QII Exercise sheet 1

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}.*

Solution: Fix $k \in [\mathrm{N}]$. We have

$$G_{\mathrm{N}}(F_{\mathrm{N}}(|k\rangle)) = G_{\mathrm{N}}(\frac{1}{\sqrt{\mathrm{N}}} \sum_{j=0}^{\mathrm{N}-1} \omega^{jk}\,|j\rangle) = \frac{1}{\mathrm{N}} \sum_{j=0}^{\mathrm{N}-1} \omega^{jk} \sum_{l=0}^{\mathrm{N}-1} \omega^{-jl}\,|l\rangle = \frac{1}{\mathrm{N}} \sum_{l=0}^{\mathrm{N}-1} (\sum_{j=0}^{\mathrm{N}-1} \omega^{j(k-l)})\,|l\rangle\,.$$

If $k = l$, we have $\sum_j \omega^{j(k-l)} = \mathrm{N}$. If $k \neq l$, we have $\sum_j \omega^{j(k-l)} = 0$. We conclude that $G_{\mathrm{N}}(F_{\mathrm{N}}\,|k\rangle) = |k\rangle$. Since this holds for each k, by linearity, we conclude 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 $P_{eq} = \sum_{y=0}^{N-1} P_{y,y} = 1$.*

Solution:

1. $|\psi_1^s\rangle = \frac{1}{\sqrt{\mathrm{N}}} \sum_{x=0}^{\mathrm{N}-1} |x\rangle\,|0\rangle$.

2. $|\psi_2^s\rangle = \frac{1}{\sqrt{\mathrm{N}}} \sum_{x=0}^{\mathrm{N}-1} |x\rangle\,|x+s\rangle$.

3. $|\psi_3^s\rangle = \frac{1}{\mathrm{N}} \sum_{x=0}^{\mathrm{N}-1} |x\rangle \sum_{j=0}^{\mathrm{N}=1} \omega^{j(x+s)}\,|j\rangle$.

4. $|\psi_4^s\rangle = \frac{1}{\mathrm{N}\sqrt{\mathrm{N}}} \sum_{x=0}^{\mathrm{N}-1} \sum_{l=0}^{\mathrm{N}-1} \omega^{-xl}\,|l\rangle \sum_{j=0}^{\mathrm{N}=1} \omega^{j(x+s)}\,|j\rangle$.

The probability of measuring (y,y) is $|\frac{1}{\mathrm{N}\sqrt{\mathrm{N}}}\omega^{ys}\sum_x \omega^{x(y-y)}|^2 = \frac{1}{\mathrm{N}}$. From there, we immediately have $P_{eq} = 1$. Notice that this is independent of s. □

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 $y \in \{1,\dots,\mathrm{N}-1\}$.*

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

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

Solution:

1. $|\phi_1^\sigma\rangle = \frac{1}{\sqrt{\mathrm{N}}} \sum_{x=0}^{\mathrm{N}-1} |x\rangle\,|0\rangle$.

2. $|\phi_2^\sigma\rangle = \frac{1}{\sqrt{\mathrm{N}}} \sum_{x=0}^{\mathrm{N}-1} |x\rangle\,|\sigma(x)\rangle$.

3. $|\phi_3^\sigma\rangle = \frac{1}{\mathrm{N}} \sum_{x=0}^{\mathrm{N}-1} |x\rangle \sum_{j=0}^{\mathrm{N}=1} \omega^{j\sigma(x)}\,|j\rangle$.

4. $|\phi_4^\sigma\rangle = \frac{1}{\mathrm{N}\sqrt{\mathrm{N}}} \sum_{x=0}^{\mathrm{N}-1} \sum_{l=0}^{\mathrm{N}-1} \omega^{-xl}\,|l\rangle \sum_{j=0}^{\mathrm{N}=1} \omega^{j(\sigma(x))}\,|j\rangle$.

