Exercise Set 8

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 state 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 $f(x) = Ax + B \bmod M$. We measure the state in the computational basis. 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 *Gates to build 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. The first gate that composes U_f realizes the operation

$$U_a |k\rangle = |ka \mod N\rangle \text{ if } k < N \text{ and } U_a |k\rangle = |k\rangle \text{ otherwise.}$$

Here, we ask you to build this first gate U_a explicitly in two particular cases:

- $a = 2$ and $N = 3$
- $a = 3$ and $N = 4$

(a) Write U_a in matrix form. Check that U_a is a permutation of the computational basis.

Thus, we can write $U_a |xy\rangle = |XY\rangle$ where $x, y, X, Y \in \{0, 1\}$. We want to express X, Y as function of x, y.

(b) Find the 4 Boolean functions $f_{XY} : \{0, 1\}^2 \to \{0, 1\}$ such that

$$f_{XY}(x, y) = \begin{cases} 1 & \text{if } U_a |xy\rangle = |XY\rangle \\ 0 & \text{otherwise.} \end{cases}$$

(c) Deduce the Boolean functions $f_{X=1} : \{0, 1\}^2 \to \{0, 1\}$ and $f_{Y=1} : \{0, 1\}^2 \to \{0, 1\}$ such that

$$f_{X=1}(x, y) = \begin{cases} 1 & \text{if } U_a |xy\rangle = |1Y\rangle \\ 0 & \text{otherwise.} \end{cases} \qquad f_{Y=1}(x, y) = \begin{cases} 1 & \text{if } U_a |xy\rangle = |X1\rangle \\ 0 & \text{otherwise.} \end{cases}$$

Simplify them as much as possible.

(d) Deduce the quantum circuit that realizes U_a.

Exercise 3 *Convergents in Shor's algorithm*

One runs Shor's algorithm in order to retrieve the period of the function $f(x) = 3^x$ mod 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) $y = 853$