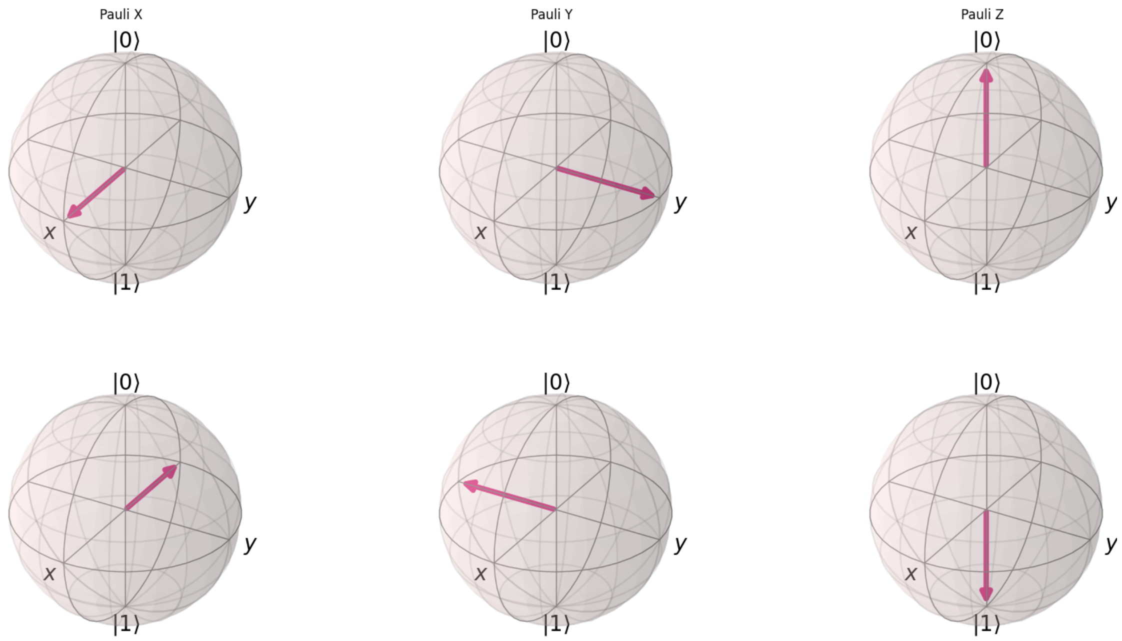
Exercise 4.1

The eigenvectors are as follows:
Pauli Z: $|0\rangle$, $|1\rangle$
Pauli X: $|0\rangle + |1\rangle$, $|0\rangle - |1\rangle$
Pauli Y: $|0\rangle + i\,|1\rangle$, $|0\rangle - i\,|1\rangle$
Bloch sphere representations:



Exercise 4.2

$$\exp(iAx) = \sum_n (iAx)^n = \sum_n (-1)^n x^{2n} I + \sum_n (-1)^n i x^n A = \cos(x) I + i \sin x A$$

Exercise 4.3

Up to a global phase:
$$T = \begin{bmatrix} e^{-i\pi/8} & 0 \\ 0 & e^{i\pi/8} \end{bmatrix} = \begin{bmatrix} e^{-i\frac{\pi}{4}/2} & 0 \\ 0 & e^{i\frac{\pi}{4}/2} \end{bmatrix} = R_z(\pi/4)$$

Exercise 4.4

First consider $R_z R_x R_z$:
$$R_z R_x R_z = \begin{bmatrix} \cos\frac{\theta}{2} e^{-i\theta} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} e^{i\theta} \end{bmatrix}$$
For $\theta = \frac{\pi}{2}$:
$$R_z R_x R_z = \frac{1}{\sqrt{2}} \begin{bmatrix} e^{-i\frac{\pi}{2}} & e^{-i\frac{\pi}{2}} \\ e^{-i\frac{\pi}{2}} & e^{i\frac{\pi}{2}} \end{bmatrix}$$
Hence, by multiplying by $e^{i\frac{\pi}{2}}$ we get,

$e^{i\frac{\pi}{2}} R_z R_x R_z = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = H$

Exercise 4.5

We have $n_x^2 + n_y^2 + n_z^2 = 1$
$\hat{n} \cdot \vec{\sigma} = \begin{bmatrix} n_z & n_x - in_y \\ n_x + in_y & n_z \end{bmatrix}$
Therefore,
$(\hat{n} \cdot \vec{\sigma})^2 = \begin{bmatrix} n_x^2 + n_y^2 + n_z^2 & 0 \\ 0 & n_x^2 + n_y^2 + n_z^2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$
Consider, $R_n(\theta)R_n(-\theta)$
$I = R_n(\theta)R_n(-\theta) = (\cos(\frac{\theta}{2})I - \sin(\frac{\theta}{2})\hat{n}\cdot\vec{\sigma})(\cos(\frac{\theta}{2})I + \sin(\frac{\theta}{2})\hat{n}\cdot\vec{\sigma}) = \cos^2(\frac{\theta}{2})I + \sin^2(\frac{\theta}{2})(\hat{n}\cdot\vec{\sigma})^2 = (\cos^2(\frac{\theta}{2}) + \sin^2(\frac{\theta}{2}))I = I$

Exercise 4.6

First, let's show that $R_Z(x)$ rotates around the Z-axis by an angle x. Consider the general state $|\psi\rangle = \begin{pmatrix} \cos\frac{\theta}{2} \\ e^{i\phi}\sin\frac{\theta}{2} \end{pmatrix}$. Then,
$R_Z(x)|\psi\rangle = (\cos\frac{x}{2}I - i\sin\frac{x}{2}Z)\begin{pmatrix} \cos\frac{\theta}{2} \\ e^{i\phi}\sin\frac{\theta}{2} \end{pmatrix} = \cos\frac{x}{2}\begin{pmatrix} \cos\frac{\theta}{2} \\ e^{i\phi}\sin\frac{\theta}{2} \end{pmatrix} - i\sin\frac{x}{2}\begin{pmatrix} \cos\frac{\theta}{2} \\ -e^{i\phi}\sin\frac{\theta}{2} \end{pmatrix} = \begin{pmatrix} e^{-ix/2}\cos\frac{\theta}{2} \\ e^{ix/2}e^{i\phi}\sin\frac{\theta}{2} \end{pmatrix} = \begin{pmatrix} \cos\frac{\theta}{2} \\ e^{i(\phi+x)}\sin\frac{\theta}{2} \end{pmatrix}$
Hence, the state has been rotated by x around the Z-axis. Similarly, we get that $R_X(x)$ and $R_Y(x)$ rotate around the X and Y axis respectively.
We also have that,
$R_n(x) = \cos\frac{x}{2}I - i\sin\frac{x}{2}(n_xX + n_yY + n_ZZ) = \cos\frac{x}{2}I - i\sin\frac{x}{2}(\sin\theta_n\cos\phi_nX + \sin\theta_n\sin\theta_nY + \cos\theta_nZ) = R_Z(\phi_n)R_X(\theta_n)(\cos\frac{x}{2}I - i\sin\frac{x}{2}Z)R_X(\theta_n)^\dagger R_Z(\phi_n)^\dagger = R_Z(\phi_n)R_X(\theta_n)R_Z(x)R_X(\theta_n)^\dagger R_Z(\phi_n)^\dagger$
Therefore, $R_n(x)$ rotates the axis of rotation to the Z axis performs the rotations by angle x and then returns the axis back to n, which is the same as rotating around n by an angle x.

