Exercises for Introduction to Quantum Computing (physics7514) Wise 2025

L. Funcke, A. Bulgarelli and N. Dichter

1 Multiplication by Quantum Fourier Transform

In last week's exercises, we considered a quantum circuit that implements *addition* mod 2^n within quantum registers. For Shor's factoring algorithm, we also need *multiplication* mod 2^n. In particular, we need a multiply-add operation between three quantum registers (called work register $|x\rangle$, input register $|y\rangle$, and output register $|z\rangle$), which leaves the work and input registers unchanged, while changing the output register to $|z + xy \mod 2^n\rangle$.

To achieve this, we start by considering a system of *two* quantum registers with n qubits each, described by a state $|x\rangle|y\rangle = |x, y\rangle$. We define a position operator acting on the first quantum register $|x\rangle$,

$$\hat{x} = \sum_x x|x\rangle\langle x|,$$

and a corresponding momentum operator acting on the first quantum register $|x\rangle$,

$$\hat{p}_x = F_x^\dagger \hat{x} F_x,$$

where $F_x \equiv \mathrm{qFT}_x$ is a short-hand notation for the quantum Fourier transform acting on the qubit register $|x\rangle$. Analogously, we can define the position operator $\hat{y}$ and the momentum operator $\hat{p}_y$ acting on the qubit register $|y\rangle$.

a) Show the following equality for the position and momentum operators:

$$e^{\mathrm{i}\,\hat{x}\hat{p}_y} \;=\; F_y^\dagger\, e^{\mathrm{i}\,\hat{x}\hat{y}}\, F_y$$

(1 point).

b) Write x, y in their binary representations, $x = x_1 x_2 \dots x_n$ and $y = y_1 y_2 \dots y_n$, and show

$$e^{ixy} \;=\; \prod_{k,l=1}^{n} e^{ix_k y_l 2^{2n-l-k}}$$

(1 point).

c) Using the previous results, show that

$$e^{2\pi\mathrm{i}\,\hat{x}\hat{p}_y/2^n}\,|x, y\rangle = |x, x + y \mod 2^n\rangle\,,$$

which reproduces the output of the addition operation in last week's exercises *(2 points).*

d) Now, consider three quantum registers $|x\rangle$, $|y\rangle$, and $|z\rangle$ with n qubits each. Based on the previous results, how can one implement the multiply-add operation defined as

$$|x, y, z\rangle \;\rightarrow\; |x, y, z + xy \mod 2^n\rangle\,?$$

Proof that your assertion is correct *(3 points)*.

e) Implement this multiply-add operation in Qiskit *(3 points)*.