta t)^{2j+1}}{(2j+1)!} b^\dagger \\ &= \sum_{j=0}^{\infty} (-1)^j \frac{(\chi\Delta t)^{2j}}{(2j)!} a^\dagger - i \sum_{j=0}^{\infty} (-1)^j \frac{(\chi\Delta t)^{2j+1}}{(2j+1)!} b^\dagger \\ &= \cos(\chi\Delta t) a^\dagger - i \sin(\chi\Delta t) b^\dagger, \end{aligned}$$

and defining $\gamma \equiv 1 - \cos^2(\chi\Delta t)$ we write $Ua^\dagger U^\dagger = \sqrt{1-\gamma}a^\dagger - i\sqrt{\gamma}b^\dagger$. The quantity that appears in the expression for E_k can therefore be calculated as

$$\begin{aligned} \left(Ua^\dagger U^\dagger\right)^n |0, 0_b\rangle &= \left(\sqrt{1-\gamma}a^\dagger - i\sqrt{\gamma}b^\dagger\right)^n |0, 0_b\rangle \\ &= \sum_{j=0}^{n} \binom{n}{j} \left(\sqrt{1-\gamma}\right)^{n-j} (-i\sqrt{\gamma})^j \left(a^\dagger\right)^{n-j} \left(b^\dagger\right)^j |0, 0_b\rangle \\ &= \sum_{j=0}^{n} (-i)^j \frac{n!}{j!(n-j)!} \sqrt{(1-\gamma)^{n-j} \gamma^j} \sqrt{(n-j)! j!} \, |n-j, j_b\rangle \\ &= \sum_{j=0}^{n} (-i)^j \frac{n!}{\sqrt{j!(n-j)!}} \sqrt{(1-\gamma)^{n-j} \gamma^j} \, |n-j, j_b\rangle \, . \end{aligned}$$

We can ignore the global phase $(-i)^j$ and substitute in the expression for E_k, finally yielding

$$\begin{aligned} E_k &= \sum_{m,n} \sum_{j=0}^{\infty} \frac{1}{\sqrt{n!}} \frac{n!}{\sqrt{j!(n-j)!}} \sqrt{(1-\gamma)^{n-j} \gamma^j} \, \langle m, k_b \,|\, n-j, j_b\rangle \, |m\rangle\langle n| \\ &= \sum_{m,n} \sum_{j=0}^{\infty} \sqrt{\binom{n}{j}} \sqrt{(1-\gamma)^{n-j} \gamma^j} \delta_{m(n-j)} \delta_{kj} \, |m\rangle\langle n| \end{aligned}$$

$$= \sum_n \sqrt{\binom{n}{k}} \sqrt{(1-\gamma)^{n-k}\gamma^k}\, |n-k\rangle\langle n| \,.$$

$$\begin{aligned}
\sum_k E_k^\dagger E_k &= \sum_k \sum_{m,n} \sqrt{\binom{m}{k}\binom{n}{k}} \sqrt{(1-\gamma)^{m+n-2k}\gamma^{2k}}\, |m\rangle \langle m-k \,|\, n-k\rangle \langle n| \\
&= \sum_n \sum_k \binom{n}{k} (1-\gamma)^{n-k}\gamma^k\, |n\rangle\langle n| \\
&= \sum_n \left((1-\gamma)+\gamma\right)^n |n\rangle\langle n| \\
&= \sum_n |n\rangle\langle n| = I,
\end{aligned}$$

meaning the elements E_k define a trace-preserving quantum operation.

8.22

$$\begin{aligned}
\mathcal{E}_{\mathrm{AD}}(\rho) &= E_0\rho E_0^\dagger + E_1\rho E_1^\dagger \\
&= \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{bmatrix} \begin{bmatrix} a & b \\ b^* & c \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{bmatrix} + \begin{bmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ b^* & c \end{bmatrix} \begin{bmatrix} 0 & 0 \\ \sqrt{\gamma} & 0 \end{bmatrix} \\
&= \begin{bmatrix} a+c\gamma & b\sqrt{1-\gamma} \\ b^*\sqrt{1-\gamma} & c\,(1-\gamma) \end{bmatrix},
\end{aligned}$$

and since $a + c = 1$

$$\mathcal{E}_{\mathrm{AD}}(\rho) = \begin{bmatrix} a+\gamma(1-a) & b\sqrt{1-\gamma} \\ b^*\sqrt{1-\gamma} & c\,(1-\gamma) \end{bmatrix} = \begin{bmatrix} 1-(1-\gamma)(1-a) & b\sqrt{1-\gamma} \\ b^*\sqrt{1-\gamma} & c\,(1-\gamma) \end{bmatrix}.$$

8.23

$$\rho \equiv |\psi\rangle\langle\psi| = \left(a\,|01\rangle + b\,|10\rangle\right)\left(a^*\,\langle 01| + b^*\,\langle 10|\right).$$

We may write $(\mathcal{E}_{\mathrm{AD}} \otimes \mathcal{E}_{\mathrm{AD}})(\rho)$ as a composition, that is, $\mathcal{E}_{\mathrm{AD}} \otimes \mathcal{E}_{\mathrm{AD}} = (I \otimes \mathcal{E}_{\mathrm{AD}})(\mathcal{E}_{\mathrm{AD}} \otimes I)$. Therefore

$$\begin{aligned}
\mathcal{E}_{\mathrm{AD}}(\rho) &= (I \otimes \mathcal{E}_{\mathrm{AD}}) \left((E_0 \otimes I)\,|\psi\rangle\langle\psi| \left(E_0^\dagger \otimes I\right) + (E_1 \otimes I)\,|\psi\rangle\langle\psi| \left(E_1^\dagger \otimes I\right) \right) \\
&= (I \otimes \mathcal{E}_{\mathrm{AD}}) \left(\left(a\,|01\rangle + \sqrt{1-\gamma}b\,|10\rangle\right) \left(a^*\,\langle 01| + \sqrt{1-\gamma}b^*\,\langle 10|\right) + \left(\sqrt{\gamma}b\,|00\rangle\right)\left(\sqrt{\gamma}b^*\,\langle 00|\right) \right) \\
&= \left(\sqrt{1-\gamma}a\,|01\rangle + \sqrt{1-\gamma}b\,|10\rangle\right) \left(\sqrt{1-\gamma}a^*\,\langle 01| + \sqrt{1-\gamma}b^*\,\langle 10|\right) \\
&\quad + \left(\sqrt{\gamma}b\,|00\rangle\right)\left(\sqrt{\gamma}b^*\,\langle 00|\right) + \left(\sqrt{\gamma}a\,|00\rangle\right)\left(\sqrt{\gamma}a^*\,\langle 00|\right) \\
&= \sqrt{1-\gamma}\left(a\,|01\rangle + b\,|10\rangle\right)\left(a^*\,\langle 01| + b^*\,\langle 10|\right)\sqrt{1-\gamma} + \sqrt{\gamma}\,(a+b)\,|00\rangle\langle 00|\,(a^*+b^*)\,\sqrt{\gamma} \\
&= \sqrt{1-\gamma}I\rho\sqrt{1-\gamma}I + \sqrt{\gamma}\left(|00\rangle\langle 01| + |00\rangle\langle 10|\right)\rho\sqrt{\gamma}\left(|01\rangle\langle 00| + |10\rangle\langle 00|\right).
\end{aligned}$$

Here we can identity the two elements of the operator-sum representation $E_0^{\text{dr}} \equiv \sqrt{1-\gamma}I$ and $E_1^{\text{dr}} \equiv \sqrt{\gamma}\left(|00\rangle\langle 01| + |00\rangle\langle 10|\right)$

8.24

The unitary operation resulting from the Jaynes-Cummings interaction with detuning $\delta = 0$ is

$$U = |00\rangle\langle 00| + \cos\Omega t\left(|01\rangle\langle 01| + |10\rangle\langle 10|\right) - i\sin\Omega t\left(|01\rangle\langle 10| + |10\rangle\langle 01|\right).$$

The corresponding quantum operation for when we trace over the field system, considering it to initially be the vacuum state, will have elements $E_k = \langle k\,|\,U\,|\,0\rangle$. This gives us

$$\begin{aligned} E_0 &= \langle 0\,|\,U\,|\,0\rangle = |0\rangle\langle 0| + \cos\Omega t\,|1\rangle\langle 1|\,, \\ E_1 &= \langle 1\,|\,U\,|\,0\rangle = -i\sin\Omega t\,|0\rangle\langle 1|\,. \end{aligned}$$

Ignoring the global phase $-i$ and defining $\gamma \equiv \sin^2\Omega t$ we get

$$E_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{bmatrix} \quad \text{and} \quad E_1 = \begin{bmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{bmatrix},$$

which correspond to the amplitude damping operation elements.

8.25

The state with temperature T is given by

$$\rho = \frac{e^{-E_0/k_{\text{B}}T}\,|0\rangle\langle 0| + e^{-E_1/k_{\text{B}}T}\,|1\rangle\langle 1|}{e^{-E_0/k_{\text{B}}T} + e^{-E_1/k_{\text{B}}T}}.$$

Comparing with ρ_∞, we see that its temperature, which we may denote T_∞, is such that

$$p = \frac{e^{-E_0/k_{\text{B}}T_\infty}}{e^{-E_0/k_{\text{B}}T_\infty} + e^{-E_1/k_{\text{B}}T_\infty}} \quad \text{and} \quad 1-p = \frac{e^{-E_1/k_{\text{B}}T_\infty}}{e^{-E_0/k_{\text{B}}T_\infty} + e^{-E_1/k_{\text{B}}T_\infty}}.$$

Dividing both relations we obtain

$$\frac{p}{1-p} = \frac{e^{-E_0/k_{\text{B}}T_\infty}}{e^{-E_1/k_{\text{B}}T_\infty}} \quad \Longrightarrow \quad e^{(E_1-E_0)/k_{\text{B}}T_\infty} = \frac{p}{1-p}.$$

And then we must simply solve for T_∞

$$\frac{E_1-E_0}{k_{\text{B}}T_\infty} = \ln\left(\frac{p}{1-p}\right) \quad \Longrightarrow \quad T_\infty = \frac{E_1-E_0}{k_{\text{B}}\ln\left(\frac{p}{1-p}\right)}.$$

Notice that in the limit for $p \to 1$, which corresponds to the usual amplitude damping, the temperature tends to zero, as expected.

8.26

Let the principal system start at state $\rho_{\text{in}} \equiv \sum_i p_i \left|\psi_i\right\rangle\!\left\langle\psi_i\right|$, with $\left|\psi_i\right\rangle = \alpha_i \left|0\right\rangle + \beta_i \left|1\right\rangle$, meaning the total state is $\rho = \sum_i p_i \left(\alpha_i \left|00\right\rangle + \beta_i \left|10\right\rangle\right)\left(\alpha_i^* \left\langle 00\right| + \beta_i^* \left\langle 10\right|\right)$. Then the action of the circuit will be

$$\rho \xrightarrow{CR_y(\theta)_{(1,2)}} \sum_i p_i \left(\alpha_i \left|00\right\rangle + \beta_i \cos\frac{\theta}{2}\left|10\right\rangle + \beta_i \sin\frac{\theta}{2}\left|11\right\rangle\right)\left(\alpha_i^* \left\langle 00\right| + \beta_i^* \cos\frac{\theta}{2}\left\langle 10\right| + \beta_i^* \sin\frac{\theta}{2}\left\langle 11\right|\right).$$

We may call this state ρ'. Then, a measurement of the environment is made, which yields

$$\begin{aligned}
\rho_{\text{out}} &= \text{tr}_{\text{env}}(\rho') \\
&= \sum_i p_i \left[\left(\alpha_i \left|0\right\rangle + \beta_i \cos\frac{\theta}{2}\left|1\right\rangle\right)\left(\alpha_i^* \left\langle 0\right| + \beta_i^* \cos\frac{\theta}{2}\left\langle 1\right|\right) + \left(\beta_i \sin\frac{\theta}{2}\left|1\right\rangle\right)\left(\beta_i^* \sin\frac{\theta}{2}\left\langle 1\right|\right)\right] \\
&= \sum_i p_i \left[\left|\alpha_i\right|^2 \left|0\right\rangle\!\left\langle 0\right| + \alpha_i\beta_i^* \cos\frac{\theta}{2}\left|0\right\rangle\!\left\langle 1\right| + \alpha_i^*\beta_i \cos\frac{\theta}{2}\left|1\right\rangle\!\left\langle 0\right| + \left|\beta_i\right|^2 \left|1\right\rangle\!\left\langle 1\right|\right] \\
&= \sum_i p_i \begin{bmatrix} \left|\alpha_i\right|^2 & \alpha_i\beta_i^* \cos\frac{\theta}{2} \\ \alpha_i^*\beta_i \cos\frac{\theta}{2} & \left|\beta_i\right|^2 \end{bmatrix}.
\end{aligned}$$

Applying the phase damping channel to the same initial state yields

$$\begin{aligned}
\mathcal{E}_{\text{PD}}(\rho_{\text{in}}) &= E_0\rho_{\text{in}}E_0^\dagger + E_1\rho_{\text{in}}E_1^\dagger \\
&= \sum_i p_i \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\lambda} \end{bmatrix}\begin{bmatrix} \left|\alpha_i\right|^2 & \alpha_i\beta_i^* \\ \alpha_i^*\beta_i & \left|\beta_i\right|^2 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\lambda} \end{bmatrix} + \sum_i p_i \begin{bmatrix} 0 & 0 \\ 0 & \sqrt{\lambda} \end{bmatrix}\begin{bmatrix} \left|\alpha_i\right|^2 & \alpha_i\beta_i^* \\ \alpha_i^*\beta_i & \left|\beta_i\right|^2 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 0 & \sqrt{\lambda} \end{bmatrix} \\
&= \sum_i p_i \begin{bmatrix} \left|\alpha_i\right|^2 & \alpha_i\beta_i^*\sqrt{1-\lambda} \\ \alpha_i^*\beta_i\sqrt{1-\lambda} & \left|\beta_i\right|^2 \end{bmatrix}.
\end{aligned}$$

From this result, we see that choosing θ such that $\cos\frac{\theta}{2} = \sqrt{1-\lambda}$, both quantities coincide.

8.27

We have the relations $\widetilde{E}_0 = u_{00}E_0 + u_{01}E_1$ and $\widetilde{E}_1 = u_{10}E_0 + u_{11}E_1$. Writing in their explicit matrix representations yields

$$\begin{aligned}
\begin{bmatrix} \sqrt{\alpha} & 0 \\ 0 & \sqrt{\alpha} \end{bmatrix} &= u_{00}\begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\lambda} \end{bmatrix} + u_{01}\begin{bmatrix} 0 & 0 \\ 0 & \sqrt{\lambda} \end{bmatrix}, \\
\begin{bmatrix} \sqrt{1-\alpha} & 0 \\ 0 & -\sqrt{1-\alpha} \end{bmatrix} &= u_{10}\begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\lambda} \end{bmatrix} + u_{11}\begin{bmatrix} 0 & 0 \\ 0 & \sqrt{\lambda} \end{bmatrix}.
\end{aligned}$$

This gives us a system with the equations

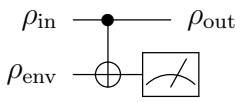
$$\begin{cases} u_{00} = \sqrt{\alpha}, \\ u_{00}\sqrt{1-\lambda} + u_{01}\sqrt{\lambda} = \sqrt{\alpha}, \\ u_{10} = \sqrt{1-\alpha}, \\ u_{10}\sqrt{1-\lambda} + u_{11}\sqrt{\lambda} = -\sqrt{1-\alpha}, \end{cases} \implies \begin{cases} u_{00} = \sqrt{\alpha}, \\ u_{01} = \sqrt{\dfrac{\alpha}{\lambda}}\left(1 - \sqrt{1-\lambda}\right), \\ u_{10} = \sqrt{1-\alpha}, \\ u_{11} = -\sqrt{\dfrac{1-\alpha}{\lambda}}\left(1 + \sqrt{1-\lambda}\right). \end{cases}$$

Using the fact that $1 + \sqrt{1-\lambda} = 2\alpha$, we can write the resulting unitary operator as

$$u = \begin{bmatrix} \sqrt{\alpha} & 2(1-\alpha)\sqrt{\frac{\alpha}{\lambda}} \\ \sqrt{1-\alpha} & -2\alpha\sqrt{\frac{1-\alpha}{\lambda}} \end{bmatrix}.$$

8.28

We wish to verify whether the circuit



can be used to model phase damping for some appropriate choice of ρ_{env}. Let the principal system start at state $\rho_{\text{in}} \equiv \sum_i q_i \left|\psi_i\right\rangle\!\left\langle\psi_i\right|$, with $\left|\psi_i\right\rangle = \alpha_i \left|0\right\rangle + \beta_i \left|1\right\rangle$, and the environment at the mixed state $\rho_{\text{env}} = p \left|+\right\rangle\!\left\langle+\right| + (1-p) \left|-\right\rangle\!\left\langle-\right|$, with $\left|\pm\right\rangle = (\left|0\right\rangle \pm \left|1\right\rangle)/\sqrt{2}$, that is,

$$\begin{aligned} \rho_{\text{env}} &= \frac{p}{2}\left(\left|0\right\rangle\!\left\langle0\right| + \left|0\right\rangle\!\left\langle1\right| + \left|1\right\rangle\!\left\langle0\right| + \left|1\right\rangle\!\left\langle1\right|\right) + \frac{1-p}{2}\left(\left|0\right\rangle\!\left\langle0\right| - \left|0\right\rangle\!\left\langle1\right| - \left|1\right\rangle\!\left\langle0\right| + \left|1\right\rangle\!\left\langle1\right|\right) \\ &= \frac{1}{2}\left|0\right\rangle\!\left\langle0\right| + \left(p - \frac{1}{2}\right)\left|0\right\rangle\!\left\langle1\right| + \left(p - \frac{1}{2}\right)\left|1\right\rangle\!\left\langle0\right| + \frac{1}{2}\left|1\right\rangle\!\left\langle1\right|. \end{aligned}$$

This results in the total state

$$\begin{aligned} \rho &= \sum_i q_i \left(\left|\alpha_i\right|^2 \left|0\right\rangle\!\left\langle0\right| + \alpha_i\beta_i^* \left|0\right\rangle\!\left\langle1\right| + \alpha_i^*\beta_i \left|1\right\rangle\!\left\langle0\right| + \left|\beta_i\right|^2 \left|1\right\rangle\!\left\langle1\right|\right) \otimes \rho_{\text{env}} \\ &= \sum_i q_i \left[\frac{\left|\alpha_i\right|^2}{2}\left(\left|00\right\rangle\!\left\langle00\right| + \left|01\right\rangle\!\left\langle01\right|\right) + \left|\alpha_i\right|^2\left(p - \frac{1}{2}\right)\left(\left|00\right\rangle\!\left\langle01\right| + \left|01\right\rangle\!\left\langle00\right|\right)\right. \\ &\quad + \frac{\alpha_i\beta_i^*}{2}\left(\left|00\right\rangle\!\left\langle10\right| + \left|01\right\rangle\!\left\langle11\right|\right) + \alpha_i\beta_i^*\left(p - \frac{1}{2}\right)\left(\left|00\right\rangle\!\left\langle11\right| + \left|01\right\rangle\!\left\langle10\right|\right) \\ &\quad + \frac{\alpha_i^*\beta_i}{2}\left(\left|10\right\rangle\!\left\langle00\right| + \left|11\right\rangle\!\left\langle01\right|\right) + \alpha_i^*\beta_i\left(p - \frac{1}{2}\right)\left(\left|10\right\rangle\!\left\langle01\right| + \left|11\right\rangle\!\left\langle00\right|\right) \\ &\quad \left. + \frac{\left|\beta_i\right|^2}{2}\left(\left|10\right\rangle\!\left\langle10\right| + \left|11\right\rangle\!\left\langle11\right|\right) + \left|\beta_i\right|^2\left(p - \frac{1}{2}\right)\left(\left|10\right\rangle\!\left\langle11\right| + \left|11\right\rangle\!\left\langle10\right|\right)\right]. \end{aligned}$$

Then the action of the circuit will be

$$\rho \xrightarrow{CX_{(1,2)}} \sum_i q_i \left[\frac{\left|\alpha_i\right|^2}{2}\left(\left|00\right\rangle\!\left\langle00\right| + \left|01\right\rangle\!\left\langle01\right|\right) + \left|\alpha_i\right|^2\left(p - \frac{1}{2}\right)\left(\left|00\right\rangle\!\left\langle01\right| + \left|01\right\rangle\!\left\langle00\right|\right)\right.$$

$$
\begin{aligned}
&+ \frac{\alpha_i\beta_i^*}{2}\left(|00\rangle\langle 11| + |01\rangle\langle 10|\right) + \alpha_i\beta_i^*\left(p-\frac{1}{2}\right)\left(|00\rangle\langle 10| + |01\rangle\langle 11|\right) \\
&+ \frac{\alpha_i^*\beta_i}{2}\left(|11\rangle\langle 00| + |10\rangle\langle 01|\right) + \alpha_i^*\beta_i\left(p-\frac{1}{2}\right)\left(|11\rangle\langle 01| + |10\rangle\langle 00|\right) \\
&+ \frac{|\beta_i|^2}{2}\left(|11\rangle\langle 11| + |10\rangle\langle 10|\right) + |\beta_i|^2\left(p-\frac{1}{2}\right)\left(|11\rangle\langle 10| + |10\rangle\langle 11|\right)\Bigg].
\end{aligned}
$$

We may call this state ρ'. Then, a measurement of the environment is made, which yields

$$
\begin{aligned}
\rho_{\text{out}} &= \text{tr}_{\text{env}}(\rho') \\
&= \sum_i q_i\left(|\alpha_i|^2|0\rangle\langle 0| + \alpha_i\beta_i^*(2p-1)|0\rangle\langle 1| + \alpha_i^*\beta_i(2p-1)|1\rangle\langle 0| + |\beta_i|^2|1\rangle\langle 1|\right) \\
&= \begin{bmatrix} |\alpha_i|^2 & \alpha_i\beta_i^*(2p-1) \\ \alpha_i^*\beta_i(2p-1) & |\beta_i|^2 \end{bmatrix}.
\end{aligned}
$$

Applying the phase damping channel to the same initial state yields

$$
\begin{aligned}
\mathcal{E}_{\text{PD}}(\rho_{\text{in}}) &= E_0\rho_{\text{in}}E_0^\dagger + E_1\rho_{\text{in}}E_1^\dagger \\
&= \sum_i p_i \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\lambda} \end{bmatrix}\begin{bmatrix} |\alpha_i|^2 & \alpha_i\beta_i^* \\ \alpha_i^*\beta_i & |\beta_i|^2 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\lambda} \end{bmatrix} + \sum_i p_i \begin{bmatrix} 0 & 0 \\ 0 & \sqrt{\lambda} \end{bmatrix}\begin{bmatrix} |\alpha_i|^2 & \alpha_i\beta_i^* \\ \alpha_i^*\beta_i & |\beta_i|^2 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 0 & \sqrt{\lambda} \end{bmatrix} \\
&= \sum_i p_i \begin{bmatrix} |\alpha_i|^2 & \alpha_i\beta_i^*\sqrt{1-\lambda} \\ \alpha_i^*\beta_i\sqrt{1-\lambda} & |\beta_i|^2 \end{bmatrix}.
\end{aligned}
$$

Comparing both results we conclude that the circuit is indeed a model for phase damping, and that given the probability λ of the scattering occuring, we must choose $p = \left(1+\sqrt{1-\lambda}\right)/2$.

8.29

Any quantum process applied to the identity can be written as $\mathcal{E}(I) = \sum_k E_k I E_k^\dagger = \sum_k E_k E_k^\dagger$. Therefore, a process is unital if $\sum_k E_k E_k^\dagger = I$. Using the operation elements of the depolarizing, phase damping, and amplitude damping channels we get

$$
\begin{aligned}
\mathcal{E}_{\text{D}}(I) &= (1-p)I^2 + \frac{p}{3}X^2 + \frac{p}{3}Y^2 + \frac{p}{3}Z^2 = I, \\
\mathcal{E}_{\text{PD}}(I) &= \begin{bmatrix} 1 & 0 \\ 0 & 1-\lambda \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & \lambda \end{bmatrix} = I, \\
\mathcal{E}_{\text{AD}}(I) &= \begin{bmatrix} 1 & 0 \\ 0 & 1-\gamma \end{bmatrix} + \begin{bmatrix} \gamma & 0 \\ 0 & 0 \end{bmatrix} = I + \gamma Z.
\end{aligned}
$$

8.30

**From errata:* T_2 should be replaced by $2T_2$.

Given a general density operator, the amplitude damping channel produces (see Exercise 8.22)

$$\mathcal{E}_{\text{AD}}(\rho) = \begin{bmatrix} 1-(1-a)(1-\gamma) & b\sqrt{1-\gamma} \\ b^*\sqrt{1-\gamma} & (1-a)(1-\gamma) \end{bmatrix}.$$

The decay of the elements in the diagonal is given by the term $1-\gamma$ while for the off-diagonal ones is $\sqrt{1-\gamma}$. This means that $1-\gamma = e^{-t/T_1}$, and $\sqrt{1-\gamma} = e^{-t/2T_2}$ and thus

$$e^{-t/T_1} = \left(e^{-t/2T_2}\right)^2 = e^{-t/T_2} \quad \Longrightarrow \quad T_2 = T_1.$$

If phase damping is also applied then the final state will be

$$\mathcal{E}_{\text{PD}}(\mathcal{E}_{\text{AD}}(\rho)) = \begin{bmatrix} 1-(1-a)(1-\gamma) & b\sqrt{1-\gamma}\sqrt{1-\lambda} \\ b^*\sqrt{1-\gamma}\sqrt{1-\lambda} & (1-a)(1-\gamma) \end{bmatrix},$$

and now we have $1-\gamma = e^{-t/T_1}$, and $\sqrt{1-\gamma}\sqrt{1-\lambda} = e^{-t/2T_2}$. Since $1-\lambda \leq 1$, we have

$$e^{-t/T_1} \geq (1-\gamma)(1-\lambda) = e^{-t/T_2} \quad \Longrightarrow \quad T_2 \leq T_1.$$

8.31

The unitary operator will be

$$U \equiv e^{-i\chi a^\dagger a(b+b^\dagger)\Delta t} = e^{-iA(b+b^\dagger)},$$

where we have defined the Hermitian operator $A \equiv (\chi\Delta t)a^\dagger a$. Using the Baker-Campbell-Hausdorff formula, we can rewrite it as (see Exercise 4.49)

$$U = e^{-iAb^\dagger}e^{-iAb}e^{\frac{A^2}{2}\left[b^\dagger,b\right]} + O(A^3).$$

But since $\left[b^\dagger, b\right] = -1$, and the terms of $O(A^3)$ involves commutation relations with this quantity, they all vanish because it is a constant. Therefore, the unitary operator can be written exactly as

$$U = e^{-iAb}e^{-iAb^\dagger}e^{-\frac{A^2}{2}}.$$

We are considering the total state to be $\rho \otimes |0\rangle\langle 0|$, thus the action of the unitary operator yields

$$U\left(\rho \otimes |0\rangle\langle 0|\right)U^\dagger = \sum_{n,m} \rho_{nm} e^{-iAb^\dagger}e^{-iAb}e^{-\frac{A^2}{2}}\left(|n\rangle\langle m| \otimes |0\rangle\langle 0|\right)e^{-\frac{A^2}{2}}e^{iAb^\dagger}e^{iAb}.$$

We have that

$$\begin{aligned} e^{-iAb^\dagger}e^{-iAb}e^{-\frac{A^2}{2}}|n\rangle \otimes |0\rangle &= e^{-\frac{(\chi\Delta t)^2}{2}n^2}|n\rangle \otimes e^{-i(\chi\Delta t)nb^\dagger}e^{-i(\chi\Delta t)nb}|0\rangle \\ &= e^{-\frac{(\chi\Delta t)^2}{2}n^2}|n\rangle \otimes \sum_{j,k=0}^{\infty} \frac{(-in\chi\Delta t)^{j+k}}{j!k!}\left(b^\dagger\right)^k b^j|0\rangle \end{aligned}$$

$$= e^{-\frac{(\chi\Delta t)^2}{2}n^2} |n\rangle \otimes \sum_{k=0}^{\infty} \frac{(-in\chi\Delta t)^k}{k!} \left(b^\dagger\right)^k |0\rangle$$
$$= e^{-\frac{(\chi\Delta t)^2}{2}n^2} |n\rangle \otimes \sum_{k=0}^{\infty} \frac{(-in\chi\Delta t)^k}{\sqrt{k!}} |k\rangle .$$

Substituting this result back we obtain

$$U\left(\rho \otimes |0\rangle\langle 0|\right) U^\dagger = \sum_{n,m} \rho_{nm} e^{-\frac{(\chi\Delta t)^2}{2}(n^2+m^2)} |n\rangle\langle m| \otimes \sum_{k,k'=0}^{\infty} \frac{(-in\chi\Delta t)^k}{\sqrt{k!}} \frac{(im\chi\Delta t)^{k'}}{\sqrt{k'!}} |k\rangle\langle k'| .$$

In order to get the resulting density operator of the harmonic oscillator we must trace out the environment, that is,

$$\begin{aligned}
\mathrm{tr}_{\mathrm{env}}\big(U(\rho \otimes |0\rangle\langle 0|)U^\dagger\big) &= \sum_{n,m} \rho_{nm} e^{-\frac{(\chi\Delta t)^2}{2}(n^2+m^2)} |n\rangle\langle m| \sum_l \sum_{k,k'=0}^{\infty} \frac{(-in\chi\Delta t)^k}{\sqrt{k!}} \frac{(im\chi\Delta t)^{k'}}{\sqrt{k'!}} \langle l \,|\, k\rangle \langle k' \,|\, l\rangle \\
&= \sum_{n,m} \rho_{nm} e^{-\frac{(\chi\Delta t)^2}{2}(n^2+m^2)} |n\rangle\langle m| \sum_{k=0}^{\infty} \frac{(-in\chi\Delta t)^k}{\sqrt{k!}} \frac{(im\chi\Delta t)^k}{\sqrt{k!}} \\
&= \sum_{n,m} \rho_{nm} e^{-\frac{(\chi\Delta t)^2}{2}(n^2+m^2)} |n\rangle\langle m| \sum_{k=0}^{\infty} \frac{(nm\chi^2\Delta t^2)^k}{k!} \\
&= \sum_{n,m} \rho_{nm} e^{-\frac{(\chi\Delta t)^2}{2}(n^2+m^2)} e^{(\chi\Delta t)^2 nm} |n\rangle\langle m| \\
&= \sum_{n,m} \rho_{nm} e^{-\frac{(\chi\Delta t)^2}{2}(n-m)^2} |n\rangle\langle m| .
\end{aligned}$$

Defining the constant $\lambda \equiv (\chi\Delta t)^2/2$, we see that the element ρ_{nm} decays as $e^{-\lambda(n-m)^2}$.

8.32

-

8.33

Given a single qubit density matrix ρ, we can always write it as

$$\rho = \frac{I + \vec{r}\cdot\vec{\sigma}}{2} = \frac{I}{2} + \frac{r_x}{2}X + \frac{r_y}{2}Y + \frac{r_z}{2}Z,$$

where $r_x^2 + r_y^2 + r_z^2 \leq 1$. This can be rewritten as

$$\begin{aligned}
\rho &= \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{bmatrix} + \begin{bmatrix} 0 & \frac{r_x}{2} \\ \frac{r_x}{2} & 0 \end{bmatrix} + \begin{bmatrix} 0 & -i\frac{r_y}{2} \\ i\frac{r_y}{2} & 0 \end{bmatrix} + \begin{bmatrix} \frac{r_z}{2} & 0 \\ 0 & -\frac{r_z}{2} \end{bmatrix} \\
&= \frac{1+r_z}{2}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \frac{1-r_z}{2}\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} + r_x \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix} + r_y \begin{bmatrix} \frac{1}{2} & -\frac{i}{2} \\ \frac{i}{2} & \frac{1}{2} \end{bmatrix} - \frac{r_x + r_y}{2}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\
&= \frac{1-r_x-r_y+r_z}{2}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \frac{1-r_x-r_y-r_z}{2}\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} + r_x \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix} + r_y \begin{bmatrix} \frac{1}{2} & -\frac{i}{2} \\ \frac{i}{2} & \frac{1}{2} \end{bmatrix} .
\end{aligned}$$

These four matrices are linearly independent and can be written in terms of the four pure states: $|0\rangle$, $|1\rangle$, $|+\rangle \equiv (|0\rangle + |1\rangle)/\sqrt{2}$, and $|i_+\rangle \equiv (|0\rangle + i\,|1\rangle)/\sqrt{2}$. Thus any single qubit density matrix can be written as a combination of the four pure states

$$\rho = \frac{1 - r_x - r_y + r_z}{2}\,|0\rangle\langle 0| + \frac{1 - r_x - r_y - r_z}{2}\,|1\rangle\langle 1| + r_x\,|+\rangle\langle +| + r_y\,|i_+\rangle\langle i_+|\,.$$

This decomposition is, of course, not unique. Even mixed states could be used for writing the decomposition, however, the description using pure states exclusively is necessary since we can only get complete information about a quantum operation when it acts on a fully known state, that is, a pure state. Thus the action of a quantum operation will be

$$\mathcal{E}(\rho) = \frac{1 - r_x - r_y + r_z}{2}\mathcal{E}(|0\rangle\langle 0|) + \frac{1 - r_x - r_y - r_z}{2}\mathcal{E}(|1\rangle\langle 1|) + r_x\mathcal{E}(|+\rangle\langle +|) + r_y\mathcal{E}(|i_+\rangle\langle i_+|).$$

So a quantum operation $\mathcal{E}$ can be fully specified if we know how it acts on a set of at least four points on the Bloch sphere.