Exercise 4.7

$\{X, Y\} = 1$ therefore, $XYX = -XXY = -Y$.
$XR_Y(\theta)X = X(\cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Y)X = \cos\frac{\theta}{2}I + i\sin\frac{\theta}{2}Y = R_Y(-\theta)$

Exercise 4.8

Any 2x2 unitary matrix for $a^2 + b^2 + c^2 + d^2 = 1$ can be written as,
1)$U = e^{i\alpha}\begin{bmatrix} a + ib & c + id \\ -c + id & a - ib \end{bmatrix}$
Consider, the given form for U,
$U = e^{i\alpha}R_n(\theta) = e^{i\alpha}\begin{bmatrix} \cos\frac{\theta}{2} - i\sin\frac{\theta}{2}n_z & -\sin\frac{\theta}{2}(n_y + in_x) \\ \sin\frac{\theta}{2}(n_y - in_x) & \cos\frac{\theta}{2} + i\sin\frac{\theta}{2}n_z \end{bmatrix}$
As, $n_x^2 + n_y^2 + n_z^2 = 1$ this has the same form as the general U, hence any arbitrary 2x2 unitary matrix can be written as $U = e^{i\alpha}R_n(\theta)$.
2) $n_z = \frac{1}{\sqrt{2}}$, $n_y = 0$, $n_x = \frac{1}{\sqrt{2}}$, $\alpha = 0$ and $\theta = \pi$.
3) $n_x, n_y = 0$, $n_z = 1$, $\alpha = \theta = \frac{\pi}{4}$.

Exercise 4.9

We can write,
$U = \begin{bmatrix} e^{i(\alpha-\beta/2-\delta/2)}\cos\frac{\gamma}{2} & -e^{i(\alpha-\beta/2+\delta/2)}\sin\frac{\gamma}{2} \\ e^{i(\alpha+\beta/2-\delta/2)}\sin\frac{\gamma}{2} & e^{i(\alpha+\beta/2+\delta/2)}\cos\frac{\gamma}{2} \end{bmatrix} = e^{i\alpha}\begin{bmatrix} e^{i(-\beta/2-\delta/2)}\cos\frac{\gamma}{2} & -e^{i(-\beta/2+\delta/2)}\sin\frac{\gamma}{2} \\ e^{i(\beta/2-\delta/2)}\sin\frac{\gamma}{2} & e^{i(\beta/2+\delta/2)}\cos\frac{\gamma}{2} \end{bmatrix} =$
$e^{i\alpha}\begin{bmatrix} a & b \\ -b^* & a^* \end{bmatrix}$
which is the general form of a 2x2 unitary matrix as $det(U) = \cos^2\frac{\gamma}{2} + \sin^2\frac{\gamma}{2} = 1$.

Exercise 4.10

$U = e^{i\alpha}R_Z(\beta)R_X(\gamma)R_Z(\delta) = \begin{bmatrix} e^{i(\alpha-\beta/2-\delta/2)}\cos\frac{\gamma}{2} & -ie^{i(\alpha-\beta/2+\delta/2)}\sin\frac{\gamma}{2} \\ -ie^{i(\alpha+\beta/2-\delta/2)}\sin\frac{\gamma}{2} & e^{i(\alpha+\beta/2+\delta/2)}\cos\frac{\gamma}{2} \end{bmatrix}$
which once again is a unitary matrix.

Exercise 4.11

Exercise 4.12

From the proof of Corollary 4.2 we have, $AXBXC = R_Z(\beta)R_Y(\gamma)R_Z(\delta)$. We can see that $\alpha = \gamma = \delta = \frac{\pi}{2}$ and $\beta = 0$ gives H. Hence, we can take $A = R_Y(\frac{\pi}{4})$,$B = R_Y(-\frac{\pi}{4})R_Z(-\frac{\pi}{4})$ and $C = R_Z(\frac{\pi}{4})$.

Exercise 4.13

$HXH = \frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 2 & 0 \\ 0 & -2 \end{bmatrix} = Z$
$HYH = \frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 0 & 2i \\ -2i & 0 \end{bmatrix} = -Y$ $HZH = HHXHH = X$

Exercise 4.14

$T = R_Z(\frac{\pi}{4})$
$HTH = HR_Z(\frac{\pi}{4})H = H(\cos\frac{\pi}{8} - i\sin\frac{\pi}{8}Z)H = \cos\frac{\pi}{8} - i\sin\frac{\pi}{8}X = R_X(\frac{\pi}{4})$

Exercise 4.15

(Check Errata for the sign in the second equation)
1)$R_{\hat{n}_2}(\beta_2)R_{\hat{n}_1}(\beta_1) = (c_2I - is_2\hat{n}_2.\sigma)(c_1I - is_1\hat{n}_1.\sigma) = c_1c_2I - s_1s_2(\hat{n}_2.\sigma)(\hat{n}_1.\sigma) - ic_2s_1\hat{n}_1.\sigma - ic_1s_2\hat{n}_2.\sigma = c_1c_2I - s_1s_2(\hat{n}_1.\hat{n}_2I + i(\hat{n}_2\times\hat{n}_1).\sigma) - ic_2s_1\hat{n}_1.\sigma - ic_1s_2\hat{n}_2.\sigma = (c_1c_2 - s_1s_2\hat{n}_1.\hat{n}_2)I - i(c_2s_1\hat{n}_1 + c_1s_2\hat{n}_2 + s_1s_2\hat{n}_2\times\hat{n}_1).\sigma$
Therefore,
$c_{12} = c_1c_2 - s_1s_2\hat{n}_1.\hat{n}_2$
$s_{12}\hat{n}_{12} = c_2s_1\hat{n}_1 + c_1s_2\hat{n}_2 + s_1s_2\hat{n}_2\times\hat{n}_1$
2)$\beta_1 = \beta_2$ and $\hat{n}_1 = \hat{z}$, hence $c_1 = c_2 = c$ and $s_1 = s_2 = s$. Therefore,
$c_{12} = c^2 - s^2\hat{z}.\hat{n}_2$
$s_{12}\hat{n}_{12} = cs(\hat{z} + \hat{n}_2) + s^2\hat{n}_2\times\hat{z}$

Exercise 4.16

$H_1 = \frac{1}{\sqrt{2}}\begin{bmatrix} I & I \\ I & -I \end{bmatrix}$

$H_2 = \frac{1}{\sqrt{2}}\begin{bmatrix} H & 0 \\ 0 & H \end{bmatrix}$

Exercise 4.17

$$\begin{bmatrix} H & 0 \\ 0 & H \end{bmatrix}\begin{bmatrix} I & 0 \\ 0 & Z \end{bmatrix}\begin{bmatrix} H & 0 \\ 0 & H \end{bmatrix} = \begin{bmatrix} HH & 0 \\ 0 & HZH \end{bmatrix} = \begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix} = CNOT$$

Exercise 4.18

When the second qubit is the control we have the following representation,

$$CZ_2 = |00\rangle\langle 00| + |01\rangle\langle 01| - |11\rangle\langle 11| + |10\rangle\langle 10| = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

Exercise 4.19

$$\text{CNOT}\rho\text{CNOT} = \begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix}\begin{bmatrix} A & B \\ C & D \end{bmatrix}\begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix} = \begin{bmatrix} A & XB \\ XC & XDX \end{bmatrix}$$

X only rearranges elements, hence the CNOT only rearranges the elements of ρ.