The probability of measuring (y,y) is equal to $|\frac{1}{\mathrm{N}\sqrt{\mathrm{N}}}\sum_x \omega^{y(\sigma(x)-x)}|^2$. First notice that $P_{0,0} = \frac{1}{\mathrm{N}}$. If $y \neq 0$, we can use the formula, to conclude that $P_{y,y} = \frac{1}{N^3} \cdot \frac{N^2}{N-1} = \frac{1}{\mathrm{N}(\mathrm{N}-1)}$. From there, we conclude that $P_{eq} = \frac{2}{\mathrm{N}}$. □

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?*

Solution: Perform the protocol described above, and measure both registers in the computational basis. If the outcomes are the same, output "$CASE2$". Otherwise, output "$CASE1$". The answer to $Q3$ and $Q5$ give us the respective winning probabilities. In order both winning probabilities to be $> 1 - \frac{1}{2N}$, we perform the following : if the outcomes are the same, output "$CASE2$" with probability $1 - \varepsilon$ and "$CASE1$" with probability ε. If the two outcomes are different, output "$CASE2$". In the first case, the test succeeds with probability $1 - \varepsilon$. In the second case, with probability $1 - \frac{2(1-\varepsilon)}{N}$. The maximum is achieved for $\varepsilon = \frac{2}{N-2}$. □

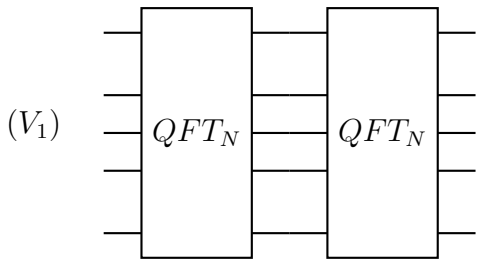
Exercise 5 (Classical complexity)**.** *Show that you can't determine with probability strictly greater than* $1/2$ *whether you are in CASE 1 or in CASE 2 using a single classical query to* O_f*. Find a procedure that will succeed with probability close to* 1 *using* 2 *classical queries to* O_f*.*

Solution: With one classical query, in each case, you get a random string. However, with 2 queries, perform the following test: query x_1, x_2 for random different values. If $f(x_1) - x_1 \mod N = f(x_2) - x_2 \mod N$ then we output CASE 1, otherwise, we output CASE 2. If we are in CASE 1, this test will always succeed, since $f(x_1) - x_1 \mod N = f(x_2) - x_2 \mod N = s$. On the other hand, if we are in CASE 2, $f(x_1), f(x_2)$ are different random strings and the probability that $f(x_1) - x_1 \mod N = f(x_2) - x_2 \mod N$ is $\Omega(\frac{1}{N})$. □

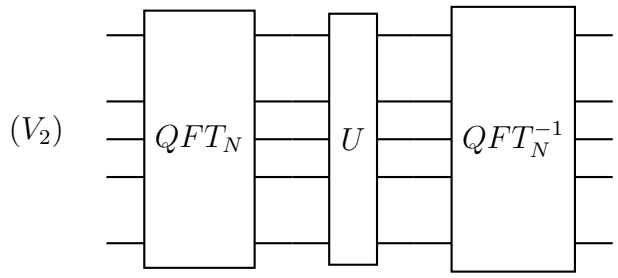
Part II: A few calculations around the QFT

Exercise 1. *We consider quantum unitaries on* n *qubits. Let* $N = 2^n$ *and* $[N] = \{0, \dots, N-1\}$ *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* $V_1(|\psi\rangle)$*.*



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 $n = 4$.*



Solution:

1.

$$\begin{aligned} V_1(|k\rangle) &= QFT_N\left(\frac{1}{\sqrt{N}}\sum_j \omega^{jk}|j\rangle\right) = \frac{1}{N}\sum_{j,l}\omega^{jk}\omega^{jl}|l\rangle \\ &= \frac{1}{N}\sum_l\left(\sum_j \omega^{(k+l)j}\right)|l\rangle = |-k \mod N\rangle = |N-k\rangle \\ V_1(|\psi\rangle) &= \frac{1}{\sqrt{2}}|0\rangle\frac{1}{\sqrt{2}}|N-1\rangle. \end{aligned}$$

2.

$$V_2(|k\rangle) = (QFT_N)^{-1} \circ U \circ \sum_j \frac{1}{\sqrt{N}}\omega^{jk}|j\rangle = \frac{1}{\sqrt{N}}(QFT_N)^{-1}\sum_j \omega^{j(k+3)}|j\rangle = |k+3 \mod N\rangle$$

We have therefore for $n = 3$:

$$V_2(|\psi\rangle) = \sqrt{\frac{1}{6}}|3\rangle + \sqrt{\frac{1}{3}}|5\rangle + \sqrt{\frac{1}{8}}(|6\rangle + |7\rangle + |1\rangle + |2\rangle).$$

and for $n = 4$:

$$V_2(|\psi\rangle) = \sqrt{\frac{1}{6}}|3\rangle + \sqrt{\frac{1}{3}}|5\rangle + \sqrt{\frac{1}{8}}(|6\rangle + |7\rangle + |9\rangle + |10\rangle).$$

□