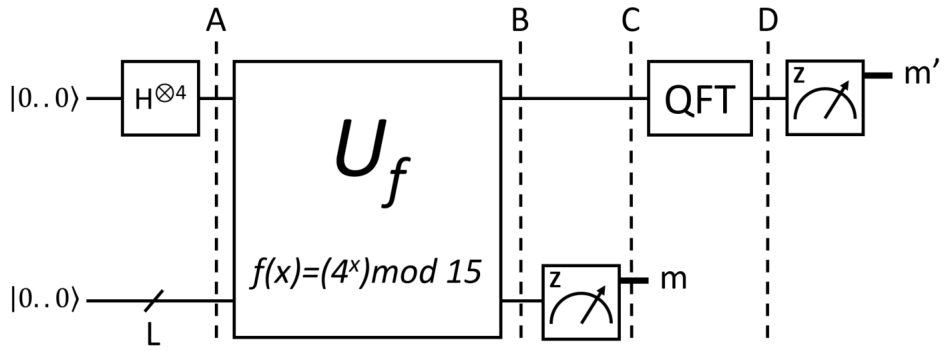
Exercise set #4
solutions

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?

$$L = \lceil log_2 N \rceil = 4$$

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

$$|\Psi_A\rangle = H^{\otimes 4} \otimes I^{\otimes 4} |0\rangle |0\rangle = \frac{1}{\sqrt{2^4}} \sum_{x=0}^{2^4-1} |x\rangle |0\rangle$$

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

$$\begin{aligned} |\Psi_B\rangle = U_f |\Psi_A\rangle &= \frac{1}{\sqrt{2^4}} \sum_{x=0}^{2^4-1} |x\rangle |4^x \ mod\ 15\rangle \\ &= \frac{1}{\sqrt{2^4}} (|0\rangle |1\rangle + |1\rangle |4\rangle + |2\rangle |1\rangle + ... + |15\rangle |4\rangle) \end{aligned}$$

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

$$\begin{aligned} |\Psi_B\rangle = &\frac{1}{\sqrt{2^3}} (|0\rangle + |2\rangle + |4\rangle + ... + |14\rangle) \otimes \frac{1}{\sqrt{2}} |1\rangle \\ &+ \frac{1}{\sqrt{2^3}} (|1\rangle + |3\rangle + |5\rangle + ... + |15\rangle) \otimes \frac{1}{\sqrt{2}} |4\rangle \end{aligned}$$

$$|\Psi_C\rangle = \frac{1}{\sqrt{2^3}} (|0\rangle + |2\rangle + |4\rangle + ... + |14\rangle)$$

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

The QFT transforms a qubit $|j\rangle$ into:

$$|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{\frac{2\pi i j k}{N}} |k\rangle$$

$$\begin{aligned} |\Psi_D\rangle &= \frac{1}{\sqrt{2^3}} \frac{1}{\sqrt{2^4}} \left(\sum_{k=0}^{15} |k\rangle + \sum_{k=0}^{15} e^{\frac{2\pi i 2k}{16}} |k\rangle + \sum_{k=0}^{15} e^{\frac{2\pi i 4k}{16}} |k\rangle + ... + \sum_{k=0}^{15} e^{\frac{2\pi i 14k}{16}} |k\rangle \right) \\ &= \frac{1}{\sqrt{2^7}} \left(\sum_{k=0}^{7} 1 |0\rangle + \sum_{k=0}^{7} e^{\frac{2\pi i 2k \cdot 1}{16}} |1\rangle + \sum_{k=0}^{7} e^{\frac{2\pi i 2k \cdot 2}{16}} |2\rangle + \sum_{k=0}^{7} e^{\frac{2\pi i 2k \cdot 3}{16}} |3\rangle + ... + \sum_{k=0}^{7} e^{\frac{2\pi i 2k \cdot 15}{16}} |15\rangle \right) \end{aligned}$$

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

$$\begin{aligned} |\Psi_D\rangle &\approx \frac{1}{\sqrt{2^7}} \left(\sum_{k=0}^{7} 1 |0\rangle + \sum_{k=0}^{7} e^{\frac{2\pi i 2k \cdot 8}{16}} |8\rangle \right) \\ &= \frac{1}{\sqrt{2^7}} \left(8 |0\rangle + 8 |8\rangle \right) \end{aligned}$$

If we measure $|0\rangle$ *we can't extract any information about* r.

If we measure $|8\rangle$ *then:*

$$\frac{m'}{16} \approx \frac{s}{r} \quad <=> \quad \frac{8}{16} = \frac{1}{2} \quad => \quad r = 2$$

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

$$
\begin{aligned}
r = 2 \quad => \quad a^{\frac{r}{2}} + 1 &= 4^1 + 1 = 5 \\
a^{\frac{r}{2}} - 1 &= 4^1 - 1 = 3 \\
p = &gcd(5, N) = gcd(5, 15) = 5 \\
q = &gcd(3, N) = gcd(3, 15) = 3
\end{aligned}
$$