8.34

-

8.35

From the four given density operators we can conclude that $\mathcal{E}_1$ is the amplitude damping channel (see Exercise 8.22). We shall use it to check the final answer. We are using

$$\rho_1 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \rho_2 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \rho_3 = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \rho_4 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

as the 2×2 matrix basis, and

$$\widetilde{E}_0 = I, \widetilde{E}_1 = X, \widetilde{E}_2 = -iY, \widetilde{E}_3 = Z$$

as basis for the operation elements. We can determine the elements λ_{jk} with the relation $\mathcal{E}_1(\rho_j) \equiv \rho'_j = \sum_k \lambda_{jk}\rho_k$. Using the experimentally obtained density matrices we have

$$\begin{bmatrix} \rho'_1 \\ \rho'_2 \\ \rho'_3 \\ \rho'_4 \end{bmatrix} = \begin{bmatrix} \rho_1 \\ \sqrt{1-\gamma}\rho_2 \\ \sqrt{1-\gamma}\rho_3 \\ \gamma\rho_1 + (1-\gamma)\rho_4 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \sqrt{1-\gamma} & 0 & 0 \\ 0 & 0 & \sqrt{1-\gamma} & 0 \\ \gamma & 0 & 0 & 1-\gamma \end{bmatrix} \begin{bmatrix} \rho_1 \\ \rho_2 \\ \rho_3 \\ \rho_4 \end{bmatrix},$$

$$\Longrightarrow \quad \lambda = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \sqrt{1-\gamma} & 0 & 0 \\ 0 & 0 & \sqrt{1-\gamma} & 0 \\ \gamma & 0 & 0 & 1-\gamma \end{bmatrix}.$$

The elements β_{jk}^{mn} can be obtained with the relation $\widetilde{E}_m \rho_j \widetilde{E}_n^\dagger = \sum_k \beta_{jk}^{mn} \rho_k$. β can be thought of as a 4×4 matrix with elements β_{jk}, where each β_{jk} is in turn a 4×4 matrix with elements β_{jk}^{mn}. To avoid working with too many nested matrices, let us consider the relation for each row j of β separately. Starting with $j = 1$, we obtain

$$\begin{bmatrix} I\rho_1 I & I\rho_1 X & I\rho_1 iY & I\rho_1 Z \\ X\rho_1 I & X\rho_1 X & X\rho_1 iY & X\rho_1 Z \\ -iY\rho_1 I & -iY\rho_1 X & -iY\rho_1 iY & -iY\rho_1 Z \\ Z\rho_1 I & Z\rho_1 X & Z\rho_1 iY & Z\rho_1 Z \end{bmatrix} = \begin{bmatrix} \rho_1 & \rho_2 & \rho_2 & \rho_1 \\ \rho_3 & \rho_4 & \rho_4 & \rho_3 \\ \rho_3 & \rho_4 & \rho_4 & \rho_3 \\ \rho_1 & \rho_2 & \rho_2 & \rho_1 \end{bmatrix} = \sum_k \beta_{1k} \rho_k,$$

meaning

$$\beta_{11} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}, \beta_{12} = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix}, \beta_{13} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \beta_{14} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

For $j = 2$ we obtain

$$\begin{bmatrix} I\rho_2 I & I\rho_2 X & I\rho_2 iY & I\rho_2 Z \\ X\rho_2 I & X\rho_2 X & X\rho_2 iY & X\rho_2 Z \\ -iY\rho_2 I & -iY\rho_2 X & -iY\rho_2 iY & -iY\rho_2 Z \\ Z\rho_2 I & Z\rho_2 X & Z\rho_2 iY & Z\rho_2 Z \end{bmatrix} = \begin{bmatrix} \rho_2 & \rho_1 & -\rho_1 & -\rho_2 \\ \rho_4 & \rho_3 & -\rho_3 & -\rho_4 \\ \rho_4 & \rho_3 & -\rho_3 & -\rho_4 \\ \rho_2 & \rho_1 & -\rho_1 & -\rho_2 \end{bmatrix} = \sum_k \beta_{2k} \rho_k,$$

meaning

$$\beta_{21} = \begin{bmatrix} 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 \end{bmatrix}, \beta_{22} = \begin{bmatrix} 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & -1 \end{bmatrix}, \beta_{23} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \beta_{24} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & -1 \\ 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

For $j = 3$ we obtain

$$\begin{bmatrix} I\rho_3 I & I\rho_3 X & I\rho_3 iY & I\rho_3 Z \\ X\rho_3 I & X\rho_3 X & X\rho_3 iY & X\rho_3 Z \\ -iY\rho_3 I & -iY\rho_3 X & -iY\rho_3 iY & -iY\rho_3 Z \\ Z\rho_3 I & Z\rho_3 X & Z\rho_3 iY & Z\rho_3 Z \end{bmatrix} = \begin{bmatrix} \rho_3 & \rho_4 & \rho_4 & \rho_3 \\ \rho_1 & \rho_2 & \rho_2 & \rho_1 \\ -\rho_1 & -\rho_2 & -\rho_2 & -\rho_1 \\ -\rho_3 & -\rho_4 & -\rho_4 & -\rho_3 \end{bmatrix} = \sum_k \beta_{3k} \rho_k,$$

meaning

$$\beta_{31} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ -1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \beta_{32} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & -1 & -1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \beta_{33} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & -1 \end{bmatrix}, \beta_{34} = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & -1 & -1 & 0 \end{bmatrix}.$$

And finally, for $j = 4$ we obtain

$$\begin{bmatrix} I\rho_4 I & I\rho_4 X & I\rho_4 iY & I\rho_4 Z \\ X\rho_4 I & X\rho_4 X & X\rho_4 iY & X\rho_4 Z \\ -iY\rho_4 I & -iY\rho_4 X & -iY\rho_4 iY & -iY\rho_4 Z \\ Z\rho_4 I & Z\rho_4 X & Z\rho_4 iY & Z\rho_4 Z \end{bmatrix} = \begin{bmatrix} \rho_4 & \rho_3 & -\rho_3 & -\rho_4 \\ \rho_2 & \rho_1 & -\rho_1 & -\rho_2 \\ -\rho_2 & -\rho_1 & \rho_1 & \rho_2 \\ -\rho_4 & -\rho_3 & \rho_3 & \rho_4 \end{bmatrix} = \sum_k \beta_{4k}\rho_k,$$

meaning

$$\beta_{14} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \beta_{24} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & -1 \\ -1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \beta_{34} = \begin{bmatrix} 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 \end{bmatrix}, \beta_{44} = \begin{bmatrix} 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 1 \end{bmatrix}.$$

In order to obtain the entries of the χ matrix we use the relation $\sum_{mn} \beta_{jk}^{mn}\chi_{mn} = \lambda_{jk}$, but we need to invert the β matrix. Since we are treating it as a 4×4 block matrix of 4×4 matrices this is an inconvenient task. However, notice that the relation shows that each entry λ_{jk}, which is a number, is uniquely related to β_{jk}, which is a 4×4 matrix. The number is calculated by summing up every entry of the β_{jk} matrix multiplied by each element of the χ matrix. Therefore, it can be interpreted as if λ and χ were column vectors of 16 entries each, where we append each row of the 4×4 matrix forming a single column, while β can be thought of as a 16×16 matrix where each row is built by flattening each β_{jk} into a single row. In practice, we are considering

$$\lambda = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ \sqrt{1-\gamma} \\ 0 \\ 0 \\ 0 \\ 0 \\ \sqrt{1-\gamma} \\ 0 \\ \gamma \\ 0 \\ 0 \\ 1-\gamma \end{bmatrix}, \beta = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 \\ 1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & -1 & 1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & -1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & -1 & -1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & -1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & -1 & -1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 1 \end{bmatrix}.$$

Calculating the inverse of β yields the matrix

$$\kappa = \frac{1}{4}\begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & -1 & 0 \\
1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & -1 & 0 & 0 & 1 & 0 & 0 & -1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & -1 & 0 & 0 & -1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & -1 & 0 & 0 & -1 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 & -1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & -1 \\
0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & -1 & 0 \\
0 & 1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 1 & 0 \\
1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 1
\end{bmatrix}.$$

Calculating $\chi = \kappa\lambda$ and rewriting χ in a 4×4 matrix format results in

$$\chi = \frac{1}{4}\begin{bmatrix}
2-\gamma+2\sqrt{1-\gamma} & 0 & 0 & \gamma \\
0 & \gamma & -\gamma & 0 \\
0 & -\gamma & \gamma & 0 \\
\gamma & 0 & 0 & 2-\gamma-2\sqrt{1-\gamma}
\end{bmatrix}.$$

In order to check this result, we can calculate the operation elements E_i from it. As it can be readily checked, this matrix has only two non-zero eigenvalues, given by $1-\gamma/2$ and $\gamma/2$, meaning $\mathcal{E}_1$ is described by only two operation elements. The two respective normalized eigenvectors are

$$u = \frac{1}{2\sqrt{1-\frac{\gamma}{2}}}\begin{bmatrix} 1+\sqrt{1-\gamma} \\ 0 \\ 0 \\ 1-\sqrt{1-\gamma} \end{bmatrix} \quad \text{and} \quad v = \frac{1}{\sqrt{2}}\begin{bmatrix} 0 \\ 1 \\ -1 \\ 0 \end{bmatrix},$$

yielding operation elements

$$E_0 = \sqrt{1-\frac{\gamma}{2}}\sum_j u_j \widetilde{E}_j = \frac{1}{2}\left[\left(1+\sqrt{1-\gamma}\right) I + \left(1-\sqrt{1-\gamma}\right) Z\right] = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{bmatrix},$$

$$E_1 = \sqrt{\frac{\gamma}{2}}\sum_j v_j \widetilde{E}_j = \frac{\sqrt{\gamma}}{2}(X+iY) = \begin{bmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{bmatrix}.$$

These are the operation elements for the amplitude damping channel, confirming that the obtained χ matrix is indeed correct.

9 Distance measures for quantum information

Exercises: 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, 9.8, 9.9, 9.10, 9.11, 9.12, 9.13, 9.14, 9.15, 9.16, 9.17, 9.18, 9.19, 9.20, 9.21, 9.22, 9.23.

9.1

For probability distributions $p_x = (1, 0)$ and $q_x = (1/2, 1/2)$:

$$D(p_x, q_x) = \frac{1}{2}\left(\left|1 - \frac{1}{2}\right| + \left|0 - \frac{1}{2}\right|\right) = \frac{1}{2}\left(\frac{1}{2} + \frac{1}{2}\right) = \frac{1}{2};$$

For probability distributions $p_x = (1/2, 1/3, 1/6)$ and $q_x = (3/4, 1/8, 1/8)$:

$$D(p_x, q_x) = \frac{1}{2}\left(\left|\frac{1}{2} - \frac{3}{4}\right| + \left|\frac{1}{3} - \frac{1}{8}\right| + \left|\frac{1}{6} - \frac{1}{8}\right|\right) = \frac{1}{2}\left(\frac{1}{4} + \frac{5}{24} + \frac{1}{24}\right) = \frac{1}{4}.$$

9.2

$$\begin{aligned} D(p_x, q_x) &= \frac{1}{2}\left(|p - q| + |(1 - p) - (1 - q)|\right) \\ &= \frac{1}{2}\left(|p - q| + |q - p|\right) \\ &= |p - q|. \end{aligned}$$

9.3

For probability distributions $p_x = (1, 0)$ and $q_x = (1/2, 1/2)$:

$$F(p_x, q_x) = \sqrt{1 \times \frac{1}{2}} + \sqrt{0 \times \frac{1}{2}} = \sqrt{\frac{1}{2}} + 0 = \frac{\sqrt{2}}{2};$$

For probability distributions $p_x = (1/2, 1/3, 1/6)$ and $q_x = (3/4, 1/8, 1/8)$:

$$F(p_x, q_x) = \sqrt{\frac{1}{2} \times \frac{3}{4}} + \sqrt{\frac{1}{3} \times \frac{1}{8}} + \sqrt{\frac{1}{6} \times \frac{1}{8}} = \sqrt{\frac{3}{8}} + \sqrt{\frac{1}{24}} + \sqrt{\frac{1}{48}} = \frac{4\sqrt{6} + \sqrt{3}}{12}.$$

9.4

$$\begin{aligned} D(p_x, q_x) &= \frac{1}{2}\sum_x |p_x - q_x| \\ &= \frac{1}{2}\left[\sum_{p_x > q_x} (p_x - q_x) + \sum_{p_x < q_x} (q_x - p_x)\right]. \end{aligned}$$

Using the fact that $\sum_x p_x = \sum_x q_x = 1$, the second sum can be rewritten as

$$\sum_{p_x < q_x} (q_x - p_x) = \sum_{p_x < q_x} q_x - \sum_{p_x < q_x} p_x$$

$$= \left(\sum_x q_x - \sum_{p_x > q_x} q_x\right) - \left(\sum_x p_x - \sum_{p_x > q_x} p_x\right)$$
$$= \sum_{p_x > q_x} (p_x - q_x),$$

thus, we obtain that

$$D(p_x, q_x) = \sum_{p_x > q_x} (p_x - q_x) = \sum_{p_x > q_x} p_x - \sum_{p_x > q_x} q_x.$$

If we consider all possible subsets S of the indices $\{x\}$, the set for which we have $p_x > q_x$ for all indices corresponds to the maximum of the sum. To see that, notice that if we remove any element $p_x - q_x$ the value of the sum will decrease, and if we add any element, it will be one such that $p_x - q_x$ is negative and the value of the sum will also decrease, therefore it is the maximum, so

$$D(p_x, q_x) = \max_S \left(\sum_{x \in S} p_x - \sum_{x \in S} q_x\right).$$

Since the maximum value of the sum will always be positive, it makes no difference to write it with absolute value signs, so we conclude Eq. (9.3)

$$D(p_x, q_x) = \max_S \left|\sum_{x \in S} p_x - \sum_{x \in S} q_x\right|.$$

9.5

See Exercise 9.4.

9.6

For density operators $\rho = \frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|$ and $\sigma = \frac{2}{3}|0\rangle\langle 0| + \frac{1}{3}|1\rangle\langle 1|$:

$$|\rho - \sigma| = \left|\frac{3}{4} - \frac{2}{3}\right||0\rangle\langle 0| + \left|\frac{1}{4} - \frac{1}{3}\right||1\rangle\langle 1| = \frac{1}{12}|0\rangle\langle 0| + \frac{1}{12}|1\rangle\langle 1|$$
$$\implies \quad D(\rho, \sigma) = \frac{1}{2}\sum_{i=0}^{1} \left\langle i \left| \frac{1}{12}|0\rangle\langle 0| + \frac{1}{12}|1\rangle\langle 1| \right| i \right\rangle = \frac{1}{2}\left(\frac{1}{12} + \frac{1}{12}\right) = \frac{1}{12}.$$

For density operators $\rho = \frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|$ and $\sigma = \frac{2}{3}|+\rangle\langle +| + \frac{1}{3}|-\rangle\langle -|$:
First, writing σ in the computational basis yields

$$\sigma = \frac{2}{3}\left(\frac{|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1|}{2}\right) + \frac{1}{3}\left(\frac{|0\rangle\langle 0| - |0\rangle\langle 1| - |1\rangle\langle 0| + |1\rangle\langle 1|}{2}\right)$$
$$= \left(\frac{1}{3} + \frac{1}{6}\right)|0\rangle\langle 0| + \left(\frac{1}{3} - \frac{1}{6}\right)|0\rangle\langle 1| + \left(\frac{1}{3} - \frac{1}{6}\right)|1\rangle\langle 0| + \left(\frac{1}{3} + \frac{1}{6}\right)|1\rangle\langle 1|$$
$$= \frac{1}{2}\left(|0\rangle\langle 0| + |1\rangle\langle 1|\right) + \frac{1}{6}\left(|0\rangle\langle 1| + |1\rangle\langle 0|\right).$$

Thus

$$\rho - \sigma = \begin{bmatrix} \frac{3}{4} - \frac{1}{2} & 0 - \frac{1}{6} \\ 0 - \frac{1}{6} & \frac{1}{4} - \frac{1}{2} \end{bmatrix} = \begin{bmatrix} \frac{1}{4} & -\frac{1}{6} \\ -\frac{1}{6} & -\frac{1}{4} \end{bmatrix}.$$

Its eigenvalues can be calculated as

$$\begin{aligned} \det(\rho - \sigma - \lambda I) = \lambda^2 - \frac{13}{144} = 0 \quad &\implies \quad \text{eigenvalues} = \pm\frac{\sqrt{13}}{12}. \\ &\implies \quad D(\rho, \sigma) = \frac{1}{2}\left(\left|\frac{\sqrt{13}}{12}\right| + \left|-\frac{\sqrt{13}}{12}\right|\right) = \frac{\sqrt{13}}{12}. \end{aligned}$$

9.7

All density operators are Hermitian, therefore $\rho - \sigma$ is Hermitian, meaning it can be diagonalized through some unitary operator U, that is, $\rho - \sigma = UDU^\dagger$. We may write the diagonal operador as

$$D = \sum_i \lambda_i |i\rangle\langle i| = \sum_{\lambda_i > 0} \lambda_i |i\rangle\langle i| - \sum_{\lambda_i < 0} |\lambda_i| |i\rangle\langle i| .$$

Defining operators $Q \equiv \sum_{\lambda_i > 0} \lambda_i U |i\rangle\langle i| U^\dagger$ and $S \equiv \sum_{\lambda_i < 0} |\lambda_i| U |i\rangle\langle i| U^\dagger$ we see that both are positive operators, and since the $\{|i\rangle\}$ form an orthonormal basis, they have orthogonal support, meaning we can always write $\rho - \sigma = Q - S$.

9.8

There exists some projector P such that

$$\begin{aligned} D\left(\sum_i p_i \rho_i, \sigma\right) &= \operatorname{tr}\left[P\left(\sum_i p_i \rho_i - \sigma\right)\right] \\ &= \sum_i p_i \operatorname{tr}(P\rho_i) - \operatorname{tr}(P\sigma) \end{aligned}$$

Since $\sum_i p_i = 1$ we may write

$$D\left(\sum_i p_i \rho_i, \sigma\right) = \sum_i p_i \operatorname{tr}[P(\rho_i - \sigma)] \leq \sum_i p_i D(\rho_i, \sigma).$$

9.9

The set of all density operators is a convex and compact Hilbert space, and all trace preserving quantum operations are continuous transformations over such space. Thus it follows from Schauder's fixed point theorem that all trace preserving quantum operations have a fixed point.

9.10

Let us suppose that $\rho \neq \sigma$ are both fixed points of a strictly contractive trace-preserving map $\mathcal{E}$. So we have

$$D(\mathcal{E}(\rho), \mathcal{E}(\sigma)) = D(\rho, \sigma),$$

which contradicts the fact that $\mathcal{E}$ is strictly contractive. So either $\rho = \sigma$ or one of them is not a fixed point. Either way, the conclusion is that $\mathcal{E}$ has a unique fixed point.

9.11

$$\begin{aligned} D(\mathcal{E}(\rho), \mathcal{E}(\sigma)) &= D(p\rho_0 + (1-p)\mathcal{E}'(\rho), p\rho_0 + (1-p)\mathcal{E}'(\sigma)) \\ &\leq pD(\rho_0, \rho_0) + (1-p)D(\mathcal{E}'(\rho), \mathcal{E}'(\sigma)) \\ &\leq (1-p)D(\rho, \sigma). \end{aligned}$$

Since $0 < p \leq 1$, we have that $D(\mathcal{E}(\rho), \mathcal{E}(\sigma)) < D(\rho, \sigma)$, meaning $\mathcal{E}$ is strictly contractive, and thus has a unique fixed point.

9.12

$$\begin{aligned} D(\mathcal{E}(\rho), \mathcal{E}(\sigma)) &= \frac{1}{2} \operatorname{tr} \left| \frac{pI}{2} + (1-p)\rho - \frac{pI}{2} - (1-p)\sigma \right| \\ &= (1-p)\frac{1}{2} \operatorname{tr} |\rho - \sigma| \\ &= (1-p)D(\rho, \sigma). \end{aligned}$$

We must assume p strictly larger than zero, otherwise $\mathcal{E}$ would be simply the trivial identity channel. Therefore, the depolarizing channel is strictly contractive.

9.13

The bit-flip channel is given by $\mathcal{E}(\rho) = p\rho + (1-p)X\rho X$. Therefore we have

$$\begin{aligned} D(\mathcal{E}(\rho), \mathcal{E}(\sigma)) &= \frac{1}{2} \operatorname{tr} |p\rho + (1-p)X\rho X - p\sigma - (1-p)X\sigma X| \\ &= \frac{1}{2} \operatorname{tr} |p(\rho - \sigma) + (1-p)X(\rho - \sigma)X| \\ &\leq \frac{p}{2} \operatorname{tr} |\rho - \sigma| + \frac{1-p}{2} \operatorname{tr} |X(\rho - \sigma)X|. \end{aligned}$$

The trace operation is invariant under cyclic permutations, meaning $\operatorname{tr} |X(\rho - \sigma)X| = \operatorname{tr} |X^2(\rho - \sigma)| = \operatorname{tr} |\rho - \sigma|$, therefore

$$D(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \leq \frac{1}{2} \operatorname{tr} |\rho - \sigma| = D(\rho, \sigma),$$

meaning the bit-flip channel is contractive but not strictly contractive.

The fixed points are the ones such that $X\rho X = \rho$. If we consider $\rho = (I + \vec{r}\cdot\vec{\sigma})/2$ we may write

$$\rho = \frac{I + r_x X + r_y Y + r_z Z}{2}, \quad \text{and} \quad X\rho X = \frac{I + r_x X - r_y Y - r_z Z}{2},$$

and we see that the condition is that $r_y = r_z = 0$. Therefore, all density operators of the form $\rho = (I + r_x X)/2$, for $0 \leq r_x \leq 1$, are fixed points.

9.14

$$\begin{aligned} F\big(U\rho U^\dagger, U\sigma U^\dagger\big) &= \operatorname{tr}\sqrt{\left(U\rho U^\dagger\right)^{1/2} U\sigma U^\dagger \left(U\rho U^\dagger\right)^{1/2}} \\ &= \operatorname{tr}\sqrt{U\rho^{1/2}U^\dagger U\sigma U^\dagger U\rho^{1/2}U^\dagger} \\ &= \operatorname{tr}\Big(U\sqrt{\rho^{1/2}\sigma\rho^{1/2}}U^\dagger\Big) \\ &= \operatorname{tr}\sqrt{\rho^{1/2}\sigma\rho^{1/2}} \\ &= F(\rho,\sigma). \end{aligned}$$

9.15

**From errata:* $A^\dagger$ should be A^{T} in Eq. (9.73), therefore Eq. (9.69) must be modified accordingly resulting in $U \equiv V_Q V_R^{\mathrm{T}} U_R^* U_Q^\dagger$ in Eq. (9.70).

Let $|\psi\rangle = \big(U_R \otimes \sqrt{\rho}U_Q\big)|m\rangle$ and $|\varphi\rangle = \big(V_R \otimes \sqrt{\rho}V_Q\big)|m\rangle$ be purifications of ρ and σ respectively, where U_R and U_Q are fixed. We know that

$$|\langle\psi|\varphi\rangle| = \big|\operatorname{tr}\big(\sqrt{\rho}\sqrt{\sigma}U\big)\big| \leq \operatorname{tr}\big|\sqrt{\rho}\sqrt{\sigma}\big| = F(\rho,\sigma),$$

where $U = V_Q V_R^{\mathrm{T}} U_R^* U_Q^\dagger$. Suppose $\big|\sqrt{\rho}\sqrt{\sigma}\big|V$ is the polar decomposition of $\sqrt{\rho}\sqrt{\sigma}$. Then if we choose $V_Q = V^\dagger U_Q$ and $V_R = U_R$ we obtain

$$|\langle\psi|\varphi\rangle| = \Big|\operatorname{tr}\Big(\big|\sqrt{\rho}\sqrt{\sigma}\big|VV^\dagger U_Q U_R^{\mathrm{T}} U_R^* U_Q^\dagger\Big)\Big| = \operatorname{tr}\big|\sqrt{\rho}\sqrt{\sigma}\big| = F(\rho,\sigma),$$

showing that equality is always attainable and therefore

$$F(\rho,\sigma) = \max_{|\varphi\rangle} |\langle\psi|\varphi\rangle|.$$

9.16

**From errata:* $A^\dagger$ should be A^{T} in Eq. (9.73).

Notice that $\big(A^{\mathrm{T}}B\big)_{jk} = \sum_i A_{ij}B_{ik}$, thus

$$\begin{aligned} \operatorname{tr}\big(A^{\mathrm{T}}B\big) &= \sum_{i,j} A_{ij}B_{ij} \\ &= \sum_{i,j} \langle i_R \,|\, A \,|\, j_R\rangle \,\langle i_Q \,|\, B \,|\, j_Q\rangle \end{aligned}$$

$$= \sum_{i,j} \langle i_R| \langle i_Q| (A \otimes B) |j_R\rangle |j_Q\rangle$$
$$= \langle m| (A \otimes B) |m\rangle .$$

9.17

$$0 \leq F(\rho, \sigma) \leq 1 \quad \Longrightarrow \quad \arccos 0 \geq \arccos F(\rho, \sigma) \geq \arccos 1.$$

We have that $\arccos 0 = \pi/2$ and $\arccos 1 = 0$, and by definition $A(\rho, \sigma) \equiv \arccos F(\rho, \sigma)$, thus

$$0 \leq A(\rho, \sigma) \leq \pi/2.$$

We know that $F(\rho, \sigma) = 1$ if and only if $\rho = \sigma$, meaning $A(\rho, \sigma) = 0$ if and only if $\rho = \sigma$.

9.18

$$F(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \geq F(\rho, \sigma) \quad \Longrightarrow \quad \arccos F(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \leq \arccos F(\rho, \sigma).$$

From the definition $A(\rho, \sigma) \equiv \arccos F(\rho, \sigma)$ it follows that $A(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \leq A(\rho, \sigma)$.

9.19

Let $|\psi_i\rangle$ and $|\varphi_i\rangle$ be the purifications of, respectively, ρ_i and σ_i such that $F(\rho_i, \sigma_i) = \langle\psi_i|\varphi_i\rangle$. If we introduce an auxiliary system with orthonormal basis $|i\rangle$ we can define the purifications $|\psi\rangle \equiv \sum_i \sqrt{p_i} |\psi_i\rangle |i\rangle$ and $|\varphi\rangle \equiv \sum_i \sqrt{p_i} |\varphi_i\rangle |i\rangle$ of the states $\sum_i p_i\rho_i$ and $\sum_i p_i\sigma_i$ respectively. From Uhlmann's formula we conclude

$$F\left(\sum_i p_i\rho_i, \sum_i p_i\sigma_i\right) \geq |\langle\psi|\varphi\rangle| = \sum_{i,j} \sqrt{p_i}\sqrt{p_j} \langle\psi_i|\varphi_j\rangle \langle i|j\rangle = \sum_i p_i F(\rho_i, \sigma_i).$$

9.20

Let $|\psi_i\rangle$ and $|\varphi\rangle$ be the purifications of, respectively, ρ_i and σ such that $F(\rho_i, \sigma) = \langle\psi_i|\varphi\rangle$. If we introduce an auxiliary system with orthonormal basis $|i\rangle$ we can define the purifications $|\psi\rangle \equiv \sum_i \sqrt{p_i} |\psi_i\rangle |i\rangle$ and $|\Phi\rangle \equiv \sum_i \sqrt{p_i} |\varphi\rangle |i\rangle$ of the states $\sum_i p_i\rho_i$ and σ respectively. From Uhlmann's formula we conclude

$$F\left(\sum_i p_i\rho_i, \sigma\right) \geq |\langle\psi|\Phi\rangle| = \sum_{i,j} \sqrt{p_i}\sqrt{p_i} \langle\psi_i|\varphi\rangle \langle i|j\rangle = \sum_i p_i F(\rho_i, \sigma).$$

9.21

Let $\{E_m\}$ be a POVM such that $p_m \equiv \mathrm{tr}(|\psi\rangle\langle\psi| E_m)$ and $q_m \equiv \mathrm{tr}(\sigma E_m)$ are the probabilities of obtaining outcome m for the pure state $|\psi\rangle$ and for the mixed state σ respectively. We can always

choose the POVM to be such that, for $m = k$, we have $E_k = |\psi\rangle\langle\psi|$. The consequence is that $p_k = 1$ and $p_j = 0$ for all $j \neq k$. With this we have the inequality

$$D(|\psi\rangle, \sigma) \geq D(p_m, q_m) = \frac{1}{2}\sum_j |p_j - q_j| = \frac{1}{2}\left(1 - q_k + \sum_{j\neq k} q_j\right) = 1 - q_k.$$

Using Eq. (9.60) we have

$$F(|\psi\rangle, \sigma)^2 = \langle\psi|\sigma|\psi\rangle .$$

If we choose a basis $|\phi_i\rangle$ that contains $|\psi\rangle$ as one of its elements we obtain

$$F(|\psi\rangle, \sigma)^2 = \sum_i \langle\phi_i|\sigma|\psi\rangle \langle\psi|\phi_i\rangle = \mathrm{tr}(\sigma|\psi\rangle\langle\psi|) = \mathrm{tr}(\sigma E_k) = q_k.$$

Substituting this result in the inequality yields

$$1 - F(|\psi\rangle, \sigma)^2 \leq D(|\psi\rangle, \sigma).$$

9.22

By the triangle inequality we have

$$d\big(VU\rho U^\dagger V^\dagger, \mathcal{F}\circ\mathcal{E}(\rho)\big) \leq d\big(VU\rho U^\dagger V^\dagger, \mathcal{F}\big(U\rho U^\dagger\big)\big) + d\big(\mathcal{F}\big(U\rho U^\dagger\big), \mathcal{F}\circ\mathcal{E}(\rho)\big),$$

and by the contractive property of trace-preserving maps we have

$$d\big(\mathcal{F}\big(U\rho U^\dagger\big), \mathcal{F}\circ\mathcal{E}(\rho)\big) \leq d\big(U\rho U^\dagger, \mathcal{E}(\rho)\big).$$

Since these two inequalities are true for any density operator, we may choose ρ to be the one that maximizes the left-hand side of the first inequality, that is, we choose ρ such that

$$E(VU, \mathcal{F}\circ\mathcal{E}) = d\big(VU\rho U^\dagger V^\dagger, \mathcal{F}\circ\mathcal{E}(\rho)\big).$$

Combining this with the two inequalities we obtain

$$E(VU, \mathcal{F}\circ\mathcal{E}) \leq d\big(VU\rho U^\dagger V^\dagger, \mathcal{F}\big(U\rho U^\dagger\big)\big) + d\big(U\rho U^\dagger, \mathcal{E}(\rho)\big).$$

Now notice that, since $U\rho U^\dagger$ is a density operator, we have that $d\big(VU\rho U^\dagger V^\dagger, \mathcal{F}\big(U\rho U^\dagger\big)\big) \leq E(V, \mathcal{F})$ and $d(U\rho U^\dagger, \mathcal{E}(\rho)) \leq E(U, \mathcal{E})$, thus

$$E(VU, \mathcal{F}\circ\mathcal{E}) \leq E(U, \mathcal{E}) + E(V, \mathcal{F}).$$

9.23

If $\mathcal{E}(\rho_j) = \rho_j$ for all j such that $p_j \neq 0$ then $F(\rho_j, \mathcal{E}(\rho_j)) = 1$ for all j such that $p_j \neq 0$, meaning $\bar{F} = \sum_j p_j = 1$. Conversely, if $\bar{F} = 1$, then we have that

$$\begin{aligned}\sum_j p_j F(\rho_j, \mathcal{E}(\rho_j))^2 = 1 = \sum_j p_j \quad &\implies \quad F(\rho_j, \mathcal{E}(\rho_j))^2 = 1 \quad \text{for all } j \text{ such that } p_j \neq 0 \\ &\implies \quad F(\rho_j, \mathcal{E}(\rho_j)) = 1 \quad \text{for all } j \text{ such that } p_j \neq 0.\end{aligned}$$

10 Quantum error-correction

Exercises: 10.1, 10.2, 10.3, 10.4, 10.5, 10.6, 10.7, 10.8, 10.9, 10.10, 10.11, 10.12, 10.13, 10.14, 10.15, 10.16, 10.17, 10.18, 10.19, 10.20, 10.21, 10.22, 10.23, 10.24, 10.25, 10.26, 10.27, 10.28, 10.29, 10.30, 10.31, 10.32, 10.33, 10.34, 10.35, 10.36, 10.37, 10.38, 10.39, 10.40, 10.41, 10.42, 10.43, 10.44, 10.45, 10.46, 10.47, 10.48, 10.49, 10.50, 10.51, 10.52, 10.53, 10.54, 10.55, 10.56, 10.57, 10.58, 10.59, 10.60, 10.61, 10.62, 10.63, 10.64, 10.65, 10.66, 10.67, 10.68, 10.69, 10.70, 10.71, 10.72, 10.73, 10.74.