Exercise 4.20

$$(H_1 \otimes H_2)\text{CNOT}(H_1 \otimes H_2) = \frac{1}{2}\begin{bmatrix} H & H \\ H & -H \end{bmatrix}\begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix}\begin{bmatrix} H & H \\ H & -H \end{bmatrix} = \frac{1}{2}\begin{bmatrix} HH + HXH & HH - HXH \\ HH - HXH & HH + HXH \end{bmatrix} =$$

$$\frac{1}{2}\begin{bmatrix} I + Z & I - Z \\ I - Z & I + Z \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} = \text{CNOT}(2^{\text{nd}} \text{ qubit control})$$

The left circuit transforms between the $|0\rangle$,$|1\rangle$ and $|+\rangle$,$|-\rangle$ basis applies a CNOT and transforms back. Hence, the effect of the CNOT on the $|\pm\rangle|\pm\rangle$ is the same as applying the CNOT with the 2^{nd} qubit as target to the state in the $|0\rangle$,$|1\rangle$ basis and then replacing 0 with $+$ and 1 with $-$. This process does indeed give the equations 4.24-4.27.

Exercise 4.21

Consider all the possible inputs,

$|00\psi\rangle \to |00\psi\rangle \to |00\psi\rangle \to |00\psi\rangle \to |00\psi\rangle \to |00\psi\rangle$

$|01\psi\rangle \to |01(V\psi)\rangle \to |01(V\psi)\rangle \to |01(V^\dagger V\psi)\rangle \to |01\psi\rangle \to |01\psi\rangle$

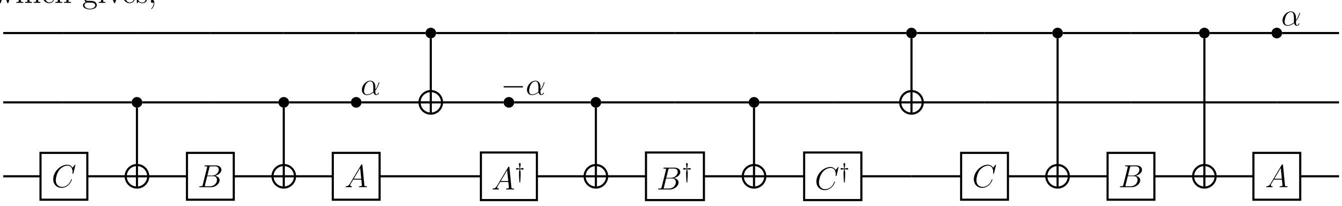
$|10\psi\rangle \to |10\psi\rangle \to |11\psi\rangle \to |11(V^\dagger\psi)\rangle \to |10(VV^\dagger\psi)\rangle \to |10\psi\rangle$

$|11\psi\rangle \to |11(V\psi)\rangle \to |10(V\psi)\rangle \to |11(V\psi)\rangle \to |11(VV\psi)\rangle \to |11U\psi\rangle$

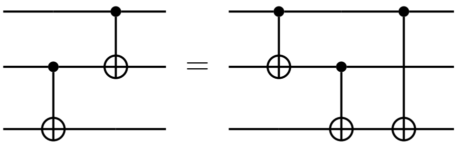
Hence, the circuit does perform the $C^2(U)$ operation.

Exercise 4.22

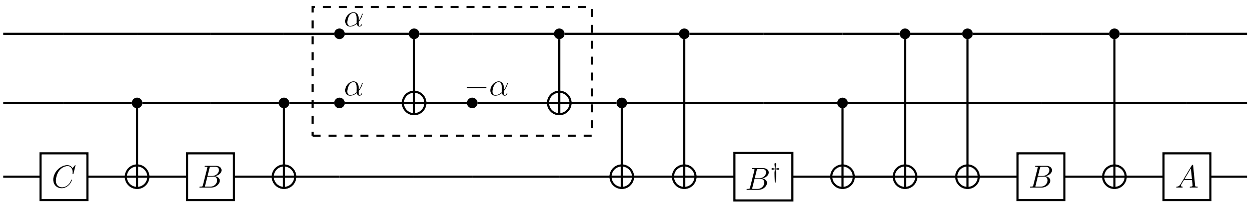
Firstly, we apply the circuit in figure 4.6 to the circuit in figure 4.8 for $V = e^{i\alpha}AXBXC$, which gives,



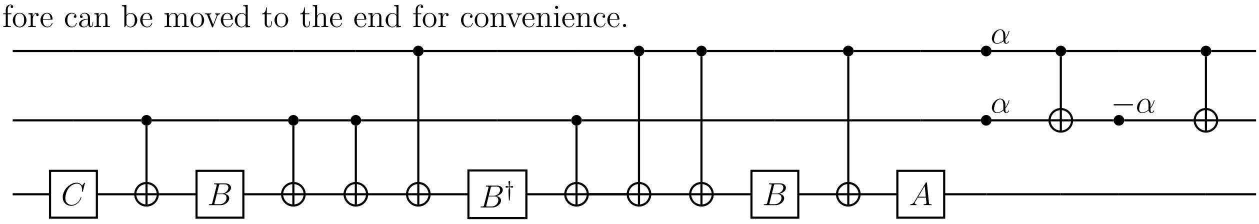
We move the 6[th] CNOT left from the 4[th] one, which involves adding CNOTs after the 4[th] and 5[th] CNOTs from first to third qubit, which is due to,



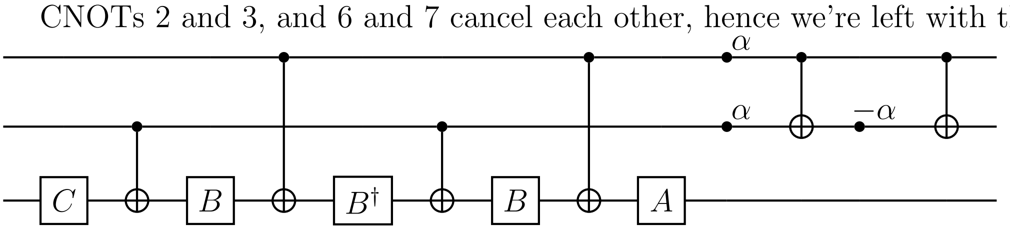
and can be checked by considering all the possible inputs. We also see that $AA^\dagger = CC^\dagger = I$. Hence we get the following circuit.



The dashed section is diagonal hence commutes with the rest of the components therefore can be moved to the end for convenience.



CNOTs 2 and 3, and 6 and 7 cancel each other, hence we're left with the circuit.



This has 8 single qubit gates and 6 CNOTs as desired.
The circuit performs the operation, $AXBXB^\dagger XBXC = (VC^\dagger)B^\dagger(A^\dagger V) = V(ABC)^\dagger = V^2 = U$. Therefore, the circuit performs the $C^2(U)$ operation.

Exercise 4.23

For $U = R_X(\theta)$ from corollary 4.2 we can see that $A = H$, $B = R_Z(-\frac{\theta}{2})$, $C = R_Z(\frac{\theta}{2})H$, which gives $ABC = I$ and $AXBXC = HXR_Z(-\frac{\theta}{2})XR_Z(\frac{\theta}{2})H = HXXR_Z(\frac{\theta}{2})R_Z(\frac{\theta}{2})H = R_X(\theta)$.
For $U = R_Y(\theta)$ we can take $A = I$, $B = R_Y(-\frac{\theta}{2})$ and $C = R_Y(\frac{\theta}{2})$, which gives $ABC = I$ and $AXBXC = XR_Y(-\frac{\theta}{2})XR_Y(\frac{\theta}{2}) = XXR_Y(\frac{\theta}{2})R_Y(\frac{\theta}{2}) = R_Y(\theta)$.

