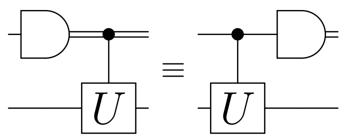
Assignment 2
Due date: 11:59pm, October 17, 2023

1. **Measuring the control qubit of a CNOT gate [10 points].** Let U be an arbitrary unitary, and consider these two procedures: (a) measure the control qubit in the computational basis and then perform a classically controlled-U; (b) perform a controlled-U and then measure the control qubit in the computational basis. Show that, for any 2-qubit input state, $\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$, the result of these two procedures is exactly the same:



In each case, the measurement outcome and residual state can be expressed as

$$\begin{cases} (0,\, |\psi_0\rangle) & \text{with probability } p_0 \\ (1,\, |\psi_1\rangle) & \text{with probability } p_1, \end{cases}$$

and you should show that p_0, p_1, $|\psi_0\rangle$, $|\psi_1\rangle$ are the same for both procedures.

2. **Distinguishing between pairs of unitaries [15 points, 5 each].** In each case, you are given a black box gate that computes one of the two given unitaries, but you are not told which one. It is chosen uniformly: each is selected with probability $\frac{1}{2}$. Your goal is to guess which of the two unitaries it is with as high a probability as you can. To help you do this, you can create any one-qubit quantum state, apply the black box gate to this qubit, and then measure the answer in some basis (that is, you can apply a unitary of your choosing and then measure in the computational basis). You can only use the black-box gate once.

   For example, consider the case where the two unitaries are $I = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $Z = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. In this case, setting the initial state to $|+\rangle$, applying the black-box unitary, followed by H and measuring yields 0 in the first case and 1 in the second case. So this is a perfect distinguishing procedure (it succeeds with probability 1).

   Give the best distinguishing procedure (i.e., highest success probability) you can find in each case below. You do not have to prove optimality.

   (a) I and $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$.

   (b) H and $\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}$ (the latter is a rotation by $\pi/4$).

   (c) I and $\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}$.

   (Hint: in two out of the above three cases there is a perfect distinguishing procedure.)

3. **Classical and quantum algorithms for the AND problem [20 points; 4 each].** In these next two questions, we consider the AND problem, where we are given as input a black box for a function $f : \{0,1\} \to \{0,1\}$ and the goal is to determine $f(0) \wedge f(1)$ (the logical AND of $f(0)$ and $f(1)$) with a *single* query to f.

   Note that it's easy to achieve *average-case success probability* $3/4$ without making *any* queries. This is because, for three of the four functions f, it holds that $f(0) \wedge f(1) = 0$. Therefore always outputting 0 succeeds with probability $3/4$ for a (uniformly distributed) randomly chosen input f.

   But here we are interested in methods that perform well for *worst-case* instances of f.

   (a) Give a classical probabilistic algorithm that makes a single query to f and predicts $f(0) \wedge f(1)$ with probability $2/3$. The probability is respect to the random choices of the algorithm; the input instance f is assumed to be arbitrary (worst-case).

   It turns out that no classical algorithm can succeed with probability greater than $2/3$ (but you are not required to show this here).

   (b) Give a quantum circuit that, with a single query to f, constructs the two-qubit state

$$\tfrac{1}{\sqrt{3}}\left((-1)^{f(0)}|00\rangle + (-1)^{f(1)}|01\rangle + |11\rangle\right).$$

   (Hints: First construct a circuit for $\frac{1}{\sqrt{3}}\left((-1)^{f(0)}|00\rangle + (-1)^{f(1)}|01\rangle + (-1)^{f(1)}|11\rangle\right)$. The gate

$$\begin{bmatrix} \sqrt{1/3} & \sqrt{2/3} \\ \sqrt{2/3} & -\sqrt{1/3} \end{bmatrix} \tag{1}$$

   and the controlled-Hadamard gate might be helpful for this. Next think about how to "supress" the phase for $|11\rangle$.)

   (c) The quantum states of the form in part (b) are three-dimensional and have real-valued amplitudes. This makes it easy for us to visualize the geometry of these four states (one for each possible f) as vectors (or lines) in $\mathbb{R}^3$. What is the absolute value of the inner product between each pair of these four states?

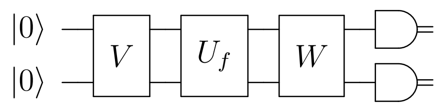
   (d) Based on the results of parts (b) and (c), give a quantum algorithm for the AND problem that makes a single query to f and succeeds with probability

$$\begin{cases} 1 & \text{whenever } f(0) \wedge f(1) = 1 \\ 8/9 & \text{whenever } f(0) \wedge f(1) = 0. \end{cases} \tag{2}$$

   (e) Note that the error probability of the algorithm from part (d) is one-sided in the sense that it is always correct in the case where $f(0) \wedge f(1) = 1$. Assuming the result in part (d), give a quantum algorithm for the AND problem that makes a single query to f and succeeds with probability $9/10$ in all four cases. (Hint: take the output of the one-sided error algorithm from part (d) and do some classical post-processing on it, in order to turn it into a two-sided error algorithm with higher success probability.)

   Note: Each part above can be tackled independently (e.g. you don't have to solve (b) in order to be able to solve (c), etc).

4. **Can a function be evaluated at two distinct points with one quantum query? [15 points; 5 each].** Here we consider the problem where we have a query oracle for a function $f : \{0,1\} \to \{0,1\}$ and show that it is impossible to obtain the values of both $f(0)$ and $f(1)$ with a single query. We assume that the query oracle is in the usual form of a unitary operator U_f that, for all $a, b \in \{0,1\}$, maps $|a\rangle|b\rangle$ to $|a\rangle|b \oplus f(a)\rangle$. For simplicity, we consider methods that employ only two qubits in all and are expressible by a circuit of the form



where V and W are two-qubit unitaries and the D-shaped gates are measurements in the computational basis. Therefore, it can be assumed that the input state to the query is a two-qubit state of the form $\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$.

   (a) For each of the four functions of the form $f : \{0,1\} \to \{0,1\}$, give the quantum state right after the query has been performed.

   (b) If there is a measurement procedure that perfectly distinguishes between the four states in part (a) then they must be mutually orthogonal. Show that, for a measurement to be able to perfectly determine the value of $f(0)$, it must be the case that $\alpha_{10} = \alpha_{11}$. (Hint: think of the orthogonality relationships that need to hold.)

   (c) Show that, if the states corresponding to the four functions are such that $f(0)$ can be determined perfectly from them, then $f(1)$ cannot be determined with probability any better than 1/2 (i.e., no better than random guessing). (Hint: You may use the result in part (b) for this.)

5. **(This is an optional question for bonus credit)**
   Distinguishing among three qutrit states [6 points].
   The analysis for question 4 is restricted to methods that use two qubits. Show that, for all $m \geq 2$, any strategy that uses m qubits (where V and W are m-qubit unitaries and the query gate U_f acts on the last two qubits) and determines $f(0)$ perfectly cannot determine $f(1)$ with probability any better than 1/2.