10.1

Initially we have the state $|\psi\rangle|0\rangle|0\rangle = a|000\rangle + b|100\rangle$, so the action of the circuit is

$$\begin{aligned}a|000\rangle + b|100\rangle &\xrightarrow{CX_{(1,2)}} a|000\rangle + b|110\rangle \\ &\xrightarrow{CX_{(1,3)}} a|000\rangle + b|111\rangle.\end{aligned}$$

10.2

The two projectors P_+ and P_- can be put in the form

$$\begin{aligned}P_+ &= \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{\langle 0| + \langle 1|}{\sqrt{2}}\right) = \frac{|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1|}{2} = \frac{1}{2}(I + X), \\ P_- &= \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\left(\frac{\langle 0| - \langle 1|}{\sqrt{2}}\right) = \frac{|0\rangle\langle 0| - |0\rangle\langle 1| - |1\rangle\langle 0| + |1\rangle\langle 1|}{2} = \frac{1}{2}(I - X),\end{aligned}$$

Thus the quantum operation $\mathcal{E}(\rho) = (1-2p)\rho + 2pP_+\rho P_+ + 2pP_-\rho P_-$ can be rewritten as

$$\begin{aligned}\mathcal{E}(\rho) &= (1-2p)\rho + \frac{p}{2}(I+X)\rho(I+X) + \frac{p}{2}(I-X)\rho(I-X) \\ &= (1-2p)\rho + \frac{p}{2}(\rho + X\rho + \rho X + X\rho X) + \frac{p}{2}(\rho - X\rho - \rho X + X\rho X) \\ &= (1-2p)\rho + p(\rho + X\rho X) \\ &= (1-p)\rho + pX\rho X.\end{aligned}$$

10.3

Operators Z_1Z_2 and Z_2Z_3 can be thought of as projective measurements by looking at their respective spectral decomposition which, by defining projectors

$$\begin{aligned}
P_{+1}^{(Z_1Z_2)} &\equiv (|00\rangle\langle 00| + |11\rangle\langle 11|) \otimes I, \\
P_{-1}^{(Z_1Z_2)} &\equiv (|01\rangle\langle 01| + |10\rangle\langle 10|) \otimes I, \\
P_{+1}^{(Z_2Z_3)} &\equiv I \otimes (|00\rangle\langle 00| + |11\rangle\langle 11|), \\
P_{-1}^{(Z_2Z_3)} &\equiv I \otimes (|01\rangle\langle 01| + |10\rangle\langle 10|),
\end{aligned}$$

can be written as

$$\begin{aligned}
Z_1Z_2 &= P_{+1}^{(Z_1Z_2)} - P_{-1}^{(Z_1Z_2)}, \\
Z_2Z_3 &= P_{+1}^{(Z_2Z_3)} - P_{-1}^{(Z_2Z_3)}.
\end{aligned}$$

Now let us analyze the four possible cases. First, if both Z_1Z_2 and Z_2Z_3 yield $+1$ we have

$$\begin{aligned}
P_{+1}^{(Z_2Z_3)} P_{+1}^{(Z_1Z_2)} &= [(I \otimes |00\rangle\langle 00| + |11\rangle\langle 11|)] [(|00\rangle\langle 00| + |11\rangle\langle 11|) \otimes I] \\
&= |000\rangle\langle 000| + |111\rangle\langle 111| = P_0.
\end{aligned}$$

If Z_1Z_2 yields -1 and Z_2Z_3 yields $+1$ we have

$$\begin{aligned}
P_{-1}^{(Z_2Z_3)} P_{+1}^{(Z_1Z_2)} &= [(I \otimes |00\rangle\langle 00| + |11\rangle\langle 11|)] [(|01\rangle\langle 01| + |10\rangle\langle 10|) \otimes I] \\
&= |100\rangle\langle 100| + |011\rangle\langle 011| = P_1.
\end{aligned}$$

If both Z_1Z_2 and Z_2Z_3 yield -1 we have

$$\begin{aligned}
P_{-1}^{(Z_2Z_3)} P_{-1}^{(Z_1Z_2)} &= [(I \otimes |01\rangle\langle 01| + |10\rangle\langle 10|)] [(|01\rangle\langle 01| + |10\rangle\langle 10|) \otimes I] \\
&= |010\rangle\langle 010| + |101\rangle\langle 101| = P_2.
\end{aligned}$$

And finally if Z_1Z_2 yields $+1$ and Z_2Z_3 yields -1 we have

$$\begin{aligned}
P_{+1}^{(Z_2Z_3)} P_{-1}^{(Z_1Z_2)} &= [(I \otimes |01\rangle\langle 01| + |10\rangle\langle 10|)] [(|00\rangle\langle 00| + |11\rangle\langle 11|) \otimes I] \\
&= |001\rangle\langle 001| + |110\rangle\langle 110| = P_3.
\end{aligned}$$

10.4

The eight projectors onto the computational basis are $|000\rangle\langle 000|$, $|001\rangle\langle 001|$, $|010\rangle\langle 010|$, $|011\rangle\langle 011|$, $|100\rangle\langle 100|$, $|101\rangle\langle 101|$, $|110\rangle\langle 110|$, and $|111\rangle\langle 111|$. If we measure either $|000\rangle\langle 000|$ or $|111\rangle\langle 111|$ we know that the state prior to the measurement was $a\,|000\rangle + b\,|111\rangle$, meaning no bit flip occurred. If we measure either $|100\rangle\langle 100|$ or $|011\rangle\langle 011|$ we know that the state prior to measurement was $a\,|100\rangle + b\,|011\rangle$, meaning qubit 1 suffered a bit flip. If we measured either $|010\rangle\langle 010|$ or $|101\rangle\langle 101|$ we know that the state prior to measurement was $a\,|010\rangle + b\,|101\rangle$, meaning qubit 2 suffered a bit flip. And if we measure either $|001\rangle\langle 001|$ or $|110\rangle\langle 110|$ we know that the state prior to measurement

was $a\,|001\rangle + b\,|110\rangle$, meaning qubit 3 suffered a bit flip.

Since these projective measurements cause the state to collapse to one of the computational basis states it could only be recovered if it was already one of them instead of a superposition. In other words, the state is not altered by the measurement only if either $a = 0$ or $b = 0$, meaning only computational basis states can be recovered.

After the three physical qubits go through the bit flip channel we obtain the state

$$\begin{aligned}\mathcal{E}(|\psi\rangle\langle\psi|) = (1-p)^3\,|\psi\rangle\langle\psi| + p(1-p)^2 X_1\,|\psi\rangle\langle\psi|\,X_1 + p(1-p)^2 X_2\,|\psi\rangle\langle\psi|\,X_2 + p(1-p)^2 X_3\,|\psi\rangle\langle\psi|\,X_3 \\ + p^2(1-p) X_1X_2\,|\psi\rangle\langle\psi|\,X_1X_2 + p^2(1-p) X_1X_3\,|\psi\rangle\langle\psi|\,X_1X_3 \\ + p^2(1-p) X_2X_3\,|\psi\rangle\langle\psi|\,X_2X_3 + p^3 X_1X_2X_3\,|\psi\rangle\langle\psi|\,X_1X_2X_3.\end{aligned}$$

If we consider the initial state to be $|\psi\rangle = a\,|000\rangle + b\,|111\rangle$, after the correction process the term where no flips occur collapses to $|000\rangle$ with probability $|a|^2$ and to $|111\rangle$ with probability $|b|^2$, and the opposite occurs for the term where three flips occur. The terms where one flip occurs collapse to $|000\rangle$ with probability $|a|^2$ and to $|111\rangle$ with probability $|b|^2$, and the opposite occurs for the terms where two flips occur. Therefore the state at the end of the protocol is given by

$$\begin{aligned}\rho = \left(|a|^2(1-p)^3 + 3|a|^2p(1-p)^2 + 3|b|^2p^2(1-p) + |b|^2p^3\right)|000\rangle\langle 000| \\ + \left(|b|^2(1-p)^3 + 3|b|^2p(1-p)^2 + 3|a|^2p^2(1-p) + |a|^2p^3\right)|111\rangle\langle 111|\,.\end{aligned}$$

The minimum fidelity occurs when the quantity

$$\begin{aligned}\langle\psi|\rho|\psi\rangle &= |a|^2\left(|a|^2(1-p)^3 + 3|a|^2p(1-p)^2 + 3|b|^2p^2(1-p) + |b|^2p^3\right) \\ &\quad + |b|^2\left(|b|^2(1-p)^3 + 3|b|^2p(1-p)^2 + 3|a|^2p^2(1-p) + |a|^2p^3\right) \\ &= \left(|a|^4 + |b|^4\right)\left[(1-p)^3 + 3p(1-p)^2\right] + 2|a|^2|b|^2\left[3p^2(1-p) + p^3\right]\end{aligned}$$

is minimal. Using the fact that $|b|^2 = 1 - |a|^2$ we can rewrite

$$\langle\psi|\rho|\psi\rangle = \left(2|a|^4 - 2|a|^2 + 1\right)\left[(1-p)^3 + 3p(1-p)^2\right] + 2\left(|a|^2 - |a|^4\right)\left[3p^2(1-p) + p^3\right].$$

For convenience, let us define $x \equiv |a|^2$ such that

$$\langle\psi|\rho|\psi\rangle = \left(2x^2 - 2x + 1\right)\left[(1-p)^3 + 3p(1-p)^2\right] + 2\left(x - x^2\right)\left[3p^2(1-p) + p^3\right].$$

If we differentiate with respect to x we obtain

$$\begin{aligned}\frac{\partial}{\partial x}\langle\psi|\rho|\psi\rangle &= (4x-2)\left[(1-p)^3 + 3p(1-p)^2 - 3p^2(1-p) - p^3\right], \\ \frac{\partial^2}{\partial x^2}\langle\psi|\rho|\psi\rangle &= 4\left[(1-p)^3 + 3p(1-p)^2 - 3p^2(1-p) - p^3\right].\end{aligned}$$

Taking $p < 1/2$, the second derivative is a positive constant, meaning the zero of the first derivative,

which occurs for $x = 1/2$, is a minimum. Therefore the minimum fidelity is calculated as

$$F_{\min} = \sqrt{\langle\psi|\rho|\psi\rangle}\Big|_{|a|^2=1/2} = \sqrt{\frac{(1-p)^3 + 3p(1-p)^2 + 3p^2(1-p) + p^3}{2}} = \frac{1}{\sqrt{2}},$$

for all $p < 1/2$. This is expected since the protocol is only able to correct computational basis states ($a = 0$ or $b = 0$), so the worst case would occur for $|a| = |b| = 1/\sqrt{2}$. For the case where we initially have a computational basis state, for example, $|\psi\rangle = |000\rangle$, meaning $a = 1$ and $b = 0$, we have

$$F_{\min} = \sqrt{(1-p)^3 + 3p(1-p)^2} > \frac{1}{\sqrt{2}} \quad \text{for } p < 1/2.$$

10.5

For detecting phase flip we must compare the signs of the three blocks of three qubits each, and we do that by applying a three-qubit X operation on two pairs of blocks. Using b_i to denote the i-th block of three qubits, we must measure the operators $X_{\mathrm{b}_1}X_{\mathrm{b}_2}$ and $X_{\mathrm{b}_2}X_{\mathrm{b}_3}$. The first block is composed by the three first qubits, meaning $X_{\mathrm{b}_1} = X_1X_2X_3$, the second by qubits 4 to 6, meaning $X_{\mathrm{b}_2} = X_4X_5X_6$, and finally, the third block by qubits 7 to 9, meaning $X_{\mathrm{b}_3} = X_7X_8X_9$. Writing the two operators explicitly, we see that we are measuring operators $X_1X_2X_3X_4X_5X_6$ and $X_4X_5X_6X_7X_8X_9$.

10.6

If one of the first three qubits suffered a phase flip then the sign in this block is wrong. Applying $Z_1Z_2Z_3$ results in

$$Z_1Z_2Z_3\left(\frac{|000\rangle \pm |111\rangle}{\sqrt{2}}\right) = Z_2Z_3\left(\frac{|000\rangle \mp |111\rangle}{\sqrt{2}}\right) = Z_3\left(\frac{|000\rangle \pm |111\rangle}{\sqrt{2}}\right) = \frac{|000\rangle \mp |111\rangle}{\sqrt{2}}.$$

Therefore applying $Z_1Z_2Z_3$ is guaranteed to invert the sign of the first block.

10.7

Let us name the operation elements $E_0 \equiv \sqrt{(1-p)^3}I$, and $E_i = \sqrt{p(1-p)^2}X_i$ for $i = 1, 2, 3$. Explicit calculation yields

$$\begin{aligned}
PE_0^\dagger E_0 P &= (1-p)^3 P, \\
PE_0^\dagger E_i P &= \sqrt{p(1-p)^5} P X_i P, \\
PE_i^\dagger E_0 P &= \sqrt{p(1-p)^5} P X_i^\dagger P, \\
PE_i^\dagger E_j P &= p(1-p)^2 P X_i^\dagger X_j P.
\end{aligned}$$

Since $X_i = X_i^\dagger$ for all indices the second and third equations are the same. Now we have that

$$\begin{aligned}
PX_iP &= (|000\rangle\langle 000| + |111\rangle\langle 111|)\, X_i\, (|000\rangle\langle 000| + |111\rangle\langle 111|) = 0, \\
PX_iX_jP &= (|000\rangle\langle 000| + |111\rangle\langle 111|)\, X_iX_j\, (|000\rangle\langle 000| + |111\rangle\langle 111|) = \delta_{ij}P.
\end{aligned}$$

Therefore, writing the equations in matrix form, the α_{ij} matrix will be

$$\alpha = \begin{bmatrix} (1-p)^3 & 0 & 0 & 0 \\ 0 & p(1-p)^2 & 0 & 0 \\ 0 & 0 & p(1-p)^2 & 0 \\ 0 & 0 & 0 & p(1-p)^2 \end{bmatrix},$$

which is a Hermitian matrix, meaning the quantum error-correction conditions are satisfied.

10.8

The projection onto the code space is $P \equiv |+++\rangle\langle+++| + |---\rangle\langle---|$. Thus using the fact that all error operators in the set are Hermitian we have

$$\begin{aligned} PIIP &= P \\ PIZ_iP &= PZ_iIP = 0, \\ PZ_iZ_jP &= \delta_{ij}P. \end{aligned}$$

The α_{ij} matrix is therefore the identity matrix, which is Hermitian, meaning the quantum error-correction conditions are satisfied.

10.9

The projection onto the code space is $R \equiv |+++\rangle\langle+++| + |---\rangle\langle---|$, and for convenience, we will use the following notation for the operators in the error set:

$$\begin{aligned} P_i &\equiv |0_i,+,+\rangle\langle 0_i,+,+| + |0_i,-,+\rangle\langle 0_i,-,+| + |0_i,+,-\rangle\langle 0_i,+,-| + |0_i,-,-\rangle\langle 0_i,-,-|, \\ Q_i &\equiv |1_i,+,+\rangle\langle 1_i,+,+| + |1_i,-,+\rangle\langle 1_i,-,+| + |1_i,+,-\rangle\langle 1_i,+,-| + |1_i,-,-\rangle\langle 1_i,-,-|, \end{aligned}$$

where the index in either 0 or 1 indicates the position of such 0 and 1, for example, the state $|0_i,+,+\rangle$ represents $|0,+,+\rangle$ for $i=1$, $|+,0,+\rangle$ for $i=2$, and $|+,+,0\rangle$ for $i=3$. Naturally, we have $RIIR = R$. Now using the fact that $|0\rangle = (|+\rangle + |-\rangle)/\sqrt{2}$ and $|1\rangle = (|+\rangle - |-\rangle)/\sqrt{2}$ we obtain

$$\begin{aligned} RIP_iR = RP_iIR &= R\left(\frac{1}{\sqrt{2}}|0_i,+,+\rangle\langle+++| + \frac{1}{\sqrt{2}}|0_i,-,-\rangle\langle---|\right) \\ &= \frac{1}{2}|+++\rangle\langle+++| + \frac{1}{2}|---\rangle\langle---| = \frac{1}{2}R, \end{aligned}$$

$$\begin{aligned} RIQ_iR = RQ_iIR &= R\left(\frac{1}{\sqrt{2}}|1_i,+,+\rangle\langle+++| - \frac{1}{\sqrt{2}}|1_i,-,-\rangle\langle---|\right) \\ &= \frac{1}{2}|+++\rangle\langle+++| + \frac{1}{2}|---\rangle\langle---| = \frac{1}{2}R. \end{aligned}$$

We also calculate

$$RP_iP_jR = \frac{1}{\sqrt{2}}\Big(|+++\rangle\langle 0_i,+,+| + |---\rangle\langle 0_i,-,-| \Big)\frac{1}{\sqrt{2}}\Big(|0_j,+,+\rangle\langle +++| + |0_j,-,-\rangle\langle ---| \Big),$$

$$RQ_iQ_jR = \frac{1}{\sqrt{2}}\Big(|+++\rangle\langle 1_i,+,+| - |---\rangle\langle 1_i,-,-| \Big)\frac{1}{\sqrt{2}}\Big(|1_j,+,+\rangle\langle +++| - |1_j,-,-\rangle\langle ---| \Big),$$

Notice that if $i = j$ the result is the same as above since $P_i^2 = P_i$ and $Q_i^2 = Q_i$ for all i. If $i \neq j$

$$RP_iP_jR = \frac{1}{2}\left(\frac{1}{2}|+++\rangle\langle +++| + \frac{1}{2}|---\rangle\langle ---|\right) = \frac{1}{4}R,$$

$$RQ_iQ_jR = \frac{1}{2}\left(\frac{1}{2}|+++\rangle\langle +++| + \frac{1}{2}|---\rangle\langle ---|\right) = \frac{1}{4}R.$$

The only remaining terms are

$$RP_iQ_jR = \frac{1}{\sqrt{2}}\Big(|+++\rangle\langle 0_i,+,+| + |---\rangle\langle 0_i,-,-| \Big)\frac{1}{\sqrt{2}}\Big(|1_j,+,+\rangle\langle +++| - |1_j,-,-\rangle\langle ---| \Big),$$

$$RQ_iP_jR = \frac{1}{\sqrt{2}}\Big(|+++\rangle\langle 1_i,+,+| - |---\rangle\langle 1_i,-,-| \Big)\frac{1}{\sqrt{2}}\Big(|0_j,+,+\rangle\langle +++| + |0_j,-,-\rangle\langle ---| \Big).$$

In this case, if $i = j$ the result will be zero because of the orthogonality of $|0\rangle$ and $|1\rangle$. If $i \neq j$

$$RP_iQ_jR = \frac{1}{2}\left(\frac{1}{2}|+++\rangle\langle +++| - \left(-\frac{1}{2}\right)|---\rangle\langle ---|\right) = \frac{1}{4}R,$$

$$RQ_iP_jR = \frac{1}{2}\left(\frac{1}{2}|+++\rangle\langle +++| - \left(-\frac{1}{2}\right)|---\rangle\langle ---|\right) = \frac{1}{4}R.$$

If we construct a matrix with entries $RO_{\mathrm{r}}O_{\mathrm{c}}R$ such that O_{r} are the operators determining the rows and O_{c} are the ones determining the column, and the order of operators is $\{I, P_1, Q_1, P_2, Q_2, P_3, Q_3\}$, we get the α_{ij} matrix to be given by

$$\alpha = \begin{bmatrix} 1 & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & 0 & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} \\ \frac{1}{2} & 0 & \frac{1}{2} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} \\ \frac{1}{2} & \frac{1}{4} & \frac{1}{4} & \frac{1}{2} & 0 & \frac{1}{4} & \frac{1}{4} \\ \frac{1}{2} & \frac{1}{4} & \frac{1}{4} & 0 & \frac{1}{2} & \frac{1}{4} & \frac{1}{4} \\ \frac{1}{2} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{2} & 0 \\ \frac{1}{2} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & 0 & \frac{1}{2} \end{bmatrix},$$

which is Hermitian, meaning the quantum error-correction conditions are satisfied.

10.10

The projection onto the code space is given by $P \equiv |0_L\rangle\langle 0_L| + |1_L\rangle\langle 1_L|$ with

$$|0_L\rangle \equiv \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}},$$
$$|1_L\rangle \equiv \frac{(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}}.$$

Naturally, we have $PIIP = P$, and since $X_i^2 = Y_i^2 = Z_i^2 = I$ for all i we conclude that all entries in the diagonal of the α_{ij} matrix are 1. Let us now analyze the elements in the first row and column of the α_{ij} matrix. They have the form $PIX_iP = PX_iIP$, $PIY_iP = PY_iIP$, and $PIZ_iP = PZ_iIP$. Since X_i and Y_i for all i will just flip the corresponding qubit in each component, and $|0\rangle$ and $|1\rangle$ are orthogonal, the result must vanish, meaning

$$PIX_iP = PX_iIP = 0,$$
$$PIY_iP = PY_iIP = 0.$$

For the Z_i notice that we can simplify the $|0_L\rangle$ and $|1_L\rangle$ to $|0_L\rangle = |+_L\rangle|+_L\rangle|+_L\rangle$ and $|1_L\rangle = |-_L\rangle|-_L\rangle|-_L\rangle$, with

$$|+_L\rangle \equiv \frac{|000\rangle + |111\rangle}{\sqrt{2}}, \quad |-_L\rangle \equiv \frac{|000\rangle - |111\rangle}{\sqrt{2}}.$$

Now it is straightforward to see that Z_1, Z_2, and Z_3 all flip the first $|+_L\rangle$ to $|-_L\rangle$ and vice versa, Z_4, Z_5 and Z_6 do the same to the second, and Z_7, Z_8 and Z_9 do the same to the third. Since $|+_L\rangle$ and $|-_L\rangle$ are orthogonal we also conclude

$$PIZ_iP = PZ_iIP = 0.$$

For the elements with two different operators but containing the same index the result must also vanish because of the relations $XY = iZ$, $YZ = iX$, and $ZX = iY$, so they will reduce to the same terms calculated above, therefore

$$PX_iY_iP = PY_iX_iP = PY_iZ_iP = PZ_iY_iP = PZ_iX_iP = PX_iZ_iP = 0.$$

So far we have 136 out of the 784 entries of the α_{ij} with only the diagonal non-vanishing. It remains to find the 216 elements for which the pair of operators are the same but with different indices, which are PX_iX_jP, PY_iY_jP, and PZ_iZ_jP, and the 432 elements with different operators and indices, which are PX_iY_jP, PY_iX_jP, PX_iZ_jP, PZ_iX_jP, PY_iZ_jP, and PZ_iY_jP. Let us then analyze the first group of elements. The operators X_jX_i and Y_jY_i will just flip the i-th and j-th qubit in each component, which will result in a state orthogonal to $|0_L\rangle$ and $|1_L\rangle$, thus

$$PX_iX_jP = PY_iY_jP = 0 \quad \forall\, i \neq j.$$

For Z_iZ_j, if they flip the same block of $|+_L\rangle$ and $|-_L\rangle$ then they amount to an identity operation, otherwise, the result will vanish for the same reason PIZ_iP and PZ_iIP vanish. The identity operation will occur only if Z_i and Z_j are both in one of these sets: $\{Z_1, Z_2, Z_3\}$, $\{Z_4, Z_5, Z_6\}$, or $\{Z_7, Z_8, Z_9\}$. Also, since Z_i and Z_j commute we have $PZ_iZ_jP = PZ_jZ_iP$. Finally, all remaining terms vanish because the presence of either X_i and/or Y_i will flip qubits, leading to a state orthogonal to $|0_L\rangle$ and $|1_L\rangle$. Therefore all entries of the α_{ij} matrix will be zero except the diagonal and some of the terms of the form $PZ_iZ_jP = PZ_jZ_iP$ (symmetrical), which will all be 1. So the matrix is Hermitian and thus the quantum error-correction conditions are satisfied.

10.11

Such quantum operation corresponds to the depolarizing channel with $p = 1$, which is simply

$$\mathcal{E}(\rho) = \frac{I}{2}.$$

We can rewrite $I/2$ as (see Exercise 8.17)

$$\frac{I}{2} = \frac{\rho + X\rho X + Y\rho Y + Z\rho Z}{4},$$

thus a set of operation elements for a quantum operation that replaces any state ρ with $I/2$ is

$$E_0 = \frac{I}{2},\ E_1 = \frac{X}{2},\ E_2 = \frac{Y}{2},\ E_3 = \frac{Z}{2}.$$

Notice that since $X^2 = Y^2 = Z^2 = I$ they satisfy $\sum_i E_i^\dagger E_i = I$.

10.12

$$\begin{aligned}
\mathcal{E}(|0\rangle\langle 0|) &= (1-p)\,|0\rangle\langle 0| + \frac{p}{3}\left(X\,|0\rangle\langle 0|\,X + Y\,|0\rangle\langle 0|\,Y + Z\,|0\rangle\langle 0|\,Z\right) \\
&= (1-p)\,|0\rangle\langle 0| + \frac{p}{3}\left(|1\rangle\langle 1| + |1\rangle\langle 1| + |0\rangle\langle 0|\right) \\
&= \left(1 - \frac{2p}{3}\right)|0\rangle\langle 0| + \frac{2p}{3}\,|1\rangle\langle 1|\,.
\end{aligned}$$

The fidelity will be

$$F(|0\rangle\,, \mathcal{E}(|0\rangle\langle 0|)) = \sqrt{\langle 0|\left[\left(1 - \frac{2p}{3}\right)|0\rangle\langle 0| + \frac{2p}{3}\,|1\rangle\langle 1|\right]|0\rangle} = \sqrt{1 - \frac{2p}{3}}.$$

Since the depolarizing channel always returns mixed states the higher the value of p is, the minimal fidelity will occur whenever the initial state is pure. Since $|0\rangle$ is a pure state the obtained fidelity must correspond to the minimum.

10.13

Let us consider $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$. Then

$$\begin{aligned}\mathcal{E}(|\psi\rangle\langle\psi|) &= \begin{bmatrix}1 & 0\\ 0 & \sqrt{1-\gamma}\end{bmatrix}\begin{bmatrix}|a|^2 & ab^*\\ a^*b & |b|^2\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & \sqrt{1-\gamma}\end{bmatrix} + \begin{bmatrix}0 & \sqrt{\gamma}\\ 0 & 0\end{bmatrix}\begin{bmatrix}|a|^2 & ab^*\\ a^*b & |b|^2\end{bmatrix}\begin{bmatrix}0 & 0\\ \sqrt{\gamma} & 0\end{bmatrix}\\ &= \begin{bmatrix}|a|^2+\gamma|b|^2 & \sqrt{1-\gamma}ab^*\\ \sqrt{1-\gamma}a^*b & (1-\gamma)|b|^2\end{bmatrix}.\end{aligned}$$

The fidelity will be

$$\begin{aligned}F(|\psi\rangle, \mathcal{E}(|\psi\rangle\langle\psi|)) &= \sqrt{\begin{bmatrix}a^* & b^*\end{bmatrix}\begin{bmatrix}|a|^2+\gamma|b|^2 & \sqrt{1-\gamma}ab^*\\ \sqrt{1-\gamma}a^*b & (1-\gamma)|b|^2\end{bmatrix}\begin{bmatrix}a\\ b\end{bmatrix}}\\ &= \sqrt{|a|^4 + (1-\gamma)|b|^4 + \left(\gamma + 2\sqrt{1-\gamma}\right)|a|^2|b|^2}.\end{aligned}$$

Using the fact that $|b|^2 = 1 - |a|^2$ we may rewrite the fidelity only in terms of a. For convenience let us define $x \equiv |a|^2$. We get

$$\begin{aligned}F(|\psi\rangle, \mathcal{E}(|\psi\rangle\langle\psi|)) &= \sqrt{x^2 + (1-\gamma)(1-x)^2 + \left(\gamma + 2\sqrt{1-\gamma}\right)x(1-x)}\\ &= \sqrt{2\left(1-\gamma-\sqrt{1-\gamma}\right)x^2 + \left(3\gamma - 2 + 2\sqrt{1-\gamma}\right)x + (1-\gamma)}.\end{aligned}$$

Since the square root is a monotonically increasing function the minimum of the fidelity corresponds to the minimum of the function inside the square root, which we will call $f(x)$. By differentiating it with respect to x we obtain

$$\frac{\mathrm{d}f}{\mathrm{d}x} = 4\left(1-\gamma-\sqrt{1-\gamma}\right)x + \left(3\gamma - 2 + 2\sqrt{1-\gamma}\right).$$

This function is non-negative for all $x \in [0,1]$. One way to verify this is to first calculate $\mathrm{d}f/\mathrm{d}x$ at $x = 1$, which results in

$$\left.\frac{\mathrm{d}f}{\mathrm{d}x}\right|_{x=1} = 2 - \gamma - 2\sqrt{1-\gamma},$$

non-negative for $0 \leq \gamma \leq 1$. Since the term proportional to x is always non-positive, any $f(x<1)$ must also be non-negative. Therefore $f(x)$ never decreases with x, so the minimum occurs for $x = 0$. Plugging it in the fidelity we find

$$F_{\min}(|\psi\rangle, \mathcal{E}(|\psi\rangle\langle\psi|)) = \sqrt{1-\gamma}.$$

10.14

The first column of G must have 1 in its r first entries and 0 elsewhere. The second column must have 1 from the $(r+1)$-th to the $(2r)$-th entry and 0 ensewhere. And the same logic applies to

the following columns up to the k-th, which will have 1 in its last r entries and zero elsewhere. For indices $i \in [1, rk]$ and $j \in [1, k]$ one possible expression for the generator matrix is

$$G_{ij} = \begin{cases} 1 & \text{for } (j-1)r < i \leq jr; \\ 0 & \text{otherwise.} \end{cases}$$

10.15

All possible codewords can be formed as a linear combination of the columns of G, that is, if G has columns $(y_1, \cdots, y_k)$ any codeword x can be written as

$$x = \sum_{i=1}^{k} x_i y_i = x_1 y_1 + \cdots + x_k y_k,$$

where all x_i are either 0 or 1. If we include one more column resulting from the addition of two columns, say columns j and l, then any codeword may be written as

$$\begin{aligned} x &= x_1 y_1 + \cdots + x_k y_k + x_{k+1}(y_j + y_l) \\ &= x_1 y_1 + \cdots + (x_j + x_{k+1}) y_j + (x_l + x_{k+1}) y_l + \cdots + x_k y_k. \end{aligned}$$

Since $x_j + x_{k+1}$ and $x_l + x_{k+1}$ will also be either 0 or 1, the set of possible x remains the same.

10.16

H is an $(n-k) \times n$ matrix and any codeword x is an n-dimensional vector. Their relation is such that for any codeword we have $Hx = 0$. Considering that the rows of H are given by $(y_1, \cdots, y_{n-k})$ and the entries of x are given by $(x_1, \cdots, x_n)$ the resulting $(n-k)$-dimensional vector will be zero if and only if

$$\sum_{j=1}^{n} y_{1j} x_j = \cdots = \sum_{j=1}^{n} y_{(n-k)j} x_j = 0.$$

If we include one more row to H resulting from the addition of two rows, say rows l and m, the vector resulting from Hx will be $(n-k+1)$-dimensional. The last entry will be given by

$$\sum_{j=1}^{n} (y_{lj} + y_{mj}) x_j = \sum_{j=1}^{n} y_{lj} x_j + \sum_{j=1}^{n} y_{mj} x_j = 0,$$

thus this action does not change the code.

10.17

We need $6 - 2 = 4$ vectors orthogonal modulo 2 to $(1, 1, 1, 0, 0, 0)$ and $(0, 0, 0, 1, 1, 1)$. The vectors $(1, 1, 0, 0, 0, 0)$, $(0, 1, 1, 0, 0, 0)$, $(0, 0, 0, 1, 1, 0)$, and $(0, 0, 0, 0, 1, 1)$ satisfy this and are all linearly

independent of each other, thus

$$H = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

10.18

Let the $n-k$ rows of the H matrix be $(x_1, \cdots, x_{n-k})$ and let the k columns of G be $(y_1, \cdots, y_k)$. The resulting $(n-k) \times k$ matrix will have entries in the i-th row and j-th column given by $x_i \cdot y_j$. By construction, all x_i are orthogonal modulo 2 to all y_j, meaning $x_i \cdot y_j = 0$, thus $HG = 0$.

10.19

Given that $H = [A|I_{n-k}]$, with A an $(n-k) \times k$ matrix, its i-th row is given by

$$x_i = (A_{i1}, \cdots, A_{ik}, 0, \cdots, 1, \cdots, 0),$$

where the 1 from the identity is at the i-th entry after the first k entries with A terms. We know that the generator matrix must be such that $HG = 0$ (see Exercise 10.18). Defining the matrix

$$G \equiv \left[\frac{I_k}{-A}\right],$$

we see that its j-th column is given by

$$y_j = (0, \cdots, 1, \cdots, 0, -A_{1j}, \cdots, -A_{(n-k)j}),$$

where the 1 from the identity is at the j-th entry. The condition $HG = 0$ means that $x_i \cdot y_j = 0$ for all i and j. By direct verification we get

$$\begin{aligned} x_i \cdot y_j &= (A_{i1}, \cdots, A_{ik}, 0, \cdots, 1, \cdots, 0) \cdot (0, \cdots, 1, \cdots, 0, -A_{1j}, \cdots, -A_{(n-k)j}) \\ &= 0 + \cdots + A_{ij} + \cdots + 0 + 0 + \cdots + -A_{ij} + \cdots + 0 \\ &= A_{ij} - A_{ij} = 0. \end{aligned}$$

Thus the generator matrix is indeed the one shown above.