Exercise 4.24

To verify the circuit we consider the state after each operation. Let the initial state be $|xyz\rangle$, where $x, y, z \in \{0, 1\}$.

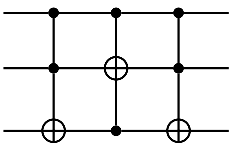
$$
\begin{aligned}
&|xyz\rangle \\
&\big\downarrow H_3 \\
&\frac{1}{\sqrt{2}}(|xy0\rangle + (-1)^z |xy1\rangle) \\
&\big\downarrow \mathrm{CNOT}_{23} \\
&\frac{1}{\sqrt{2}}(|xyy\rangle + (-1)^z |xy\bar{y}\rangle) \\
&\big\downarrow T_3^\dagger \\
&\frac{1}{\sqrt{2}}(e^{-iy\pi/4} |xyy\rangle + e^{-i\bar{y}\pi/4}(-1)^z |xy\bar{y}\rangle) \\
&\big\downarrow \mathrm{CNOT}_{13} \\
&\frac{1}{\sqrt{2}}(e^{-iy\pi/4} |xy(y \oplus x)\rangle + e^{-i\bar{y}\pi/4}(-1)^z |xy(\bar{y} \oplus x)\rangle) \\
&\big\downarrow T_3 \\
&\frac{1}{\sqrt{2}}(e^{i(y\oplus x - y)\pi/4} |xy(y \oplus x)\rangle + e^{i(\bar{y}\oplus x - \bar{y})\pi/4}(-1)^z |xy(\bar{y} \oplus x)\rangle) \\
&\big\downarrow \mathrm{CNOT}_{23} \\
&\frac{1}{\sqrt{2}}(e^{i(y\oplus x - y)\pi/4} |xyx\rangle + e^{i(\bar{y}\oplus x - \bar{y})\pi/4}(-1)^z |xy\bar{x}\rangle) \\
&\big\downarrow T_3^\dagger \\
&\frac{1}{\sqrt{2}}(e^{i(y\oplus x - y - x)\pi/4} |xyx\rangle + e^{i(\bar{y}\oplus x - \bar{y} - \bar{x})\pi/4}(-1)^z |xy\bar{x}\rangle) \\
&\big\downarrow \mathrm{CNOT}_{13} \\
&\frac{1}{\sqrt{2}}(e^{i(y\oplus x - y - x)\pi/4} |xy0\rangle + e^{i(\bar{y}\oplus x - \bar{y} - \bar{x})\pi/4}(-1)^z |xy1\rangle) \\
&\big\downarrow T_2^\dagger T_3 \\
&\frac{1}{\sqrt{2}}(e^{i(y\oplus x - 2y - x)\pi/4} |xy0\rangle + e^{i(\bar{y}\oplus x - \bar{x})\pi/4}(-1)^z |xy1\rangle) \\
&\big\downarrow \mathrm{CNOT}_{12} H_3 \\
&\frac{1}{2}(e^{i(y\oplus x - 2y - x)\pi/4} + e^{i(\bar{y}\oplus x - \bar{x})\pi/4}) |x(y \oplus x)0\rangle + \frac{1}{2}(e^{i(y\oplus x - 2y - x)\pi/4} - e^{i(\bar{y}\oplus x - \bar{x})\pi/4}(-1)^z) |x(y \oplus x)1\rangle \\
&\big\downarrow T_2^\dagger \\
&\frac{1}{2}(e^{i(-2y - x)\pi/4} + e^{i((1-2y)(1-2x) - \bar{x})\pi/4}) |x(y \oplus x)0\rangle + \frac{1}{2}(e^{i(-2y - x)\pi/4} - e^{i((1-2y)(1-2x) - \bar{x})\pi/4}(-1)^z) |x(y \oplus x)1\rangle \\
&\big\downarrow \mathrm{CNOT}_{23} \\
&\frac{1}{2}(e^{i(-2y - x)\pi/4} + e^{i((1-2y)(1-2x) - \bar{x})\pi/4}) |xy0\rangle + \frac{1}{2}(e^{i(-2y - x)\pi/4} - e^{i((1-2y)(1-2x) - \bar{x})\pi/4}(-1)^z) |xy1\rangle \\
&\big\downarrow T_1 S_2
\end{aligned}
$$

$$\frac{1}{2}(1 + e^{i((1-2y)(1-2x)-1+2x+2y)\pi/4}) |xy0\rangle + \frac{1}{2}(1 - e^{i((1-2y)(1-2x)-1+2x+2y)\pi/4}(-1)^z) |xy1\rangle$$
$$=$$
$$\frac{1}{2}(1 + (-1)^{xy+z}) |xy0\rangle + \frac{1}{2}(1 - (-1)^{(xy+z)}) |xy1\rangle$$

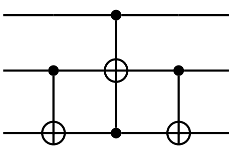
If $x, y = 1$ then we get $|xy\bar{z}\rangle$ and $|xyz\rangle$ otherwise, hence the circuit does indeed implement the Toffoli gate.

Exercise 4.25

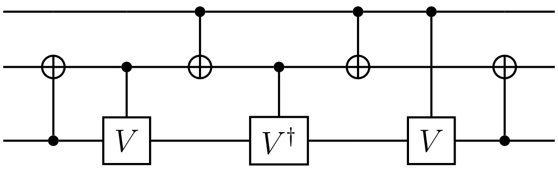
1)



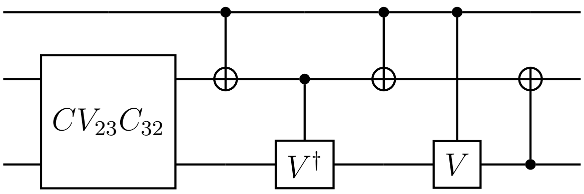
2)



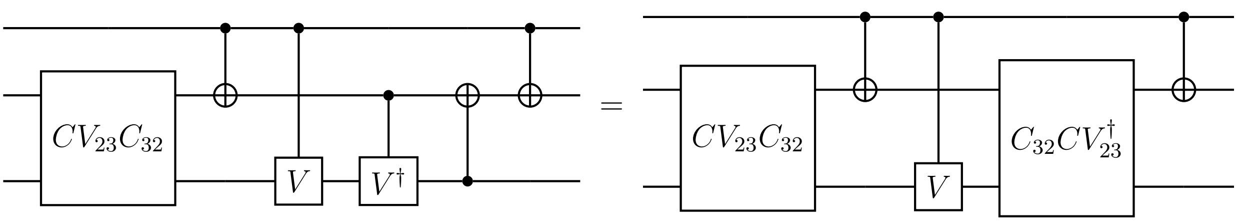
If the first qubit is 0, then the Toffoli just performs the identity, hence the CNOTs cancel leading to an overall identity. If the first qubit is 1, then the Toffoli performs a CNOT on the last 2 qubits, which overall performs the SWAP operation.
3) For the Toffoli we take $V = \frac{(1-i)(1+iX)}{2}$, which gives $V^2 = X$. Then, after changing the order of the last 2 qubits the circuit is,



Which simplifies to,



4)As V is unitary the CV_{13} gate commutes with the $CV_{23}^\dagger$ and C_{12} gates, hence we can move it to the left of $CV_{23}^\dagger$. Afterwards, the last to CNOTs commute as well, hence we get



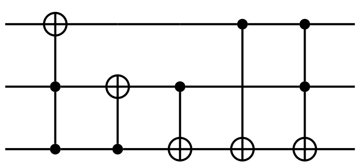
which contains 5 two-qubit gates.

