Exercises for Introduction to Quantum Computing (physics7514) Wise 2025

L. Funcke, A. Bulgarelli and N. Dichter

---

1 Addition by Quantum Fourier Transform

For Shor's factoring algorithm, we need a quantum circuit that implements addition mod 2^n within quantum registers. For this, we consider the qFT of the n-qubit state $|x\rangle = |x_1 x_2 ... x_n\rangle$,

$$\mathrm{qFT}\,|x\rangle = \frac{1}{\sqrt{2^n}} \left(|0\rangle + e^{2\pi i 0.x_n} |1\rangle\right) \left(|0\rangle + e^{2\pi i 0.x_{n-1}x_n} |1\rangle\right) ... \left(|0\rangle + e^{2\pi i 0.x_1 ... x_n} |1\rangle\right) ,$$

where $x = x_1 2^{n-1} + x_2 2^{n-2} + ... + x_n$ and $0.x_l x_{l+1} ... x_m = \frac{x_l}{2} + \frac{x_{l+1}}{2^2} + ... + \frac{x_m}{2^{m-l+1}}$. Using the periodicity of the exponential, we can rewrite the resulting state as

$$\mathrm{qFT}\,|x\rangle = \frac{1}{\sqrt{2^n}} \left(|0\rangle + e^{2\pi i \frac{x}{2}} |1\rangle\right) \left(|0\rangle + e^{2\pi i \frac{x}{2^2}} |1\rangle\right) ... \left(|0\rangle + e^{2\pi i \frac{x}{2^n}} |1\rangle\right) .$$

a) Find a gate $R_j(y)$ acting on the qubit j, such that

$$R_j(y) \left(|0\rangle + e^{2\pi i x 2^{-j}} |1\rangle\right) = \left(|0\rangle + e^{2\pi i (x 2^{-j} + y 2^{-j})} |1\rangle\right)$$

(1 point).

b) Assuming $y + x < 2^n$, find the result of the operation

$$A(y) = \mathrm{qFT}^\dagger \big(R_n(y) R_{n-1}(y) ... R_1(y)\big) \mathrm{qFT}$$

acting on an n-qubit register $|x\rangle = |x_1 x_2 ... x_n\rangle$ *(2 points).*

c) What is the result in the case of $y + x \geq 2^n$ *(1 point)*?

d) Implement the operation $A(y)$ in Qiskit, using a 3-qubit system prepared in the state $|x\rangle = |000\rangle$. Using your Qiskit implementation, verify:

$$A(5)\,|000\rangle = |101\rangle ,$$
$$A(5)\,|101\rangle = |010\rangle .$$

(3 points).

e) Now, consider y being a quantum register $|y\rangle = |y_1 y_2 ... y_n\rangle$. We define the controlled rotation gate $cR_{y_l x_j}(z)$ acting on the qubit j of $|x\rangle$ and controlled by the qubit l of $|y\rangle$:

$$cR_{y_l x_j}(z)\,|y\rangle\,|x\rangle = |y_1 ... y_n\rangle\,|x_1 ... x_{j-1}\rangle\,(R_j(z))^{y_l}\,|x_j\rangle\,|x_{j+1} ... x_n\rangle ,$$

where the rotation gate R_j is the gate of part a). Compute analytically the result of the operation

$$cA_{y,x}\left|y\right\rangle\left|x\right\rangle = \mathrm{qFT}_x^\dagger\Big(\prod_{\ell_n=1}^{n} cR_{y_{\ell_n}x_n}(2^{n-\ell_n})\prod_{\ell_{n-1}=2}^{n} cR_{y_{\ell_{n-1}}x_{n-1}}(2^{n-\ell_{n-1}})\ldots\prod_{\ell_1=n}^{n} cR_{y_{\ell_1}x_1}(2^{n-\ell_1})\Big)\mathrm{qFT}_x\left|y\right\rangle\left|x\right\rangle$$

(3 points).