10.20

Considering H has entries H_{ij} with $i \in [1, n-k]$ and $j \in [1, n]$, and any codeword x has entries $(x_1, \cdots, x_n)$ we have $\sum_{j=1}^{n} H_{ij} x_j = 0$ for all i, thus summing for all i yields

$$\sum_{i=1}^{n-k} \sum_{j=1}^{n} H_{ij} x_j = x_1 \sum_{i=1}^{n-k} H_{i1} + \cdots + x_n \sum_{i=1}^{n-k} H_{in} = 0.$$

Notice that $\sum_{i=1}^{n-k} H_{ij}$ corresponds to the j-th column of H, naming it h_j we get

$$x_1 h_1 + \cdots + x_n h_n = 0.$$

Since any $d-1$ columns of H are linearly independent, meaning a sum of $d-1$ of them cannot vanish, any codeword with $d-1$ or fewer entries equal to 1 cannot belong in the code since it would be a contradiction. Therefore the minimum number of entries equal to 1 a codeword in the code can have is d, thus $d(C) = d$.

10.21

Since H can always be written as $[A|I_{n-k}]$, A containing only 0 and 1 entries, it has at most $n-k$ linearly independent columns. All $[n, k, d]$ codes have a matrix H with any set of $d-1$ columns being linearly independent (see Exercise 10.20). Both statements combined implies $n - k \geq d - 1$.

10.22

All $2^r - 1$ columns of H are different, meaning it contains all possible 2^r binary strings with length r excluding the one containing all zeros. But because it contains all possible strings with at least one non-zero entry in its columns, any combination of two such strings will result in a string with two non-zero entries, which must also correspond to a column, meaning there are always groups of three columns which are linearly dependent. It follows that any Hemming code has distance 3 (see Exercise 10.20). Given that $3 = 2t + 1$ for $t = 1$, all Hamming codes can correct errors on one bit.

10.23

-

10.24

For any code C it is always true that the generator matrix G and parity check matrix H satisfy $HG = 0$ (see Exercise 10.18). The analogous relation for $C^\perp$ is $G^{\mathrm{T}} H^{\mathrm{T}} = 0$. If C is weakly self-dual, that is $C \subseteq C^\perp$, then any codeword in C is also a codeword of $C^\perp$, meaning the columns of G or a linear combination of them must be present in H^{T}, thus since $G^{\mathrm{T}} H^{\mathrm{T}} = 0$ it follows that $G^{\mathrm{T}} G = 0$. Conversely, if it is given that $G^{\mathrm{T}} G = 0$ then for any two messages x_1 and x_2 we have two codewords $y_1 = G x_1$ and $y_2 = G x_2$ in C are such that $y_1 \cdot y_2 = x_1^{\mathrm{T}} G^{\mathrm{T}} G x_2 = 0$ by hypothesis, therefore all codewords in C are orthogonal to each other, meaning $C \subseteq C^\perp$, so C is weakly self-dual.

10.25

If $x \in C^\perp$ then for all $y \in C$ we have that $x \cdot y = 0$. Thus $(-1)^{x \cdot y} = 1$ for all y, meaning

$$\sum_{y \in C} (-1)^{x \cdot y} = |C|.$$

If $x \notin C^{\perp}$ we can consider the columns of the generator matrix G to be given by $(y_1, \cdots, y_n)$, ordered such that from y_1 to y_j are codewords that are not orthogonal to x and from y_{j+1} to y_n they are orthogonal to x. Any $y \in C$ can be written as a linear combination of these y_i. If y is a codeword that contains an even number of elements from the set $(y_1, \cdots, y_j)$ then $x \cdot y = 0$ since it would correspond to a sum modulo 2 of an even number of 1's. Analogously, if y contains an odd number of elements from $(y_1, \cdots, y_j)$ then $x \cdot y = 1$. The number of possible codewords with an even number of elements from this set is

$$\sum_{i=0}^{\lfloor j/2 \rfloor} \binom{j}{2i} = \frac{2^j}{2} = 2^{j-1},$$

and the number of possible codewords containing an odd number of elements is

$$\sum_{i=0}^{\lfloor (j-1)/2 \rfloor} \binom{j}{2i+1} = \frac{2^j}{2} = 2^{j-1}.$$

Since they are equal then in exactly half of the cases we have $(-1)^{x \cdot y} = 1$ and in the other half we have $(-1)^{x \cdot y} = -1$, meaning

$$\sum_{y \in C} (-1)^{x \cdot y} = 0.$$

10.26

First, since H is an $(n - (k_1 - k_2)) \times n$ matrix, the resulting vector Hx has $n - (k_1 - k_2)$ entries, meaning the ancilla $|0\rangle$ is formed by $n - (k_1 - k_2)$ qubits, each initially in state zero. The i-th element of this vector is given by $\sum_{j=1}^{n} H_{ij} x_j$. H_{ij} and x_j are both either 0 or 1. If $H_{ij} = 0$ then this term will contribute nothing to the sum for the i-th qubit of $|Hx\rangle$ independently of x_j. This corresponds to doing nothing to the i-th qubit of the ancilla system. If $H_{ij} = 1$ then this term will either contribute nothing to the sum if $x_j = 0$, and will sum 1 if $x_j = 1$. This corresponds to applying a bit-flip to the i-th qubit if $x_j = 1$, which is a CNOT gate. Therefore, to create the state $|Hx\rangle$ one must apply CNOT gates with the j-th qubit of $|x\rangle$ acting as control and the i-th qubit of the ancilla system as target for each $H_{ij} = 1$, and apply nothing for each $H_{ij} = 0$.

10.27

Naming e_1 the vector with entries 1 where a bit flip occurred and e_2 the vector with entries 1 where a phase flip occurred, the state after the error will be given by

$$\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{u \cdot y} (-1)^{(x+y+v) \cdot e_2} \left| x + y + v + e_1 \right\rangle .$$

Since $x + y \in C_1$ we can use the parity check matrix H_1 of C_1 to create the state $|H_1(x + y + v + e_1)\rangle = |H_1 v + H_1 e_1\rangle$ in an ancilla system A_1. Given that the parametrization state $|v\rangle$ is known we may also create another ancilla system V in state $|H_1 v\rangle$ with the same procedure. If we apply CNOT gates with the i-th qubit of V as control and the i-th qubit of A_1 as target we effectively put A_1

in the state $|H_1 e_1\rangle$. By measuring the syndrome in system A_1 and discarding it we can correct the bit-flip errors and the resulting state in the original system will be

$$\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{u \cdot y} (-1)^{(x+y+v)\cdot e_2} |x+y+v\rangle .$$

Applying a Hadamard gate to each qubit we get the state

$$\begin{aligned} &\frac{1}{\sqrt{|C_2|2^n}} \sum_z \sum_{y \in C_2} (-1)^{u \cdot y} (-1)^{(x+y+v)\cdot(e_2+z)} |z\rangle \\ = &\frac{1}{\sqrt{|C_2|2^n}} \sum_z \sum_{y \in C_2} (-1)^{y \cdot (u+e_2+z)} (-1)^{(x+v)\cdot(e_2+z)} |z\rangle \end{aligned}$$

Defining $z' \equiv z + u + e_2$ we may rewrite the state as

$$\frac{1}{\sqrt{|C_2|2^n}} \sum_{z'} \sum_{y \in C_2} (-1)^{y \cdot z'} (-1)^{(x+v)\cdot(z'+u)} |z' + u + e_2\rangle .$$

We know that $\sum_{y \in C_2} (-1)^{y \cdot z'}$ is either $|C_2|$ for $z' \in C_2^\perp$ or 0 otherwise (see Exercise 10.25), so we may rewrite the state as

$$\sqrt{\frac{|C_2|}{2^n}} \sum_{z' \in C_2^\perp} (-1)^{(x+v)\cdot(z'+u)} |z' + u + e_2\rangle .$$

Since $z' \in C_2^\perp$ for all terms in the sum we can use the parity check matrix H_2 of $C_2^\perp$ to create the state $|H_2(z' + u + e_2)\rangle = |H_2 u + H_2 e_2\rangle$ in an ancilla system A_2. Knowing the parametrization state $|u\rangle$ we can also create another ancilla system U in state $|H_2 u\rangle$. If we apply CNOT gates with the i-th qubit of U as control and the i-th qubit of A_2 as target we effectively put A_2 in the state $|H_2 e_2\rangle$. Just like before, we can measure the syndrome in system A_2 and correct the bit-flip errors (which correspond to the phase flip errors in the original base), and after discarding it and making the corrections we are left in the state

$$\sqrt{\frac{|C_2|}{2^n}} \sum_{z' \in C_2^\perp} (-1)^{(x+v)\cdot(z'+u)} |z' + u\rangle .$$

By applying Hadamard gates on each qubit again we return to what we had before the first application but with $e_2 = 0$, yielding

$$|x + C_2\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{u \cdot y} |x + y + v\rangle ,$$

which is the intended state. So such code is equivalent to $\mathrm{CSS}(C_1, C_2)$.

10.28

The transpose of Eq. (10.77) is

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}.$$

In order for it to be the generator matrix for the $[7, 4, 3]$ Hamming code it must have all of its columns linearly independent, which is clearly satisfied, and it must be such that $HG = 0$ (see Exercise 10.18), where H is the parity check matrix shown in Eq. (10.76). By direct verification we get

$$HG = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

10.29

Let $|\psi_1\rangle, |\psi_2\rangle \in V_S$, then for all $\sigma \in S$ we have $\sigma |\psi_1\rangle = |\psi_1\rangle$ and $\sigma |\psi_2\rangle = |\psi_2\rangle$. Thus for a linear combination $|\phi\rangle \equiv a |\psi_1\rangle + b |\psi_2\rangle$ we obtain

$$\sigma |\phi\rangle = \sigma (a |\psi_1\rangle + b |\psi_2\rangle) = a\sigma |\psi_1\rangle + b\sigma |\psi_2\rangle = a |\psi_1\rangle + b |\psi_2\rangle = |\phi\rangle,$$

meaning $|\phi\rangle$ is stalibilized by S, and therefore $|\phi\rangle \in V_S$.

Let $S = \{\sigma_1, \cdots, \sigma_n\}$, and $\{V_1, \cdots, V_n\}$ be the subspaces stabilized by each individual operator in S. By definition, any state $|\psi\rangle \in V_S$ must be contained in the subspaces V_i for all i. Furthermore, any state that fails to be in at least one of the V_i cannot possibly be in V_S. Therefore we can write

$$V_S = \bigcap_{i=1}^{n} V_i.$$

10.30

If S contains $\pm iI$, it cannot be considered a group without the element $-I$ because $(\pm iI)^2 = -I$, meaning it would not be closed, and therefore not a subgroup. Thus, if $-I \notin S$ then $\pm iI \notin S$.

10.31

If $S = \langle g_1, \cdots, g_l \rangle$ then any two elements in S can be written as products of such generators, that is, $\sigma_a \equiv g_{i_1} \cdots g_{i_a}$, and $\sigma_b \equiv g_{j_1} \cdots g_{j_b}$, where all indices from i_1 to i_a and from j_1 to j_b can assume integer values in the range $[1, \cdots, l]$. Since these combinations are arbitrary, any σ_a will commute with any σ_b only if all g_i and g_j commute for each pair i and j. Conversely, if g_i and g_j commute for each pair i and j then S is clearly Abelian, meaning all of its elements commute.

10.32

From Equation (10.78), we can write the codewords of C_2 implicitly with the state

$$|0_L\rangle = \frac{1}{\sqrt{8}}\Big[\, |0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle \\ + |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle \,\Big].$$

The stabilizer generators are $g_1 = X_4X_5X_6X_7$, $g_2 = X_2X_3X_6X_7$, $g_3 = X_1X_3X_5X_7$, $g_4 = Z_4Z_5Z_6Z_7$, $g_5 = Z_2Z_3Z_6Z_7$, $g_6 = Z_1Z_3Z_5Z_7$. By direct verification we get

$$\begin{aligned}
g_1|0_L\rangle &= \frac{1}{\sqrt{8}}\Big[\, |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle \\
&\quad + |0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle \,\Big] = |0_L\rangle\,, \\
g_2|0_L\rangle &= \frac{1}{\sqrt{8}}\Big[\, |0110011\rangle + |1100110\rangle + |0000000\rangle + |1010101\rangle \\
&\quad + |0111100\rangle + |1101001\rangle + |0001111\rangle + |1011010\rangle \,\Big] = |0_L\rangle\,, \\
g_3|0_L\rangle &= \frac{1}{\sqrt{8}}\Big[\, |1010101\rangle + |0000000\rangle + |1100110\rangle + |0110011\rangle \\
&\quad + |1011010\rangle + |0001111\rangle + |1101001\rangle + |0111100\rangle \,\Big] = |0_L\rangle\,, \\
g_4|0_L\rangle &= \frac{1}{\sqrt{8}}\Big[\, |0000000\rangle + (-1)^2|1010101\rangle + (-1)^2|0110011\rangle + (-1)^2|1100110\rangle \\
&\quad + (-1)^4|0001111\rangle + (-1)^2|1011010\rangle + (-1)^2|0111100\rangle + (-1)^2|1101001\rangle \,\Big] = |0_L\rangle\,, \\
g_5|0_L\rangle &= \frac{1}{\sqrt{8}}\Big[\, |0000000\rangle + (-1)^2|1010101\rangle + (-1)^4|0110011\rangle + (-1)^2|1100110\rangle \\
&\quad + (-1)^2|0001111\rangle + (-1)^2|1011010\rangle + (-1)^2|0111100\rangle + (-1)^2|1101001\rangle \,\Big] = |0_L\rangle\,, \\
g_6|0_L\rangle &= \frac{1}{\sqrt{8}}\Big[\, |0000000\rangle + (-1)^4|1010101\rangle + (-1)^2|0110011\rangle + (-1)^2|1100110\rangle \\
&\quad + (-1)^2|0001111\rangle + (-1)^2|1011010\rangle + (-1)^2|0111100\rangle + (-1)^2|1101001\rangle \,\Big] = |0_L\rangle\,.
\end{aligned}$$

So these codewords are clearly stabilized. The remaining ones are represented by the state $|1_L\rangle \equiv X^{\otimes 7}|0_L\rangle$. $X^{\otimes 7}$ clearly commutes with g_1, g_2, and g_3, and since g_4, g_5, and g_6 all contain an even number of Z operators, it also commutes with them, thus for all i we have

$$g_i|1_L\rangle = g_i X^{\otimes 7}|0_L\rangle = X^{\otimes 7} g_i|0_L\rangle = X^{\otimes 7}|0_L\rangle = |1_L\rangle\,.$$

Therefore these generators stabilize the codewords of the Steane code.

10.33

Let $r(g) \equiv [x|z]$ and $r(g') \equiv [x'|z']$, where x, x', z, and z' denote n-bit strings containing the information about the positions of the Pauli operators within g and g'. Considering that $x = (x_1, \cdots, x_n)$ and $z = (z_1, \cdots, z_n)$, we obtain

$$r(g)\Lambda = \begin{bmatrix} x_1 & \cdots & x_n & z_1 & \cdots & z_n \end{bmatrix} \begin{bmatrix} 0 & I \\ I & 0 \end{bmatrix} = \begin{bmatrix} z_1 & \cdots & z_n & x_1 & \cdots & x_n \end{bmatrix},$$

and thus, considering that $x' = (x'_1, \cdots, x'_n)$ and $z' = (z'_1, \cdots, z'_n)$, we get

$$r(g)\Lambda r(g')^{\mathrm{T}} = \begin{bmatrix} z_1 & \cdots & z_n & x_1 & \cdots & x_n \end{bmatrix} \begin{bmatrix} x'_1 \\ \vdots \\ x'_n \\ z'_1 \\ \vdots \\ z'_n \end{bmatrix} = \bigoplus_{i=1}^{n} (z_i x'_i \oplus x_i z'_i).$$

Let us start by considering $r(g)\Lambda r(g') = 0$. This can only happen if $z_i x'_i \oplus x_i z'_i = 0$ for all i, or if $z_i x'_i \oplus x_i z'_i = 1$ for an even number of indices. The first scenario occur for the following situations: either $x_i = z_i = 0$ or $x'_i = z'_i = 0$, meaning either g or g' has I in the i-th entry; or $x_i = x'_i$ and $z_i = z'_i$, meaning both operators have the same Pauli matrix in the i-th entry. In both cases we get that g and g' commute. The second scenario occurs if, for an even number of indices, we have $z_i x'_i \neq x_i z'_i$, which is only possible if g and g' have different Pauli matrices (which anti-commute) in the i-th entry. With an even number of operators anti-commuting we get that g and g' commute. Therefore if $r(g)\Lambda r(g')^{\mathrm{T}} = 0$ then g and g' commute. Conversely, if g and g' commute, then for all i, their i-th entries must be either an identity operator (meaning either $x_i = z_i = 0$ or $x'_i = z'_i = 0$) or the same operator in both (meaning $x_i = x'_i$ and $z_i = z'_i$), both cases leading to $z_i x'_i \oplus x_i z'_i = 0$. Alternatively they must have an even number of entries where the matrices anti-commute (meaning $z_i x'_i \neq x_i z'_i \Rightarrow z_i x'_i \oplus x_i z'_i = 1$), leading to $\bigoplus_{i=1}^{n} (z_i x'_i \oplus x_i z'_i) = 0$. Therefore if g and g' commute then $r(g)\Lambda r(g')^{\mathrm{T}} = 0$

10.34

If $-I \notin S$ then evidently $g_j \neq -I$ for all j. Furthermore, we must also have $g_j \neq \pm i\sigma$ for all j, where σ is any tensor product of Pauli matrices, because we would have $(\pm i\sigma)^2 = -I$, which would be a contradiction. There can also not be, simultaneously, elements σ and $-\sigma$, because we would have $\sigma(-\sigma) = (-\sigma)\sigma = -I$, which would also be a contradiction. Therefore, if $-I \notin S$, all generators must be tensor products of Pauli matrices with the same phase factors of either 1 or -1, meaning $g_j^2 = I$ and $g_j \neq -I$ for all j. The converse is immediate, but only true if we add that all generators must commute. A counter example would be, for a single qubit, $S = \langle X, Z \rangle$. Here clearly we have $g_j^2 = I$ and $g_j \neq -I$ for all j, but S would contain the element $ZXZX = (iY)(iY) = -I$.

10.35

If $-I \notin S$ then all generators of g_j of S are commuting tensor products of Pauli matrices with the same phase factors of either 1 or -1 (see Exercise 10.34). Since the generators satisfy $g_j^2 = I$ for all j, and any element $g \in S$ can be written as finite product of k generators, that is, $g = g_{i_1} \cdots g_{i_k}$, we get $g^2 = (g_{i_1} \cdots g_{i_k})^2 = (g_{i_1})^2 \cdots (g_{i_k})^2 = I \cdots I = I$. Thus $g^{-1} = g$ for all $g \in S$, and since any tensor product of Pauli matrices is unitary, we have that $g^{-1} = g^\dagger$, meaning $g^\dagger = g$.

10.36

$$UX_1U^\dagger = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} = X_1X_2,$$

$$UX_2U^\dagger = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = X_2,$$

$$UZ_1U^\dagger = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} = Z_1,$$

$$UZ_2U^\dagger = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = Z_1Z_2.$$

10.37

$$UY_1U^\dagger = -iUZ_1X_1U^\dagger = -iUZ_1U^\dagger UX_1U^\dagger = -iZ_1X_1X_2 = Y_1X_2.$$

10.38

We have that $UgU^\dagger = VgV^\dagger$ for all $g \in \{Z_1, Z_2, X_1, X_2\}$, which generates the G_2 Pauli group. We can rewrite this equality as $V^\dagger UgU^\dagger V = g$, which means that $U^\dagger V$ commutes with all elements of G_2. This can only happen if $U^\dagger V$ is proportional to the identity, that is,

$$U^\dagger V = \lambda I \quad \Longrightarrow \quad V = \lambda U.$$

Since both U and V are unitary, we have that $|\lambda| = 1$, meaning it is just an immaterial global phase. Thus we can always choose $\lambda = 1$ and conclude that $U = V$.

10.39

$$SXS^\dagger = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -i \end{bmatrix} = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = Y,$$
$$SZS^\dagger = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -i \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = Z.$$

10.40

Given that

$$HXH^\dagger = Z, \quad HZH^\dagger = X, \quad HYH^\dagger = -Y,$$
$$SXS^\dagger = Y, \quad SYS^\dagger = -X, \quad SZS^\dagger = Z,$$

we need $O(1)$ applications of Hadamard and phase gates to perform normalizer operations on a single qubit up to global phase. Let us define $U \in N(G_{n+1})$ as an operator over $n+1$ qubits such that $UZ_1U^\dagger = X_1 \otimes g$ and $UX_1U^\dagger = Z_1 \otimes g'$, with $g, g' \in N(G_n)$. If we take the state $|0\rangle \otimes |\psi\rangle$, where $|\psi\rangle$ is an n-qubit eigenstate of an element of G_n, we see that

$$U\left(|0\rangle \otimes |\psi\rangle\right) = \frac{1}{\sqrt{2}}\left(|0\rangle \otimes |\phi_0\rangle + |1\rangle \otimes |\phi_1\rangle\right),$$

where $|\phi_0\rangle$ and $|\phi_1\rangle$ are also n-qubit eigenstates of elements of G_n. We can define U' as a reduction of the action of U to n qubits as

$$U'|\psi\rangle \equiv \sqrt{2}\langle 0| U\left(|0\rangle \otimes |\psi\rangle\right) = |\phi_0\rangle,$$

meaning U' can be seen as a normalizer of G_n. The goal is to analyze how many Hadamard, phase, and CNOT gates are necessary to construct U from U'. As a hypothesis, let us consider that U' can be constructed with $O(n^2)$ Hadamard, phase, and CNOT gates. Then after adding one qubit, constructing U will require at most $O(n)$ CNOT gates connecting the added qubit to the others, $O(n)$ Hadamard and phase gates for the other qubits, and $O(1)$ Hadamard and phase gates for the added qubit, amounting to $O(n)+O(n)+O(1) = O(n)$ extra gates. Therefore, $O(n^2)+O(n) = O(n^2)$ gates would be necessary in total to construct U. By induction, for any number n of qubits it is possible to build a normalizer using $O(n^2)$ Hadamard, phase, and CNOT gates.

10.41

$$TZT^\dagger = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & e^{-i\pi/4} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = Z,$$
$$TXT^\dagger = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & e^{-i\pi/4} \end{bmatrix} = \begin{bmatrix} 0 & e^{-i\pi/4} \\ e^{i\pi/4} & 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 & 1-i \\ 1+i & 0 \end{bmatrix} = \frac{X+Y}{\sqrt{2}}.$$

$$UZ_1U^\dagger = \begin{bmatrix} 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&1&0 \end{bmatrix} \begin{bmatrix} 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&-1&0&0&0\\ 0&0&0&0&0&-1&0&0\\ 0&0&0&0&0&0&-1&0\\ 0&0&0&0&0&0&0&-1 \end{bmatrix} \begin{bmatrix} 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&1&0 \end{bmatrix}$$

$$= \begin{bmatrix} 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&-1&0&0&0\\ 0&0&0&0&0&-1&0&0\\ 0&0&0&0&0&0&-1&0\\ 0&0&0&0&0&0&0&-1 \end{bmatrix} = Z_1,$$

$$UX_1U^\dagger = \begin{bmatrix} 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&1&0 \end{bmatrix} \begin{bmatrix} 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&1\\ 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0 \end{bmatrix} \begin{bmatrix} 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&1&0 \end{bmatrix}$$

$$= \begin{bmatrix} 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&1&0\\ 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&1&0&0&0&0&0 \end{bmatrix} = X \otimes CX_{(2,3)}.$$

Notice that in the subspace of two of the qubits, a CNOT gate with the first qubit as control and second as target can be decomposed as

$$CX = \begin{bmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&0&0&1\\ 0&0&1&0 \end{bmatrix} = \begin{bmatrix} \frac{1}{2}&0&0&0\\ 0&\frac{1}{2}&0&0\\ 0&0&\frac{1}{2}&0\\ 0&0&0&\frac{1}{2} \end{bmatrix} + \begin{bmatrix} \frac{1}{2}&0&0&0\\ 0&\frac{1}{2}&0&0\\ 0&0&-\frac{1}{2}&0\\ 0&0&0&-\frac{1}{2} \end{bmatrix} + \begin{bmatrix} 0&\frac{1}{2}&0&0\\ \frac{1}{2}&0&0&0\\ 0&0&0&\frac{1}{2}\\ 0&0&\frac{1}{2}&0 \end{bmatrix} - \begin{bmatrix} 0&\frac{1}{2}&0&0\\ \frac{1}{2}&0&0&0\\ 0&0&0&-\frac{1}{2}\\ 0&0&-\frac{1}{2}&0 \end{bmatrix}$$

$$= \frac{I \otimes I + Z \otimes I + I \otimes X - Z \otimes X}{2},$$

thus, for qubits 2 (control) and 3 (target) we can write $CX_{(2,3)} = \frac{1}{2}(I + Z_2 + X_3 - Z_2X_3)$, and therefore

$$UX_1U^\dagger = X_1 \otimes \frac{I + Z_2 + X_3 - Z_2X_3}{2}.$$

Since the second qubit is a control qubit exactly like the first one, the results for $UZ_2U^\dagger$ and $UX_2U^\dagger$ must be the same just exchanging the indices 1 and 2, that is,

$$\begin{aligned} UZ_2U^\dagger &= Z_2, \\ UX_2U^\dagger &= X_2 \otimes \frac{I + Z_1 + X_3 - Z_1X_3}{2}. \end{aligned}$$

For the remaining relations we get

$$\begin{aligned} UX_3U^\dagger &= \begin{bmatrix} 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&1&0 \end{bmatrix} \begin{bmatrix} 0&1&0&0&0&0&0&0\\ 1&0&0&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&1&0 \end{bmatrix} \begin{bmatrix} 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&1&0 \end{bmatrix} \\ &= \begin{bmatrix} 0&1&0&0&0&0&0&0\\ 1&0&0&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&1&0 \end{bmatrix} = X_3, \\ UZ_3U^\dagger &= \begin{bmatrix} 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&1&0 \end{bmatrix} \begin{bmatrix} 1&0&0&0&0&0&0&0\\ 0&-1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&-1&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&-1&0&0\\ 0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&-1 \end{bmatrix} \begin{bmatrix} 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&1&0 \end{bmatrix} \end{aligned}$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} = CZ_{(1,2)} \otimes Z.$$

Analogously to the CNOT gate, in the subspace of two qubits we can make the decomposition

$$CZ = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} = \begin{bmatrix} \frac{1}{2} & 0 & 0 & 0 \\ 0 & \frac{1}{2} & 0 & 0 \\ 0 & 0 & \frac{1}{2} & 0 \\ 0 & 0 & 0 & \frac{1}{2} \end{bmatrix} + \begin{bmatrix} \frac{1}{2} & 0 & 0 & 0 \\ 0 & \frac{1}{2} & 0 & 0 \\ 0 & 0 & -\frac{1}{2} & 0 \\ 0 & 0 & 0 & -\frac{1}{2} \end{bmatrix} + \begin{bmatrix} \frac{1}{2} & 0 & 0 & 0 \\ 0 & -\frac{1}{2} & 0 & 0 \\ 0 & 0 & \frac{1}{2} & 0 \\ 0 & 0 & 0 & -\frac{1}{2} \end{bmatrix}$$
$$- \begin{bmatrix} \frac{1}{2} & 0 & 0 & 0 \\ 0 & -\frac{1}{2} & 0 & 0 \\ 0 & 0 & -\frac{1}{2} & 0 \\ 0 & 0 & 0 & \frac{1}{2} \end{bmatrix}$$
$$= \frac{I + Z \otimes I + I \otimes Z - Z \otimes Z}{2},$$

thus, for qubits 1 and 2 we can write $CZ_{(1,2)} = \frac{1}{2}(I + Z_1 + Z_2 - Z_1 Z_2)$, and therefore

$$UZ_3U^\dagger = Z_3 \otimes \frac{I + Z_1 + Z_2 - Z_1 Z_2}{2}.$$

10.42

Let us consider the unknown state $|\psi\rangle$ is stabilized by $S_\psi \equiv aX_1 + bY_1 + cZ_1$. So the total initial state $|\psi\rangle \otimes (|00\rangle + |11\rangle)/\sqrt{2}$ has stabilizer $\langle S_\psi, Z_2Z_3, X_2X_3\rangle$. First a $CX_{(1,2)}$ is applied, transforming the stabilizer as

$$\langle aX_1 + bY_1 + cZ_1, Z_2Z_3, X_2X_3\rangle \quad \longrightarrow \quad \langle aX_1X_2 + bY_1X_2 + cZ_1, Z_1Z_2Z_3, X_2X_3\rangle,$$

and then a Hadamard gate is applied to the first qubit, transforming the stabilizer to

$$\langle aX_1X_2 + bY_1X_2 + cZ_1, Z_1Z_2Z_3, X_2X_3\rangle \quad \longrightarrow \quad \langle aZ_1X_2 - bY_1X_2 + cX_1, X_1Z_2Z_3, X_2X_3\rangle.$$

The end of the circuit consists of the measurements of Z_1 and X_2. We see that both Z_1 and X_2 anti-commute with $X_1Z_2Z_3$ and commute with X_2X_3. **Incomplete...**

10.43

Since S is a subgroup it must satisfy the *closure* property, meaning for all $g \in S$ we have $gSg^\dagger \in S$. Thus $g \in N(S)$ for all $g \in S$, and therefore $S \subseteq N(S)$.

10.44

For all $E \in Z(S)$ and $g \in S$, we have $Eg = gE \Rightarrow EgE^\dagger = g \in S$, meaning $Z(S) \subseteq N(S)$. Since $-I \notin S$, all elements in S are commuting elements with the same phase of either 1 or -1 (see Exercise 10.34). For some $g \in S$ and all $E \in N(S)$ we have $EgE^\dagger = g' \in S$. But since g and g' commute, we have $g' = \pm g$. They can't differ by phase, so we conclude $g' = g$, meaning $Eg = gE$ and thus $N(S) \subseteq Z(S)$. Combining both statements, we get $N(S) = Z(S)$.

10.45

-

10.46

The spaces stabilized by X_1X_2 and X_2X_3 are spanned by $\{|++\rangle, |++-\rangle, |--+\rangle, |---\rangle\}$, and $\{|+++\rangle, |-++\rangle, |+--\rangle, |---\rangle\}$, respectively. Their intersection is the space of the three qubit phase flip code, and thus its stabilizer is $\langle X_1X_2, X_2X_3\rangle$.

10.47

All elements from g_1 to g_6 contain two Z operators on the same block of three qubits, so

$$\begin{aligned} & g_Z \frac{(|000\rangle \pm |111\rangle)(|000\rangle \pm |111\rangle)(|000\rangle \pm |111\rangle)}{2\sqrt{2}} \\ = & \frac{(|000\rangle \pm (-1)^2 |111\rangle)(|000\rangle \pm (-1)^2 |111\rangle)(|000\rangle \pm (-1)^2 |111\rangle)}{2\sqrt{2}} \\ = & \frac{(|000\rangle \pm |111\rangle)(|000\rangle \pm |111\rangle)(|000\rangle \pm |111\rangle)}{2\sqrt{2}}, \end{aligned}$$

where g_Z is any composition of the first 6 generators, thus they stabilize both codewords. Elements g_7 and g_8 both apply a logical X operation over two of the three blocks of qubits, so

$$\begin{aligned} g_X |0_L\rangle &= g_X |+_L\rangle |+_L\rangle |+_L\rangle = |+_L\rangle |+_L\rangle |+_L\rangle = |0_L\rangle, \\ g_X |1_L\rangle &= g_X |-_L\rangle |-_L\rangle |-_L\rangle = (-1)^2 |-_L\rangle |-_L\rangle |-_L\rangle = |1_L\rangle, \end{aligned}$$

where g_X is any combination of g_7 and g_8, and $|\pm_L\rangle \equiv (|000\rangle \pm |111\rangle)/\sqrt{2}$, thus they also stabilize both codewords. Since all elements from g_1 to g_8 commute, they generate the stabilizer for the two codewords of the Shor nine qubit code.

10.48

$$\begin{aligned} \bar{Z} |0_L\rangle &= X_1X_2X_3X_4X_5X_6X_7X_8X_9 \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}} \\ &= \frac{(|111\rangle + |000\rangle)(|111\rangle + |000\rangle)(|111\rangle + |000\rangle)}{2\sqrt{2}} = |0_L\rangle, \end{aligned}$$

$$\bar{Z}\left|1_L\right\rangle = X_1X_2X_3X_4X_5X_6X_7X_8X_9\frac{(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}}$$
$$= \frac{(|111\rangle - |000\rangle)(|111\rangle - |000\rangle)(|111\rangle - |000\rangle)}{2\sqrt{2}} = -\left|1_L\right\rangle.$$

From this we see $\bar{Z}$ acts as a logical Z on states $|0_L\rangle$ and $|1_L\rangle$.

$$\bar{X}\left|0_L\right\rangle = Z_1Z_2Z_3Z_4Z_5Z_6Z_7Z_8Z_9\frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}}$$
$$= \frac{(|000\rangle + (-1)^3|111\rangle)(|000\rangle + (-1)^3|111\rangle)(|000\rangle + (-1)^3|111\rangle)}{2\sqrt{2}} = \left|1_L\right\rangle,$$
$$\bar{X}\left|1_L\right\rangle = Z_1Z_2Z_3Z_4Z_5Z_6Z_7Z_8Z_9\frac{(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}}$$
$$= \frac{(|000\rangle - (-1)^3|111\rangle)(|000\rangle - (-1)^3|111\rangle)(|000\rangle - (-1)^3|111\rangle)}{2\sqrt{2}} = \left|0_L\right\rangle.$$

From this we see that $\bar{X}$ acts as a logical X on states $|0_L\rangle$ and $|1_L\rangle$. Since all generators have an even number of entries with Pauli matrices, both $\bar{Z}$ and $\bar{X}$ commute with them, and since $\bar{Z}$ and $\bar{X}$ have an odd number (nine) of non-commuting entries, they anti-commute.

