1. **Linear algebra review: Hermitian and unitary matrices.**

   Recall that a matrix $H$ is called **Hermitian** if $H = H^\dagger$ (where $\dagger$ denotes the conjugate transpose), and a matrix $U$ is called **unitary** if $U^\dagger = U^{-1}$, the matrix inverse of $U$. The **matrix exponential** is defined by its Taylor series as $\exp(A) = \sum_{j=0}^{\infty} A^j/j!$.

   (a) [3 points] Prove that if $H$ is Hermitian, then its eigenvalues are real.

   **Solution:** A Hermitian matrix is normal, so by the spectral theorem, there exists a unitary matrix $V$ and a diagonal matrix $D$ such that $H = VDV^\dagger$. We have $H^\dagger = (VDV^\dagger)^\dagger = VDV^\dagger$, so $D = D^\dagger$. Therefore the diagonal entries of $D$ (which are the eigenvalues of $H$) are unchanged by complex conjugation, i.e., they are real.

   (b) [7 points] Prove that if $H$ is Hermitian, then $\exp(iH)$ is unitary.

   **Solution:** Using the decomposition in the previous part, observe that $(VDV^\dagger)^j = VD^jV^\dagger$, so

   $$\exp(iH) = \sum_{j=0}^{\infty} \frac{(iVDV^\dagger)^j}{j!} = \sum_{j=0}^{\infty} \frac{(iD)^j}{j!} V^\dagger = V \exp(iD)V^\dagger.$$ 

   Therefore

   $$\exp(iH)\exp(iH)^\dagger = V \exp(iD)V^\dagger V \exp(iD)^\dagger V^\dagger = V \exp(iD)\exp(iD)^\dagger V^\dagger.$$

   Since $D$ is diagonal, we see that $\exp(iD)$ is simply a diagonal matrix in which the diagonal entry $d$ of $D$ is replaced by $\exp(id)$. Therefore the corresponding entry of $\exp(iD)\exp(iD)^\dagger$ is $\exp(id)\exp(-id) = 1$, i.e., $\exp(iD)\exp(-iD) = I$. But therefore $\exp(iH)\exp(iH)^\dagger = I$, so $\exp(iH)^\dagger$ is the inverse of $\exp(iH)$, which is therefore unitary.

   (Hint: Use the spectral theorem.)

2. **Mach-Zehnder interferometer with a phase shift.**
Analyze the experiment depicted above using the mathematical model described in class. (Note that the model from class differs slightly from the model described in the textbook; in particular, you should use the matrix $\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ to model the beamsplitters.)

(a) [6 points] Compute the quantum state of the system just before reaching the detectors. Express your answer using Dirac notation.

**Solution:** We represent the photon being on the lower horizontal path and the right vertical path by $|0\rangle$, and the photon being on the left vertical path and the top horizontal path by $|1\rangle$. The initial state $|0\rangle$ evolves as follows:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

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

$$\mapsto \begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 + e^{i\varphi} \\ 1 \end{pmatrix}$$

$$\mapsto \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 + e^{i\varphi} \\ 1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 + e^{i\varphi} + 1 - e^{i\varphi} \\ 1 \end{pmatrix}$$

$$= \frac{1 + e^{i\varphi}}{2} |0\rangle + \frac{1 - e^{i\varphi}}{2} |1\rangle.$$

(b) [4 points] Compute the probability that the “0” detector clicks as a function of $\varphi$, and plot your result for $\varphi \in [0, 2\pi]$.

**Solution:** The desired probability is

$$\Pr(0) = \left| \frac{1 + e^{i\varphi}}{2} \right|^2$$

$$= \frac{1}{4} (1 + e^{i\varphi} + e^{-i\varphi} + 1)$$

$$= \frac{1}{2} (1 + \cos \varphi)$$

$$= \cos^2 \frac{\varphi}{2}.$$

Plotting this gives the following:
3. **Universality of reversible logic gates.**

The CCCNOT (triple-controlled NOT) gate is a four-bit reversible gate that flips its fourth bit if and only if the first three bits are all in the state 1.

(a) [5 points] Show how to compute CCCNOT using AND, OR, NOT and FANOUT gates.

**Solution:**

\[
\begin{align*}
\text{CCCNOT:} & \quad x_1 \quad x_2 \quad x_3 \quad x_4 \\
& \quad (x_1 \land x_2 \land x_3) \oplus x_4
\end{align*}
\]

(b) [5 points] Show how to implement a CCCNOT gate using Toffoli gates. You may use additional workspace as needed. You may assume that bits in the workspace start with a particular value, either 0 or 1, provided you return them to that value.

