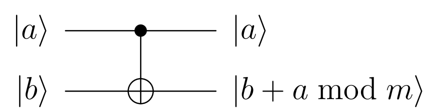
Assignment 3 [question 3(c) revised]
Due date: 11:59pm, October 27, 2022

1. **A simple collision-finding problem [15 points].** Call $f : \{0,1\}^2 \to \{0,1\}$ a *two-to-one function* if there are exactly two $a \in \{0,1\}^2$ such that $f(a) = 0$ and exactly two $a \in \{0,1\}^2$ such that $f(a) = 1$. Consider the problem where one is given such a function as a black-box and the goal is to find a *collision*, which is a pair $a, b \in \{0,1\}^2$ such that $a \neq b$ and $f(a) = f(b)$.

   (a) [3 points] How many queries to f does a *classical* algorithm require to find a collision? The algorithm must always succeed (the error probability for any run should be 0).

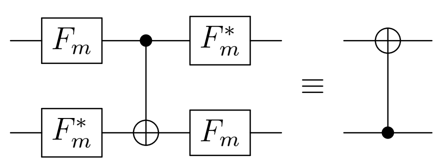
   (b) [12 points] Show how to solve this problem by a *quantum* algorithm that makes one single query to f. The algorithm must always succeed (the error probability for any run should be 0).

2. **Control-target inversion for mod m registers [15 points].** Consider a scenario where the registers are m-dimensional ($m \geq 2$). Let the computational basis states be $|0\rangle, |1\rangle, \ldots, |m-1\rangle$. Define the two-register *addition (mod m)* gate as the unitary operation that acts on the computational basis states as



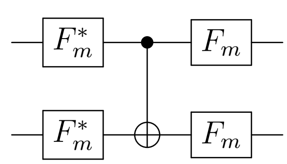
   (where $a, b \in \mathbb{Z}_m$). In the above circuit diagram, each wire represents an m-dimensional system (a qubit in the special case where $m = 2$).

   (a) [9 points] Prove that, for any $m \geq 2$, the following circuit equivalence holds:



   where F_m is the $m \times m$ Fourier transform.

   (b) [6 points] Consider the following circuit diagram where the F_m and F_m^* are arranged in a slightly different way:



   Give a simple expression for what the circuit does to computational basis states $|a\rangle|b\rangle$ (for $a, b \in \mathbb{Z}_m$). There is a very simple expression.

3. **Computing F_{pq} in terms of F_p and F_q [15 points].** Our construction of F_{2^n} is in terms of n computations of F_2 (Hadamard gates) with phase adjustment gates inserted between these F_2 gates. For the case where $m = p_1 p_2 \cdots p_k$, where p_1, p_2, …, p_k are distinct primes, there is a construction of F_m in terms of F_{p_1}, F_{p_2}, …, F_{p_m} that doesn't require any phase adjustments. The idea is that F_m is the same matrix as $F_{p_1} \otimes F_{p_2} \otimes \cdots \otimes F_{p_k}$ up to a reordering of the rows and columns. Here we explore a simple case of this.

   (a) [3 points] Write out the 6×6 matrix of F_6, the 3×3 matrix of F_3, and the 2×2 matrix of F_2.

   (b) [4] Write out the 6×6 matrix of $F_2 \otimes F_3$.

   (c) [8] Show that there exist 6×6 permutation matrices P and Q such that

   $$F_6 = P(F_2 \otimes F_3)Q, \tag{1}$$

   where a permutation a matrix has exactly one 1 in each row, and in each column, and all other entries are 0.

   (In fact, this generalizes to $F_{m_1 m_2} = P(F_{m_1} \otimes F_{m_2})Q$ whenever m_1 and m_2 are relatively prime, but you are not asked to show this more general result.)

4. **Computing the "square root" of a quantum circuit [15 points].** Suppose that you are given a quantum circuit acting on n qubits consisting of m 2-qubit gates. It corresponds to *some* $2^n \times 2^n$ unitary matrix U, but, in general, there is no way of efficiently calculating all the entries of U from the circuit. Suppose that we want to construct another circuit that computes a square root of U (i.e., a unitary V such that $V^2 = U$). You can check that just taking the square root of each individual gate in the original circuit U does not yield such a V.