10.49

The set of all single qubit errors over five qubits is $\{X_i, Y_i, Z_i\}$, with i ranging from 1 to 5. By direct verification we see that

$$\begin{array}{lll} X_1g_4 = -g_4X_1, & Y_1g_1 = -g_1Y_1, & Z_1g_1 = -g_1Z_1, \\ X_2g_1 = -g_1X_2, & Y_2g_1 = -g_1Y_2, & Z_2g_2 = -g_2Z_2, \\ X_3g_1 = -g_1X_3, & Y_3g_1 = -g_1Y_3, & Z_3g_3 = -g_3Z_3, \\ X_4g_2 = -g_2X_4, & Y_4g_1 = -g_1Y_4, & Z_4g_1 = -g_1Z_4, \\ X_5g_3 = -g_3X_5, & Y_5g_2 = -g_2X_5, & Z_5g_2 = -g_2Z_5, \end{array}$$

that is, all single qubit errors anti-commute with at least one of the generators. Therefore, from Theorem 10.8, any arbitrary single qubit error may be corrected.

10.50

The quantum Hamming bound is given by

$$\sum_{j=0}^{t}\binom{n}{j}3^j2^k \leq 2^n.$$

In this case, we have $n = 5$, $k = 1$, and are able to correct errors on $t = 1$ qubits. The left-hand side of the quantum Hamming bound then yields

$$\binom{5}{0}3^02^1 + \binom{5}{1}3^12^1 = 32 = 2^n,$$

meaning the Hamming bound is saturated.

10.51

Let C_1 and C_2 be $[n, k_1]$ and $[n, k_2]$ codes such that C_1 and $C_2^{\perp}$ both corrects t errors, and $C_2 \subset C_1$. The check matrix satisfy the commutativity condition because $H(C_2^{\perp})H(C_1)^{\mathrm{T}} = G(C_2)^{\mathrm{T}}H(C_1)^{\mathrm{T}} = [H(C_1)G(C_2)]^{\mathrm{T}} = 0$, where we used the fact that $C_2 \subset C_1$. Given that the rows of the parity check matrices $H(C_2^{\perp})$ and $H(C_1)$ give, respectively, the entries with X and Z for the corresponding operators, the resulting code has $(n-k_1)+(n-k_2) = 2n-(k_1+k_2)$ generators. By hypothesis, and using Theorem 10.8, $C_2^{\perp}$ can correct phase flip errors and C_1 can correct bit flip errors, both on up to t qubits, so the resulting code with $2n-(k_1+k_2)$ generators can correct arbitrary errors on up to t qubits. This corresponds to the $CSS(C_1, C_2)$ code.

10.52

Using the two codewords shown in Equations (10.78) and (10.79) we get

$$\begin{aligned}
\bar{Z}\,|0_L\rangle &= \frac{Z_1Z_2Z_3Z_4Z_5Z_6Z_7}{\sqrt{8}}\Big[\,|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle \\
&\qquad + |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle\,\Big] \\
&= \frac{1}{\sqrt{8}}\Big[\,|0000000\rangle + (-1)^4\,|1010101\rangle + (-1)^4\,|0110011\rangle + (-1)^4\,|1100110\rangle \\
&\qquad + (-1)^4\,|0001111\rangle + (-1)^4\,|1011010\rangle + (-1)^4\,|0111100\rangle + (-1)^4\,|1101001\rangle\,\Big] = |0_L\rangle\,, \\
\bar{Z}\,|1_L\rangle &= \frac{Z_1Z_2Z_3Z_4Z_5Z_6Z_7}{\sqrt{8}}\Big[\,|1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle \\
&\qquad + |1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle\,\Big] \\
&= \frac{1}{\sqrt{8}}\Big[(-1)^7\,|1111111\rangle + (-1)^3\,|0101010\rangle + (-1)^3\,|1001100\rangle + (-1)^3\,|0011001\rangle \\
&\qquad + (-1)^3\,|1110000\rangle + (-1)^3\,|0100101\rangle + (-1)^3\,|1000011\rangle + (-1)^3\,|0010110\rangle\,\Big] = -\,|1_L\rangle\,, \\
\bar{X}\,|0_L\rangle &= \frac{X_1X_2X_3X_4X_5X_6X_7}{\sqrt{8}}\Big[\,|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle \\
&\qquad + |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle\,\Big] \\
&= \frac{1}{\sqrt{8}}\Big[\,|1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle \\
&\qquad + |1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle\,\Big] = |1_L\rangle\,, \\
\bar{X}\,|1_L\rangle &= \frac{X_1X_2X_3X_4X_5X_6X_7}{\sqrt{8}}\Big[\,|1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle \\
&\qquad + |1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle\,\Big] \\
&= \frac{1}{\sqrt{8}}\Big[\,|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle \\
&\qquad + |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle\,\Big] = |0_L\rangle\,.
\end{aligned}$$

10.53

The fact that a $k \times k$ identity matrix appears in the check matrix $[000|A_2^{\mathrm{T}} 0 I]$ for the k encoded Z operators means that all operators have at least one entry with Z while all the others have identity in this same entry. Thus, all encoded Z operators are independent of each other.

10.54

-

10.55

We identify $E = (1, 1, 0)^{\mathrm{T}}$ and $C = (0, 0, 0)^{\mathrm{T}}$. The encoded X will have check matrix given by $[0E^{\mathrm{T}} I|C^{\mathrm{T}} 00]$, where the number of entries in each block are respectively $\{r = 3, n-k-r = 3, k = 1\}$. Therefore the check matrix for the encoded X will be $[0001101|0000000]$, corresponding to $X_4 X_5 X_7$. Given that qubits 1 and 4 were swapped, then 3 and 4, then 6 and 7, this corresponds to $X_3 X_5 X_6$ in the original code. If we multiply this by $g_1 g_2 g_3 = X_1 X_2 X_4 X_7$ we obtain $\bar{X}$ of Equation (10.107).

10.56

Since all encoded X and Z operators commute with all elements of the stabilizer, for any codeword $|\psi\rangle$ and g in the stabilizer we have

$$gX|\psi\rangle = Xg|\psi\rangle = X|\psi\rangle,$$
$$gZ|\psi\rangle = Zg|\psi\rangle = Z|\psi\rangle,$$

where we used the fact that $g|\psi\rangle = |\psi\rangle$.

10.57

For the five qubit code, using the generators in Figure 10.12 we get the check matrix

$$\left[\begin{array}{ccccc|ccccc} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{array}\right].$$

In this case we have $n = 5$, $k = 1$, and all rows in the first block are independent, such that $r = 4$. Therefore, for the check matrix to be in standard form, it must be shaped $[I^{(4\times4)} A^{(4\times1)}|B^{(4\times4)} C^{(4\times1)}]$. We begin by relabeling qubits 1 and 4, and then 4 and 5, which means swapping the corresponding columns in each block, yielding

$$\left[\begin{array}{ccccc|ccccc} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{array}\right].$$

Now we can sum rows 1 and 2 to row 4, and then sum row 4 to row 2, yielding

$$\left[\begin{array}{ccccc|ccccc} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \end{array}\right],$$

and this is a check matrix in standard form.

For the nine qubit code, using the generators in Figure 10.11, and relabeling them such that g_7 and g_8 become g_2 and g_1 respectively, and the generators from g_1 to g_6 become g_3 to g_8 respectively, we get the check matrix

$$\left[\begin{array}{ccccccccc|ccccccccc} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{array}\right].$$

In this case we have $n = 9$, $k = 1$, and the first block has only two independent rows, such that $r = 2$. Therefore, the matrix in standard form will be shaped

$$\left[\begin{array}{ccc|ccc} I^{(2\times 2)} & A_1^{(2\times 6)} & A_2^{(2\times 1)} & B^{(2\times 2)} & 0^{(2\times 6)} & C^{(2\times 1)} \\ 0^{(6\times 2)} & 0^{(6\times 6)} & 0^{(6\times 1)} & D^{(6\times 2)} & I^{(6\times 6)} & E^{(6\times 1)} \end{array}\right].$$

We begin by swapping columns 1 and 3, then 1 and 4, then 1 and 5, and finally 1 and 9, yielding

$$\left[\begin{array}{ccccccccc|ccccccccc} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{array}\right].$$

Now we only need to sum row 8 to row 7, yielding

$$\left[\begin{array}{ccccccccc|ccccccccc} 1&0&0&0&1&1&1&1&1&0&0&0&0&0&0&0&0&0\\ 0&1&1&1&1&1&0&0&1&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&1&0&1&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1\\ 0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0 \end{array}\right],$$

and this is a check matrix in standard form.

10.58

For Figure 10.13:

See Exercise 4.34.

For Figure 10.14:

The action of the first circuit is the same as the one shown in Figure 10.13. The action of the second circuit on a state $|\Psi\rangle \equiv |0\rangle (a|+\rangle + b|-\rangle)$ is

$$\begin{aligned} |\Psi\rangle &\xrightarrow{I\otimes H} |0\rangle (a|0\rangle + b|1\rangle) \\ &\xrightarrow{CX_{(2,1)}} a|00\rangle + b|11\rangle \\ &\xrightarrow{I\otimes H} a|0\rangle|+\rangle + b|1\rangle|-\rangle . \end{aligned}$$

This is the same state before measurement that we obtain using the first circuit, so they are equivalent.

For Firgure 10.15:

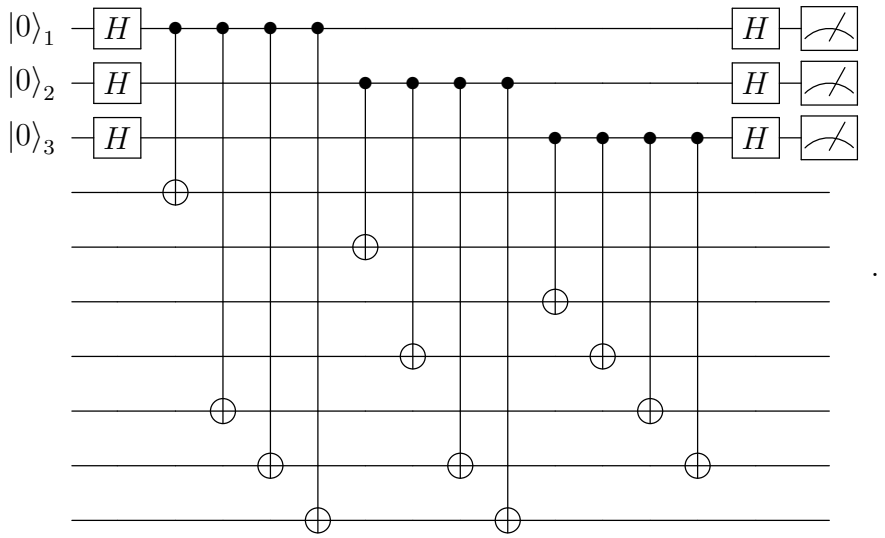
The action os the first circuit is the same as the one shown in Figure 10.13. The action of the second circuit on a state $|\Phi\rangle \equiv |0\rangle (c|0\rangle + d|1\rangle)$ is

$$|\Psi\rangle \xrightarrow{CX_{(2,1)}} a|0\rangle|0\rangle + b|1\rangle|1\rangle .$$

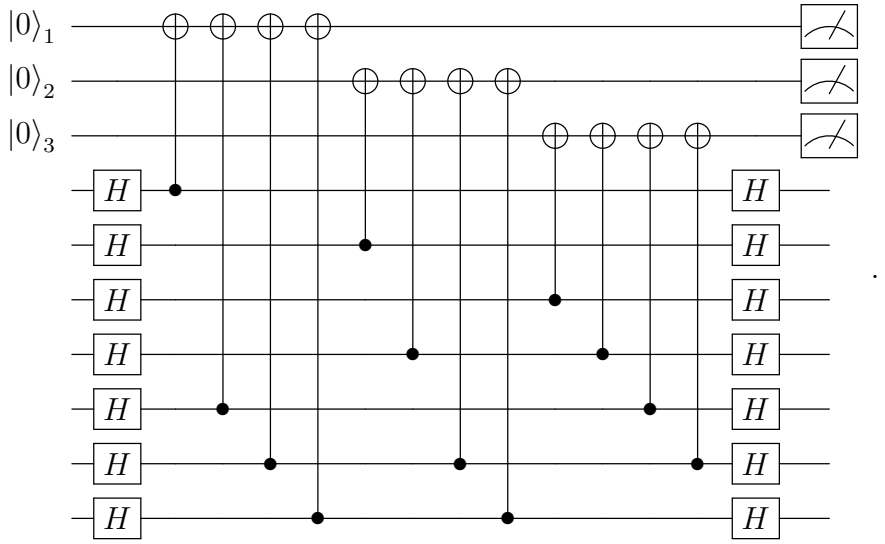
This is the same state before measurement that we obtain using the first circuit, so they are equivalent.

10.59

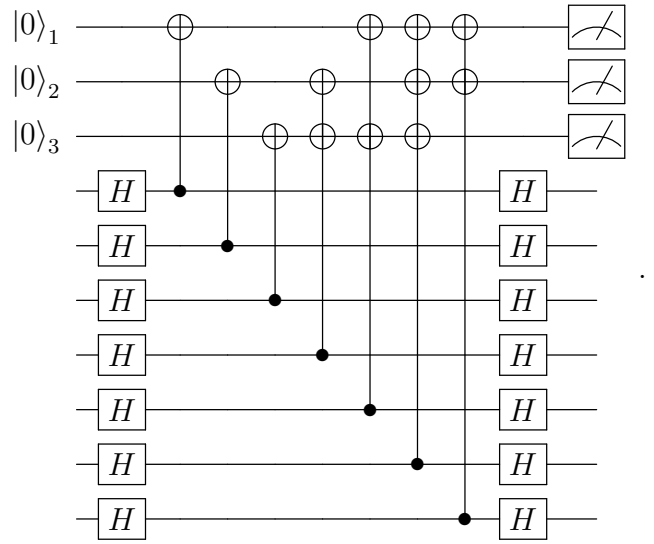
Let us first take the operations involving only the first three ancillas. Writing the CNOT gates explicitly yields



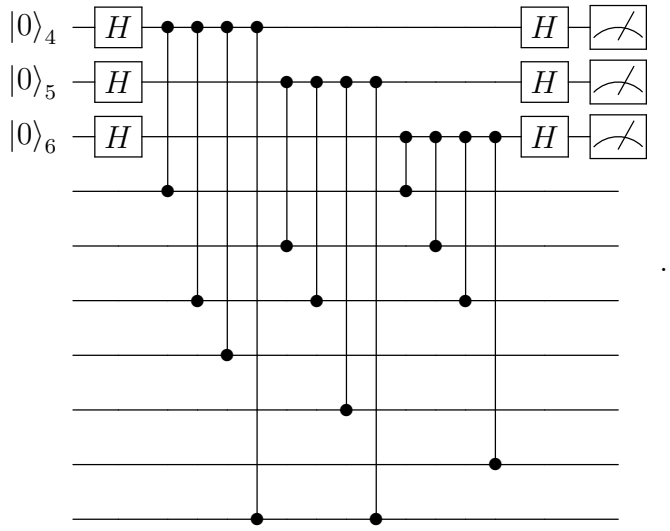
Now, using the identity in Figure 10.14 for each CNOT operation we get



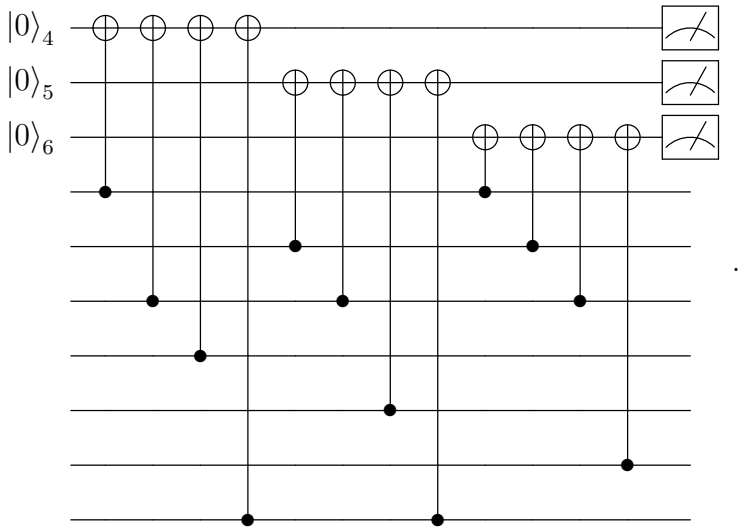
All these CNOT operations commute. Thus, rearranging the order and combining operations that have the same control qubit we obtain



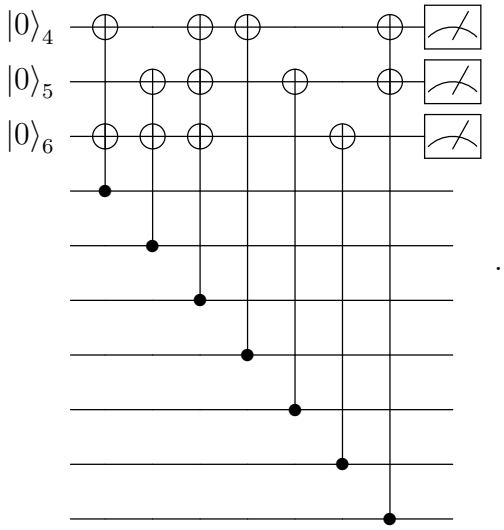
Let us now look at the operations involving the last three ancillas. Writing the Controlled-Z operations explicitly yields



Now, using the identity in Figure 10.15 for each Controlled-Z operation we get



Analogously to the other circuit, we can rearrange the operations and combine those that have the same control qubit, yielding

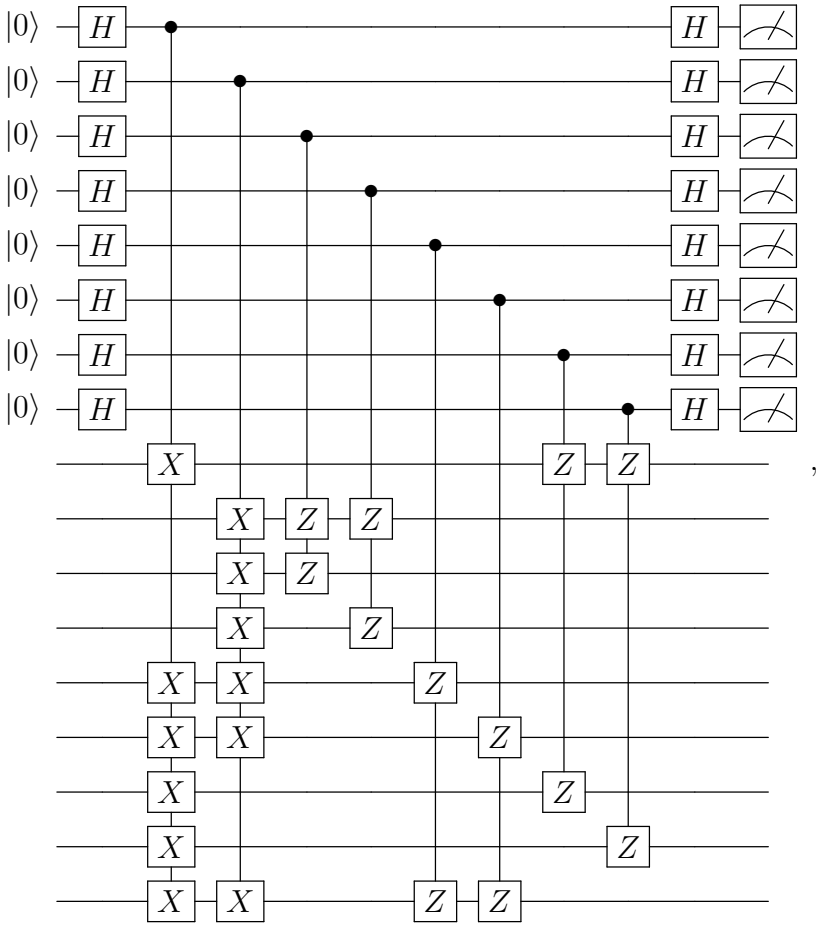


.

Combining both results into a single circuit, we obtain the circuit of Figure 10.17.

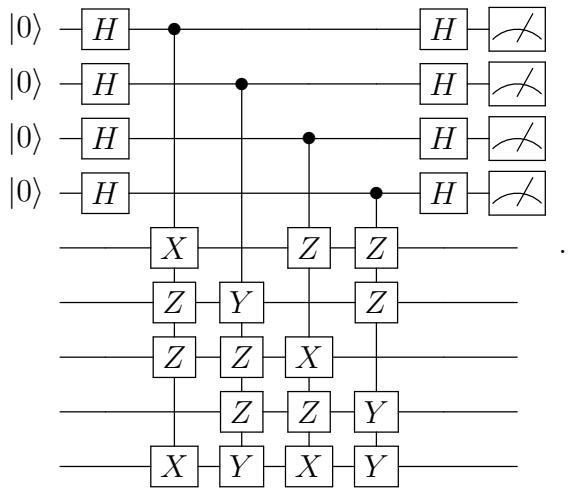
10.60

We can directly use the check matrices in standard form obtained in Exercise 10.57. For the nine qubit code, we get



,

and for the five qubit code we get



10.61

It is more insightful to use the circuit of Figure 10.17, equivalent to the one shown in Figure 10.16 (see Exercise 10.59). Notice that all qubits serve as control qubits for exactly two controlled operations: one in the middle of Hadamard gates and the other not. The system in logic state $|\psi\rangle$ is encoded, so no errors occurring means all control operations have no effect, so the result of the array of error syndromes would be $(+1, +1, +1, +1, +1, +1)$. Now, from the relations $HXH = Z$, $HZH = X$, and $HYH = -Y$, we see that if a bit flip error occurs in one qubit, then the initial state for the circuit will be some $X_i |\psi\rangle$ instead of $|\psi\rangle$, then after the first Hadamard gate, the state to be used as control will be $HX_i |\psi\rangle = Z_i H |\psi\rangle$. The Z_i operation will have no effect over the controlled operation, so the target ancilla qubits will not be altered. Then after going through the second Hadamard gate, the control state will be $HZ_iH |\psi\rangle = X_i |\psi\rangle$, meaning the second control operation will flip the target ancilla qubits, and the error syndrome for this error will consist of -1 in the qubits that are the target of the second operation controlled by the i-th system qubit. Analogously, if a phase flip error occurs in one qubit, the initial state will be $Z_i |\psi\rangle$, and the state will be $X_iH |\psi\rangle$ during the first controlled operation, meaning the target ancilla qubits will be flipped. After the second Hadamard, the state will be $Z_i |\psi\rangle$, which does nothing to the target ancilla qubits, so now the error syndrome will consist of -1 in the qubits that are the target of the first operation controlled by the i-th system qubit. Naturally, if both errors occur, the initial state will be proportional to $Y_i |\psi\rangle$, which will affect both controlled operations, so the syndrome would consist of -1 in all qubits targeted by the controlled operations that have the i-th qubit as control.

As an example, let us analyze the syndrome for the case when the first qubit is affected by errors. If it is a bit flip error, ancilla qubits 4 and 6 are flipped, so the syndrome is $(+1, +1, +1, -1, +1, -1)$, and the correction operation is X_1. If it is a phase flip error, ancilla qubit 1 is flipped, so the syndrome is $(-1, +1, +1, +1, +1, +1)$, and the correction operation is Z_1, and if both errors occur, the syndrome is just both cases combined: $(-1, +1, +1, -1, +1, -1)$, and the correction is X_1Z_1, up

to global phase. Applying the same logic to the other qubits, we can construct the table

error syndrome	correction operator
$(+1,+1,+1,+1,+1,+1)$	not needed
$(+1,+1,+1,-1,+1,-1)$	X_1
$(-1,+1,+1,+1,+1,+1)$	Z_1
$(-1,+1,+1,-1,+1,-1)$	X_1Z_1
$(+1,+1,+1,+1,-1,-1)$	X_2
$(+1,-1,+1,+1,+1,+1)$	Z_2
$(+1,-1,+1,+1,-1,-1)$	X_2Z_2
$(+1,+1,+1,-1,-1,-1)$	X_3
$(+1,+1,-1,+1,+1,+1)$	Z_3
$(+1,+1,-1,-1,-1,-1)$	X_3Z_3
$(+1,+1,+1,-1,+1,+1)$	X_4
$(+1,-1,-1,+1,+1,+1)$	Z_4
$(+1,-1,-1,-1,+1,+1)$	X_4Z_4
$(+1,+1,+1,+1,-1,+1)$	X_5
$(-1,+1,-1,+1,+1,+1)$	Z_4
$(-1,+1,-1,+1,-1,+1)$	X_5Z_5
$(+1,+1,+1,+1,+1,-1)$	X_6
$(-1,-1,-1,+1,+1,+1)$	Z_6
$(-1,-1,-1,+1,+1,-1)$	X_6Z_6
$(+1,+1,+1,-1,-1,+1)$	X_7
$(-1,-1,+1,+1,+1,+1)$	Z_7
$(-1,-1,+1,-1,-1,+1)$	X_7Z_7

10.62

Let the $[n_1, 1]$ stabilizer code have generators $\{g_1, \cdots, g_{n_1-1}\}$, and the $[n_2, 1]$ stabilizer code have generators $\{h_1, \cdots, h_{n_2-1}\}$. After the concatenation, the fully encoded states must be stabilized by all generators $\{g_1 \otimes h_1, \cdots, g_1 \otimes h_{n_2-1}, g_2 \otimes h_1, \cdots, g_2 \otimes h_{n_2-1}, \cdots, g_{n_1-1} \otimes h_1, \cdots, g_{n_1-1} \otimes h_{n_2-1}\}$ in addition to the original ones, which would then be $\{g_1 \otimes I, \cdots, g_{n_1-1} \otimes I\}$ and $\{I \otimes h_1, \cdots, I \otimes h_{n_2-1}\}$. This gives us a total of $(n_1-1)+(n_2-1)+(n_1-1)(n_2-1) = n_1n_2-1$ generators, which corresponds to an $[n_1n_2, 1]$ stabilizer code.

10.63

Given that $\bar{Z}$ and $\bar{X}$ act as logical Z and X operations respectively, and knowing the identities $\bar{H}\bar{Z}\bar{H}^\dagger = \bar{X}$, and $\bar{H}\bar{X}\bar{H}^\dagger = \bar{Z}$, we conclude that U acts as a logical Hadamard gate up to a global phase, that is, $U = e^{i\theta}\bar{H}$ for some θ, therefore its action on the logical basis up to global phase is

$$U|0_L\rangle = \frac{|0_L\rangle + |1_L\rangle}{\sqrt{2}}, \quad \text{and} \quad U|1_L\rangle = \frac{|0_L\rangle - |1_L\rangle}{\sqrt{2}}.$$

10.64

Let qubit 1 be the control and qubit 2 be the target. Using the stabilizer formalism we know that $CX_{(1,2)}Z_2CX_{(1,2)} = Z_1Z_2$ (see Exercise 10.36). Thus if a Z_2 error occurs before the application of the CNOT, the actual operator applied is $Z_2CX_{(1,2)} = CX_{(1,2)}Z_1Z_2$. Therefore, it is equivalent to the CNOT being applied correctly, followed by an error on both qubits, so a Z error on the target qubit propagates to the control qubit when a CNOT is applied.

Using circuits identities, we have that $CX_{(1,2)}|\pm\rangle|+\rangle = |\pm\rangle|+\rangle$ and $CX_{(1,2)}|\pm\rangle|-\rangle = |\mp\rangle|-\rangle$ (see Exercise 4.20). That is, while X acts as a bit flip on the Z basis, Z acts as a bit flip on the X basis with the roles of control and target exchanged. As it can be seen from these results, if the target is in the $|+\rangle$ state, nothing happens, but if it is in the $|-\rangle$ state, then the control is flipped.

Therefore, a Z error occurring on the target qubit propagates to the control qubit when a CNOT gate is applied.

10.65

Let $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$. For the first circuit we get

$$
\begin{aligned}
|0\rangle\,|\psi\rangle &\xrightarrow{CX_{(2,1)}} a\,|00\rangle + b\,|11\rangle \\
&\xrightarrow{I\otimes H} \left(\frac{a\,|0\rangle + b\,|1\rangle}{\sqrt{2}}\right)|0\rangle + \left(\frac{a\,|0\rangle - b\,|1\rangle}{\sqrt{2}}\right)|1\rangle \\
&\xrightarrow{\text{measurement qubit 2}} \begin{cases} (a\,|0\rangle + b\,|1\rangle)\,|0\rangle & \text{if outcome is } +1; \\ (a\,|0\rangle - b\,|1\rangle)\,|1\rangle & \text{if outcome is } -1; \end{cases} \\
&\xrightarrow{Z\otimes I\ [\text{if } -1]} |\psi\rangle\,|0\rangle \text{ or } |\psi\rangle\,|1\rangle\,.
\end{aligned}
$$

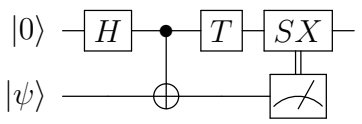
For the second circuit we get

$$
\begin{aligned}
|0\rangle\,|\psi\rangle &\xrightarrow{H\otimes I} \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)(a\,|0\rangle + b\,|1\rangle) \\
&\xrightarrow{CX_{(1,2)}} \left(\frac{a\,|0\rangle + b\,|1\rangle}{\sqrt{2}}\right)|0\rangle + \left(\frac{a\,|1\rangle + b\,|0\rangle}{\sqrt{2}}\right)|1\rangle \\
&\xrightarrow{\text{measurement qubit 2}} \begin{cases} (a\,|0\rangle + b\,|1\rangle)\,|0\rangle & \text{if outcome is } +1; \\ (a\,|1\rangle + b\,|0\rangle)\,|1\rangle & \text{if outcome is } -1; \end{cases} \\
&\xrightarrow{X\otimes I\ [\text{if } -1]} |\psi\rangle\,|0\rangle \text{ or } |\psi\rangle\,|1\rangle\,.
\end{aligned}
$$

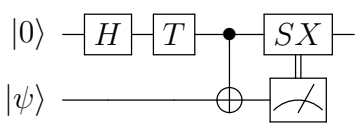
10.66

**From errata:* $TX = exp(-i\pi/4)SX$ should be $TXT^\dagger = exp(-i\pi/4)SX$.

If the measurement outcome is $+1$, then X is not applied to the first qubit, and thus we can obviously commute the operation controlled by the classical qubit with T. If the outcome is -1, we can use the first relation to write $TX = \exp(-i\pi/4)SXT$. Therefore, for all cases we conclude that the circuit is equivalent to



and using the second relation we get



which is the circuit of Figure 10.25.

10.67

Considering the initial state as a (normalized) superposition of all four possibilities for the control qubits 1 and 2 with the target qubit 3, given by $|\Psi\rangle = (a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle)\,|\psi\rangle$, for the first relation we obtain

$$\begin{aligned}\text{left-hand side:}\quad |\Psi\rangle &\xrightarrow{X\otimes I\otimes I} (a\,|10\rangle + b\,|11\rangle + c\,|00\rangle + d\,|01\rangle)\,|\psi\rangle \\ &\xrightarrow{CCX_{(1,2,3)}} (a\,|10\rangle + c\,|00\rangle + d\,|01\rangle)\,|\psi\rangle + b\,|11\rangle\,X\,|\psi\rangle\,;\end{aligned}$$

$$\begin{aligned}\text{right-hand side:}\quad |\Psi\rangle &\xrightarrow{CCX_{(1,2,3)}} (a\,|00\rangle + b\,|01\rangle + c\,|10\rangle)\,|\psi\rangle + d\,|11\rangle\,X\,|\psi\rangle \\ &\xrightarrow{X_1\otimes CX_{(2,3)}} (a\,|10\rangle + c\,|00\rangle)\,|\psi\rangle + b\,|11\rangle\,X\,|\psi\rangle + d\,|01\rangle\,X^2\,|\psi\rangle \\ &= (a\,|10\rangle + c\,|00\rangle + d\,|01\rangle)\,|\psi\rangle + b\,|11\rangle\,X\,|\psi\rangle\,.\end{aligned}$$

For the second relation we get

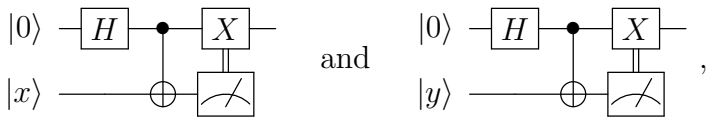
$$\begin{aligned}\text{left-hand side:}\quad |\Psi\rangle &\xrightarrow{I\otimes I\otimes Z} (a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle)Z\,|\psi\rangle \\ &\xrightarrow{CCX_{(1,2,3)}} (a\,|00\rangle + b\,|01\rangle + c\,|10\rangle)Z\,|\psi\rangle + d\,|11\rangle\,XZ\,|\psi\rangle\end{aligned}$$

$$\begin{aligned}\text{right-hand side:}\quad |\Psi\rangle &\xrightarrow{CCX_{(1,2,3)}} (a\,|00\rangle + b\,|01\rangle + c\,|10\rangle)\,|\psi\rangle + d\,|11\rangle\,X\,|\psi\rangle \\ &\xrightarrow{CZ_{(1,2)}\otimes Z_3} (a\,|0\rangle\,|0\rangle + b\,|0\rangle\,|1\rangle + c\,|1\rangle\,Z\,|0\rangle)Z\,|\psi\rangle + d\,|1\rangle\,Z\,|1\rangle\,ZX\,|\psi\rangle \\ &= (a\,|00\rangle + b\,|01\rangle + c\,|10\rangle)Z\,|\psi\rangle - d\,|11\rangle\,ZX\,|\psi\rangle \\ &= (a\,|00\rangle + b\,|01\rangle + c\,|10\rangle)Z\,|\psi\rangle + d\,|11\rangle\,XZ\,|\psi\rangle\,.\end{aligned}$$

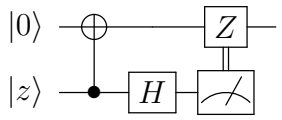
Therefore both circuit identities hold.

