Assignment 3

***Due**: Friday, Apr 1st, 2022 @ 5:00PM*

CPSC 447/547 Introduction to Quantum Computing (Spring 2022)

1 Introduction

Welcome to Assignment 3 for CPSC 447/547 (Introduction to Quantum Computing). As usual, collaboration is encouraged; if you discussed with anyone besides the course staff about the assignment, *please list their names* in your submission.

Getting Started.

This assignment has *only one* part, the *written portion*. Typesetting your solutions to the written portion is not mandatory but highly encouraged. See the instructor's note on Ed for details about Latex for quantum computing. To start,

- Create a folder for Assignment 3, e.g., `A3/`
- Download the starter files for this assignment to that folder from the course website:
  - `A3.pdf`
  - `written.tex`
- Write your solutions in `written.tex`

New Structure.

There are now two types of tasks, *mandatory* or *optional*. *Only the mandatory tasks will be counted towards your final grade for this assignment.* Different from the mandatory tasks, the optional tasks will be marked with "**($\star$ pts)**".

Submission.

Once you have completed and are ready to submit, upload to Canvas: `written.pdf`. Late submissions (for up to two days) will receive a 50% penalty. Your written solution will be graded manually by our course staff.

WRITTEN PORTION
This portion of the assignment has a total of 100 *points.*
Any tasks marked with (⋆ pts) are optional.

2 Quantum Oracles

Task 2.1 (10 pts)

Recall from lecture, we have defined the phase oracle for a function $f : \{0,1\}^n \to \{0,1\}$ as follows:

$$O_f^{\pm} |x\rangle = (-1)^{f(x)} |x\rangle .$$

Suppose we have an oracle to the following function $f : \{0,1\}^2 \to \{0,1\}$:

$$f(x) = \begin{cases} 1, \text{ if } x = 01 \\ 0, \text{ otherwise} \end{cases}$$

Given an input quantum state $|\psi\rangle = \frac{1}{\sqrt{3}}(|00\rangle + |01\rangle + |10\rangle)$. What is its state after applying the phase oracle to $|\psi\rangle$. That is, compute $O_f^{\pm} |\psi\rangle$.

Task 2.2 (15 pts)

What is the unitary matrix for the $O_f^{\pm}$ from the previous question? (Hint: $O_f^{\pm}$ can be viewed as a reflection operator.)

Task 2.3 (⋆ pts)

Give a circuit implementation of the $O_f^{\pm}$ from the previous questions.

Task 2.4 (⋆ pts)

Suppose now we are given an oracle to the following function $f : \{0,1\}^2 \to \{0,1\}$:

$$f(x) = \begin{cases} 1, \text{ if } x = 01 \text{ or } 00 \\ 0, \text{ otherwise} \end{cases}$$

Answer the previous three questions. That is, compute $O_f^{\pm} |\psi\rangle$, write down the unitary matrix for $O_f^{\pm}$, and give a quantum circuit for $O_f^{\pm}$.

3 Simon's Algorithm

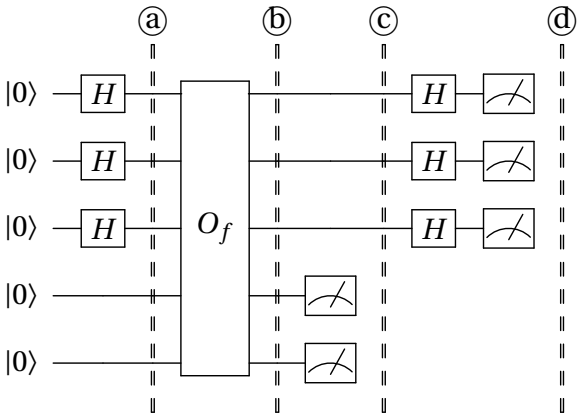
Task 3.1 (20 pts)

In Simon's algorithm, we are given a "periodic", two-to-one function and want to find its period. Let's analyze how this algorithm works for a particular function $f : \{0,1\}^3 \to \{0,1\}^2$, where $f(x + a) = f(x)$ for some unknown period a. Importantly, here addition $(+)$ is a *bit-wise addition modulo 2*. For example, $010 + 011 = 001$. Its truth table looks like this in Table 1.

Input	Output
000	$f(000) = 01$
001	$f(001) = 10$
010	$f(010) = 10$
011	$f(011) = 01$
100	$f(100) = 11$
101	$f(101) = 00$
110	$f(110) = 00$
111	$f(111) = 11$

Table 1: Truth table of function f.

We have colored the output so that you can visually inspect the period easily. In Simon's algorithm, we use the following quantum circuit to find the period:



We have labeled four important time steps in the quantum circuit. Answer the following questions.

