Exercise Set 5
Quantum Computation

**Exercise 1** *Upper bound on the period of* $f(x) = a^x \,(mod\ N)$

Let us consider an integer $N = p \cdot q$, where $p$ and $q$ are distinct primes. Let $1 \leq a \leq N-1$ be another integer such that $\gcd(a, N) = 1$. The aim of the present exercise is to show that in this case, the period $r$ of the function $f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$ defined as $f(x) = a^x \,(\text{mod } N)$ satisfies the inequality

$$r \leq (p-1)\,(q-1) \tag{1}$$

(a) Let $G = \{1 \leq n \leq N-1 \,:\, \gcd(n, N) = 1\}$. Show that this set, equipped with the *multiplication modulo* $N$, is a group.

(b) Under the assumption that $N = p \cdot q$, where $p$ and $q$ are distinct primes, what is the number of elements in $G$?

(c) Let $a \in G$ and consider the set

$$H = \{1,\, a,\, a^2 \,(\text{mod } N),\, a^3 \,(\text{mod } N), \ldots,\, a^{k-1} \,(\text{mod } N)\}$$

where $k \geq 1$ is the smallest integer such that $a^k (\text{mod } N) = 1$. Show that $H$ is a subgroup of $G$.

(d) Use then Lagrange's theorem to conclude that inequality (1) holds. Recall: Lagrange's theorem asserts that, given a group $G$ and a subgroup $H$ of $G$, then $|H|$ divides $|G|$ .

**Exercise 2** *Quantum Fourier Transform*

The Quantum Fourier Transform is the linear map acting on $\mathcal{H} = \mathbb{C}^M$ (with $M = 2^m$) defined as

$$QFT\,|x\rangle = \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} \exp(2\pi i x y/M)\,|y\rangle\,, \quad 0 \leq x \leq M-1$$

*Remarks:*

- Watch out that here, the product $xy$ is the actual product of the two numbers $x$ and $y$, and *not* the dot product $x \cdot y$ of the binary (vector) representations of $x$ and $y$, as defined in Deutsch-Josza's algorithm. For example, if $x = 2$ and $y = 2$, then $xy = 4$, whereas $x \cdot y = (1,0) \cdot (1,0) = 1 + 0 = 1$.
- Nevertheless, $|x\rangle$ and $|y\rangle$ are still here the short-hand notations for $|x_1, \ldots, x_m\rangle$ and $|y_1, \ldots, y_m\rangle$, where $x_1, \ldots, x_m$ and $y_1, \ldots, y_m$ are the binary representations of $x$ and $y$.

(a) When $M = 2$, write down explicitly the matrix representation of QFT. What gate is that?

(b) When $M = 4$, write down explicitly the matrix representation of QFT, and check that it is unitary.

(c) Still when $M = 4$, show that QFT satisfies the equality

$$QFT\,|x\rangle = \frac{1}{2}\left(|0\rangle + (-1)^x\,|1\rangle\right) \otimes \left(|0\rangle + i^x\,|1\rangle\right)$$

(d) Can QFT be written as a tensor product of two $2 \times 2$ matrices $A$ and $B$ in this case? Justify.

**Exercise 3** *Another algorithm involving the QFT*

Let $M = 2^m$. For $x \in \{0, \ldots, M-1\}$ 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 $f : \{0, \ldots, M-1\} \to \{0, \ldots, M-1\}$ 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 $\{|x\rangle, x = 0, \ldots, M-1\}$? 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 $0 \in \{0, \ldots, M-1\}$. Explain *briefly* how we represent the state $|x\rangle$, $x \in \{0, ..., M-1\}$ in the quantum circuit formalism with qubits. Then draw the circuit (there is no need to decompose $QFT$ and $V_f$ into smaller circuits).

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

(d) Let $A, B \in \{0, \ldots, M-1\}$ 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.