1. In the Deutsch-Josza problem, the oracle \( f \) was assumed to be either constant (\( f \equiv 0 \) or \( f \equiv 1 \)) or balanced, meaning that exactly half of the inputs give the value 1. Suppose that \( f \) were not perfectly balanced, but only approximately balanced, giving a value of 1 on \( k \) extra values (beyond the expected half of the inputs).

(a) Assuming that \( f \) takes \( n \) bits as input (so there are \( 2^n \) possible inputs), what is the probability that measurement at the end of the Deutsch-Josza circuit gives a result of 0? \( \text{Hint:} \) you should not need to redo any of the analysis from lecture except the final measurement probability calculation. Note, however, that the slides have an error in that calculation, writing \( 2^{n/2} \) when it should say \( 2^{n-1} \).

(b) What is the largest that \( k \) can be while the algorithm still fails less than 1/3 of the time? What is this amount as a percentage of the inputs?

2. In this problem, we will look at the how to implement the quantum Fourier transform \( F \) used, for example, in our phase estimation algorithm.

(a) Write out the matrix for the quantum Fourier transform on 1 qubit, \( F^1 \).

(b) What is other (more familiar) name for the matrix from part (a)?

(c) Write out the matrix for the quantum Fourier transform on 2 qubits, \( F^2 \). The formula for \( F \) assumes that the states are numbers \( 0, 1, \ldots, 2^n - 1 \), but recall that we can identify numbers with their corresponding binary representation: \( 00 = 0, 01 = 1, 10 = 2, 11 = 3 \).

(d) Let \( Z_k \) be the matrix defined by

\[
Z_k := \begin{bmatrix}
1 & 0 \\
0 & e^{2\pi i/2^k}
\end{bmatrix}
\]

What is the other (more familiar) name for \( Z_1 \)? What is the matrix for \( Z_2 \)?

(e) Verify that the following circuit implements \( F_2 \):

\[
\text{\begin{align*}
F^1 & \quad Z \quad F^1 \\
\text{swap} & \quad F^1
\end{align*}}
\]

\text{\textbf{Hint:} it is sufficient to calculate the result of the circuit for} \( |00\rangle, |01\rangle, |10\rangle, |11\rangle \) and verify that they match those from the matrix in part (b).

In part (e), above, we showed that \( F_2 = (I \otimes F^1)[CZ_2]_{2,1}(F^1 \otimes I) \) followed by a reversal of the bits. In general, it can be shown that \( F_n = (I \otimes F^1)[CZ_n]_{n,1}[CZ_{n-1}]_{n,2} \cdots [CZ_2]_{n,n-1}(F_{n-1} \otimes I) \) followed by a reversal of all the qubits. (See the textbook for a proof.) This recursive formula makes it fairly easy to draw circuits for \( F_3, F_4, \) and so on.
3. Lecture 19, on diagrammatic reasoning, included the following claim:

Prove, from the linear algebra definitions, that this claim is true assuming that the wire represents a single qubit and

\[ U = \begin{bmatrix} a & b \\ c & d \end{bmatrix}. \]

**Hint:** recall that the cup shape is shorthand for a “prepare” followed by a “copy”, both operations that were defined via linear algebra in the lecture slides.

4. In lecture, we discussed matrices formed by multiplying one of \{I, X, Z, XZ\} by one of \{1, -1, i, -i\}. These sixteen matrices are called the “Pauli group”. Show that the inverse of any matrix in the Pauli group is another matrix in the Pauli group.

**Hint:** note that all of these matrices are unitary.

Suppose that we want to measure our state \(|\phi\rangle\) to see if we get the result \(x\) (e.g., \(x\) could be 010 if this is a 3-qubit state). In lecture, we learned that the probability of this occurring is \(|c|^2\), where \(c\) is the coefficient of \(|x\rangle\) in the vector \(|\phi\rangle\). Since \(c = \langle x|\phi\rangle\), we can also write this as

\[
|c|^2 = c^*c = \langle x|\phi\rangle \langle \langle x|\phi\rangle \rangle = \langle x|\phi\rangle \langle x|\phi\rangle = \text{tr}(\langle x|\phi\rangle \langle x|\phi\rangle) = \text{tr}(\langle \phi|\phi\rangle |x\rangle \langle x|) = \text{tr}(\langle \phi|\phi\rangle |x\rangle \langle x|)
\]

where we have used the fact that \(\text{tr}(a) = a\), when \(a\) is just a number, and the cyclical property of the trace (i.e., that \(\text{tr}(AB) = \text{tr}(BA)\)), proven in lecture.

5. Suppose that we have a mixed state that is state \(|\phi\rangle\) with probability \(p\) and state \(|\xi\rangle\) with probability \(1 - p\). Define the matrix \(\rho = p|\phi\rangle\langle \phi| + (1 - p)|\xi\rangle\langle \xi|\). Prove that \(\text{tr}(\rho |x\rangle \langle x|)\) is the probability that we get the result \(x\) when measuring this mixed state.

**Hint:** use the properties of trace, in particular, the fact that it is a linear mapping.

A matrix like \(\rho\) above is called a **density matrix**. It is an alternative way of representing a mixed state. A pure state like \(|\phi\rangle\) has a corresponding density matrix \(|\phi\rangle\langle \phi|\) with rank 1.

6. Consider a mixed qubit state that is \(|\phi\rangle\) or some orthogonal state \(|\phi^\perp\rangle\), each with probability \(1/2\). These are called “completely mixed” states. Prove that the density matrices corresponding to all completely mixed qubit states are the same. Identify that density matrix.

**Hint:** define \(V = |\phi\rangle\langle 0| + |\phi^\perp\rangle\langle 1|\), representing a change of basis from \(|0\rangle\) and \(|1\rangle\) to \(|\phi\rangle\) and \(|\phi^\perp\rangle\), respectively. Write \(|\phi\rangle = V |0\rangle\) and \(|\phi^\perp\rangle = V |1\rangle\) and then calculate the density matrix.

---

\(^1\)Actually, the slides said \(U^\dagger\) rather than \(U^T\), but the latter is correct.
Problem 6 and the calculation prior to it showed that we can calculate a measurement probability for a pure or mixed state using just the density matrix. If our density matrix is \( \rho \), then the probability of measuring \( x \) is given by \( \text{tr}(\rho |x\rangle \langle x|) \).

It is also possible to calculate the density matrix representing the mixed state that results from applying a unitary \( U \) to an initial mixed state. In our example above, we would have \( U |\phi\rangle \) with probability \( p \) and \( U |\xi\rangle \) with probability \( 1 - p \), and the corresponding density matrix would be

\[
p(U |\phi\rangle)(U |\phi\rangle)^\dagger + (1 - p)(U |\xi\rangle)(U |\xi\rangle)^\dagger = p U |\phi\rangle \langle \phi | U^\dagger + (1 - p) U |\xi\rangle \langle \xi | U^\dagger = U \rho U^\dagger
\]

Hence, if we start in a mixed state with density matrix \( \rho \), then the mixed state we get after applying \( U \) to our state has a density matrix of \( U \rho U^\dagger \).

7. Explain why all completely mixed qubit states are indistinguishable from one another.

\textbf{Hint:} Use your answers to Problem 5 and 6 along with the comments, just above, about how unitary operations change density matrices.