Exercise Set 9
Quantum Computation

Exercise 1 *Another algorithm involving the QFT*

Let $M = 2^m$. For $x \in \{0, \dots, M-1\}$ an integer, let us recall that the QFT is defined as

$$QFT\,|x\rangle = \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} e^{\frac{2\pi i}{M} xy} |y\rangle$$

Let $f : \{0, \dots, M-1\} \to \{0, \dots, M-1\}$ be an arithmetic function and V_f be the $M \times M$ matrix defined as

$$V_f |x\rangle = e^{-\frac{2\pi i}{M} f(x)} |x\rangle$$

(a) What are the matrix elements of both QFT and V_f in the basis $\{|x\rangle, x = 0, \dots, M-1\}$? Prove that these two matrices are unitary.

(b) Let

$$|\Psi\rangle = (QFT)(V_f) H^{\otimes m} |0\rangle$$

where $|0\rangle$ is the sate corresponding to the integer $0 \in \{0, \dots, M-1\}$. Explain how to represent this identity by a quantum circuit, notably how to represent the various states with qubits and the number of needed qubits, then draw the circuit.

(c) Compute the state at each stage in the circuit, and in particular the output state $|\Psi\rangle$.

(d) Let $A, B \in \{0, \dots, M-1\}$ and $f(x) = Ax + B \text{mod } M$. We measure the state in the computational bases. What is the minimum number of measures need to determine the value of A? Can we also determine the value of B with this process? Justify your answers.

Exercise 2 *Gate 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. Here, we ask you to build this gate explicitly in two particular cases:

(a) $a = 3$ and $N = 8$

(b) $a = 3$ and $N = 16$

Hints: - For this exercise, it helps to think first at what are the possible values taken by $a^x \bmod N$ for all values $0 \le x \le N-1$.
- For the purpose of the exercise, use $n = \log_2(N)$ bits for each variable x or y (instead of $m = \log_2(M)$ bits, where $M = N^2$, as seen in class).