10.68

(1) The parts of the circuit involving the first two pairs of ancilla-system qubits $|0\rangle\,|x\rangle$ and $|0\rangle\,|y\rangle$, before the final Toffoli gate, can be written as

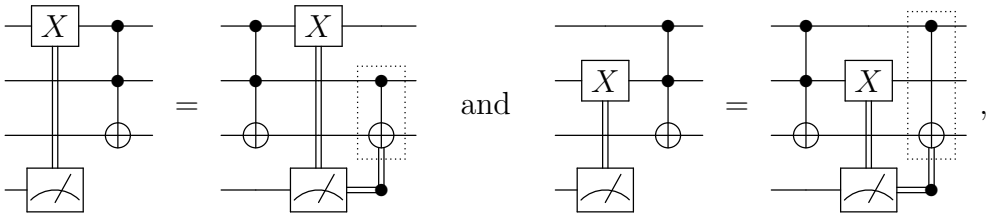


and the part involving the last pair $|0\rangle\,|z\rangle$ can be written as

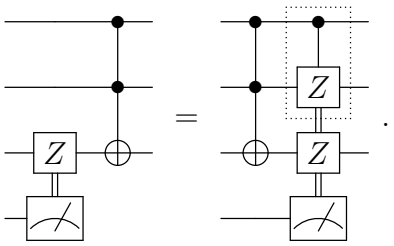


These circuits result, respectively, in the transformations $|0\rangle \to |x\rangle$, $|0\rangle \to |y\rangle$, and $|0\rangle \to |z\rangle$ (see Exercise 10.65). Therefore the circuit indeed implements a SWAP operation of the state $|x\rangle\,|y\rangle\,|z\rangle$ to the three qubits originally in the state $|000\rangle$, followed by a final Toffoli gate on these qubits.

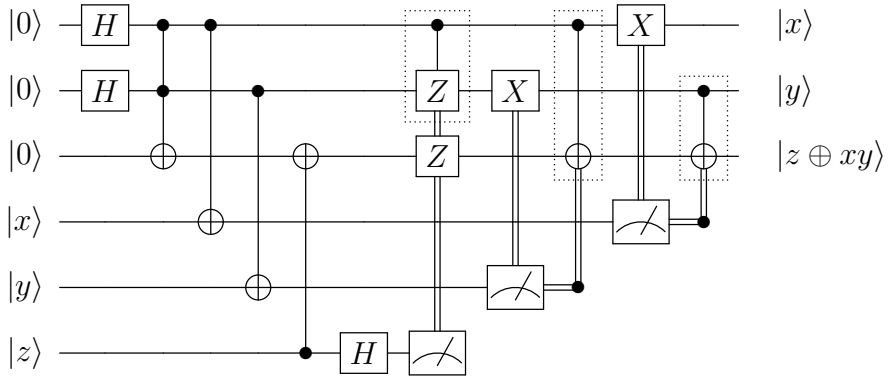
(2) Using circuit identity (a) of Exercise 10.67, we get



and using identity (b), we get



After the three gates controlled by the measurement outcomes, the Toffoli gate commutes the CNOT gate that has the third ancilla qubit as target, and naturally commutes with the other two CNOT gates, since the first two ancilla qubits are just control qubits for both the Toffoli and the CNOT gates. So we end up with the circuit



(3) Assuming the operation $CCX_{(1,2,3)}(H \otimes H \otimes I)$ in the ancilla subspace can be implemented fault-tolerantly, the remaining operations are all Hadamard and CNOT gates, which can be implemented fault-tolerantly, and controlled-Z gates, which can be constructed using only Hadamard and CNOT gates, and can therefore, by extension, also be applied fault-tolerantly. Hence, this circuit can be used to obtain a fault-tolerant Toffoli gate.

10.69

If there are any X or Y errors resulting from the preparations, they are detected during the verification step, and the process starts over. So the only errors after the preparation that survive are Z errors on one ancilla qubit. Similarly, if any X or Y errors occur in the extra qubits or ancilla qubits during the verification step, they will result in the wrong parity after measuring the extra qubits, and the process also starts over. The only errors that survive are Z errors, which propagate as Z_iZ_j $(i \neq j)$, considering the faulty extra qubit was connected with CNOT gates to the i-th and j-th ancilla qubits, or just as Z_i errors, considering the faulty qubit was one of the ancilla. So we

can identify two possible scenarios: 1. A Z_i error in the ancilla system due to a failure during the preparation or verification step; 2. A Z_iZ_j error due to a failure in the verification step. Let us analyze the ancilla output for the two possibilities.

1. Z_i error:

   If $i = 1$, the error propagates as $Z_1 \to X_1$ after the Hadamard gate application, and if $i \neq 1$, then it propagates as $Z_i \to Z_1Z_i$ after the CNOT operation, then as $Z_1Z_i \to X_1Z_i$ after the Hadamard operation. In any case, there is at most one X error in the ancilla output.

2. Z_iZ_j error ($i \neq j$):

   If $i = 1$, the error propagates as $Z_1Z_j \to Z_1^2Z_j = Z_j$ after the CNOT operation, and if both i and j are not 1 then the error propagates as $Z_iZ_j \to Z_1^2Z_iZ_j = Z_iZ_j$ after the CNOT operations. In any case, there are no X or Y errors in the ancilla output.

The single X error can also be a Y error if the Z_i error is not a full phase flip, but an arbitrary relative phase error.

10.70

A Z error in the ancilla will cause the cat state to be $|0\cdots0\rangle - |1\cdots1\rangle$ instead of $|0\cdots0\rangle + |1\cdots1\rangle$, that is, it only introduces a relative phase. All controlled operations are indifferent to relative phases, since they only depend on whether the control qubit has a $|1\rangle$ component or not, so the qubits in the code are not affected. For the ancilla system, however, if the Z error occurred in the first qubit, then the error propagates as $Z_1 \to X_1$ after the Hadamard operation, and if it occurs in any of the other ancilla qubits, say, the i-th, then it propagates as $Z_i \to X_1Z_i$ after the CNOT and Hadamard operations. In any case, the final measurement will be affected.

10.71

-

10.72

-

10.73

-

10.74

-

11 Entropy and information

Exercises: 11.1, 11.2, 11.3, 11.4, 11.5, 11.6, 11.7, 11.8, 11.9, 11.10, 11.11, 11.12, 11.13, 11.14, 11.15, 11.16, 11.17, 11.18, 11.19, 11.20, 11.21, 11.22, 11.23, 11.24, 11.25, 11.26.

11.1

Fair coin:

$$H(X) = 2\left(-\frac{1}{2}\log\frac{1}{2}\right) = 1.$$

Fair die:

$$H(X) = 6\left(-\frac{1}{6}\log\frac{1}{6}\right) = \log 6 \approx 2.585.$$

If they were unfair, the entropy would be smaller. Since there would be at least one outcome more probable than another, the average information gain after each toss would be smaller.

11.2

From property (1) we know that p and q are real values in the range $[0, 1]$, so there are always numbers a and b in the range $(-\infty, 0]$ such that $p = 2^a$ and $q = 2^b$. So we have $I(pq) = I(2^a 2^b) = I(2^{a+b})$, thus from property (3) we obtain that

$$I(2^{a+b}) = I(2^a) + I(2^b).$$

If we define the function $f(x) \equiv I(2^x)$, we get $f(a+b) = f(a) + f(b)$. Because of property (2), we know that f must be continuous and smooth, and therefore, has a Taylor series form. For $a = b = 0$ we get $f(0) = 0$, and for $b = -a$ we get $f(-a) = -f(a)$, so it is clearly an odd function, hence

$$f(x) = \sum_{j=0}^{\infty} k_j x^{2j+1}.$$

Considering $x = a + b$ we obtain

$$f(a+b) = \sum_{j=0}^{\infty} k_j (a+b)^{2j+1} = k_0(a+b) + \sum_{j=1}^{\infty} k_j \sum_{n=0}^{2j+1} \binom{2j+1}{n} a^n b^{2j+1-n},$$

but using the property that f must satisfy, we get

$$f(a) + f(b) = \sum_{j=0}^{\infty} k_j (a^{2j+1} + b^{2j+1}) = k_0(a+b) + \sum_{j=1}^{\infty} k_j (a^{2j+1} + b^{2j+1}).$$

Therefore, the only way for the property to be true is if $k_j = 0$ for all $j > 0$, meaning $f(x) = kx$ for some constant k. Now, since $f(x) = I(2^x)$, it is also true that $I(x) = f(\log x)$, and this gives us

$$I(p) = k \log p.$$

The average of this function over the values of the set $\{p_1, \cdots, p_n\}$ is precisely the Shannon entropy up to a multiplicative constant k

$$H(X) \equiv \langle I(p) \rangle = \sum_{i=1}^{n} p_i I(p_i) = k \sum_{j=1}^{n} p_i \log p_i.$$

11.3

$$\begin{aligned}
\frac{\mathrm{d}H_{\text{bin}}}{\mathrm{d}p} &= -\frac{\mathrm{d}}{\mathrm{d}p}\left[p \log(p)\right] - \frac{\mathrm{d}}{\mathrm{d}p}\left[(1-p)\log(1-p)\right] \\
&= -\log(p) - 1 + \log(1-p) + 1 \\
&= \log(1-p) - \log(p).
\end{aligned}$$

Considering $p \in [0, 1]$, $\mathrm{d}H_{\text{bin}}/\mathrm{d}p = 0$ only for $p = 1/2$. The second derivative yields

$$\frac{\mathrm{d}^2 H_{\text{bin}}}{\mathrm{d}p^2} = -\frac{1}{1-p} - \frac{1}{p} = -\frac{1}{p(1-p)} \quad \Longrightarrow \quad \frac{\mathrm{d}^2 H_{\text{bin}}}{\mathrm{d}p^2} < 0 \quad \forall\, p \in (0, 1),$$

corresponding to constant negative concavity, so $p = 1/2$ corresponds to a maximum.

11.4

The second derivative of the binary entropy is negative for all $p \in (0, 1)$ (see Exercise 11.3). It follows that for all, $p, x_1, x_2 \in [0, 1]$, it holds

$$H_{\text{bin}}(px_1 + (1-p)x_2) \geq pH_{\text{bin}}(x_1) + (1-p)H_{\text{bin}}(x_2),$$

with the innequality being strict for all values $p \in (0, 1)$. Since $H_{\text{bin}}(0) = H_{\text{bin}}(1) \equiv 0$, we get equality in the trivial cases: $x_1 = x_2$, or $p = 0$, or $p = 1$.

11.5

$$\begin{aligned}
H(p(x,y)||p(x)p(y)) &= \sum_{x,y} p(x,y) \log\left[\frac{p(x,y)}{p(x)p(y)}\right] \\
&= \sum_{x,y} p(x,y) \log[p(x,y)] - \sum_{x,y} p(x,y) \log[p(x)p(y)] \\
&= \sum_{x,y} p(x,y) \log[p(x,y)] - \sum_{x} p(x) \log[p(x)] - \sum_{y} p(y) \log[p(y)] \\
&= H(p(x)) + H(p(y)) - H(p(x,y)).
\end{aligned}$$

Considering that x are the possible outcomes of the random variable X, and y the possible outcomes of the random variable Y, we have $H(p(x)) \equiv H(X)$, $H(p(y)) \equiv H(Y)$, and $H(p(x,y)) \equiv H(X,Y)$. From the non-negativity of the relative entropy, we get $H(X,Y) \leq H(X) + H(Y)$. If we consider equality, then $H(p(x,y)||p(x)p(y)) = 0$, which means $p(x,y) = p(x)p(y)$, hence X and Y are independent random variables. The converse is immediate.

11.6

Let us use the probability distribution given by $p(x|y)p(z|y)p(y)$. The relative entropy between this distribution and $p(x,y,z)$ will be

$$H(p(x,y,z)||p(x|y)p(z|y)p(y)) = \sum_{x,y,z} p(x,y,z) \log\left[\frac{p(x,y,z)}{p(x|y)p(z|y)p(y)}\right].$$

From Bayes' rule we can write $p(x|y) = p(x,y)/p(y)$, and $p(z|y) = p(y,z)/p(y)$, hence

$$\begin{aligned} H(p(x,y,z)||p(x|y)p(z|y)p(y)) &= \sum_{x,y,z} p(x,y,z) \log\left[\frac{p(x,y,z)p(y)}{p(x,y)p(y,z)}\right] \\ &= \sum_{x,y,z} p(x,y,z) \log[p(x,y,z)] + \sum_{y} p(y) \log[p(y)] \\ &\quad - \sum_{x,y} p(x,y) \log[p(x,y)] - \sum_{y,z} p(y,z) \log[p(y,z)] \\ &= -H(X,Y,Z) - H(Y) + H(X,Y) + H(Y,Z). \end{aligned}$$

Using the fact that $H(p(x,y,z)||p(x|y)p(z|y)p(y)) \geq 0$ we get strong subadditivity

$$H(X,Y,Z) + H(Y) \leq H(X,Y) + H(Y,Z).$$

If we consider equality, then $H(p(x,y,z)||p(x|y)p(z|y)p(y)) = 0$, which means (see Exercise)

$$p(x,y,z) = p(x|y)p(z|y)p(y) = p(z)p(y|z)p(x|y),$$

hence $Z \to Y \to X$ forms a Markov chain. The converse is immediate.

11.7

Let n_Y be the number of possible outcomes for the variable Y. The uniform distribution $u(y)$ over Y is then given by $u(y) = 1/n_Y$ for all y. The relative entropy $H(p(x,y)||p(x)u(y))$ yields

$$\begin{aligned} H(p(x,y)||p(x)u(y)) &= \sum_{x,y} p(x,y) \log\left[\frac{p(x,y)}{p(x)\frac{1}{n_Y}}\right] \\ &= \sum_{x,y} p(x,y) \log[p(x,y)] - \sum_{x} p(x) \log[p(x)] - \log\tfrac{1}{n_Y} \\ &= -H(X,Y) + H(X) + \log n_Y. \end{aligned}$$

By definition, we have $H(Y|X) = H(X,Y) - H(X)$, thus

$$H(Y|X) = \log n_Y - H(p(x,y)||p(x)u(y)).$$

Notice that $\log n_Y$ corresponds to the Shannon entropy of Y when it is completely independent of X and its probability distribution is the uniform distribution $u(y)$, which is where it has its maximum value, thus $0 \leq H(p(x,y)||p(x)u(y)) \leq \log n_Y$ and therefore $H(Y|X) \geq 0$. Equality will hold when $p(x,y)$ is the farthest possible from $p(x)u(y)$, which is when Y is given by a deterministic function f of X, that is, $p(x,y) = p(x)\delta(y - f(x))$. To verify that, we can explicitly calculate

$$H(p(x)\delta(y-f(x))||p(x)u(y)) = \sum_{x,y} p(x)\delta(y-f(x)) \log\left[\frac{\delta(y-f(x))}{\frac{1}{n_Y}}\right] = \sum_x p(x)\log n_Y = \log n_Y$$
$$\implies \quad H(Y|X) = 0.$$

11.8

There are only four possible joint outcomes, which are given by: $(x=0, y=0, z=0)$, $(x=1, y=0, z=1)$, $(x=0, y=1, z=1)$, and $(x=1, y=1, z=0)$, all with equal probability of $1/4$. So we can calculate the entropies

$$H(X) = H(Y) = H(Z) = 2\left(-\frac{1}{2}\log\frac{1}{2}\right) = 1,$$
$$H(X,Y) = H(X,Z) = H(Y,Z) = H(X,Y,Z) = 4\left(-\frac{1}{4}\log\frac{1}{4}\right) = 2.$$

By definition, we obtain

$$H(X,Y:Z) = H(X,Y) + H(Z) - H(X,Y,Z) = 1,$$
$$H(X:Z) = H(X) + H(Z) - H(X,Z) = 0,$$
$$H(Y:Z) = H(Y) + H(Z) - H(Y,Z) = 0,$$

and thus conclude that $H(X,Y:Z) \nleq H(X:Z) + H(Y:Z)$.

11.9

There are only two possible joint outcomes, which are given by: $(x_1 = x_2 = y_1 = y_2 = 0)$, and $(x_1 = x_2 = y_1 = y_2 = 1)$, all with equal probability of $1/2$. So we calculate the entropies

$$H(X_i) = H(Y_i) = H(X_i,Y_i) = H(X_1,X_2) = H(Y_1,Y_2) = H(X_1,X_2,Y_1,Y_2) = 2\left(-\frac{1}{2}\log\frac{1}{2}\right) = 1,$$

for $i \in \{1,2\}$. By definition, we obtain

$$H(X_1:Y_1) = H(X_1) + H(Y_1) - H(X_1,Y_1) = 1,$$
$$H(X_2:Y_2) = H(X_2) + H(Y_2) - H(X_2,Y_2) = 1,$$

$$H(X_1, X_2 : Y_1, Y_2) = H(X_1, X_2) + H(Y_1, Y_2) - H(X_1, X_2, Y_1, Y_2) = 1,$$

and thus conclude that $H(X_1 : Y_1) + H(X_2 : Y_2) \not\leq H(X_1, X_2 : Y_1, Y_2)$.

11.10

If $X \to Y \to Z$ is a Markov chain, then the probability of $Y = y$ is conditioned on $X = x$, and the probability of $Z = z$ is conditioned on $Y = y$. In practice, this means that the probability of the joint result $(X, Y, Z) = (x, y, z)$ is given by $p(x)p(y|x)p(z|y)$. But from Bayes' rule (see Exercise)

$$p(x)p(y|x)p(z|y) = p(x|y)p(y)p(z|y) = p(x|y)p(y|z)p(z),$$

which is the probability of $(X, Y, Z) = (x, y, z)$ when $Z \to Y \to X$ is a Markov chain.

11.11

$$\rho = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}: \quad S(\rho) = -1 \times \log 1 - 0 \times \log 0 = 0.$$

$$\rho = \frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}: \quad \text{this is } \rho = |+\rangle\langle+| \text{ in the } X \text{ basis, so}$$

$$S(\rho) = -1 \times \log 1 - 0 \times \log 0 = 0.$$

$$\rho = \frac{1}{3}\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}: \quad \det(\rho - \lambda I) = \lambda^2 - \lambda + \frac{1}{9} = 0 \implies \text{eigenvalues} = \left\{\frac{3-\sqrt{5}}{6}, \frac{3+\sqrt{5}}{6}\right\}, \text{ so}$$

$$S(\rho) = -\left(\frac{3-\sqrt{5}}{6}\right)\log\left(\frac{3-\sqrt{5}}{6}\right) - \left(\frac{3+\sqrt{5}}{6}\right)\log\left(\frac{3+\sqrt{5}}{6}\right) \approx 0.55.$$

11.12

$$\rho = p\,|0\rangle\langle 0| + (1-p)\,|+\rangle\langle+| = p\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \frac{1-p}{2}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$$

$$= \frac{1}{2}\begin{bmatrix} 1+p & 1-p \\ 1-p & 1-p \end{bmatrix}.$$

$$\det(\rho - \lambda I) = \lambda^2 - \lambda + \frac{p(1-p)}{2} = 0$$

$$\implies \text{eigenvalues} = \left\{\frac{1-\sqrt{1-2p(1-p)}}{2}, \frac{1+\sqrt{1-2p(1-p)}}{2}\right\}.$$

If we define $q \equiv \frac{1-\sqrt{1-2p(1-p)}}{2}$, these eigenvalues can be rewritten as $\{q, 1-q\}$, so the von Neumann entropy will be

$$S(\rho) = -q\log(q) - (1-q)\log(1-q).$$

The Shannon entropy $H(p, 1-p)$ will be

$$H(p, 1-p) = -p\log(p) - (1-p)\log(1-p).$$

11.13

Let $\{|i\rangle\}$ be a basis for which ρ is diagonal, so we can write $\rho = \sum_i p_i |i\rangle\langle i|$. Using the joint entropy theorem we have

$$\begin{aligned} S(\rho\otimes\sigma) \equiv S\left(\sum_i p_i |i\rangle\langle i| \otimes \sigma\right) &= H(p_i) + \sum_i p_i S(\sigma) \\ &= H(p_i) + S(\sigma). \end{aligned}$$

Using the definition of entropy, we have

$$\begin{aligned} S(\rho) &= -\operatorname{tr}(\rho\log\rho) \\ &= -\operatorname{tr}\left(\sum_{i,j} p_i |i\rangle\langle i| \log p_j |j\rangle\langle j|\right) \\ &= -\operatorname{tr}\left(\sum_i p_i \log p_i |i\rangle\langle i|\right) \\ &= -\sum_i p_i \log p_i \equiv H(p_i). \end{aligned}$$

Substituting this result in the expression for $S(\rho\otimes\sigma)$, we obtain $S(\rho\otimes\sigma) = S(\rho) + S(\sigma)$.

11.14

Given that $|AB\rangle$ is pure, it is immediate that $S(A,B) = 0$. If $|AB\rangle$ is entangled then it can not be written as a product state $|\psi_A\rangle \otimes |\psi_B\rangle$, meaning it has a Schmidt decomposition

$$|AB\rangle = \sum_i \lambda_i |i_A\rangle \otimes |i_B\rangle ,$$

where $\{|i_A\rangle\}$ and $\{|i_B\rangle\}$ are basis for A and B respectively, and $\lambda_i \neq 0$ for at least two different values of i. We can calculate the density matrix ρ^A of system A as

$$\rho^A \equiv \operatorname{tr}_B(\rho^{AB}) = \operatorname{tr}_B\left(\sum_{i,j} \lambda_i\lambda_j^* |i_A\rangle\langle j_A| \otimes |i_B\rangle\langle j_B|\right) = \sum_i |\lambda_i|^2 |i_A\rangle\langle i_A| ,$$

and so, the entropy of system A will be

$$S(A) = -\sum_i |\lambda_i|^2 \log|\lambda_i|^2.$$

It holds that $\sum_i |\lambda_i|^2 = 1$, and $|\lambda_i|^2 < 1$ for all i, thus $S(A) > 0$, which results in

$$S(B|A) = -S(A) < 0.$$

The converse is immediate.

11.15

Let us consider that in the computational basis ρ has the general form

$$\rho = \sum_{i,j=0}^{1} a_{ij} \left|i\right\rangle\!\left\langle j\right|,$$

with $a_{00} + a_{11} = 1$. The generalized measurement described by the operators M_1 and M_2 is such that the post measurement state is

$$\begin{aligned}
\rho' &= M_1 \rho M_1^\dagger + M_2 \rho M_2^\dagger \\
&= |0\rangle\langle 0| \left(\sum_{i,j=0}^{1} a_{ij} \left|i\right\rangle\!\left\langle j\right| \right) |0\rangle\langle 0| + |0\rangle\langle 1| \left(\sum_{i,j=0}^{1} a_{ij} \left|i\right\rangle\!\left\langle j\right| \right) |1\rangle\langle 0| \\
&= a_{00} \left|0\right\rangle\!\left\langle 0\right| + a_{11} \left|0\right\rangle\!\left\langle 0\right| \\
&= \left|0\right\rangle\!\left\langle 0\right|.
\end{aligned}$$

We see that this measurement process always results in the pure state $\rho' = |0\rangle\langle 0|$, meaning $S(\rho') = 0$, which is the smallest value possible for the entropy. Since the entropy of the original state could have be non-negative value between 0 and $\log 2$, we have that $S(\rho') \leq S(\rho)$, which means that this generalized measurement process can decrease the entropy of the qubit.

11.16

-

11.17

-

11.18

Let us first consider that all ρ_is are the same, that is, $\rho_i \equiv \rho$ for all i. Then the left-hand side of (11.79) becomes

$$S\left(\sum_i p_i \rho \right) = S(\rho),$$

and the right-hand side becomes

$$\sum_i p_i S(\rho) = S(\rho),$$

where in both cases we used the fact that $\sum_i p_i = 1$, thus equality holds. Conversely, if we consider that equality holds then we will have

$$S\left(\sum_i p_i \rho_i\right) = \sum_i p_i S(\rho_i).$$

Using the definition of entropy we can write

$$\begin{aligned} \operatorname{tr}\left[\sum_i p_i \rho_i \log\left(\sum_j p_j \rho_j\right)\right] &= \sum_i p_i \operatorname{tr}[\rho_i \log(\rho_i)] \\ \implies \quad \sum_i p_i \operatorname{tr}\left[\rho_i \log\left(\sum_j p_j \rho_j\right)\right] &= \sum_i p_i \operatorname{tr}[\rho_i \log(\rho_i)]. \end{aligned}$$

This equality only holds if

$$\sum_j p_j \rho_j = \rho_i$$

for all i. Since the left-hand side does not depend on i, all ρ_i are the same.

11.19

-

11.20

-

11.21

For any probability distribution p_i, consider a density operator written in its diagonal basis such that the elements p_i correspond to its eigenvalues. Its von Neumann entropy is

$$S(\rho) = -\sum_i p_i \log p_i \equiv H(p_i).$$

Since $S(\rho)$ is always concave, so is the Shannon entropy $H(p_i)$.

11.22

Defining $f(p) \equiv S(p\rho + (1-p)\sigma)$, we have that S is concave if and only if $S(p\rho + (1-p)\sigma) \leq pS(\rho) + (1-p)S(\sigma)$ for $p \in [0,1]$. So S is concave if and only if $f(p) \leq pS(\rho) + (1-p)S(\sigma)$.

Differentiating both sides with respect to p we obtain

$$f'(p) \leq S(\rho) - S(\sigma),$$

and differentiating again we obtain $f''(p) \leq 0$. So if this is proven to be satisfied, we obtain that the von Neumann entropy is concave.

For the proof, it will be convenient to define the function $M(p) \equiv p\rho + (1-p)\sigma$. Notice that

$$M' = \rho - \sigma \quad \text{and} \quad M'' = 0.$$

From the definition of entropy we can explicitly write

$$f(p) = -\operatorname{tr}[M(p)\log M(p)] \quad \Longrightarrow \quad f'(p) = -\operatorname{tr}\left[\frac{\mathrm{d}}{\mathrm{d}p}\left(M(p)\log M(p)\right)\right]$$

Since ρ and σ are non-negative matrices and $p \in [0,1]$, $M(p)$ is also a non-negative matrix and thus $g(M(p)) \equiv M(p)\log M(p)$ is analytic, meaning it admits a series representation

$$g(M) = \sum_{j=0}^{\infty} a_j M^j,$$

which prompts us to write

$$\begin{aligned}
\operatorname{tr}\left[\frac{\mathrm{d}}{\mathrm{d}p} g(M)\right] &= \operatorname{tr}\left[\sum_{j=1}^{\infty} a_j \sum_{k=0}^{j-1} M^k \frac{\mathrm{d}M}{\mathrm{d}p} M^{j-1-k}\right] \\
&= \operatorname{tr}\left[\sum_{j=1}^{\infty} a_j \sum_{k=0}^{j-1} M^{j-1} \frac{\mathrm{d}M}{\mathrm{d}p}\right] \\
&= \operatorname{tr}\left[\sum_{j=1}^{\infty} a_j (j-1) M^{j-1} \frac{\mathrm{d}M}{\mathrm{d}p}\right] \\
&= \operatorname{tr}\left[\frac{\mathrm{d}g}{\mathrm{d}M}\frac{\mathrm{d}M}{\mathrm{d}p}\right],
\end{aligned}$$

where we have used the cyclic invariance of the trace. We have $\mathrm{d}g/\mathrm{d}M = I + \log M(p)$, thus

$$f'(p) = -\operatorname{tr}[(I + \log M)\, M'].$$

Since $\operatorname{tr}[M'] = \operatorname{tr}[\rho] - \operatorname{tr}[\sigma] = 0$, we can drop the first term, and for a more clean notation, we will denote $M' \equiv C$ since it is a constant matrix. With that, the first derivative of $f(p)$ becomes

$$f'(p) = -\operatorname{tr}[C\log M(p)] \quad \Longrightarrow \quad f''(p) = -\operatorname{tr}\left[C\frac{\mathrm{d}}{\mathrm{d}p}\log M(p)\right].$$

For the second derivative we can use the operator identity

$$\log M = \int_0^{\infty} \mathrm{d}t \left[\frac{1}{1+t} I - (M + tI)^{-1}\right].$$

This expression requires $M + tI$ to be invertible for all $t \geq 0$, which is not satisfied at $t = 0$ in the case where ρ and σ have null eigenvalues. We will address this problem later, for now, let us consider that ρ and σ are both invertible matrices. Differentiating with respect to p on both sides yields

$$\frac{\mathrm{d}}{\mathrm{d}p} \log M = -\int_0^\infty \mathrm{d}t \, \frac{\mathrm{d}}{\mathrm{d}p} \left(M + tI\right)^{-1}.$$

The quantity in the integrand can be obtained by implicitly differentiating the relation $(M+tI)(M+tI)^{-1} = I$, which will yield

$$\frac{\mathrm{d}}{\mathrm{d}p} \log M = \int_0^\infty \mathrm{d}t \, \left(M + tI\right)^{-1} C \left(M + tI\right)^{-1}.$$

Substituting back in the expression for $f''(p)$ yields

$$\begin{aligned} f''(p) &= -\operatorname{tr}\left[\int_0^\infty \mathrm{d}t \, C \left(M + tI\right)^{-1} C \left(M + tI\right)^{-1}\right] \\ &= -\operatorname{tr}\left[\int_0^\infty \mathrm{d}t \, \left(M + tI\right)^{-1/2} C \left(M + tI\right)^{-1/2} \left(M + tI\right)^{-1/2} C \left(M + tI\right)^{-1/2}\right], \end{aligned}$$

where again, we have used the cyclic invariance of the trace. Notice that the quantity $X(p,t) \equiv \left(M(p) + tI\right)^{-1/2} C \left(M(p) + tI\right)^{-1/2}$ has real eigenvalues since $M(p)$ always has real eigenvalues, thus this integral is always a non-negative matrix, meaning

$$f''(p) = -\operatorname{tr}\left[\int_0^\infty \mathrm{d}t \, X^2(p,t)\right] \leq 0.$$

For the case where ρ and σ are not invertible, we can define a "regularized" version of entropy as $S_\varepsilon(x) \equiv -\operatorname{tr}[(x + \varepsilon I)\log(x + \varepsilon I)]$. Notice that the only difference would be that, instead of having $M(p)$ defined as it is, we would have $M_\varepsilon(p) \equiv p\rho + (1-p)\sigma + \varepsilon I$, which satisfies $M'_\varepsilon = M' \equiv C$ and equals $M(p)$ in the limit where $\varepsilon \to 0$, thus the same result is obtained when this limit is taken at the end of the process.

11.23

Helding B fixed means to consider $B_1 = B_2 \equiv B$ in the inequality, which will become

$$f(\lambda A_1 + (1-\lambda)A_2, B) \geq \lambda f(A_1, B) + (1-\lambda) f(A_2, B),$$

meaning $f(A, B)$ is concave in A.

Take the function $f(A, B) \equiv \operatorname{tr}(AB)$. Since the trace is linear, we have

$$\begin{aligned} f(\lambda A_1 + (1-\lambda)A_2, B) &= \lambda f(A_1, B) + (1-\lambda) f(A_2, B), \\ f(A, \lambda B_1 + (1-\lambda)B_2) &= \lambda f(A, B_1) + (1-\lambda) f(A, B_2), \end{aligned}$$

so f is clearly concave in each input (in fact, it is also convex since the inequality is saturated). But

notice that

$$f(\lambda A_1 + (1-\lambda)A_2, \lambda B_1 + (1-\lambda)B_2) = \lambda^2 f(A_1, B_1) + \lambda(1-\lambda)\left[f(A_1, B_2) + f(A_2, B_1)\right] + (1-\lambda)^2 f(A_2, B_2),$$

which is not always greater than or equal to $\lambda f(A_1, B_1) + (1-\lambda) f(A_2, B_2)$. Considering $n \times n$ matrices, one example would be $A_1 = B_1 = I$ and $A_2 = B_2 = 0$. We would obtain $f(A_1, B_1) = n$ and $f(A_1, B_2) = f(A_2, B_1) = f(A_2, B_2) = 0$, thus

$$f(\lambda A_1 + (1-\lambda)A_2, \lambda B_1 + (1-\lambda)B_2) = \lambda^2 n,$$
$$\lambda f(A_1, B_1) + (1-\lambda) f(A_2, B_2) = \lambda n.$$

Since $0 < \lambda < 1$, we clearly have $f(\lambda A_1 + (1-\lambda)A_2, \lambda B_1 + (1-\lambda)B_2) < \lambda f(A_1, B_1) + (1-\lambda) f(A_2, B_2)$, and therefore, $f(A, B) = \mathrm{tr}(AB)$ is an example of a function that is concave in each of its inputs but is not jointly concave (in fact, it is also not jointly convex).

