Exercise Set 8 (graded)
Quantum Computation

Exercise 1 *Quantum Fourier Transorm*

The Quantum Fourier Transform is the linear map acting on $\mathcal{H} = \mathbb{C}^M$ (with $M = 2^m$) defined as

$$QFT\,|x\rangle = \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} \exp(2\pi i xy/M)\,|y\rangle\,, \quad 0 \leq x \leq M-1$$

Remarks:

- Watch out that here, the product xy is the actual product of the two numbers x and y, and *not* the dot product $x \cdot y$ of the binary (vector) representations of x and y, as defined in Deutsch-Josza's algorithm. For example, if $x = 2$ and $y = 2$, then $xy = 4$, whereas $x \cdot y = (1,0) \cdot (1,0) = 1 + 0 = 1$.

- Nevertheless, $|x\rangle$ and $|y\rangle$ are still here the short-hand notations for $|x_1, \ldots, x_m\rangle$ and $|y_1, \ldots, y_m\rangle$, where $x_1, \ldots, x_m$ and $y_1, \ldots, y_m$ are the binary representations of x and y.

(a) When $M = 2$, write down explicitly the matrix representation of QFT. What gate is that?

(b) When $M = 4$, write down explicitly the matrix representation of QFT, and check that it is unitary.

(c) Still when $M = 4$, show that QFT satisfies the equality

$$QFT\,|x\rangle = \frac{1}{2}\left(|0\rangle + (-1)^x\,|1\rangle\right) \otimes \left(|0\rangle + i^x\,|1\rangle\right)$$

(d) Can QFT be written as a tensor product of two 2×2 matrices A and B in this case? Justify.

Exercise 2 *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.

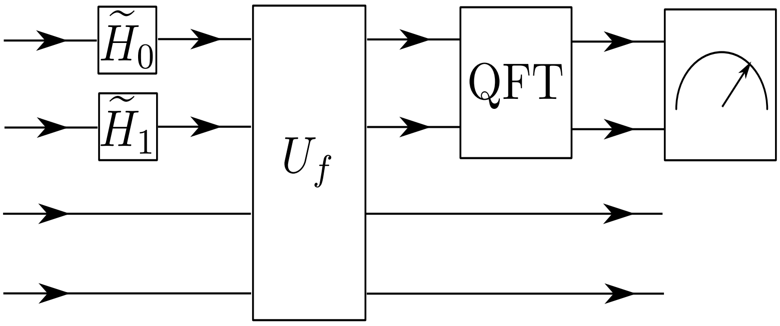
Exercise 3 *Effect of imperfections in some gates in Shor's algorithm*

We consider a function on $\mathbb{Z}$ with a period equal to 2, i.e., $f(x) = f(x+2)$, $x \in \mathbb{Z}$. We would like to study the circuit below (see figure on the next page) where the usual Hadamard gates are modified with a random perturbation:

$$\widetilde{H}_0\,|b\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^b e^{i\varphi_0}\,|1\rangle\right), \text{ where } b = 0, 1$$

$$\widetilde{H}_1\,|b\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^b e^{i\varphi_1}\,|1\rangle\right), \text{ where } b = 0, 1$$

and φ_0 and φ_1 are uniformly distributed on $[0, 2\pi]$.



The circuit is initialized with the state $|\psi_0\rangle = |0\rangle \otimes |0\rangle \otimes |0\rangle \otimes |0\rangle$. We will denote $|0\rangle \otimes |0\rangle = |0\rangle$; $|0\rangle \otimes |1\rangle = |1\rangle$; $|1\rangle \otimes |0\rangle = |2\rangle$; $|1\rangle \otimes |1\rangle = |3\rangle$ and define for $x, y \in \mathbb{Z}$:

$$U_f |x\rangle \otimes |y\rangle = |x\rangle \otimes |y + f(x)\rangle$$

$$\text{QFT}\, |x\rangle = \frac{1}{\sqrt{4}} \sum_{y=0}^{3} \exp\left(\frac{2\pi i}{4} xy\right) |y\rangle$$

(a) Show that the state after the gates of Hadamard type is:

$$|\psi_1\rangle = \frac{1}{\sqrt{4}} \left(|0\rangle + e^{i\varphi_1} |1\rangle + e^{i\varphi_0} |2\rangle + e^{i(\varphi_0+\varphi_1)} |3\rangle\right) \otimes |0\rangle$$

(b) Show that the state right before the measurement is

$$|\psi_3\rangle = \frac{1}{4} \sum_{y=0}^{3} \left(1 + e^{i(\varphi_0+\pi y)}\right) |y\rangle \otimes |f(0)\rangle + \left(e^{i\left(\varphi_1+\frac{\pi}{2}y\right)} + e^{i\left(\varphi_0+\varphi_1+\frac{3\pi}{2}y\right)}\right) |y\rangle \otimes |f(1)\rangle$$

(c) We measure two first qubits in the basis defined by the projectors:

$$\{P_y \otimes \mathbb{I}_{4\times4} = |y\rangle \langle y| \otimes \mathbb{I}_{4\times4};\ y = 0, 1, 2, 3\}$$

Find the state right after the measurement (up to the normalizing constant). Then, calculate the probability of getting y. You should see that the result is independent of φ_1.

(d) In the previous question, you calculated the probability given fixed φ_0 and φ_1. If done correctly, your derivations gave a result depending only on φ_0. Draw a plot of $\Pr(y|\varphi_0)$ for $\varphi_0 = 0, \frac{\pi}{2}, \frac{3\pi}{4}, \pi$. Calculate and draw a plot of the total probability $\Pr(y)$ considering that φ_0 is uniformly distributed on $[0, 2\pi]$.