Exercise Set 7
Quantum Computation

Exercise 1 *Convergents in Shor's algorithm*

One runs Shor's algorithm in order to retrieve the period of the function $f(x) = 3^x \bmod N$, where $N = 35$ (yes, we all know that $N = 35 = 5 \cdot 7$, but let us pretend that this factorization is not easy...). The algorithm uses $m = 11$ qubits (so that $M = 2^m = 2'048 \geq N^2 = 1'225$). Using the method of convergents seen in class, describe which of the following outcomes y of the quantum circuit lead(s) to the identification of the correct period r of f:

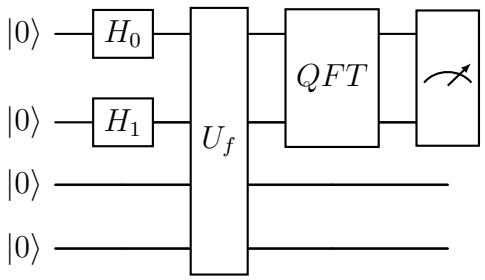
(a) $y = 171$ (b) $y = 512$ (c) $y = 853$

Exercise 2 *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 $[0, 2\pi]$.



(1)

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 $x, y \in \mathbb{Z}$:

$$U_f |x\rangle \otimes |y\rangle = |x\rangle \otimes |y + f(x)\rangle$$
$$\mathrm{QFT} |x\rangle = \frac{1}{\sqrt{4}} \sum_{y=0}^{3} \exp\left(\frac{2\pi i}{4} xy \right) |y\rangle$$

(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 carry out a partial measurement on the first two qubits. In other words, we measure the first two qubits by applying the projectors:

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

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 $[0, 2\pi]$.

Exercise 3 *Simon's algorithm*

Consider the function $f : \{0,1\}^4 \to \{0,1\}^2$ defined as

$$f(x_1, x_2, x_3, x_4) = (x_1 \oplus x_2 \oplus x_3, x_3 \oplus x_4)$$

One applies Simon's algorithm in order to study this function f.

(a) Note that f is invariant under the transformation

$$x \mapsto x \oplus (1,1,0,0)\ , \tag{2}$$

for any $x \in \{0,1\}^4$, namely, for all values of (x_1, x_2, x_3, x_4) we have

$$f(x_1, x_2, x_3, x_4) = f(x_1 \oplus 1, x_2 \oplus 2, x_3, x_4)\ . \tag{3}$$

Here, "$\oplus$" stands for addition mod 2. Find all the vectors $s \in \{0,1\}^4$ such that f is invariant under the transformation

$$f(x) = f(x \oplus s)\ . \tag{4}$$

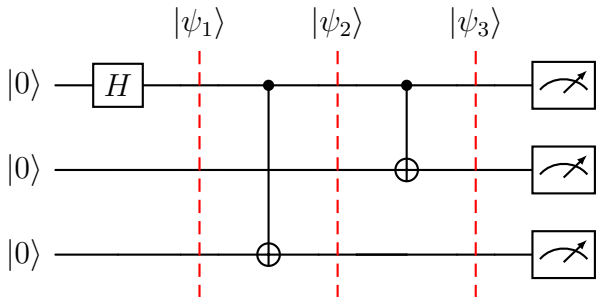
Here, "$x \oplus s$" stands for component-wise addition mod 2. Verify that the space of the vectors s you found is closed under addition.

(b) Apply Simon's Algorithm with the oracle for f. Note that it should be applied on 6 qubits. Compute the output distribution of the algorithm's outcomes.

(c) Explain how one can recover the space of vectors $\{s\}$ you found in section (a), using Simon's Algorithm.

Exercise 4 *The action of basic circuits*

In this exercise, we analyze the following circuit:



(5)

(a) Write out the states $|\psi_n\rangle$ shown in the diagram, for $n = 1, 2, 3$.

(b) Write $|\psi_3\rangle$ in the Hadamard basis.

(c) What are the outcome statistics, measuring $|\psi_3\rangle$?

Exercise 5 *The Fourier Transform of a periodic vector (Optional)*

The goal of the following exercise is to stress the connection between the Fourier transform and periodic functions, a connection that can be made (as seen in class) by defining the Fourier-basis for the vector space on which the transform acts. In this exercise, we work with more general periodic functions.
Recall the QFT on an N-dimensional space:

$$QFT\,|x\rangle = \frac{1}{\sqrt{N}} \sum_{z=0}^{N-1} \exp\left(\frac{2\pi i x z}{N}\right) |z\rangle \ . \tag{6}$$

Let $N = m \cdot r$ for $m, r \in \mathbb{N}$.

(a) Compute the Fourier transform of the vector $|\psi\rangle = (\psi_1, \psi_2, ..., \psi_N)$ whose coefficients form a periodic function dictated by:

$$|\psi\rangle = \sum_{s=0}^{m-1} |s \cdot r\rangle \ . \tag{7}$$

In other words, $\psi_k = 1$ for any k that is an integer multiple of r, and otherwise $\psi_k = 0$.

(b) Let $a \in \{0, ..., r-1\}$. Compute the Fourier Transform of the shifted periodic function,

$$\left|\psi^{(a)}\right\rangle = \sum_{s-0}^{m-1} |s \cdot r + a\rangle \ . \tag{8}$$

(c) Now we are given a vector whose coefficients are a general periodic function (of their indices), $|\psi\rangle = (\psi_1, \psi_2, ..., \psi_N)$ with a period r that divides N, namely $\psi_k = \psi_{k+r}$. We denote the output vector by:

$$\left|\tilde{\psi}\right\rangle = QFT\,|\psi\rangle \ . \tag{9}$$

For which values of k do we have $\tilde{\psi}_k \neq 0$?