   We will use a clever trick involving the eigenvalue-estimation algorithm to do this efficiently. We just consider a simplified case where we are *promised* that all the eigenvalues of U are in $\{+1, -1\}$; however, the basic approach can be extended to the arbitrary case.

   If the eigenvalues of U are assumed to be in $\{+1, -1\}$, there exists a unitary matrix W such that $U = W^* D W$, where D is a diagonal matrix of the form

   $$D = \begin{pmatrix} (-1)^{d_0} & 0 & \cdots & 0 \\ 0 & (-1)^{d_1} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & (-1)^{d_{2^n-1}} \end{pmatrix} \tag{2}$$

   for some $d_0, d_1, \ldots, d_{2^n-1} \in \{0, 1\}$. It's easy to see that a square root of D is

   $$\begin{pmatrix} i^{\,d_0} & 0 & \cdots & 0 \\ 0 & i^{\,d_1} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & i^{\,d_{2^n-1}} \end{pmatrix}, \tag{3}$$

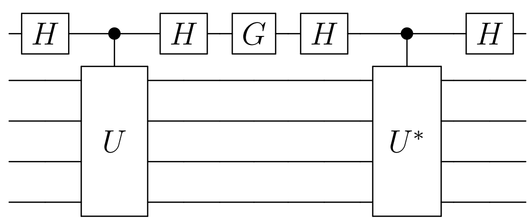
   where $i = \sqrt{-1}$.

Now, assume that we're given a circuit computing U with m 2-qubit gates and are promised that the eigenvalues of U are all in $\{+1, -1\}$. To be clear, although the aforementioned W and D exist mathematically, the circuit for U that we're given is not in the form of a composition separate circuits for W^*, D, W; our circuit is just some jumble of 2-qubit gates.

(a) [3 points] Explain how, given a circuit for U consisting of m 2-qubit gates, we can construct a circuit for a controlled-U and a controlled-U^*, where each consists of m 3-qubit gates. (These could be converted to circuits consisting of $O(m)$ 2-qubit gates, but you are not asked to show that.)

(b) [3 points] Prove that, for all $k \in \{0,1\}^n \equiv \{0, 1, \ldots, 2^n - 1\}$, the vector $W^*|k\rangle$ is an eigenvector of U with eigenvalue $(-1)^{d_k}$. (W is as explained on the previous page.)

(c) [6 points] Consider this quantum circuit that we'll refer to as C (where the 1-qubit gate G is yet to be determined):



Notice that this circuit begins as a circuit for phase estimation, followed by a 1-qubit gate G, followed by the inverse of the phase estimation circuit. Of course, if we were to set $G = I$ then the above circuit would just compute the identity operation on $n + 1$ qubits. Choosing the right setting for G will make the circuit interesting.

Show how to set the 1-qubit gate G so that, for all $k \in \{0, 1, \ldots, 2^n - 1\}$,

$$C\big(|0\rangle \otimes (W^*|k\rangle)\big) = |0\rangle \otimes (i^{d_k}\, W^*|k\rangle) \tag{4}$$

(where $i = \sqrt{-1}$). Include an explanation of why your choice of G works.

(d) [3 points] Explain why Eq. (4) from part (c) implies that, for some unitary V such that $V^2 = U$, it holds that, for all n-qubit states $|\psi\rangle$,

$$C\big(|0\rangle \otimes |\psi\rangle\big) = |0\rangle \otimes \big(V|\psi\rangle\big). \tag{5}$$

5. **(This is an optional question for bonus credit)**
Fully identifying a function $f : \{0,1\} \to \{0,1\}$ **[6 points].** Recall that, in Deutsch's problem, we are given a black-box for an arbitrary function $f : \{0,1\} \to \{0,1\}$, but we are not required to fully identify which of the four possible functions f is. Here we consider the problem where the goal is to correctly guess which of the four functions f is.

It's easy to deduce that, with a single *classical* f-query, the best success probability achievable is $\frac{1}{2}$.

Give a *quantum* algorithm that makes a single f-query and correctly guesses f with success probability $\frac{3}{4}$. Assume that the f is a worst-case instance for your algorithm.

(Warning: this might be more challenging than the two previous bonus questions.)