Exercise set #4

Exercise 1 (Hw2):

Suppose we have two qubits in the following states:

$$|\Psi_1\rangle = \alpha_1 |0\rangle + \beta_1 |1\rangle$$

$$|\Psi_2\rangle = \alpha_2 |0\rangle + \beta_2 |1\rangle$$

e) A convenient way to write down the probabilities of obtaining measurement outcomes when measuring the control qubit in the computational basis is by computing

$$p_0 = \langle\Phi| |0\rangle \langle 0| \otimes I \otimes I |\Phi\rangle$$

$$p_1 = \langle\Phi| |1\rangle \langle 1| \otimes I \otimes I |\Phi\rangle$$

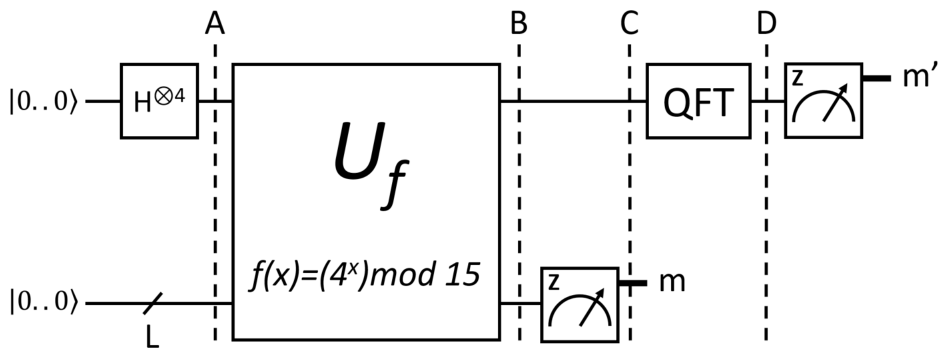
Apply this rule to show that

$$p_0 = \frac{1}{2} + \frac{|\langle \Psi_1 | \Psi_2 \rangle|^2}{2}$$
$$p_1 = \frac{1}{2} - \frac{|\langle \Psi_1 | \Psi_2 \rangle|^2}{2}$$

f) How can you use this circuit for testing whether $|\Psi_1\rangle = |\Psi_2\rangle$? Explain when your procedure works well, and when you will only gain some confidence.

Exercise 2:

We will go through the steps of Shor's algorithm to find the period r and factorize $N = 15$ for $a = 4$.



a) For simplicity, we will only use 4 qubits for the top register. How many qubits L do we need for the bottom register?

b) What is the state $|\Psi_A\rangle$ of all the qubits at point A?

c) What is the state $|\Psi_B\rangle$ of all the qubits at point B?

d) What is the state $|\Psi_C\rangle$ of all the qubits at point C if we measured $|1\rangle$ in the bottom register?

e) What is the state $|\Psi_D\rangle$ of the top register at point D?

f) What are the possible measurement outcomes for the top register? What is the value of r in each case?

g) Use the r from e) to determine the prime factors of N.