QCLG Exercise sheet 7

PART I: Distinguishing the one time shift from a random permutation

Let $n \in \mathbb{N}^*$, $\mathrm{N} = 2^n$ and $[\mathrm{N}] = \{0, \ldots, \mathrm{N}-1\}$. Let $\omega = e^{\frac{2i\pi}{\mathrm{N}}}$ the canonical N^{th} root of unity. Let S_N the set of permutations from [N] to [N] and let F_N the quantum Fourier transform acting on n qubits. Recall that $\forall k \in [\mathrm{N}]$, we have $F_\mathrm{N}(|k\rangle) = \frac{1}{\sqrt{\mathrm{N}}} \sum_{j=0}^{\mathrm{N}-1} \omega^{jk} |j\rangle$. For each $s \in [\mathrm{N}]$, we define the function

$$\mathrm{Shift}_s(x) := (x + s) \ mod \ \mathrm{N}.$$

For any classical function f from $[N]$ to $[N]$, we define the quantum unitary O_f such that for each $x, z \in [\mathrm{N}]$, $O_f(|x\rangle |z\rangle) = |x\rangle |f(x) \oplus z\rangle$. In particular, $O_f(|x\rangle |0^n\rangle) = |x\rangle |f(x)\rangle$.

We are given a black box quantum circuit O_f such that

- With probability $\frac{1}{2}$, $f = \mathrm{Shift}_s$ for a randomly chosen $s \in [\mathrm{N}]$ (CASE 1).
- With probability $\frac{1}{2}$, $f = \sigma$ for a randomly chosen $\sigma \in S_\mathrm{N}$ (CASE 2).

We only have a black box access to O_f meaning that we don't have access to the internal wirings of the circuit. The only thing we can do is perform the unitary O_f. Our goal is, given O_f, to determine, *with only one application of the quantum circuit* O_f whether we are in CASE 1 or in CASE 2.

We consider the following distinguishing protocol:

Distinguishing Protocol given O_f.

1. Start from $|\psi_0\rangle = |0^n\rangle |0^n\rangle$ and apply the Fourier transform F_N on the first register.
2. Apply the quantum unitary O_f to both registers.
3. Apply the Fourier transform F_N on the second register.
4. Apply the inverse Fourier transform F_N^{-1} on the first register.
5. Measure both registers in the computational (standard) basis to get some outcome (y, y')

Exercise 1 (Preliminary question). *Let G_N the quantum unitary operation acting on n qubits such that $\forall k \in [\mathrm{N}]$, we have $G(|k\rangle) = \frac{1}{\sqrt{N}} \sum_{j=0}^{\mathrm{N}-1} \omega^{-jk} |j\rangle$. For each $k \in [\mathrm{N}]$, compute $G_\mathrm{N}(F_\mathrm{N}(|k\rangle))$. Show that G_N is the inverse of F_N.*

Exercise 2 (One time Shift). *We first study what happens in the distinguishing protocol when $f = \mathrm{Shift}_s$ for a fixed $s \in [\mathrm{N}]$.*

1. *For a fixed s, Let $|\psi_i^s\rangle$ the state after step i of the distinguishing protocol given O_{Shift_s}. Compute $|\psi_1^s\rangle, |\psi_2^s\rangle, |\psi_3^s\rangle, |\psi_4^s\rangle$.*
2. *For each y, what is the probability $P_{y,y}$ of measuring (y, y) during step 5? Show that $P_{eq} = \sum_{y=0}^{N-1} P_{y,y} = 1$.*

Exercise 3 (Random permutation). *We now study what happens in the distinguishing procedure when $f = \sigma$ for a random permutation $\sigma \in S_\mathrm{N}$.*

1. *For a fixed permutation σ, Let $|\phi_i^\sigma\rangle$ the state after step i of the distinguishing protocol given O_σ. Compute $|\phi_1^\sigma\rangle, |\phi_2^\sigma\rangle, |\phi_3^\sigma\rangle, |\phi_4^\sigma\rangle$.*
2. *For each y, what is the probability $Q_{y,y}$ of measuring (y, y) on average on σ? Show that $Q_{eq} = \sum_y Q_{y,y} = \frac{2}{\mathrm{N}}$. One can use the following formula which holds for any $y \in \{1, \ldots, \mathrm{N}-1\}$.*

$$\mathrm{E}_{\sigma \leftarrow S_\mathrm{N}}[|\sum_x \omega^{y(\sigma(x)-x)}|^2] = \frac{\mathrm{N}^2}{\mathrm{N}-1}$$

where $\mathrm{E}_{\sigma \leftarrow S_\mathrm{N}}[\cdot]$ denotes the expected value over a random permutation σ.

Exercise 4 (Distinguishing protocol given O_f)**.** *Describe a test with the following properties: if you are in case 1, the test outputs "$CASE1$" with probability 1, if you are in case 2, the test outputs "$CASE2$" with probability $1 - \frac{2}{N}$. Moreover, we require the test to make one oracle call. Can you think of a test that answers the correct $CASE$ with probability $> 1 - \frac{2}{N}$ in both cases?*

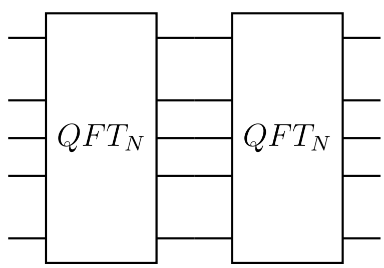
Exercise 5 (Classical complexity)**.** *Show that you can't determine with probability strictly greater than 1/2 whether you are in CASE 1 or in CASE 2 using a single classical query to O_f. Find a procedure that will succeed with probability close to 1 using 2 classical queries to O_f.*

Part II: A few calculations around the QFT

Exercise 1. *We consider quantum unitaries on n qubits. Let $N = 2^n$ and $[N] = \{0, \ldots, N-1\}$ so that any n qubit state $|\psi\rangle$ can be written as $|\psi\rangle = \sum_{i \in [N]} \alpha_i |i\rangle$ with $\sum_{i \in [N]} |\alpha_i|^2 = 1$. Let $QFT_N : |k\rangle \to \sum_{j \in [N]} \omega^{jk} |j\rangle$ be the Quantum Fourier transform on n qubits with $\omega = e^{\frac{2i\pi}{N}}$. Recall that $(QFT_N)^{-1} : |k\rangle \to \sum_{j \in [N]} \omega^{-jk} |j\rangle$*

1. *Let $V_1 = QFT_N \circ QFT_N$. Compute $V_1(|k\rangle)$ for any $k \in [N]$. Let $|\psi\rangle = \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle$. Compute $V_1(|\psi\rangle)$.*

(V_1)



2. *Let $n \geq 3$. Let U the unitary such that $U(|k\rangle) = w^{3k} |k\rangle$ for each $k \in [N]$. Let $V_2 = (QFT_N)^{-1} \circ U \circ QFT_N$. Let $|\psi\rangle = \sqrt{\frac{1}{6}} |0\rangle + \sqrt{\frac{1}{3}} |2\rangle + \sqrt{\frac{1}{8}} (|3\rangle + |4\rangle + |6\rangle + |7\rangle)$.*

Compute $V_2(|\psi\rangle)$ *when* $n = 3$ *and when* $n = 4$.

(V₂)