11.24

Consider a joint system BCD. Strong subadditivity implies

$$S(B, C, D) + S(B) \leq S(B, D) + S(B, C).$$

Let us introduce another system A that purifies BCD, that is, such that $ABCD$ is pure. We have that $S(B, C, D) = S(A)$ and $S(B, D) = S(A, C)$. Substituting these results in the inequality yields

$$S(A) + S(B) \leq S(A, C) + S(B, C).$$

11.25

Consider an ensemble of density operators ρ_i^{AB} of a bipartite system AB, then let

$$\rho^{AB} \equiv \sum_i p_i \rho_i^{AB},$$

with $\rho^A = \sum_i p_i \rho_i^A$ and $\rho^B = \sum_i p_i \rho_i^B$. We can then introduce an auxiliary system C such that

$$\rho^{ABC} \equiv \sum_i p_i \rho_i^{AB} \otimes |i\rangle\langle i|^C .$$

Let us now explicitly calculate the entropies $S(A, B, C)$, and $S(B, C)$. We obtain

$$\begin{aligned} S(A, B, C) &= -\,\mathrm{tr}\left[\rho^{ABC} \log \rho^{ABC}\right] \\ &= -\,\mathrm{tr}\left[\sum_i p_i \rho_i^{AB} \otimes |i\rangle\langle i|^C \sum_j \log\left(p_j \rho_j^{AB}\right) \otimes |j\rangle\langle j|^C\right] \end{aligned}$$

$$
\begin{aligned}
&= -\operatorname{tr}\left[\sum_{i,j} p_i \rho_i^{AB} \left(\log p_j + \log \rho_j^{AB}\right) \otimes |i\rangle\langle i|^C \, |j\rangle\langle j|^C\right] \\
&= -\sum_i p_i \log p_i \operatorname{tr}\left[\rho_i^{AB}\right] - \sum_i p_i \operatorname{tr}\left[\rho_i^{AB} \log \rho_i^{AB}\right] \\
&= H(p_i) + \sum_i p_i S(\rho_i^{AB}),
\end{aligned}
$$

and equivalently,

$$
S(B,C) = H(p_i) + \sum_i p_i S(\rho_i^B).
$$

Notice also that $S(A,B) \equiv S(\rho^{AB})$ and $S(B) \equiv S(\rho^B)$. Substituting these results in the strong subadditivity innequality we obtain

$$
H(p_i) + \sum_i p_i S(\rho_i^{AB}) + S(\rho^B) \leq S(\rho^{AB}) + H(p_i) + \sum_i p_i S(\rho_i^B).
$$

We can rearrange the terms and get

$$
\sum_i p_i \left[S(\rho_i^{AB}) - S(\rho_i^B)\right] \leq S(\rho^{AB}) - S(\rho^B).
$$

The differences of entropies are, by definition, the conditional entropies ($S(A|B) = S(A,B) - S(B)$), so this inequality indicates that the conditional entropy is concave.

11.26

From strong subadditivity we may write

$$
S(B) + S(C) - S(A,B) - S(A,C) \leq 0.
$$

Adding $2S(A)$ on both sides we get

$$
2S(A) + S(B) + S(C) - S(A,B) - S(A,C) \leq 2S(A).
$$

Now we must only identify the mutual information functions on the left-hand side, which are $S(A:B) \equiv S(A) + S(B) - S(A,B)$ and $S(A:C) \equiv S(A) + S(C) - S(A,C)$, so

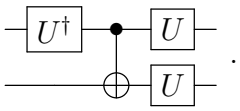
$$
S(A:B) + S(A:C) \leq 2S(A).
$$

12 Quantum information theory

Exercises: 12.1, 12.2, 12.3, 12.4, 12.5, 12.6, 12.7, 12.8, 12.9, 12.10, 12.11, 12.12, 12.13, 12.14, 12.15, 12.16, 12.17, 12.18, 12.19, 12.20, 12.21, 12.22, 12.23, 12.24, 12.25, 12.26, 12.27, 12.28, 12.29, 12.30, 12.31, 12.32, 12.33, 12.34, 12.35, 12.36, 12.37, 12.38.

12.1

If $|\psi\rangle$ and $|\varphi\rangle$ are orthogonal states, there is a unitary operator U such that $U|0\rangle = |\psi\rangle$ and $U|1\rangle = |\varphi\rangle$. The following circuit will output either $|\psi\rangle|\psi\rangle$ or $|\varphi\rangle|\varphi\rangle$ depending on the state of the data qubit.



We can verify this explicitly as

$$\begin{aligned}
|\psi\rangle|0\rangle \text{ or } |\varphi\rangle|0\rangle &\xrightarrow{U^\dagger\otimes I} |0\rangle|0\rangle \text{ or } |1\rangle|0\rangle \\
&\xrightarrow{CX} |0\rangle|0\rangle \text{ or } |1\rangle|1\rangle \\
&\xrightarrow{U\otimes U} |\psi\rangle|\psi\rangle \text{ or } |\varphi\rangle|\varphi\rangle\,.
\end{aligned}$$

12.2

-

12.3

The Holevo bound implies that $H(X:Y) \leq H(X)$. For n bits, we have $H(X) \leq n$, with equality when the bits are sampled from a uniform distribution. Therefore, using n qubits, we can transmit at most n bits of information.

12.4

Denoting $\rho_i \equiv |X_i\rangle\langle X_i|$, the state sent by Alice is

$$\begin{aligned}
\rho &= \frac{1}{4}\left(\rho_1+\rho_2+\rho_3+\rho_4\right) \\
&= \frac{1}{4}\begin{bmatrix}1 & 0\\ 0 & 0\end{bmatrix} + \frac{1}{4}\begin{bmatrix}\frac{1}{3} & \frac{\sqrt{2}}{3}\\ \frac{\sqrt{2}}{3} & \frac{2}{3}\end{bmatrix} + \frac{1}{4}\begin{bmatrix}\frac{1}{3} & \frac{\sqrt{2}}{3}e^{-2\pi i/3}\\ \frac{\sqrt{2}}{3}e^{2\pi i/3} & \frac{2}{3}\end{bmatrix} + \frac{1}{4}\begin{bmatrix}\frac{1}{3} & \frac{\sqrt{2}}{3}e^{2\pi i/3}\\ \frac{\sqrt{2}}{3}e^{-2\pi i/3} & \frac{2}{3}\end{bmatrix} \\
&= \begin{bmatrix}\frac{1}{2} & 0\\ 0 & \frac{1}{2}\end{bmatrix},
\end{aligned}$$

and so $S(\rho) = 1$. Since the four states are all pure we have $S(|X_i\rangle\langle X_i|) = 0$ for all i, and so $H(X:Y) \leq 1$. But since the four states do not have orthogonal support, the inequality is strict, and thus the mutual information is less than one bit.

The four states $|X_i\rangle$ form the vertices of a regular tetrahedron in the Bloch sphere. The POVM that maximizes the mutual information is constructed using the four states forming another regular tetrahedron whose vertices are maximally far away from the vertices of the tetrahedron formed by the $|X_i\rangle$. Such states are given by

$$|Y_1\rangle = |1\rangle\,,$$

$$|Y_2\rangle = \sqrt{\frac{1}{3}}\left[\sqrt{2}\,|0\rangle - |1\rangle\right]$$
$$|Y_3\rangle = \sqrt{\frac{1}{3}}\left[\sqrt{2}\,|0\rangle + e^{i\pi/3}\,|1\rangle\right]$$
$$|Y_4\rangle = \sqrt{\frac{1}{3}}\left[\sqrt{2}\,|0\rangle + e^{-i\pi/3}\,|1\rangle\right].$$

We then define the POVM elements as $E_i \equiv \frac{1}{2}\,|Y_i\rangle\langle Y_i|$. Now, we may calculate the mutual information as $H(X:Y) = H(X) + H(Y) - H(X,Y)$. Using "$p$" to denote probability and using the fact that $p(X_j) = 1/4$ for all j, we obtain

$$H(X) = -\sum_{j=1}^{4} p(X_j)\log(p(X_j)) = 2.$$

We have that $H(Y) = -\sum_i p(Y_i)\log(p(Y_i))$, where $p(Y_i) = \sum_j p(X_j)p(Y_i|X_j)$, with $p(Y_i|X_j) = \mathrm{tr}(E_i\rho_j)$, therefore

$$\begin{aligned} H(Y) &= -\sum_{i=1}^{4}\left(\sum_{j=1}^{4} p(X_j)p(Y_i|X_j)\right)\log\left(\sum_{j=1}^{4} p(X_j)p(Y_i|X_j)\right) \\ &= -\sum_{i=1}^{4}\frac{1}{4}\left(\sum_{j=1}^{4}\mathrm{tr}(E_i\rho_j)\right)\log\left(\frac{1}{4}\sum_{j=1}^{4}\mathrm{tr}(E_i\rho_j)\right) = 2. \end{aligned}$$

And finally, we use the fact that $p(X_j, Y_i) = p(X_j)p(Y_i|X_j)$ to obtain

$$\begin{aligned} H(X,Y) &= -\sum_{i,j=1}^{4} p(X_j,Y_i)\log(p(X_j,Y_i)) \\ &= -\sum_{i,j=1}^{4}\frac{1}{4}\,\mathrm{tr}(E_i\rho_j)\log\left(\frac{1}{4}\,\mathrm{tr}(E_i\rho_j)\right) \approx 3.585. \end{aligned}$$

With these results, we get $H(X:Y) \approx 2 + 2 - 3.585 = 0.415$.

12.5

-

12.6

-

12.7

-

12.8

-

12.9

-

12.10

-

12.11

-

12.12

-

12.13

-

12.14

-

12.15

-

12.16

-

12.17

-

12.18

-

12.19

-

12.20

-

12.21

-

12.22

-

12.23

-

12.24

-

12.25

-

12.26

-

12.27

-

12.28

-

12.29

-

12.30

-

12.31

-

12.32

-

12.33

-

12.34

-

12.35

-

12.36

-

12.37

-

12.38

-

Appendices

Exercises: A1.1, A1.2, A1.3, A1.4, A1.5, A1.6, A2.1, A2.2, A2.3, A2.4, A2.5, A2.6, A2.7, A2.8, A2.9, A2.10, A2.11, A2.12, A2.13, A2.14, A2.15, A2.16, A2.17, A2.18, A2.19, A2.20, A2.21, A2.22, A2.23, A2.24, A3.1, A3.2, A3.3, A3.4, A3.5, A3.6, A4.1, A4.2, A4.3, A4.4, A4.5, A4.6, A4.7, A4.8, A4.9, A4.10, A4.11, A4.12, A4.13, A4.14, A4.15, A4.16, A4.17, A4.18, A4.19, A5.1, A5.2, A6.1, A6.2, A6.3, A6.4, A6.5, A6.7, A6.8.

Notes on basic probability theory

A1.1

From the definition of conditional probability we have

$$p(y|x) = \frac{p(x,y)}{p(x)} \quad \text{and} \quad p(x|y) = \frac{p(x,y)}{p(y)}.$$

From the first equality the joint probability for $X = x$ and $Y = y$ is $p(x, y) = p(y|x)p(x)$. Substituting in the second equality we obtain Bayes' rule

$$p(x|y) = p(y|x)\frac{p(x)}{p(y)}.$$

A1.2

From the definition of conditional probability we have that $p(x, y) = p(y|x)p(x)$, summing both sides over all possible values for the random variable X we get

$$\sum_x p(x, y) = \sum_x p(y|x)p(x) \quad \Longrightarrow \quad p(y) = \sum_x p(y|x)p(x)$$

A1.3

Let us suppose that the statement is false, that is, for all x such that $p(x) > 0$ we have $x < \mathbf{E}(X)$. Then we conclude that

$$\sum_{x<\mathbf{E}(X)} p(x)x = \sum_x p(x)x < \sum_x p(x)\mathbf{E}(X) = \mathbf{E}(X),$$

which is a contradiction to the definition of $\mathbf{E}(X)$. Therefore the premise must be wrong and we conclude that there exists a value $x \geq \mathbf{E}(X)$ such that $p(x) > 0$.

A1.4

$$\begin{aligned}
\mathbf{E}(X + Y) &= \sum_{x,y} p(x, y)(x + y) \\
&= \sum_{x,y} p(x, y)x + \sum_{x,y} p(x, y)y \\
&= \sum_x x \sum_y p(x, y) + \sum_y y \sum_x p(x, y) \\
&= \sum_x xp(x) + \sum_y yp(y) \\
&= \mathbf{E}(X) + \mathbf{E}(Y).
\end{aligned}$$

A1.5

$$\begin{aligned}
\mathbf{E}(XY) &= \sum_{x,y} p(x, y)xy \\
&= \sum_{x,y} p(x)p(y)xy \\
&= \sum_x p(x)x \sum_y p(y)y \\
&= \mathbf{E}(X)\mathbf{E}(Y).
\end{aligned}$$

A1.6

Let us define an indicator function $\mathbf{1}(X)$ for the random variable X, defined as

$$\mathbf{1}(X) = \begin{cases} 1 & \text{if } |X - \mathbf{E}(X)| \geq \lambda\Delta(X); \\ 0 & \text{if } |X - \mathbf{E}(X)| < \lambda\Delta(X), \end{cases}$$

where $\lambda > 0$ is a real number. From the definition of expectation it follows immediately that

$$\mathbf{E}(\mathbf{1}(X)) = p(|X - \mathbf{E}(X)| \geq \lambda\Delta(X)).$$

Now let us analyze the two possible values the indicator function can assume. When $|X - \mathbf{E}(X)| \geq \lambda\Delta(X)$ we may write

$$\frac{|X - \mathbf{E}(X)|}{\lambda\Delta(X)} \geq 1 = \mathbf{1}(X) \quad \Longrightarrow \quad \mathbf{1}(X) \leq \frac{|X - \mathbf{E}(X)|^2}{\lambda^2\Delta(X)^2}$$

And when $|X - \mathbf{E}(X)| < \lambda\Delta(X)$ we have $\mathbf{1}(X) = 0$, meaning it is also true for this case that

$$\mathbf{1}(X) \leq \frac{|X - \mathbf{E}(X)|^2}{\lambda^2\Delta(X)^2}.$$

So since this relation is true for all possible cases, we may take the expectation on both sides, yielding

$$p(|X - \mathbf{E}(X)| \geq \lambda\Delta(X)) \leq \frac{1}{\lambda^2\Delta(X)^2}\mathbf{E}\big(|X - \mathbf{E}(X)|^2\big).$$

But the standard deviation is defined as $\Delta(X) \equiv \big[\mathbf{E}\big(|X - \mathbf{E}(X)|^2\big)\big]^{1/2}$. Using this fact we obtain Chebyshev's inequality

$$p(|X - \mathbf{E}(X)| \geq \lambda\Delta(X)) \leq \frac{1}{\lambda^2}.$$

Group theory

A2.1

Because of the *closure* property, if $g \in G$ then $g^n \in G$ for all integers n. If G is a finite group then it has a finite number of elements $|G|$. So if we take the set $\big\{g, g^2, \cdots, g^{|G|}, g^{|G|+1}\big\}$ at least two of the elements must be the same, that is, there exist a and b such that $g^a = g^b$. Without loss of generality we may consider that $b > a$ and thus $g^{b-a} = e$. So there always exists a positive integer $r \coloneqq b - a$ such that $g^r = e$.

A2.2

Let $g_1, g_2 \in G$. We may define two distinct sets given by $g_1H \equiv \{g_1h | h \in H\}$ and $g_2H \equiv \{g_2h | h \in H\}$. It is straightforward that $|g_1H| = |g_2H| = |H|$. Now consider $g \in G$ such that

$g \in g_1 H$ and $g \in g_2 H$ simultaneously. This means that $g = g_1 h_1$ for some $h_1 \in H$ and $g = g_2 h_2$ for some $h_2 \in H$, thus

$$g_1 h_1 = g_2 h_2 \quad \Longrightarrow \quad g_1 = g_2 h_2 h_1^{-1}.$$

Since H is also a group, we have $h_2 h_1^{-1} \in H$, meaning $g_1 \in g_2 H$ and therefore $g_1 H \subseteq g_2 H$. Analogously, we could write

$$g_1 h_1 = g_2 h_2 \quad \Longrightarrow \quad g_2 = g_1 h_1 h_2^{-1},$$

and conclude $g_2 H \subseteq g_1 H$, leading to $g_1 H = g_2 H$, which contradicts the fact that these two sets are distinct. Therefore, all $g \in G$ must belong exclusively in one set of the form $g_i H$ for $g_i \in G$, and since G is a finite group, there is a finite number n of distinct sets $g_i H$, which form a partition of G. The union of these n sets of size $|H|$ must result in G, so we have $|G| = n|H|$, meaning $|H|$ divides $|G|$, proving Lagrange's theorem.

A2.3

If the order of $g \in G$ is r, then the set $H \equiv \{e, g, \cdots, g^{r-1}\}$ is a subgroup of G because it satisfies all properties of a group, and all its elements are in G. Using Lagrange's theorem and the fact that $|H| = r$, we find that r divides $|G|$.

A2.4

If $y \in G_x$, it can be written as $y \equiv h^{-1} x h$ for some $h \in G$. The conjugacy class of y is

$$G_y \equiv \left\{k^{-1} y k | k \in G\right\} = \left\{k^{-1} h^{-1} x h k | k, h \in G\right\}.$$

By the *closure* property we have that $g \equiv hk \in G$ and $g^{-1} \equiv k^{-1} h^{-1} \in G$, therefore

$$G_y = \left\{g^{-1} x g | g \in G\right\} = G_x.$$

A2.5

If G is Abelian then for all $g \in G$ we have $xg = gx$, meaning $g^{-1} x g = g^{-1} g x = x$. Thus $G_x = \{x\}$.

A2.6

Let G be a group of order $p \geq 2$, where p is a prime number. Consider an element $a \neq e \in G$, then we must have $\langle a \rangle \leq G$, that is, $\langle a \rangle$ is a subgroup of G. By Lagrange's theorem $|\langle a \rangle|$ divides $|G|$, but since $|G| = p$ it follows that either $|\langle a \rangle| = 1$ or $|\langle a \rangle| = p$. The first would only be true if $a = e$, which is not the case, thus $|\langle a \rangle| = p$, which implies $\langle a \rangle = G$, meaning G is cyclic.

A2.7

Let G be a cyclic group. Its elements can be written as $\left\{e, a, \cdots, a^{|G|-1}\right\}$, where $e = a^{|G|}$. Any subgroup must have the identity element e and may have elements of the form a^k, k integer. From Lagrange's theorem, any subgroup will have order $|G|/n$ for some integer n that divides $|G|$, meaning its elements will be given by $\left\{e, a^{|G|/n}, \cdots, a^{(n-1)|G|/n}\right\}$. From this, we conclude that any subgroup will always be given by $\left\langle a^{|G|/n}\right\rangle$, and therefore be cyclic.

A2.8

If $g \in G$ has order r, then $e = g^{kr}$ for any integer k, and by extension $g^m = g^m g^{kr} = g^{m+kr}$. So if $g^m = g^n$, we must have $n = m + kr$, which means $m = n \pmod r$. The converse is immediate.

A2.9

Consider the coset gH for some $g \in G$. If both g_1 and g_2 are in this same coset then we have $g_1 = gh_1$ and $g_2 = gh_2$ for some $h_1, h_2 \in H$. But then $g = g_1 h_1^{-1} = g_2 h_2^{-1}$, meaning $g_2 = g_1 h_1^{-1} h_2$. since H is a group $h \equiv h_1^{-1} h_2 \in H$, thus we can always write $g_2 = g_1 h$. Conversely, if $g_2 = g_1 h$ then evidently $g_2 \in g_1 H$. But since $e \in H$, we have $g_1 \equiv g_1 e \in g_1 H$, thus g_1 and g_2 are in the same coset.

A2.10

Any coset of H has $|H|$ elements. Since an element $g \in G$ belongs exclusively in a single coset, the union of all cosets must result in G, that is, $|G| = n|H|$, where n is the number of cosets. Therefore, the number of cosets of H in G is $|G|/|H|$.

A2.11

Property (1):
Since I is the $n \times n$ identity matrix, we have $\chi(e) = \mathrm{tr}(I) = n$.

Property (2):
Since G is finite, all elements have a finite order, meaning all elements must satisfy $g^r = e$ for some integer r. Thus, all eigenvalues of the representation must correspond to possible r-th roots of the number 1, that is, all eigenvalues of the elements $\rho(g)$ have the form $\lambda = \exp(i2\pi k/r)$ for integers k ranging from 0 to $r - 1$. The norm of the character is then calculated to be

$$|\chi(g)| = |\mathrm{tr}(\rho(g))| = \left|\sum_{j=1}^{n} \lambda_j\right| \leq \sum_{j=1}^{n} |\lambda_j| = n.$$

Property (3):
If $|\chi(g)| = n$, then $|\mathrm{tr}(\rho(g))| = \left|\sum_{j=1}^{n} \lambda_j\right| = \sum_{j=1}^{n} |\lambda_j|$, meaning all its eigenvalues must correspond to the same value $e^{i\theta}$ and thus $\rho(g)$ must be proportional to the identity. Therefore, $\rho(g) = e^{i\theta} I$.

Property (4):
Consider $x \in G$. For any element in the conjugacy class G_x of this element we have $\chi(g^{-1}xg) = \mathrm{tr}(\rho(g^{-1}xg)) = \mathrm{tr}(\rho(g^{-1})\rho(x)\rho(g)) = \mathrm{tr}(\rho(g)\rho(g^{-1})\rho(x)) = \mathrm{tr}(\rho(x)) = \chi(x)$.

Property (5):
We may write any group element as $g = h^{-1}dh$, where $h, d \in G$ and d is such that $\rho(d)$ is a diagonal matrix. Analogously we have $g^{-1} = h^{-1}d^{-1}h$. From property (4) we have $\chi(g) = \chi(d)$ and $\chi(g^{-1}) = \chi(d^{-1})$. Also, note that since all eigenvalues lie on the complex unit circle, we have $\rho(d^{-1}) = \rho(d^*)$. Therefore, $\chi(g^{-1}) = \chi(d^*) = \chi^*(d) = \chi^*(g)$.

Property (6):
Since for $g \in G$ all eigenvalues of $\rho(g)$ are r-th roots of the number 1 for some r, they all satisfy the equation $\lambda^r - 1 = 0$, which is a polynomial equation with rational coefficients. Thus all eigenvalues are algebraic numbers, and since the character is calculated as a sum of such eigenvalues, $\chi(g)$ is also an algebraic number.

A2.12

Let us define the matrix

$$P \equiv \frac{1}{|G|} \sum_{g \in G} \rho^\dagger(g)\rho(g).$$

For all $h \in G$ we have

$$\rho^\dagger(h)P\rho(h) = \frac{1}{|G|} \sum_{g \in G} \rho^\dagger(h)\rho^\dagger(g)\rho(g)\rho(h) = \frac{1}{|G|} \sum_{g \in G} \rho^\dagger(gh)\rho(gh),$$

but since $k \equiv gh \in G$, because of the *closure* property, we have that P is left invariant, that is,

$$\rho^\dagger(h)P\rho(h) = \frac{1}{|G|} \sum_{k \in G} \rho^\dagger(k)\rho(k) = P.$$

It is also direct to see that P is Hermitian, thus there exists a unitary matrix U such that $U^\dagger PU = D$, where D is a diagonal matrix. Now, taking any vector $|v\rangle \neq 0$, we get that

$$\langle v|P|v\rangle = \frac{1}{|G|} \sum_{g \in G} |\rho(g)\,|v\rangle|^2$$

is always positive. If we define another vector $|w\rangle \equiv U^\dagger\,|v\rangle$, we also obtain

$$\langle v|P|v\rangle = \langle v|UU^\dagger PUU^\dagger|v\rangle = \langle w|D|w\rangle = \frac{1}{|G|} \sum_i D_{ii}\,\langle w|w\rangle\,.$$

Since $|w\rangle$ is arbitrary and $\langle w|w\rangle > 0$, it must hold that each D_{ii} is real and non-negative, meaning $D^\dagger = D$. We can then define another matrix $d \equiv \sqrt{D}$. Since D is diagonal, it follows that $d_{ii} = \sqrt{D_{ii}}$ and $d_{ij} = 0$ for all $i \neq j$, and also $d = d^\dagger$. We can then write

$$P = U^\dagger DU = U^\dagger ddU = U^\dagger dUU^\dagger dU \equiv QQ,$$

where we set $Q \equiv U^\dagger dU$. Let us then define a new representation given by $\sigma(g) \equiv Q\rho(g)Q^{-1}$, which equivalently means that $\rho(g) = Q^{-1}\sigma(g)Q$. Notice that Q is also Hermitian. Using the fact that

$\rho^\dagger(g)P\rho(g) = P$ for all $g \in G$ we obtain

$$\begin{aligned}\rho^\dagger(g)P\rho(g) &= \left(Q^{-1}\sigma(g)Q\right)^\dagger QQ\left(Q^{-1}\sigma(g)Q\right)\\ &= \left(Q\sigma^\dagger(g)Q^{-1}\right)QQ\left(Q^{-1}\sigma(g)Q\right)\\ &= Q\sigma^\dagger(g)\sigma(g)Q.\end{aligned}$$

Since this must result in $P = QQ$, it follows that $\sigma^\dagger(g)\sigma(g) = I$, meaning $\sigma(g)$ is a unitary representation. Therefore, any finite representation $\rho(g)$ is equivalent to a unitary matrix representation.

A2.13

Applying Schur's lemma for $G = H$, we have that for any $g \in G$, a matrix S satisfying $S\rho(g) = \rho(g)S$ is either the zero matrix or a nonsingular square matrix. If G is an Abelian group, S can be any matrix of the representation itself, meaning $S \neq 0$. Considering an eigenvector $|v\rangle$ of S, we have $S|v\rangle = \lambda|v\rangle$ for some number λ. Notice that $\rho(g)|v\rangle$ must also be an eigenvector since

$$S\rho(g)|v\rangle = \rho(g)S|v\rangle = \lambda\rho(g)|v\rangle.$$

Since this is true for any $\rho(g)$, it means the entire representation vector space is spanned by a single vector. If this representation is irreducible, then $|v\rangle$ must be one dimensional, otherwise, there would be invariant subspaces with lower dimensions, which would be a contradiction.

A2.14

For irreducible representations, we can use Equation (A2.2) to write

$$\sum_{g\in G}\chi(g)\chi^*(g) = |G|.$$

Instead of denoting the sum over all group elements, we can consider a sum over all conjugacy classes of G because of property (4). Considering the i-th conjugacy class has size r_i, we can write

$$\sum_i r_i\chi_i\chi_i^* = |G|,$$

where the index i runs over all conjugacy classes, and χ_i denotes the value of the character of any element belonging in the i-th conjugacy class. Now, dividing both sides by $\chi(e) = d_\rho$ we get

$$\sum_i \frac{r_i\chi_i}{d_\rho}\chi_i^* = \frac{|G|}{d_\rho}.$$

From the property (6) of characters, we know $\chi(g)$ is always an algebraic number. Furthermore, since all eigenvalues of $\rho(g)$ are i-th roots of unity (they must satisfy $\lambda^r - 1 = 0$), they are algebraic integers, meaning all characters are in fact algebraic integers. so χ_i^* is also an algebraic integer. Now

consider that for the i-th conjugacy class $C_i \subseteq G$ we define

$$\sigma \equiv \sum_{g \in C_i} \rho(g).$$

Let us also consider that such conjugacy class has size r_i and the character of any $g \in C_i$ is χ_i. Notice that for any $h \in G$ we have

$$\rho(h^{-1})\sigma\rho(h) = \sum_{g \in C_i} \rho(h^{-1}gh) = \sum_{g \in C_i} \rho(g) = \sigma,$$

where we used the fact that $h^{-1}gh$ is still in the conjugacy class C_i. But then $\rho(h^{-1})\sigma\rho(h) = \sigma$ means that $\sigma\rho(h) = \rho(h)\sigma$ for all $h \in G$. Applying Schur's lemma, σ must be a multiple of the identity, that is $\sigma \equiv \lambda I$ for some number λ. It is possible to determine the value of the eigenvalue λ by taking the trace of σ. First, we have that $\mathrm{tr}(\sigma) = \lambda \,\mathrm{tr}(I) = \lambda d_\rho$, but also

$$\mathrm{tr}(\sigma) = \sum_{g \in C} \mathrm{tr}(\rho(g)) = r_i \chi_i \quad \Longrightarrow \quad \lambda = \frac{r_i \chi_i}{d_\rho}.$$

We have that σ is an integer linear combination of matrices with algebraic integer eigenvalues, thus λ must also be an algebraic integer. This means that the entire sum $\sum_i (r_i \chi_i / d_\rho)\chi_i^*$ is an algebraic integer, and so is $|G|/d_\rho$. But given that both $|G|$ and d_ρ are integers, the only way for this quotient to be an algebraic integer is if $|G|/d_\rho$ is in fact an integer.

A2.15

For the first relation we multiply both sides by $\delta_{ij}\delta_{kl}$, and sum over i, k, j, and l yielding

$$\sum_{g \in G} \sum_{i=1}^{d_\rho} \sum_{k=1}^{d_{\rho^q}} \sum_{j=1}^{d_\rho} \sum_{l=1}^{d_{\rho^q}} \delta_{ij}\delta_{kl} \left[\rho^p(g)\right]^{-1}_{ij} \left[\rho^q(g)\right]_{kl} = \frac{|G|}{d_\rho} \sum_{i=1}^{d_\rho} \sum_{k=1}^{d_{\rho^q}} \sum_{j=1}^{d_\rho} \sum_{l=1}^{d_{\rho^q}} \delta_{ij}\delta_{kl}\delta_{il}\delta_{jk}\delta_{pq}.$$

Since any finite representation is equivalent to a unitary matrix representation, we may consider that $\left[\rho^p(g)\right]^{-1} = \left[\rho^p(g)\right]^\dagger$, and thus simplifying both sides yields

$$\sum_{g \in G} \sum_{i=1}^{d_\rho} \sum_{k=1}^{d_{\rho^q}} \left[\rho^p(g)\right]^\dagger_{ii} \left[\rho^q(g)\right]_{kk} = \frac{|G|}{d_\rho} \sum_{i=1}^{d_\rho} \sum_{k=1}^{d_{\rho^q}} \delta_{ik}\delta_{pq}.$$

The right-hand side simplifies to $|G|\delta_{pq}$, and using the definition of character, the left-hand side simplifies to

$$\begin{aligned} \sum_{g \in G} \sum_{i=1}^{d_\rho} \sum_{k=1}^{d_{\rho^q}} \left[\rho^p(g)\right]^\dagger_{ii} \left[\rho^q(g)\right]_{kk} &= \sum_{g \in G} \left(\sum_{i=1}^{d_\rho} \left[\rho^p(g)\right]^\dagger_{ii} \right) \left(\sum_{k=1}^{d_{\rho^q}} \left[\rho^q(g)\right]_{kk} \right) \\ &= \sum_{g \in G} \left[\chi^p(g)\right]^* \chi^q(g), \end{aligned}$$

thus

$$\sum_{g\in G}\left[\chi^p(g)\right]^*\chi^q(g)=|G|\delta_{pq}.$$

The final step is to notice that, since the character is the same for all elements of a conjugacy class, instead of summing over each element individually, we may sum over the conjugacy classes of g, accounting for their sizes r_i, that is

$$\sum_{g\in G}\left[\chi^p(g)\right]^*\chi^q(g)=\sum_{i=1}^{r}r_i\left(\chi_i^p\right)^*\chi_i^q \quad\Longrightarrow\quad \sum_{i=1}^{r}r_i\left(\chi_i^p\right)^*\chi_i^q=|G|\delta_{pq}.$$

For the second relation, we begin with the first one. Dividing both sides by $|G|$, it is possible to rewrite it as an equality between two $r\times r$ matrices as

$$\frac{1}{|G|}\begin{bmatrix}\sum_{i=1}^r r_i(\chi_i^1)^*\chi_i^1 & \sum_{i=1}^r r_i(\chi_i^1)^*\chi_i^2 & \cdots & \sum_{i=1}^r r_i(\chi_i^1)^*\chi_i^r\\ \sum_{i=1}^r r_i(\chi_i^2)^*\chi_i^1 & \sum_{i=1}^r r_i(\chi_i^2)^*\chi_i^2 & \cdots & \sum_{i=1}^r r_i(\chi_i^2)^*\chi_i^r\\ \vdots & \vdots & \ddots & \vdots\\ \sum_{i=1}^r r_i(\chi_i^r)^*\chi_i^1 & \sum_{i=1}^r r_i(\chi_i^r)^*\chi_i^2 & \cdots & \sum_{i=1}^r r_i(\chi_i^r)^*\chi_i^r\end{bmatrix}=\begin{bmatrix}1&0&\cdots&0\\0&1&\cdots&0\\\vdots&\vdots&\ddots&\vdots\\0&0&\cdots&1\end{bmatrix}.$$

Defining the matrices

$$A\equiv\frac{1}{|G|}\begin{bmatrix}r_1(\chi_1^1)^* & r_2(\chi_2^1)^* & \cdots & r_r(\chi_r^1)^*\\ r_1(\chi_1^2)^* & r_2(\chi_2^2)^* & \cdots & r_r(\chi_r^2)^*\\ \vdots & \vdots & \ddots & \vdots\\ r_1(\chi_1^r)^* & r_2(\chi_2^r)^* & \cdots & r_r(\chi_r^r)^*\end{bmatrix}\quad\text{and}\quad B\equiv\begin{bmatrix}\chi_1^1 & \chi_1^2 & \cdots & \chi_1^r\\ \chi_2^1 & \chi_2^2 & \cdots & \chi_2^r\\ \vdots & \vdots & \ddots & \vdots\\ \chi_r^1 & \chi_r^2 & \cdots & \chi_r^r\end{bmatrix},$$

this equality takes the form $AB=I_{r\times r}$, from which we conclude that $B=A^{-1}$. But then we must also have $BA=I_{r\times r}$, meaning

$$BA=\frac{1}{|G|}\begin{bmatrix}\sum_{p=1}^r r_1(\chi_1^p)^*\chi_1^p & \sum_{p=1}^r r_2(\chi_2^p)^*\chi_1^p & \cdots & \sum_{p=1}^r r_r(\chi_r^p)^*\chi_1^p\\ \sum_{p=1}^r r_1(\chi_1^p)^*\chi_2^p & \sum_{p=1}^r r_2(\chi_2^p)^*\chi_2^p & \cdots & \sum_{p=1}^r r_r(\chi_r^p)^*\chi_2^p\\ \vdots & \vdots & \ddots & \vdots\\ \sum_{p=1}^r r_1(\chi_1^p)^*\chi_r^p & \sum_{p=1}^r r_2(\chi_2^p)^*\chi_r^p & \cdots & \sum_{p=1}^r r_r(\chi_r^p)^*\chi_r^p\end{bmatrix}=\begin{bmatrix}1&0&\cdots&0\\0&1&\cdots&0\\\vdots&\vdots&\ddots&\vdots\\0&0&\cdots&1\end{bmatrix}.$$

Reverting back to index notation we obtain

$$\frac{1}{|G|}\sum_{p=1}^{r}r_i(\chi_i^p)^*\chi_j^p=\delta_{ji}\quad\Longrightarrow\quad\sum_{p=1}^{r}(\chi_i^p)^*\chi_j^p=\frac{|G|}{r_i}\delta_{ij}.$$

A2.16

Let us name the group elements respectively as $\{e, g_-, g_+, g_{12}, g_{23}, g_{13}\}$. The composition table of these elements (row then column) can be written as

	e	g_-	g_+	g_{12}	g_{23}	g_{13}
e	e	g_-	g_+	g_{12}	g_{23}	g_{13}
g_-	g_-	g_+	e	g_{13}	g_{12}	g_{23}
g_+	g_+	e	g_-	g_{23}	g_{13}	g_{12}
g_{12}	g_{12}	g_{23}	g_{13}	e	g_-	g_+
g_{23}	g_{23}	g_{13}	g_{12}	g_+	e	g_-
g_{13}	g_{13}	g_{12}	g_{23}	g_-	g_+	e

The trivial function $\rho^1 : S_3 \to 1$, which maps all elements to 1, is a representation because $\rho^1(g_a)\rho^1(g_b) = 1 = \rho^1(g_a g_b)$ for any $g_a, g_b \in S_3$. And since it is one-dimensional, it is irreducible.