Exercise 4.26

Consider all the possible controls,
$|00t\rangle \rightarrow |00(R_Y(\pi/4)R_Y(\pi/4)R_Y(-\pi/4)R_Y(-\pi/4))t\rangle = |00t\rangle$
$|01t\rangle \rightarrow |01(R_Y(\pi/4)XR_Y(\pi/4)R_Y(-\pi/4)XR_Y(-\pi/4))t\rangle =$
$|01(R_Y(\pi/4)R_Y(-\pi/4)XXR_Y(\pi/4)R_Y(-\pi/4))t\rangle = |01t\rangle$
$|10t\rangle \rightarrow |10(R_Y(\pi/4)R_Y(\pi/4)XR_Y(-\pi/4)R_Y(-\pi/4))t\rangle =$
$|10(R_Y(\pi/4)R_Y(\pi/4)R_Y(\pi/4)R_Y(\pi/4)X)t\rangle = |10(R_Y(\pi)X)t\rangle = -|10(Zt)\rangle$
$|11t\rangle \rightarrow |11(R_Y(\pi/4)XR_Y(\pi/4)XR_Y(-\pi/4)XR_Y(-\pi/4))t\rangle =$
$|11(R_Y(\pi/4)R_Y(-\pi/4)R_Y(-\pi/4)R_Y(\pi/4)X)t\rangle = |11(Xt)\rangle$
Hence, the circuit does indeed implement the Toffoli gate, with the angle for the phase factor being,
$$\theta(c_1, c_2, t) = \begin{cases} \pi, & \text{for } (c_1, c_2, t) = (1, 0, 0) \\ 0, & \text{otherwise} \end{cases}$$

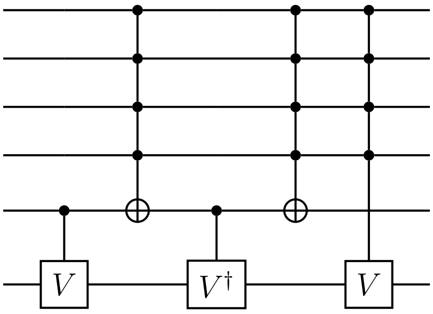
Exercise 4.27

We can write the matrix as,
$U = |000\rangle\langle 000| + |010\rangle\langle 001| + |011\rangle\langle 010| + |100\rangle\langle 011| + |101\rangle\langle 100| + |110\rangle\langle 101| + |111\rangle\langle 110| + |001\rangle\langle 111|$
Which implies the following inputs and outputs
$|000\rangle \rightarrow |000\rangle$
$|001\rangle \rightarrow |010\rangle$
$|101\rangle \rightarrow |110\rangle$
$|010\rangle \rightarrow |011\rangle$
$|011\rangle \rightarrow |100\rangle$
$|100\rangle \rightarrow |101\rangle$
$|110\rangle \rightarrow |111\rangle$
$|111\rangle \rightarrow |001\rangle$
Firstly, we can notice that the first qubit only changes when both the other ones are set, hence we start the circuit with a Toffoli(2,3,1) with the first qubit as target. Looking at $|001\rangle \rightarrow |010\rangle$, $|101\rangle \rightarrow |110\rangle$, $|010\rangle \rightarrow |011\rangle$, $|110\rangle \rightarrow |111\rangle$ and $|111\rangle \rightarrow |001\rangle$ we can see that $C_{23}C_{32}$ after the Toffoli gives the desired results. For $|011\rangle \rightarrow |100\rangle$ and $|100\rangle \rightarrow |101\rangle$ we require a C_{13} after the rest of the gates. However, this changes $|110\rangle \rightarrow |111\rangle$ to $|110\rangle \rightarrow |110\rangle$, hence we apply a Toffoli(1,2,3), as no other final state has both first and second qubit set. Hence the circuit will be,



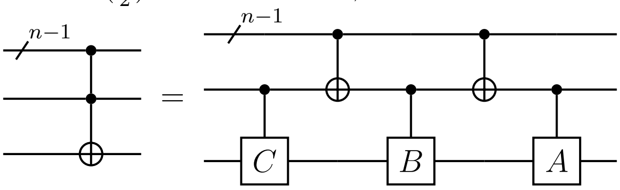
Exercise 4.28

Analogous to the circuit for $C^2(U)$ we have,



Exercise 4.29

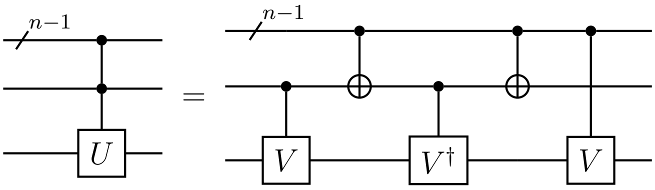
A recursive circuit analogous to figure 4.6, using $A = R_Z(\frac{\pi}{2})$, $B = R_Z(-\frac{\pi}{2})R_Y(-\frac{\pi}{2})$ and $C = R_Y(\frac{\pi}{2})$. The circuit is,



Each recursion requires $O(n)$ gates, hence the overall cost is $\sum_n O(n) = O(n^2)$.
For more details, arXiv:quant-ph/9503016v1.

Exercise 4.30

A recursive circuit can be used for this with $V^2 = U$, which analogous with figure 4.8 is,



The cost of the CV gates is $O(1)$. Let the cost of the $C^n(U)$ be C_n. The cost of the $C^{n-1}(X)$ is $O(n)$, hence the total cost from recursion will be $C_n = C_{n-1} + O(n) = O(n^2)$.
For more details, arXiv:quant-ph/9503016v1.

Exercise 4.31

$$CX_1C = \begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix} \begin{bmatrix} 0 & I \\ I & 0 \end{bmatrix} \begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix} = \begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix} \begin{bmatrix} 0 & X \\ I & 0 \end{bmatrix} = \begin{bmatrix} 0 & X \\ X & 0 \end{bmatrix} = X_1X_2$$

$$CY_1C = \begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix} \begin{bmatrix} 0 & -iI \\ iI & 0 \end{bmatrix} \begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix} = \begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix} \begin{bmatrix} 0 & -iX \\ iI & 0 \end{bmatrix} = \begin{bmatrix} 0 & -iX \\ iX & 0 \end{bmatrix} = Y_1X_2$$

$$CZ_1C = \begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix} \begin{bmatrix} I & 0 \\ 0 & -I \end{bmatrix} \begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix} = \begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix} \begin{bmatrix} I & 0 \\ 0 & -X \end{bmatrix} = \begin{bmatrix} I & 0 \\ 0 & -I \end{bmatrix} = Z_1$$

$$CX_2C = \begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix} \begin{bmatrix} X & 0 \\ 0 & X \end{bmatrix} \begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix} = \begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix} \begin{bmatrix} X & 0 \\ 0 & I \end{bmatrix} = \begin{bmatrix} X & 0 \\ 0 & X \end{bmatrix} = X_2$$

$$CY_2C = \begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix} \begin{bmatrix} Y & 0 \\ 0 & Y \end{bmatrix} \begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix} = \begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix} \begin{bmatrix} Y & 0 \\ 0 & YX \end{bmatrix} = \begin{bmatrix} Y & 0 \\ 0 & -Y \end{bmatrix} = Z_1Y_2$$

$$CZ_2C = \begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix} \begin{bmatrix} Z & 0 \\ 0 & Z \end{bmatrix} \begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix} = \begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix} \begin{bmatrix} Z & 0 \\ 0 & ZX \end{bmatrix} = \begin{bmatrix} Z & 0 \\ 0 & -Z \end{bmatrix} = Z_1Z_2$$

