Exercise Set 6
Quantum Computation

Exercise 1 *Phase estimation based on the Quantum Fourier Transform*

Let U be an unitary $2^n \times 2^n$ matrix (here, $n \geq 1$) with an eigenvector $|u\rangle$ and corresponding eigenvalue $e^{2\pi i\varphi}$. That means:

$$U\,|u\rangle = e^{2\pi i\varphi}\,|u\rangle\,.$$

We assume

$$\varphi = \frac{\varphi_1}{2} + \frac{\varphi_0}{4}$$

with binary $\varphi_1, \varphi_0 \in \{0,1\}$. In this problem, we study an "algorithm of phase estimation" which allows us to find φ assuming that the eigenvector $|u\rangle$ is known.

Recall that the Quantum Fourier Transform acting on two qubits is defined as

$$QFT\,|x_1, x_0\rangle = \frac{1}{2}\sum_{y_0,y_1\in\{0,1\}} e^{\frac{2\pi i}{4}(2x_1+x_0)(2y_1+y_0)}\,|y_1, y_0\rangle$$

where $x_1, x_0 \in \{0,1\}$. We also define the following (controlled) operations which are performed on $2+n$ qubits (here, $x, y \in \{0,1\}$ and $|\psi\rangle \in \mathbb{C}^{\otimes n}$)

$$R_1\;|x\rangle \otimes |y\rangle \otimes |\psi\rangle = |x\rangle \otimes |y\rangle \otimes U^{2x}\,|\psi\rangle$$

$$R_2\;|x\rangle \otimes |y\rangle \otimes |\psi\rangle = |x\rangle \otimes |y\rangle \otimes U^{y}\,|\psi\rangle\,.$$

Now, let S be the following unitary matrix:

$$S = ((QFT)^\dagger \otimes I_n)\;R_2\;R_1\;(H \otimes H \otimes I_n)$$

where H is the usual Hadamard matrix and I_n is the identity matrix acting on n qubits. Here, $(QFT)^\dagger$ is the conjugate transpose of QFT.

(a) What is the size of the unitary matrix S? Draw the circuit corresponding to S.

(b) We initialize the circuit with the state $|0\rangle \otimes |0\rangle \otimes |u\rangle$. Calculate the state of $2+n$ qubits right before the gate $(QFT)^\dagger$.

(c) Check that the expression found in (b) is the same as $QFT\,|\varphi_1, \varphi_0\rangle \otimes |u\rangle$. What is, therefore, the output state of the circuit?

(d) Deduce that we can find φ by doing *one and only one measurement* of the two first qubits of the circuit output.

Exercise 2 *Gates to build U_f for $f(x) = a^x \,(mod\ N)$*

In class, you have seen the construction of the gate U_f in the general case. The first gate that composes U_f realizes the operation

$$U_a \left|k\right\rangle = \left|ka \,(\mathrm{mod}\ N)\right\rangle \text{ if } k < N \text{ and } U_a \left|k\right\rangle = \left|k\right\rangle \text{ otherwise.}$$

Here, we ask you to build this first gate U_a explicitly in two particular cases:

- $a = 2$ and $N = 3$
- $a = 3$ and $N = 4$

(a) Write U_a in matrix form. Check that U_a is a permutation of the computational basis.

Thus, we can write $U_a \left|xy\right\rangle = \left|XY\right\rangle$, where $x, y, X, Y \in \{0, 1\}$. We want to express X, Y as a function of x, y.

(b) Find the 4 Boolean functions $f_{XY} : \{0,1\}^2 \to \{0,1\}$ such that

$$f_{XY}(x,y) = \begin{cases} 1 & \text{if } U_a \left|xy\right\rangle = \left|XY\right\rangle \\ 0 & \text{otherwise.} \end{cases}$$

(c) Deduce the Boolean functions $f_{X=1} : \{0,1\}^2 \to \{0,1\}$ and $f_{Y=1} : \{0,1\}^2 \to \{0,1\}$ such that

$$f_{X=1}(x,y) = \begin{cases} 1 & \text{if } U_a \left|xy\right\rangle = \left|1Y\right\rangle \\ 0 & \text{otherwise.} \end{cases} \qquad f_{Y=1}(x,y) = \begin{cases} 1 & \text{if } U_a \left|xy\right\rangle = \left|Y1\right\rangle \\ 0 & \text{otherwise.} \end{cases}$$

Simplify them as much as possible.

(d) Deduce the quantum circuit that realizes U_a.

Exercise 3 *Approximating QFT*

For n qubits, the number of gates we use for the Quantum Fourier Transform scales as $O(n^2)$. This complexity can be improved further if we settle for an approximate version of QFT; in this exercise we will investigate how. The main idea behind the approximation is to remove some of the controlled-R_d gates, noting that when d is large,

$$R_d = \begin{pmatrix} 1 & 0 \\ 0 & e^{\pi i/2^d} \end{pmatrix}$$

is almost equal to the identity.

Let us define the distance between unitary operators U and V as

$$D(U,V) = \max_{\|\psi\|_2 = 1} \left\|(U - V)\left|\psi\right\rangle\right\|_2 .$$

(a) Show that D is subadditive:

$$D(U_1 U_2, V_1 V_2) \leq D(U_1, V_1) + D(U_2, V_2).$$

(b) Show that

$$D(R_d, I_2) = O(2^{-d}).$$

Why does the same hold for the controlled version,

$$D(I_2 \oplus R_d, I_4)?$$

(c) Describe a quantum circuit for an approximate QFT described by an operator $\tilde{Q}_N$ for n qubits ($N = 2^n$), such that it uses $O(n \log n)$ gates and

$$D(\tilde{Q}_N, Q_N) = O\left(\frac{1}{n}\right).$$

Hint. Compare the circuit for Q_N from the script/lecture with the circuit you obtain when removing all controlled-R_d gates with $d \geq k$. Let us call the latter operation $\tilde{Q}_N$. Show that for any $k \in \mathbb{N}$ we have

$$D(\tilde{Q}_N, Q_N) = O(n2^{-k}).$$

How should you choose k in terms of n to achieve the desired scaling?