From the table, we can also see that the function $\rho^\pm : S_3 \to \{-1, 1\}$, which maps the subset $S_3^{(1)} \equiv \{e, g_-, g_+\}$ to 1 and the subset $S_3^{(2)} \equiv \{g_{12}, g_{23}, g_{13}\}$ to -1, is also a representation. To see that, notice that we have two possible cases:

- $(g_a, g_b \in S_3^{(1)}) \vee (g_a, g_b \in S_3^{(2)})$:
  from the table $g_a g_b \in S_3^{(1)} \implies \rho^\pm(g_a g_b) = 1$
  we have $\rho^\pm(g_a) = \rho^\pm(g_b) \implies \rho^\pm(g_a)\rho^\pm(g_b) = 1 = \rho^\pm(g_a g_b)$;
- $(g_a \in S_3^{(1)}; g_b \in S_3^{(2)}) \vee (g_a \in S_3^{(2)}; g_b \in S_3^{(1)})$:
  from the table $g_a g_b \in S_3^{(2)} \implies \rho^\pm(g_a g_b) = -1$
  we have $\rho^\pm(g_a) \neq \rho^\pm(g_b) \implies \rho^\pm(g_a)\rho^\pm(g_b) = -1 = \rho^\pm(g_a g_b)$.

Like the trivial representation, since $\rho^\pm$ is one-dimensional, it is also irreducible.

One last representation $\rho : S_3 \to M_2$ can be obtained by considering a generating set of S_3, which can be chosen as $\{g_-, g_{12}\}$. The reason is that using the table we can directly verify that

$$\begin{aligned} g_- g_- g_- = g_{12} g_{12} &= e, \\ g_- g_- &= g_+, \\ g_- g_{12} &= g_{13}, \\ g_{12} g_- &= g_{23}, \end{aligned}$$

and since we know this set is closed, we conclude that $S_3 = \langle g_-, g_{12} \rangle$. Thus it suffices to find a function ρ whose compositions satisfy these relations and assign the identity matrix to the identity element. We start by setting

$$\rho(g_-) \equiv \frac{1}{2}\begin{bmatrix} -1 & -\sqrt{3} \\ \sqrt{3} & -1 \end{bmatrix}, \quad \rho(g_{12}) \equiv \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Direct verification yields

$$\rho(g_-)\rho(g_-)\rho(g_-) = \frac{1}{8}\begin{bmatrix}-1 & -\sqrt{3}\\ \sqrt{3} & -1\end{bmatrix}\begin{bmatrix}-1 & -\sqrt{3}\\ \sqrt{3} & -1\end{bmatrix}\begin{bmatrix}-1 & -\sqrt{3}\\ \sqrt{3} & -1\end{bmatrix} = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} \equiv \rho(e),$$
$$\rho(g_{12})\rho(g_{12}) = \begin{bmatrix}-1 & 0\\ 0 & 1\end{bmatrix}\begin{bmatrix}-1 & 0\\ 0 & 1\end{bmatrix} = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} \equiv \rho(e),$$

showing that the identity matrix can be correctly assigned to the identity element, satisfying the first condition. The remaining three give the representation of the other three elements, which are

$$\rho(g_-)\rho(g_-) = \frac{1}{4}\begin{bmatrix}-1 & -\sqrt{3}\\ \sqrt{3} & -1\end{bmatrix}\begin{bmatrix}-1 & -\sqrt{3}\\ \sqrt{3} & -1\end{bmatrix} = \frac{1}{2}\begin{bmatrix}-1 & \sqrt{3}\\ -\sqrt{3} & -1\end{bmatrix} \equiv \rho(g_+),$$
$$\rho(g_-)\rho(g_{12}) = \frac{1}{2}\begin{bmatrix}-1 & -\sqrt{3}\\ \sqrt{3} & -1\end{bmatrix}\begin{bmatrix}-1 & 0\\ 0 & 1\end{bmatrix} = \frac{1}{2}\begin{bmatrix}1 & -\sqrt{3}\\ -\sqrt{3} & -1\end{bmatrix} \equiv \rho(g_{13}),$$
$$\rho(g_{12})\rho(g_-) = \frac{1}{2}\begin{bmatrix}-1 & 0\\ 0 & 1\end{bmatrix}\begin{bmatrix}-1 & -\sqrt{3}\\ \sqrt{3} & -1\end{bmatrix} = \frac{1}{2}\begin{bmatrix}1 & \sqrt{3}\\ \sqrt{3} & -1\end{bmatrix} \equiv \rho(g_{23}).$$

Therefore, the matrices

$$\rho(e) = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}, \quad \rho(g_-) = \frac{1}{2}\begin{bmatrix}-1 & -\sqrt{3}\\ \sqrt{3} & -1\end{bmatrix}, \quad \rho(g_+) = \frac{1}{2}\begin{bmatrix}-1 & \sqrt{3}\\ -\sqrt{3} & -1\end{bmatrix},$$
$$\rho(g_{12}) = \begin{bmatrix}-1 & 0\\ 0 & 1\end{bmatrix}, \quad \rho(g_{23}) = \frac{1}{2}\begin{bmatrix}1 & \sqrt{3}\\ \sqrt{3} & -1\end{bmatrix}, \quad \rho(g_{13}) = \frac{1}{2}\begin{bmatrix}1 & -\sqrt{3}\\ -\sqrt{3} & -1\end{bmatrix},$$

form a representation of the S_3 group. To see that it is irreducible, notice that $|\chi(e)|^2 = 4$, $|\chi(g_-)|^2 = |\chi(g_+)|^2 = 1$, and $|\chi(g_{12})|^2 = |\chi(g_{23})|^2 = |\chi(g_{13})|^2 = 0$, thus $\sum_{g\in S_3}|\chi(g)|^2 = 6 = |S_3|$, so it is an irreducible representation according to Theorem A2.3.

To verify their orthogonality we only need the characters. For the ρ^1 representation we have $\chi^1(g) = 1$ for all $g \in S_3$. For $\rho^\pm$ we have $\chi^\pm(g) = 1$ for $g \in S_3^{(1)}$ and $\chi^\pm(g) = -1$ for $g \in S_3^{(2)}$. And finally, for ρ we have $\chi(e) = 2$, $\chi(g_-) = \chi(g_+) = -1$, and $\chi(g_{12}) = \chi(g_{23}) = \chi(g_{13}) = 0$. Thus

$$\sum_{g\in S_3}[\chi^1(g)]^*\chi^\pm(g) = 1+1+1-1-1-1 = 0,$$
$$\sum_{g\in S_3}[\chi^1(g)]^*\chi(g) = 2-1-1+0+0+0 = 0,$$
$$\sum_{g\in S_3}[\chi^\pm(g)]^*\chi(g) = -2+1+1+0+0+0 = 0,$$

showing that they are orthogonal among them.

A2.17

Since there are $|G|$ distinct matrices and G has $|G|$ elements, it is possible to create a one-to-one map between the elements of G and the permutation matrices, meaning this representation is an isomorphism, thus faithful.

A2.18

A permutation matrix that sends the i-th entry of $\vec{v}$ to the j-th position has a 1 in the i-th row and j-th column, and zeros in all other entries of this row and column. For $g, g_i \in G$, the only way to get $gg_i = g_i$ is if g is the identity element e. This means that, except for the identity, all permutation matrices must rearrange all entries of $\vec{v}$, so the positions containing a 1 are always such that $i \neq j$. Therefore all permutation matrices have null diagonals, meaning $\chi(g) = 0$ for all $g \neq e$. The identity on the other hand has $|G|$ entries with 1 in the diagonal, meaning $\chi(e) = |G|$.

A2.19

From Theorem A2.5 we have that $\rho = \bigoplus_p c_p \rho^p$, meaning any ρ can be put in a block diagonal form containing, for all p, c_p copies of the p-th irreducible representation. By taking the trace in both sides we get

$$\mathrm{tr}(\rho) = \sum_p c_p \,\mathrm{tr}(\rho^p) \quad \Longrightarrow \quad \chi = \sum_p c_p \chi^p.$$

Also according to Theorem A2.5, the multiplicities are given by

$$c_p = \frac{1}{|G|} \sum_{i=1}^{r} r_i (\chi_i^p)^* \chi_i.$$

If the representation is the regular one, R, then we know that χ^R is zero for all group elements except the identity, for which we have $\chi^R(e) = |G|$. The conjugacy class of the identity contains only the identity itself so its size is 1. Therefore the multiplicity is calculated as

$$c_p = \frac{1}{|G|} \sum_{i=1}^{r} r_i (\chi_i^p)^* \chi_i^R = \frac{1}{|G|} [\chi^p(e)]^* \chi^R(e) = \chi^p(e).$$

But for any representation ρ^p, $\chi^p(e)$ will be the dimension of that representation, so $c_p = d_{\rho^p}$. Thus the regular representation contains d_{ρ^p} instances of each representation ρ^p, and the character relation in this case will be

$$\chi^R = \sum_{\rho \in \hat{G}} d_\rho \chi^\rho.$$

A2.20

Applying the relation $\chi^R = \sum_{\rho \in \hat{G}} d_\rho \chi^\rho$ to some element $g \in G$ we have

$$\chi^R(g) = \sum_{\rho \in \hat{G}} d_\rho \chi^\rho(g).$$

We know that $\chi^R(g) = |G| \delta_{ge}$, so defining $N \equiv |G|$ we get

$$\sum_{\rho \in \hat{G}} d_{\rho^p} \chi^p(g) = N \delta_{ge}.$$

A2.21

Applying the relation $\chi^R = \sum_{\rho\in\hat{G}} d_\rho \chi^\rho$ to the identity element e we have

$$\chi^R(e) = \sum_{\rho\in\hat{G}} d_\rho \chi^\rho(e).$$

We know that $\chi^R(e) = |G|$, and $\chi^\rho(e) = d_\rho$ for all representations, so

$$\sum_{\rho\in\hat{G}} d_\rho^2 = |G|.$$

A2.22

Substituting (A2.10) into (A2.9) yields

$$\begin{aligned}\hat{f}(\rho) &= \sqrt{\frac{d_\rho}{N}} \sum_{g\in G} \left[\frac{1}{\sqrt{N}} \sum_{\sigma\in\hat{G}} \sqrt{d_\sigma}\, \mathrm{tr}\Big(\hat{f}(\sigma)\sigma(g^{-1})\Big) \right] \rho(g) \\ &= \frac{1}{N} \sum_{\sigma\in\hat{G}} \sqrt{d_\rho d_\sigma} \sum_{g\in G} \mathrm{tr}\Big(\hat{f}(\sigma)\sigma(g^{-1})\Big)\rho(g).\end{aligned}$$

It will be convenient to write this relation in terms of the matrix indices. In both sides we set the pair of i-th row and j-th column with $[\hat{f}(\rho)]_{ij}$ and $[\rho(g)]_{ij}$. Now notice that $[\hat{f}(\sigma)\sigma(g^{-1})]_{kl} = \sum_m [\hat{f}(\sigma)]_{km}[\sigma(g)]^{-1}_{ml}$, and taking the trace adds a sum over k with $k = l$. Thus we can write

$$\big[\hat{f}(\rho)\big]_{ij} = \frac{1}{N} \sum_{\sigma\in\hat{G}} \sqrt{d_\rho d_\sigma} \sum_{g\in G} \sum_{k,m} \big[\hat{f}(\sigma)\big]_{km} \big[\sigma(g)\big]^{-1}_{mk} \big[\rho(g)\big]_{ij}.$$

Using the orthogonality relation shown in Equation (A2.3) we get

$$\begin{aligned}\big[\hat{f}(\rho)\big]_{ij} &= \frac{1}{N} \sum_{\sigma\in\hat{G}} \sqrt{d_\rho d_\sigma} \sum_{k,m} \big[\hat{f}(\sigma)\big]_{km} \frac{N}{d_\sigma} \delta_{mj}\delta_{ki}\delta_{\sigma\rho} \\ &= \sum_{\sigma\in\hat{G}} \frac{\sqrt{d_\rho d_\sigma}}{d_\sigma} \delta_{\sigma\rho} \sum_{k,m} \big[\hat{f}(\sigma)\big]_{km} \delta_{ki}\delta_{mj} \\ &= \big[\hat{f}(\rho)\big]_{ij}.\end{aligned}$$

A2.23

From the definition of $\hat{f}$ we have

$$\hat{f}(\rho) = \sqrt{\frac{d_\rho}{N}} \sum_{g\in G} f(g)\rho(g).$$

In this case, we have an additive Abelian group with elements represented by $g \in [0, N-1]$, and the representation given by $\rho_h(g) \equiv \exp[-2\pi i g h/N]$, with dimension $d_\rho = 1$. Since the number h uniquely identifies each representation ρ_h, we can directly use it for identification, instead of using

ρ_h. In other words, we can do the relabeling $\rho_h \to h$. Direct substitution yields

$$\hat{f}(h) = \frac{1}{\sqrt{N}} \sum_{g=0}^{N-1} f(g) e^{-2\pi i g h/N}.$$

From the definition of f we have

$$f(g) = \frac{1}{\sqrt{N}} \sum_{\rho \in \hat{G}} \sqrt{d_\rho}\, \mathrm{tr}\Big(\hat{f}(\rho)\rho(g^{-1})\Big).$$

Since the group is Abelian, all its irreducible representations are one-dimensional. So given that $|G| = N$, it must have N representations ρ_h, meaning $h \in [0, N-1]$ exactly like g. With these considerations, we can write

$$f(g) = \frac{1}{\sqrt{N}} \sum_{h=0}^{N-1} \hat{f}(h)\rho_h(g^{-1}).$$

Given that $\rho_h(g^{-1})\rho_h(g) = 1$, we obtain $\rho_h(g^{-1}) = \exp[2\pi i g h/N]$, and since the set g and the indices h are isomorphic, we may relabel $g \leftrightarrow h$ in the sum, yielding

$$f(h) = \frac{1}{\sqrt{N}} \sum_{g=0}^{N-1} \hat{f}(g) e^{2\pi i g h/N}.$$

A2.24

Starting with the trivial representation ρ^1, with $\rho^1(g) = 1$ for all $g \in G$, the Fourier transform is

$$\begin{aligned}\hat{f}(\rho^1) &= \sqrt{\frac{d_{\rho^1}}{|S_3|}} \sum_{g\in S_3} f(g)\rho^1(g) = \frac{1}{\sqrt{6}} \sum_{g\in S_3} f(g) \\ &= \frac{1}{\sqrt{6}} \left[f(e) + f(g_-) + f(g_+) + f(g_{12}) + f(g_{23}) + f(g_{13})\right].\end{aligned}$$

For the representation $\rho^\pm$, with $\rho^\pm(g) = 1$ for $g \in S_3^{(1)} \equiv \{e, g_-, g_+\}$, and $\rho^\pm(g) = -1$ for $g \in S_3^{(2)} \equiv \{g_{12}, g_{23}, g_{13}\}$, we write the Fourier transform as

$$\begin{aligned}\hat{f}(\rho^\pm) &= \sqrt{\frac{d_{\rho^\pm}}{|S_3|}} \sum_{g\in S_3} f(g)\rho^\pm(g) = \frac{1}{\sqrt{6}} \sum_{g\in S_3^{(1)}} f(g) - \frac{1}{\sqrt{6}} \sum_{g\in S_3^{(2)}} f(g) \\ &= \frac{1}{\sqrt{6}} \left[f(e) + f(g_-) + f(g_+) - f(g_{12}) - f(g_{23}) - f(g_{13})\right].\end{aligned}$$

For the two-dimensional representation ρ, for each matrix component we will have

$$\Big[\hat{f}(\rho)\Big]_{ij} = \sqrt{\frac{d_\rho}{|S_3|}} \sum_{g\in S_3} f(g) \Big[\rho(g)\Big]_{ij} = \frac{1}{\sqrt{3}} \sum_{g\in S_3} f(g) \Big[\rho(g)\Big]_{ij},$$

where the $\rho(g)$ are given by

$$\rho(e) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \rho(g_-) = \frac{1}{2}\begin{bmatrix} -1 & -\sqrt{3} \\ \sqrt{3} & -1 \end{bmatrix}, \quad \rho(g_+) = \frac{1}{2}\begin{bmatrix} -1 & \sqrt{3} \\ -\sqrt{3} & -1 \end{bmatrix},$$
$$\rho(g_{12}) = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \rho(g_{23}) = \frac{1}{2}\begin{bmatrix} 1 & \sqrt{3} \\ \sqrt{3} & -1 \end{bmatrix}, \quad \rho(g_{13}) = \frac{1}{2}\begin{bmatrix} 1 & -\sqrt{3} \\ -\sqrt{3} & -1 \end{bmatrix}.$$

So explicitly we have

$$\left[\hat{f}(\rho)\right]_{11} = \frac{1}{\sqrt{3}}\left[f(e) - \frac{f(g_-)}{2} - \frac{f(g_+)}{2} - f(g_{12}) + \frac{f(g_{23})}{2} + \frac{f(g_{13})}{2}\right],$$
$$\left[\hat{f}(\rho)\right]_{12} = \frac{1}{2}\left[-f(g_-) + f(g_+) + f(g_{23}) - f(g_{13})\right],$$
$$\left[\hat{f}(\rho)\right]_{21} = \frac{1}{2}\left[f(g_-) - f(g_+) + f(g_{23}) - f(g_{13})\right],$$
$$\left[\hat{f}(\rho)\right]_{22} = \frac{1}{\sqrt{3}}\left[f(e) - \frac{f(g_-)}{2} - \frac{f(g_+)}{2} + f(g_{12}) - \frac{f(g_{23})}{2} - \frac{f(g_{13})}{2}\right].$$

Ordering the array of values of $f(g)$ as $(f(e), f(g_-), f(g_+), f(g_{12}), f(g_{23}), f(g_{13}))$ and looking at the obtained coefficients, we can write the Fourier transform as the unitary matrix

$$\hat{f} \equiv \begin{bmatrix} \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} \\ \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} & -\frac{1}{\sqrt{6}} & -\frac{1}{\sqrt{6}} & -\frac{1}{\sqrt{6}} \\ \frac{1}{\sqrt{3}} & -\frac{1}{2\sqrt{3}} & -\frac{1}{2\sqrt{3}} & -\frac{1}{\sqrt{3}} & \frac{1}{2\sqrt{3}} & \frac{1}{2\sqrt{3}} \\ 0 & -\frac{1}{2} & \frac{1}{2} & 0 & \frac{1}{2} & -\frac{1}{2} \\ 0 & \frac{1}{2} & -\frac{1}{2} & 0 & \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{\sqrt{3}} & -\frac{1}{2\sqrt{3}} & -\frac{1}{2\sqrt{3}} & \frac{1}{\sqrt{3}} & -\frac{1}{2\sqrt{3}} & -\frac{1}{2\sqrt{3}} \end{bmatrix},$$

which, upon acting on the array of $f(g)$, will yield $(\hat{f}(\rho^1), \hat{f}(\rho^\pm), [\hat{f}(\rho)]_{11}, [\hat{f}(\rho)]_{12}, [\hat{f}(\rho)]_{21}, [\hat{f}(\rho)]_{22})$.

The Solovay–Kitaev theorem

A3.1

-

A3.2

-

A3.3

-

A3.4

-

A3.5

-

A3.6

-

Number theory

A4.1

If $a|b$ and $b|c$ there exist integers k_1 and k_2 such that $b = ak_1$ and $c = bk_2$, which implies $c = ak_1k_2$. Since the product k_1k_2 is also an integer we have $a|c$.

A4.2

If $d|a$ and $d|b$ there exist integers k_1 and k_2 such that $a = dk_1$ and $b = dk_2$. So for integers x and y we may write the linear combination

$$\begin{aligned} ax + by &= dk_1x + dk_2y \\ &= d(k_1x + k_2y), \end{aligned}$$

and since $k_1x + k_2y$ is an integer, the linear combnation $ax + by$ is divisible by d .

A4.3

If $a|b$ then there exists a positive integer k such that $b = ak$. Being a positive integer, we must have $k \geq 1$, which implies $a \leq b$. If $b|a$ then $b \leq a$. Combining both conditions yields $a = b$.

A4.4

$$\begin{aligned} 697 &= 17 \times 41, \\ 36300 &= 2^2 \times 3 \times 5^2 \times 11^2. \end{aligned}$$

A4.5

If a number p is prime then it does not share any common factors with any number in the range $[1, p-1]$, that is, for all $x \in [1, p-1]$ we have $\gcd(x, p) = 1$, meaning every x in this range has a multiplicative inverse modulo p.

Now, for numbers in the range $[1, p^2 - 1]$, the ones that do not have a multiplicative inverse modulo p^2 are the ones with p as a prime factor. Those are $\{p, 2p, \cdots, (p-1)p\}$.

A4.6

The inverse a will be the solution to the equation $17a - 24b = 1$ for some integer b such that a is also an integer. That is, a is the smallest integer such that

$$a = \frac{1 + 24b}{17}.$$

The smallest b possible is $b = 12$, which yields $a = 17$, meaning 17 is its own inverse modulo 24.

A4.7

We may write $n^2 = (n+1)(n-1)+1$, which means that $(n+1)(n-1) = -1 \pmod{n^2}$. Multiplying both sides by -1 yields $(n+1)(1-n) = 1 \pmod{n^2}$. So $1 - n$ is the multiplicative inverse of $n + 1$ modulo n^2. If we want only numbers in the range $[1, n^2 - 1]$ we just have to sum n^2, meaning the multiplicative inverse is $n^2 - n + 1$.

A4.8

If both b and b' are multiplicative inverses of a modulo n then $ab \equiv 1 \pmod{n} \equiv ab' \pmod{n}$. Dividing both extremes of the congruence relations by a yields $b \equiv b' \pmod{n}$.

A4.9

If we have $a = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ and $b = p_1^{\beta_1} \cdots p_n^{\beta_n}$, then the gcd can be calculated as

$$\gcd(a, b) = \prod_{i=1}^{n} p_i^{\min\{\alpha_i, \beta_i\}}.$$

For 6825 and 1430 we have

$$6825 = 3^1 \times 5^2 \times 7^1 \times 13^1,$$
$$1430 = 2^1 \times 5^1 \times 11^1 \times 13^1,$$

thus

$$\gcd(6825, 1430) = 5^1 \times 13^1 = 65.$$

A4.10

The prime factorization yields $187 = 11^1 \times 17^1$, thus

$$\varphi(187) = (11 - 1)(17 - 1) = 160.$$

A4.11

First, consider the case where n is the α-th power of some prime number p, that is $n = p^\alpha$. So all the numbers d that divides n belong in the set $\{1, p, p^2, \cdots, p^\alpha\}$. The Euler totient function for some number p^m $(m > 0)$ in this set is

$$\varphi(p^m) = p^{m-1}(p-1).$$

If we sum the Euler totient function for all divisors d we get

$$\begin{aligned}\sum_{d|n} \varphi(d) &= \varphi(1) + (p-1)\sum_{m=1}^{\alpha} p^{m-1} \\ &= 1 + (p-1)\frac{p^\alpha - 1}{p-1} \\ &= p^\alpha = n.\end{aligned}$$

The result can be extended immediately for the case of general n since it could be written as $n = \prod_i n_i$, where each n_i is the power of some prime number p_i, that is, $n_i = p_i^{a_i}$. The relation would be valid for each n_i, and because of the property $\varphi(ab) = \varphi(a)\varphi(b)$, it would also be valid for n.

To see this extension explicitly let us consider that $n = p^\alpha q$, where $q \neq p$ is a prime number. Now, besides $\{1, p, p^2, \cdots, p^\alpha\}$, the set $\{q, pq, p^2q, \cdots, p^\alpha q\}$ also contains possible divisors d. The Euler totient function for some number $p^m q$ $(m > 0)$ is

$$\varphi(p^m q) = p^{m-1}(p-1)(q-1),$$

thus summing for all divisors yields

$$\begin{aligned}\sum_{d|n} \varphi(d) &= \varphi(1) + (p-1)\sum_{m=1}^{\alpha} p^{m-1} + \varphi(q) + (p-1)(q-1)\sum_{m=1}^{\alpha} p^{m-1} \\ &= 1 + (p-1)\frac{p^\alpha - 1}{p-1} + (q-1) + (p-1)(q-1)\frac{p^\alpha - 1}{p-1} \\ &= p^\alpha + p^\alpha(q-1) \\ &= p^\alpha q = n.\end{aligned}$$

A4.12

$\mathbf{Z}_n^*$ is the set off all elements in $\mathbf{Z}_n$ that have an inverse modulo n, those are, all numbers $x < n$ such that $\gcd(x, n) = 1$, and there are, by definition, $\varphi(n)$ of these numbers. Now we must only show this set satisfies the group properties:

- *closure*

Let $a, b \in \mathbf{Z}_n^*$. Both, a and b, do not share common factors with n, so $(a \cdot b \mod n) \in \mathbf{Z}_n^*$.

- *associativity*

Naturally satisfied by the properties of modular multiplication.

- *identity*

The number $1 \in \mathbf{Z}_n^*$ is the identity since for any $a \in \mathbf{Z}_n^*$ we have $1 \cdot a = a \cdot 1 = a$.

- *inverses*

An integer a has a multiplicative inverse modulo n if and only if $\gcd(a, n) = 1$, but since by definition all elements of $\mathbf{Z}_n^*$ satisfy this property, all elements have an inverse.

A4.13

If $a \in \mathbf{Z}_n^*$ then a does not share any common factors with n, meaning $a^k \in \mathbf{Z}_n^*$ for any integer k. So if we take the set $S = \{1, a, a^2, \cdots, a^{r-1}\}$, where $a^r \equiv 1 \pmod{n}$, we clearly have a subset of $\mathbf{Z}_n^*$ with size r. We must only show it satisfies the group properties:

- *closure*

Naturally satisfied by the construction of the set.

- *associativity*

Naturally satisfied by the properties of modular multiplication.

- *identity*

The identity $1 \in \mathbf{Z}_n^*$ also belongs in this set.

- *inverses*

Since there exists $r \coloneqq x + y$ such that $a^r \equiv 1 \pmod{n}$ there is always a pair a^x and a^y, with $x < r$ and $y < r$, such that $a^x \cdot a^y = a^{x+y} \equiv 1 \pmod{n}$, that is, all elements have an inverse.

A4.14

If g is a generator of $\mathbf{Z}_n^*$ then all $\varphi(n)$ elements of the group can be written as powers of g, that is, $\mathbf{Z}_n^* = \left\{1, g, g^2, \cdots, g^{\varphi(n)-1}\right\}$, where $g^{\varphi(n)} \equiv 1 \pmod{n}$, meaning that g has order $\varphi(n)$.

A4.15

Consider the element $a \in \mathbf{Z}_n^*$ and the subgroup $\{1, a, a^2, \cdots, a^{r-1}\}$ of the group $\mathbf{Z}_n^*$, where r is some number such that $a^r = 1 \pmod{n}$. Using Lagrange's theorem we have that r must divide the size of $\mathbf{Z}_n^*$, that is, $\varphi(n)/r$ is an integer. Alternatively, we may write $\varphi(n) = \alpha r$, where α is a positive integer. Now, if $a^r = 1 \pmod{n}$ then there exists some integer k such that

$$a^r = kn + 1.$$

If we exponentiate both sides with α we obtain

$$\begin{aligned} a^{\varphi(n)} &= (kn+1)^\alpha \\ &= 1 + \sum_{i=1}^{\alpha} \binom{\alpha}{i} (kn)^i. \end{aligned}$$

The second term is clearly divisible by n, thus we have that $a^{\varphi(n)} = 1 \pmod{n}$, *Q.E.D.*

A4.16

If r is the order of x modulo N then $x^r \equiv 1 \pmod{N}$. Since r is the smallest number that satisfies such relation, any other number that also satisfies it must necessarily be a multiple integer of r. From Theorem A4.9 we have that $x^{\varphi(N)} = 1 \pmod{N}$, so there exists some integer α such that $\varphi(N) = \alpha r$, or equivalently $\varphi(N)/r = \alpha$, meaning $r|\varphi(N)$.

A4.17

If we have an efficient factoring algorithm we can efficiently compute the list $P = \{p_1^{\alpha_1}, \cdots p_m^{\alpha_m}\}$ of prime factors of a number N. We know that the order r of x modulo N is such that $r \leq N$, so we can run Euclid's algorithm to compute $\gcd(x^{s/2} - 1, N)$ and $\gcd(x^{s/2} + 1, N)$ for all even $s \in [1, N]$ until we get a number belonging in the list P. When we do we output the order $r = s$, and in the worst case scenario we need to run Euclid's algorithm $O(N)$ times. And similarly to the reduction of factoring to order-finding, we would have a probability $p \leq 1/2^m$ of failing, which would occur if r is odd or if $x^{s/2} = -1 \pmod{N}$ for all s.

A4.18

$$\frac{19}{17} = 1 + \frac{1}{\frac{17}{2}} = 1 + \frac{1}{8 + \frac{1}{2}} \quad \Longrightarrow \quad \frac{19}{17} = [1, 8, 2],$$

$$\frac{77}{65} = 1 + \frac{1}{\frac{65}{12}} = 1 + \frac{1}{5 + \frac{1}{\frac{12}{5}}} = 1 + \frac{1}{5 + \frac{1}{2 + \frac{1}{\frac{5}{2}}}} = 1 + \frac{1}{5 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2}}}} \quad \Longrightarrow \quad \frac{77}{65} = [1, 5, 2, 2, 2]$$

A4.19

Let us first check for the case $n = 1$. From the definitions we have the relations: $p_0 = a_0$, $q_0 = 1$, $p_1 = 1 + a_0 a_1$ and $q_1 = a_1$, thus we verify that

$$\begin{aligned} q_1 p_0 - p_1 q_0 &= a_1 a_0 - (1 + a_0 a_1) \\ &= -1 = (-1)^1. \end{aligned}$$

So the relation is clearly true for $n = 1$. Now we must only show that, for $n \geq 2$, we have $q_{n+1} p_n - p_{n+1} q_n = (-1) \times (q_n p_{n-1} + p_n q_{n-1})$. From the definitions we have, for $n \geq 2$, the relations: $p_{n+1} = a_{n+1} p_n + p_{n-1}$ and $q_{n+1} = a_{n+1} q_n + q_{n-1}$, thus

$$\begin{aligned} q_{n+1} p_n - p_{n+1} q_n &= (a_{n+1} q_n + q_{n-1}) p_n - (a_{n+1} p_n + p_{n-1}) q_n \\ &= p_n q_{n-1} - q_n p_{n-1} \\ &= (-1) \times (q_n p_{n-1} - p_n q_{n-1}). \end{aligned}$$

So this relation is true for all $n \geq 1$. Now, this relation can always be written in the form $\alpha p_n + \beta q_n = 1$, and using Theorem A4.2 we conclude that $\gcd(p_n, q_n) = 1$.

Public key cryptography and the RSA cryptosystem

A5.1

-

A5.2

-

Proof of Lieb's theorem

A6.1

-

A6.2

-

A6.3

-

A6.4

-

A6.5

-

A6.6

-

A6.7

-

A6.8

-