$R_{Z,1}(\theta)C = (\cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Z_1)C = \cos\frac{\theta}{2}CI - i\sin\frac{\theta}{2}CZ_1 = CR_{Z,1}(\theta)$
$R_{X,2}(\theta)C = (\cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}X_2)C = \cos\frac{\theta}{2}CI - i\sin\frac{\theta}{2}CZ_2 = CR_{X,2}(\theta)$

Exercise 4.32

The state after measurement is $\frac{P_0\rho P_0}{tr(P_0\rho P_0)}$ with probability $tr(P_0\rho P_0)$ for measurement result 0 and $\frac{P_1\rho P_1}{tr(P_1\rho P_1)}$ with probability $tr(P_1\rho P_1)$ for measurement result 1. Hence,
$\rho' = tr(P_0\rho P_0)\frac{P_0\rho P_0}{tr(P_0\rho P_0)} + tr(P_1\rho P_1)\frac{P_1\rho P_1}{tr(P_1\rho P_1)} = P_0\rho P_0 + P_1\rho P_1$
$tr_2(\rho) = \sum_i \langle i_2| \rho |i_2\rangle$
$tr_2(\rho') = \sum_i \langle i_2| \rho' |i_2\rangle = \sum_{i,j} \langle i_2| (|j_2\rangle \langle j_2| \rho |j_2\rangle \langle j_2|) |i_2\rangle = \sum_{i,j} \delta_{ij} \langle j_2| \rho |j_2\rangle = \sum_i \langle i_2| \rho |i_2\rangle$
Therefore, $tr_2(\rho) = tr_2(\rho')$.

Exercise 4.33

The circuit performs the following,
$|xy\rangle \xrightarrow{\text{CNOT}} |x(y\oplus x)\rangle \xrightarrow{H_1} \frac{1}{\sqrt{2}}(|0(y\oplus x)\rangle + (-1)^x |1(y\oplus x)\rangle)$
Hence, the possible input outputs are,
$|00\rangle \to \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$
$|01\rangle \to \frac{1}{\sqrt{2}}(|01\rangle + |11\rangle)$
$|10\rangle \to \frac{1}{\sqrt{2}}(|01\rangle - |11\rangle)$
$|11\rangle \to \frac{1}{\sqrt{2}}(|00\rangle - |10\rangle)$
Hence, the circuits effect on the Bell states is as follows,
$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \to |00\rangle$
$\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \to |10\rangle$
$\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \to |01\rangle$
$\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \to |11\rangle$
Therefore, by performing a measurement in the computational basis at the end of the circuit, we are overall performing a bell measurement.
The state $|\psi\rangle$ after the measurement is given by $\frac{M_m^\dagger|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}$. Hence, comparing with the effect of the circuit on the bell states we see that the measurement elements are,
$M_0 = (|00\rangle + |11\rangle)(\langle 00| + \langle 11|)$
$M_1 = (|00\rangle - |11\rangle)(\langle 00| - \langle 11|)$
$M_2 = (|01\rangle + |10\rangle)(\langle 01| + \langle 10|)$
$M_3 = (|01\rangle - |10\rangle)(\langle 01| - \langle 10|)$
As this are projective measurements the POVM elements are equal to these.

Exercise 4.34

This can be done by using a controlled gate to entangle the system to a qubit whose measurement will collapse the state into the +1 or −1 eigenbasis, while will also give us the state on the original qubit. The circuit performs the following,
$|0\psi_{in}\rangle \xrightarrow{H_1} \frac{1}{\sqrt{2}}(|0\psi_{in}\rangle + |1\psi_{in}\rangle) \xrightarrow{CU} \frac{1}{\sqrt{2}}(|0\psi_{in}\rangle + |1(U\psi_{in})\rangle) \xrightarrow{H_1} \frac{1}{2}(|0\psi_{in}\rangle + |1\psi_{in}\rangle + |0(U\psi_{in})\rangle - |1(U\psi_{in})\rangle) = \frac{1}{2}(|0\rangle (I+U) |\psi_{in}\rangle + |1\rangle (I-U) |\psi_{in}\rangle)$
If the measurement value is 0 then the state is $|\psi_{out}\rangle = (I+U)|\psi_{in}\rangle$ for which $U|\psi_{out}\rangle = U(I+U)|\psi_{in}\rangle = (I+U)|\psi_{in}\rangle$, therefore the result with eigenvalue +1 has taken place.

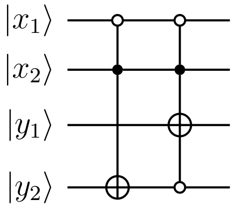
If the measurement value is 1 then the state is $|\psi_{out}\rangle = (I - U)|\psi_{in}\rangle$ for which $U|\psi_{out}\rangle = U(I-U)|\psi_{in}\rangle = -(I-U)|\psi_{in}\rangle$, therefore the result with eigenvalue -1 has taken place.

Exercise 4.35

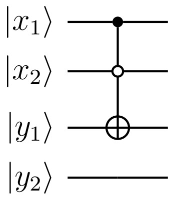
Let the system be in the state $a|0\psi\rangle + b|1\psi\rangle$. Then the effect of the circuits are,
1)$a|0\psi\rangle + b|1\psi\rangle \xrightarrow{CU} a|0\psi\rangle + b|1(U\psi)\rangle \xrightarrow{\text{Mes.}} 0$ with $p = |a|^2$ and state $|\psi\rangle$ or 1 with $p = |b|^2$ and state $U|\psi\rangle$
2)$a|0\psi\rangle + b|1\psi\rangle \xrightarrow{\text{Mes.}} 0$ with $p = |a|^2$ or 1 with $p = |b|^2$, both with state $|\psi\rangle \xrightarrow{CU} |\psi\rangle$ with $p = |a|^2$ or $U|\psi\rangle$ with $p = |b|^2$
Hence, the two circuits perform the same operation.