(a) Visually inspecting the whole truth table in Table 1. What is the period a, such that $f(x+a) = f(x)$ for all inputs x?

(b) What is the quantum state at time step ⓐ, i.e., after $H^{\otimes 3}$?

(c) What is the quantum state at time step ⓑ, i.e., after the oracle O_f?

(d) What is the quantum state at time step ⓒ, i.e., after measuring the bottom two qubits, given that the measurement outcome is 01? Please write your answer in the form of $(\alpha_{000}|000\rangle + \alpha_{001}|001\rangle + \alpha_{010}|010\rangle + \alpha_{011}|011\rangle + \alpha_{100}|100\rangle + \alpha_{101}|101\rangle + \alpha_{110}|110\rangle + \alpha_{111}|111\rangle) \otimes |01\rangle$ with the appropriate values for α_i. Here we assume top qubit in the circuit is the most-significant bit in the state, that is $|x\rangle = |x_2 x_1 x_0\rangle$, $x = \sum_s x_s 2^s$, and $|x_2\rangle$ is the top qubit.

(e) What are the possible measurement outcomes at time step ⓓ? Write down all possible outcomes and their associated probabilities.

Task 3.2 (⋆ pts)

Following the previous question,

1. If the measurement outcome at time step ⓓ is 100, what do we know about the period a? In other words, what are the possible values of a that are consistent with this measurement outcome?

2. If we repeat Simon's algorithm and obtain another measurement outcome 111 at time step ⓓ, what do we know about the period now? In other words, what are the possible values of a that are consistent with both the first measurement outcome 100 and the second measurement outcome 111?

4 Quantum Fourier Transform

Task 4.1 **(25 pts)**

Quantum Fourier Transform (QFT) is a very useful primitive in quantum algorithms. In this question, we will explore quantum computer's number format in the computational basis and in the Fourier basis, and discover QFT's role in this.

The standard binary representation of a non-negative integer $j \in \{0,1,2,\ldots,2^n-1\}$ is defined by a length-n bitstring: $j_{n-1}j_{n-2}\cdots j_1 j_0$ such that $j = \sum_{s=0}^{n-1} j_s 2^s$,, where $j_s \in \{0,1\}$. Let's use the number j to index the amplitude of an n-qubit quantum state:

$$|\psi\rangle = \sum_{j=0}^{2^n-1} \alpha_j |j_{n-1}j_{n-2}\cdots j_1 j_0\rangle \equiv \sum_{j=0}^{2^n-1} \alpha_j |j\rangle,$$

for complex amplitudes satisfying $\sum_j |\alpha_j|^2 = 1$.

Quantum Fourier Transform (QFT) maps one quantum state to another as follows:

$$|\psi\rangle \xrightarrow{QFT} |\phi\rangle = F_{2^n}|\psi\rangle \equiv \sum_{k=0}^{2^n-1} \beta_k |k_{n-1}k_{n-2}\cdots k_1 k_0\rangle,$$

where $\beta_k = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} w^{jk}\alpha_j$ and $w = e^{i2\pi/2^n}$.

(a) Suppose we only consider two numbers $\{0,1\}$, that is, $n = 1$. What is w? And what is the unitary matrix of F_2?

(b) In the computational basis, we define two quantum states as the basis states, $|0\rangle, |1\rangle$. We can also represent the two numbers in the Fourier basis, $\widetilde{|0\rangle} = F_2|0\rangle, \widetilde{|1\rangle} = F_2|1\rangle$. Write down the Fourier basis states in the computational basis. That is, write down $\widetilde{|0\rangle}, \widetilde{|1\rangle}$ in the form of $\alpha|0\rangle + \beta|1\rangle$ for some values of α, β.

(c) Suppose we consider four numbers $\{0,1,2,3\}$, that is, $n = 2$. What is w? And what is the unitary matrix of F_4?

(d) Since F_4 is unitary, it should be invertible. What is the matrix for the inverse, F_4^{-1}?

Task 4.2 **($\star$ pts)**

Continuing from the previous question,

(a) We can define the computational basis, $|0\rangle = |00\rangle, |1\rangle = |01\rangle, |2\rangle = |10\rangle, |3\rangle = |11\rangle$. We also can use Fourier transform to represent the four numbers in the Fourier basis: $\{\widetilde{|0\rangle}, \widetilde{|1\rangle}, \widetilde{|2\rangle}, \widetilde{|3\rangle}\}$. Write down the four quantum states: $\widetilde{|0\rangle} = F_4|0\rangle, \widetilde{|1\rangle} = F_4|1\rangle, \widetilde{|2\rangle} = F_4|2\rangle, \widetilde{|3\rangle} = F_4|3\rangle$.