**Solution:** The following circuit shows a simple construction using one bit of workspace in the 0 state:

\[
\begin{align*}
\text{Solution:} & \quad \text{The first gate computes the AND of the first two bits in the fifth (workspace) bit. The second gate computes the AND of the third and fifth bits (i.e., the AND of the first three bits) in the fourth (target) bit. The final gate uncomputes the value in the workspace.}
\end{align*}
\]

4. **Computing reversibly.**

The function EQ: \(\{0,1\}^3 \rightarrow \{0,1\}\) determines whether its three input bits are equal, namely

\[
\text{EQ}(x, y, z) = \begin{cases} 
1 & \text{if } x = y = z \\
0 & \text{otherwise.}
\end{cases}
\]

(a) [5 points] Show how to compute the function EQ using AND, OR, NOT, and FANOUT gates.

**Solution:** We have \(\text{EQ}(x, y, z) = \text{OR}(\text{AND}(x, y, z), \text{AND}(\text{NOT}(x), \text{NOT}(y), \text{NOT}(z)))\), so the
following circuit computes $E\!Q(x, y, z)$.

(b) [5 points] Show how to compute the function $E\!Q$ reversibly using Toffoli gates. You may use ancilla bits initialized to either 0 or 1 provided you return them to that value. You may use gates other than Toffoli gates provided you explain how to implement any such gates using Toffoli gates.

**Solution:** We can easily convert the AND and OR gates to multiply-controlled NOT gates (using De Morgan’s laws to express OR in terms of AND and NOT gates), giving the following circuit.

To erase the junk bits, we copy the result into another register and perform the computation in reverse, giving the following circuit.

Finally, we can express the CCCNOT gates in terms of Toffoli gates using any of the constructions from problem 3b, and we can easily express the NOT and CNOT gates using ancilla bits set to 1).

Note that this solution is far from unique, and could probably be optimized to use many fewer gates.

5. **Pauli operators.**

(a) [3 points] Express each of the three Pauli operators,

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$
using Dirac notation in the computational basis.

**Solution:**

\[
X = |0\rangle\langle 1| + |1\rangle\langle 0|, \quad Y = -i|0\rangle\langle 1| + i|1\rangle\langle 0|, \quad Z = |0\rangle\langle 0| - |1\rangle\langle 1|
\]

(b) [3 points] Find the eigenvalues and the corresponding eigenvectors of each Pauli operator. Express the eigenvectors using Dirac notation.

**Solution:** All three operators have eigenvalues \( \pm 1 \). They are as follows:

\[
\begin{array}{ccc}
\text{operator} & +1 \text{ eigenvector} & -1 \text{ eigenvector} \\
X & |0\rangle + |1\rangle & |0\rangle - |1\rangle \\
Y & |0\rangle + i|1\rangle & |0\rangle - i|1\rangle \\
Z & |0\rangle & |1\rangle
\end{array}
\]

(c) [2 points] Write the operator \( X \otimes Z \) as a matrix and using Dirac notation (in both cases using the computational basis).

**Solution:**

\[
X \otimes Z = \begin{pmatrix}
0 & 0 & 1 & 0 \\
0 & 0 & 0 & -1 \\
1 & 0 & 0 & 0 \\
0 & -1 & 0 & 0
\end{pmatrix} = |10\rangle\langle 00| - |11\rangle\langle 01| + |00\rangle\langle 10| - |01\rangle\langle 11|
\]

(d) [2 points] What are the eigenspaces of the operator \( X \otimes Z \)? Express them using Dirac notation.

**Solution:** We can obtain eigenvectors of \( X \otimes Z \) by taking tensor products of the eigenvectors of \( X \) and of \( Z \). Since this gives a basis for the entire four-dimensional space, we can find bases for all the eigenspaces in this way. The corresponding products of eigenvalues of \( X \) and of \( Z \) give the eigenvalues of \( X \otimes Z \), which are \( \pm 1 \). The +1 eigenspace is

\[
\text{span}\{(|0\rangle + |1\rangle) \otimes |0\rangle, (|0\rangle - |1\rangle) \otimes |1\rangle\}
\]

and the -1 eigenspace is

\[
\text{span}\{(|0\rangle + |1\rangle) \otimes |1\rangle, (|0\rangle - |1\rangle) \otimes |0\rangle\}.
\]

**Total points:** 50