Exercise 4.36

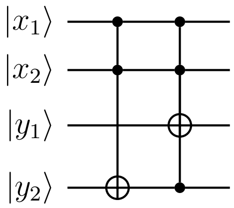
Consider all the possible input states.
If $x = 00$ then nothing needs to be applied.
If $x = 01$ we have for y,
$|00\rangle \to |01\rangle$, $|01\rangle \to |10\rangle$, $|10\rangle \to |11\rangle$, and $|11\rangle \to |00\rangle$. The circuit for this is,



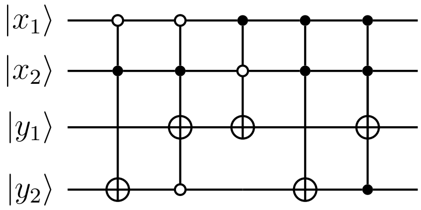
If $x = 10$ we have for y,
$|00\rangle \to |10\rangle$, $|01\rangle \to |11\rangle$, $|10\rangle \to |00\rangle$, and $|11\rangle \to |01\rangle$. The circuit for this is,



If $x = 01$ we have for y,
$|00\rangle \to |11\rangle$, $|01\rangle \to |00\rangle$, $|10\rangle \to |01\rangle$, and $|11\rangle \to |10\rangle$. The circuit for this is,



Hence, the full circuit is,



Exercise 4.37

Identical to the 3x3 matrix we do the following,

$$U_1 = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$U_1U = \frac{1}{2}\begin{bmatrix} \sqrt{2} & \frac{1}{\sqrt{2}}(1+i) & 0 & \frac{1}{\sqrt{2}}(1-i) \\ 0 & \frac{1}{\sqrt{2}}(1-i) & \sqrt{2} & \frac{1}{\sqrt{2}}(1+i) \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix}$$

$$U_2 = \begin{bmatrix} \sqrt{\frac{2}{3}} & 0 & \frac{1}{\sqrt{3}} & 0 \\ 0 & 1 & 0 & 0 \\ \frac{1}{\sqrt{3}} & 0 & -\sqrt{\frac{2}{3}} & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$U_2U_1U = \frac{1}{2}\begin{bmatrix} \sqrt{3} & \frac{i}{\sqrt{3}} & \frac{1}{\sqrt{3}} & -\frac{i}{\sqrt{3}} \\ 0 & \frac{1}{\sqrt{2}}(1-i) & \sqrt{2} & \frac{1}{\sqrt{2}}(1+i) \\ 0 & \frac{1}{\sqrt{2}}(\sqrt{3}+\frac{i}{\sqrt{3}}) & -\sqrt{\frac{2}{3}} & \frac{1}{\sqrt{2}}(\sqrt{3}-\frac{i}{\sqrt{3}}) \\ 1 & -i & -1 & i \end{bmatrix}$$

$$U_3 = \begin{bmatrix} \frac{\sqrt{3}}{2} & 0 & 0 & \frac{1}{2} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \frac{1}{2} & 0 & 0 & -\frac{\sqrt{3}}{2} \end{bmatrix}$$

$$U_3U_2U_1U = \frac{1}{2}\begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}}(1-i) & \sqrt{2} & \frac{1}{\sqrt{2}}(1+i) \\ 0 & \frac{1}{\sqrt{2}}(\sqrt{3}+\frac{i}{\sqrt{3}}) & -\sqrt{\frac{2}{3}} & \frac{1}{\sqrt{2}}(\sqrt{3}-\frac{i}{\sqrt{3}}) \\ 0 & i\frac{2}{\sqrt{3}} & \frac{2}{\sqrt{3}} & -i\frac{2}{\sqrt{3}} \end{bmatrix}$$

$$U_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{\sqrt{3}}{4}(1+i) & \frac{\sqrt{3}}{4}(\sqrt{3}-\frac{i}{\sqrt{3}}) & 0 \\ 0 & \frac{\sqrt{3}}{4}(\sqrt{3}+\frac{i}{\sqrt{3}}) & -\frac{\sqrt{3}}{4}(1-i) & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$U_4U_3U_2U_1U = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \sqrt{\frac{2}{3}} & i\frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} \\ 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}i \\ 0 & \frac{1}{\sqrt{3}}i & \frac{1}{\sqrt{3}} & -\frac{1}{\sqrt{3}}i \end{bmatrix}$$

$$U_5 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \sqrt{\frac{2}{3}} & 0 & -\frac{1}{\sqrt{3}}i \\ 0 & 0 & 1 & 0 \\ 0 & \frac{1}{\sqrt{3}}i & 0 & -\sqrt{\frac{2}{3}} \end{bmatrix}$$

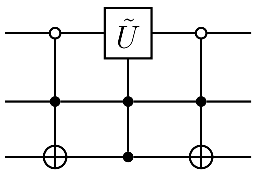
$$U_5U_4U_3U_2U_1U = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & i\frac{1}{\sqrt{2}} \\ 0 & 0 & -\frac{1}{\sqrt{2}} & i\frac{1}{\sqrt{2}} \end{bmatrix}$$

$$U_6 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ 0 & 0 & -i\frac{1}{\sqrt{2}} & -i\frac{1}{\sqrt{2}} \end{bmatrix}$$
$U_6U_5U_4U_3U_2U_1U = I$
Therefore, $U = U_1^\dagger U_2^\dagger U_3^\dagger U_4^\dagger U_5^\dagger U_6^\dagger$.

Exercise 4.38

Exercise 4.39

U acts non-trivially on $|010\rangle$ and $|111\rangle$. Hence, from considering the Gray code $|010\rangle \rightarrow |011\rangle \rightarrow |111\rangle$, we read off the circuit to be,



Exercise 4.40

$E(R_{\hat{n}}(\alpha), R_{\hat{n}}(\alpha+\beta)) = E(R_{\hat{n}}(\alpha), R_{\hat{n}}(\beta)R_{\hat{n}}(\alpha)) = ||(1-R_{\hat{n}}(\beta))R_{\hat{n}}(\alpha)|\psi\rangle|| = ||(1-e^{-i\beta\hat{n}.\sigma/2})|\psi\rangle|| = \sqrt{\langle\psi|(2-(e^{i\beta\hat{n}.\sigma/2}+e^{-i\beta\hat{n}.\sigma/2}))|\psi\rangle} = \sqrt{\langle\psi|(2-2\cos\frac{\beta}{2})|\psi\rangle} = \sqrt{2-2\cos\frac{\beta}{2}} = |1-e^{i\beta/2}|$
For a small β such that $\alpha+\beta+m\theta = n\theta$ for $m<n$ we have,
$E(R_{\hat{n}}(\alpha), R_{\hat{n}}(\theta)^n) = E(R_{\hat{n}}(\alpha), R_{\hat{n}}(\alpha)R_{\hat{n}}(\beta)R_{\hat{n}}(\theta)^m) = E(I, R_{\hat{n}}(\beta)R_{\hat{n}}(\theta)^m) \le E(I, R_{\hat{n}}(\beta)) + mE(I, R_{\hat{n}}(\theta)^m) = |1-e^{i\beta/2}| + m|1-e^{i\theta/2}|$
As $|\beta|, |\theta| < \delta$ we have that $|1-e^{i\beta/2}| + m|1-e^{i\theta/2}| < \frac{\epsilon}{3}$, hence $E(R_{\hat{n}}(\alpha), R_{\hat{n}}(\theta)^n) < \frac{\epsilon}{3}$.

