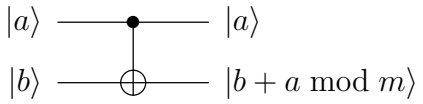
Assignment 4

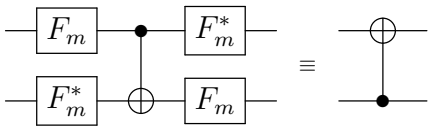
Due: 11:59pm, November 9, 2026

1. **Control-target inversion for mod m registers [12 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



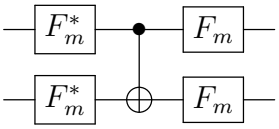
(where $a, b \in \mathbb{Z}_m$). In the above circuit diagram, each wire represents an m-dimensional system (a qubit in the special case where $m = 2$).

   (a) [8 points] Prove that, for every $m \geq 2$, the following circuit equivalence holds:



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

   (b) [4 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.

2. **A simple variant of the phase estimation problem [12 points].**

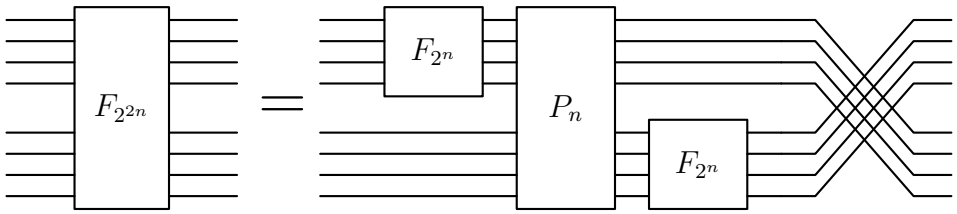
   Suppose that you're given a two-qubit gate that is a controlled-U gate, for some unknown one-qubit unitary U. You are given this gate as a black box and you are also given a qubit whose state is *promised* to be an eigenvector of U, with eigenvalue either $\lambda_1 = e^{2\pi i/3}$ or $\lambda_2 = e^{4\pi i/3}$ (you don't know which case it is). Your goal is to determine whether the eigenvalue is λ_1 or λ_2.

   Show how this can be accomplished *exactly* (with success probability 1) with *two* queries to the controlled-U gate. Of course, you may also use other gates of your choosing (that are independent of U and the state of the qubit, which you do not know).

3. **Another construction of the quantum Fourier transform [12 points].** Here we consider another, recursive, construction of F_{2^n}, the quantum Fourier transform on n qubits. This construction works if n is a power of 2. The base case of the recursion is where $n = 1$, in which case $F_{2^n} = H$. Suppose that we have an implementation of F_{2^n} and want to implement $F_{2^{2n}}$. Divide the $2n$ qubits into two registers: the first n qubits, and the last n qubits. Define the unitary P_n on two registers such that

$$P_n|a\rangle|b\rangle = \left(e^{2\pi i/2^{2n}}\right)^{m(a,b)}|a\rangle|b\rangle, \tag{1}$$

for all $a, b \in \{0,1\}^n$, and where $m(a,b)$ denotes the product of a and b as n-bit integers (e.g., 1101 denotes 13, and 0100 denotes 4, so $m(1101, 0100) = 13 \times 4 = 52$). Then the following circuit computes $F_{2^{2n}}$ in terms of two instances of F_{2^n}, P_n, and SWAP gates:



(a) Show that this recursive construction holds for the $n = 1$ case, where $F_{2^2} = F_4$ is computed in terms of two instances of $F_{2^1} = F_2 = H$, one instance of P_1, and a SWAP gate. (Note: F_4 is a 2-qubit unitary.)

(b) Show that this recursive construction holds for the $n = 2$ case, where $F_{2^{2\cdot 2}} = F_{16}$ is computed in terms of two instances of $F_{2^2} = F_4$, one instance of P_2, and two SWAP gates. (Note: F_{16} is a 4-qubit unitary.)

(c) Show that this recursive construction holds for all $n \geq 1$, where $F_{2^{2n}}$ is computed in terms of F_{2^n}, P_n and SWAP gates. (If you answer part (c) correctly, you receive full marks for question 4.)

Note: This approach leads to a construction of F_{2^n} consisting of $O(n \log n)$ gates, but we don't go into further details of this here.

4. **Grover's algorithm for some densities of satisfying inputs [12 points].**

Let $f : \{0,1\}^n \to \{0,1\}$ (where $n \geq 2$). Recall that Grover's algorithm creates the initial state $H|00...0\rangle|-\rangle$ and then iterates the operation $-HU_0HU_f$.

In each case below, determine the state after *one single iteration* of Grover's algorithm. Also, what's the probability that, if this state is measured, the outcome is a satisfying input to f?

(a) The case where f has no satisfying inputs.

(b) The case where f has $\frac{1}{4}2^n$ satisfying inputs.

(c) The case where f has $\frac{3}{4}2^n$ satisfying inputs.

5. **(This is an optional challenge question)**
Search problem for $\frac{3}{4}$ density of satisfying inputs [0 points].

Let $f : \{0,1\}^n \to \{0,1\}$ (where $n \geq 2$) and assume that f has $\frac{3}{4}2^n$ satisfying inputs. Does there exist a quantum algorithm that makes just one f-query and is guaranteed to find a satisfying input? Answer yes or no and justify your answer by: giving such an algorithm (if the answer is yes); or proving that no such algorithm exists (if the answer is no).

(As usual, an f-query is the unitary operation that maps $|x\rangle|y\rangle$ to $|x\rangle|y \oplus f(x)\rangle$, for all $x \in \{0,1\}^n$ and $y \in \{0,1\}$.)

There is a solution that can be explained in less than one page. If you submit a solution to this question then please explain it clearly and do not exceed two pages.