(b) For the following tasks, let's consider $n = 3$. We can count numbers from 0 to 7 in the computational basis or the Fourier basis. In the computational basis, a number j is represented by the standard binary format: $|j\rangle = |j_2 j_1 j_0\rangle$. In the Fourier basis, a number j is represented by

$$\widetilde{|j\rangle} = F_8|j\rangle = \frac{1}{\sqrt{8}}\sum_{k=0}^{7} w^{jk}|k\rangle = \frac{1}{\sqrt{8}}\sum_{k_0,k_1,k_2\in\{0,1\}} w^{jk}|k_2 k_1 k_0\rangle.$$

Show that $F_8|j\rangle$ is *unentangled*, by writing the quantum state as a product state: $\big(\alpha_2|0\rangle + \beta_2|1\rangle\big)\otimes \big(\alpha_1|0\rangle + \beta_1|1\rangle\big)\otimes\big(\alpha_0|0\rangle + \beta_0|1\rangle\big)$. Write your answers in terms of w.

(c) Complete the following table. Write your answers in terms of w.

Integer	0	1	2	3	4	5	6	7
Computational basis ($\|j\rangle$)	$\|000\rangle$	$\|001\rangle$	$\|010\rangle$	$\|011\rangle$	$\|100\rangle$	$\|101\rangle$	$\|110\rangle$	$\|111\rangle$
Fourier basis ($F_8\|j\rangle$)								

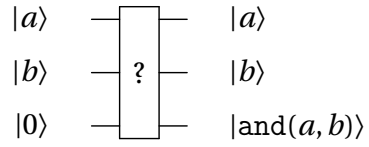
Table 2: Counting numbers in the computational basis and the Fourier basis.

5 Arithmetic

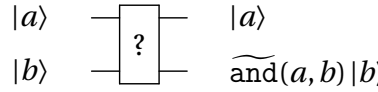
Task 5.1 ($\star$ pts)

The following questions are some hands-on practice on simple arithmetic using quantum circuits. Let's start with the standard computational basis.

(a) Consider the $\texttt{and}: \{0,1\}^2 \to \{0,1\}$ function, which computes the logical and of two input bits. Write down the full truth table of the function. Draw the circuit that implements the and function reversibly (i.e., $|ab\rangle \otimes |0\rangle \to |ab\rangle \otimes |\texttt{and}(a,b)\rangle$).



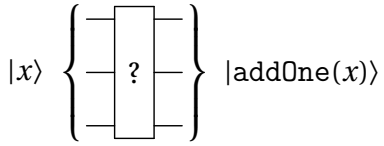
(b) Consider the $\widehat{\texttt{and}} : \{0,1\}^2 \to \{+1,-1\}$ function, which computes the logical and of two input bits and outputs ± 1. Specifically, $\widehat{\texttt{and}}(a,b) = (-1)^{\texttt{and}(a,b)}$. With this new definition, we can compute and as phase of quantum states. Write down the full truth table of the function. Draw the circuit that implements the $\widehat{\texttt{and}}$ function (i.e., $|ab\rangle \to \widehat{\texttt{and}}(a,b)|ab\rangle$).



Task 5.2 (30 pts)

Let's now consider arithmetic on integers $\mathbb{Z}_8 = \{0,1,2,3,4,5,6,7\}$. In this question, we are going to explore how to perform arithmetic in the computational basis and the Fourier basis.

(a) We can define the function $\texttt{addOne} : \mathbb{Z}_8 \to \mathbb{Z}_8$, which adds 1 (modulo 8) to the input. That is, $\texttt{addOne}(x) = x+1 \mod 8$. Notice that this function is reversible. In the computational basis, $|x\rangle = |x_2 x_1 x_0\rangle$ where $x = \sum_s x_s 2^s$. Implement a quantum circuit C that computes addOne: $|x\rangle \xrightarrow{C} |\texttt{addOne}(x)\rangle$.



(b) Suppose we denote $\widetilde{\mathbb{Z}}_8 = \{\widetilde{0},\widetilde{1},\widetilde{2},\widetilde{3},\widetilde{4},\widetilde{5},\widetilde{6},\widetilde{7}\}$ in the Fourier basis. We define the function $\widetilde{\texttt{addOne}} : \widetilde{\mathbb{Z}}_8 \to \widetilde{\mathbb{Z}}_8$, which adds 1 (modulo 8) to the input. Implement a quantum circuit C that computes $\widetilde{\texttt{addOne}}$: $|\widetilde{x}\rangle \xrightarrow{C} |\widetilde{\texttt{addOne}}(\widetilde{x})\rangle$. It is required that the solution should not transform $|\widetilde{x}\rangle$ back to $|x\rangle$ to perform addition in the computational basis. (Hint: Phase gates will be useful.)