Exercise 4.41

For an initial state $|00\psi\rangle$ the circuit performs the following,
$|00\psi\rangle \xrightarrow{H_1H_2} \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)|\psi\rangle \xrightarrow{\text{Toffoli}} \frac{1}{2}(|00\psi\rangle + |01\psi\rangle + |10\psi\rangle + |11(X\psi)\rangle) \xrightarrow{S} \frac{1}{2}(|00(S\psi)\rangle + |01(S\psi)\rangle + |10(S\psi)\rangle + |11(SX\psi)\rangle) \xrightarrow{\text{Toffoli}} \frac{1}{2}(|00(S\psi)\rangle + |01(S\psi)\rangle + |10(S\psi)\rangle + |11(XSX\psi)\rangle) \xrightarrow{H_1H_2} \frac{1}{4}(((|0\rangle+|1\rangle)(|0\rangle+|1\rangle)+(|0\rangle+|1\rangle)(|0\rangle-|1\rangle)+(|0\rangle-|1\rangle)(|0\rangle+|1\rangle))|S\psi\rangle + \frac{1}{4}(|0\rangle-|1\rangle)(|0\rangle-|1\rangle)|XSX\psi\rangle = \frac{1}{4}(|00\rangle(3S+XSX)|\psi\rangle + (|01\rangle+|10\rangle)(S-XSX)|\psi\rangle + |11\rangle(XSX-S)|\psi\rangle) = \frac{1}{4}(|00\rangle(3S+XSX)|\psi\rangle + (|01\rangle+|10\rangle-|11\rangle)(S-XSX)|\psi\rangle)$
If both measurements give 0 then $\frac{1}{4}(3S+XSX)$ is applied to $|\psi\rangle$.
$\frac{1}{4}(3S+XSX) = \frac{1}{4}\begin{bmatrix} 3+i & 0 \\ 0 & 1+3i \end{bmatrix} = \frac{1}{4}\begin{bmatrix} i(1-3i) & 0 \\ 0 & 1+3i \end{bmatrix} = \frac{\sqrt{10}}{4}e^{i\pi/4}\begin{bmatrix} e^{i\pi/4}e^{-i\arctan 3} & 0 \\ 0 & e^{-i\pi/4}e^{i\arctan 3} \end{bmatrix} = \frac{\sqrt{10}}{4}e^{\pi/4}R_Z(\theta)$,
as $\cos\frac{\theta}{2}\cos(\arctan 3 - \frac{\pi}{4}) = \frac{2}{\sqrt{5}}$, hence $\cos\theta = 2\cos^2\frac{\theta}{2} - 1 = \frac{3}{5}$.
Otherwise, Z is applied, as
$S - XSX = \begin{bmatrix} 1-i & 0 \\ 0 & i-1 \end{bmatrix} = e^{-i\pi/4}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
The final state is $\frac{1}{4}(\sqrt{10}e^{i\pi/4}|00(R_Z(\theta)\psi)\rangle + e^{-i\pi/4}(|01\rangle+|10\rangle-|11\rangle)Z|\psi\rangle)$.
Therefore, $p(|00\rangle) = \left|\frac{\sqrt{10}e^{i\pi/4}}{4}\right| = \frac{5}{8}$.
If anything other then $|00\rangle$ is measured we apply a $-Z$ gate if the measurement is $|11\rangle$ and Z gate otherwise to the last qubit and afterwards apply the circuit again. Then for the

overall circuit,
$p(R_Z(\theta)) = \lim_{n\to+\infty} \sum_n \left(\frac{3}{8}\right)^{n-1} \frac{5}{8} = 1$

Exercise 4.42

1)As θ is rational $\exists m$ such that $m\theta = 2\pi n$, hence raising both sides to the power of this m we have,
$e^{i2\pi n} = \frac{(3+4i)^m}{5^m}$
$1 = \frac{(3+4i)^m}{5^m}$
$(3+4i)^m = 5^m$
2)$3+4i = 3+4i \mod 5$
$(3+4i)^2 = -7+24i = 3+4i \mod 5$
Let us show that if for some a and n we have $a = a \mod n$ and $a^2 = a \mod n$ then $a^m = a \mod n$. For a^3 we have $a^3 = aa^2 = anq_1 + a^2 = n(aq_1+q_2) + a = a \mod n$. Assume true for $m-1$. Then $a^m = aa^{m-1} = anq_1 + a^2 = n(aq_1+q_2) + a = a \mod n$, hence by induction it's true for all $m \in \mathbb{N}$. Therefore, we have that, $(3+4i)^m = 3+4i \mod 5$. Hence, $(3+4i)^m$ is not a multiple of 5, therefore $\nexists m \in \mathbb{N}$ such that, $(3+4i)^m = 5^m$.

Exercise 4.43

The circuit shown in Exercise 4.41 implements an $R_Z(\theta)$ gate with an irrational θ as shown in Exercise 4.42. $HR_Z(\theta)H = R_X(\theta)$, hence we can convert between $R_{\hat{n}}(\theta)$ and $R_Z(\theta)$ as in Exercise 4.6 by only using Hadamard, phase and Toffoli gates. Hence, in accordance with equation 4.76 we have $E(R_Z(\alpha), R_Z(\theta)^n) = E(R_{\hat{n}}(\alpha), R_{\hat{n}}(\theta)^n) < \frac{\epsilon}{3}$. Therefore, Hadamard, phase, CNOT and Toffoli gates are universal for quantum computation.

Exercise 4.44

Exercise 4.45

Exercise 4.46

ρ is a complex $2^n x 2^n$ hermitian matrix with trace 1. There are $2 * 2^{2n}$ real components. The diagonal has to be real so we get $2 * 2^{2n} - 2^n$. As the matrix is hermitian only half of the components other then the diagonal elements are independent, hence the number of components is $2*2^{2n} - 2^n - (2 * \frac{2^{2n}-2^n}{2}) = 4^n$. The trace being 1 fixes one of the diagonal elements, hence the number of independent real components is $4^n - 1$.

Exercise 4.47

If $[A,B] = 0$
$$e^{A+B} = \sum_{n=0}^{\infty} \frac{(A+B)^n}{n!} = \sum_{n=0}^{\infty}\sum_{k=0}^{n} \binom{n}{k} \frac{A^{n-k}B^k}{n!} = \sum_{n=0}^{\infty}\sum_{k=0}^{n} \frac{A^{n-k}B^k}{(n-k)!k!} = \sum_{k=0}^{\infty}\sum_{n=k}^{\infty} \frac{A^{n-k}B^k}{(n-k)!k!} = \sum_{k=0}^{\infty}\sum_{n-k=0}^{\infty} \frac{A^{n-k}B^k}{(n-k)!k!} = e^A e^B$$
Hence, applying this to e^{-iHt} we get the desired result.

Exercise 4.48

$$L \leq \sum_{i=0}^{n} \binom{n}{i} < c\binom{n}{c} = c\frac{n!}{(n-c)!c!} = c\frac{n(n-1)\dots(n-c+1)}{c!} = O(n^c)$$

Exercise 4.49

$e^{(A+B)\Delta t} = 1 + (A+B)\Delta t + \frac{1}{2}(A+B)^2\Delta t^2 + O(\Delta t^3) = 1 + (A+B)\Delta t + \frac{1}{2}(A^2 + B^2 + AB + BA)\Delta t^2 + O(\Delta t^3) = 1 + (A+B)\Delta t + \frac{1}{2}(A^2 + B^2 + 2AB - (AB - BA))\Delta t^2 + O(\Delta t^3) = e^{A\Delta t}e^{B\Delta t}e^{-\frac{1}{2}[A,B]\Delta t^2} + O(\Delta t^3)$

$e^{i(A+B)\Delta t} = 1 + i(A+B)\Delta t + O(\Delta t^2) = e^{iA\Delta t}e^{iB\Delta t} + O(\Delta t^2)$

$e^{i(A+B)\Delta t} = 1 + i(A+B)\Delta t - \frac{1}{2}(A^2 + B^2 + AB + BA)\Delta t^2 + O(\Delta t^3) = 1 + i(\frac{1}{2}A + B + \frac{1}{2}A)\Delta t - (\frac{1}{4}A^2 + \frac{1}{2}B^2 + \frac{1}{4}AB + \frac{1}{4}BA)\Delta t^2 + O(\Delta t^3) = e^{iA\Delta t/2}e^{iB\Delta t}e^{A\Delta t/2} + O(\Delta t^3)$