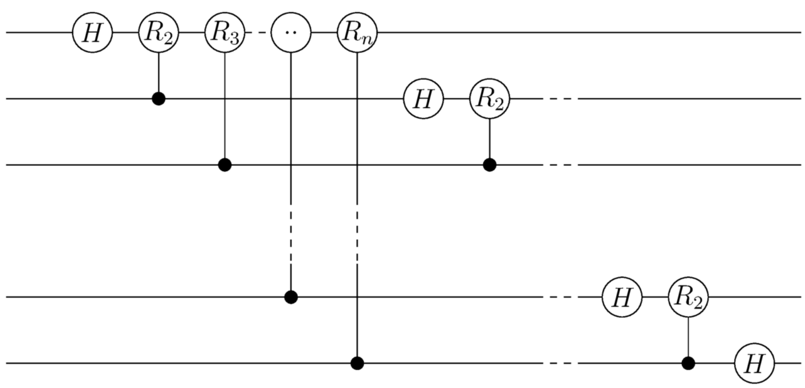
ACCQ206

Lecturer: Alex B. Grilo
Lecture # 04 - Simon's algorithm, QFT and Shor's algorithm

Quantum Fourier transform

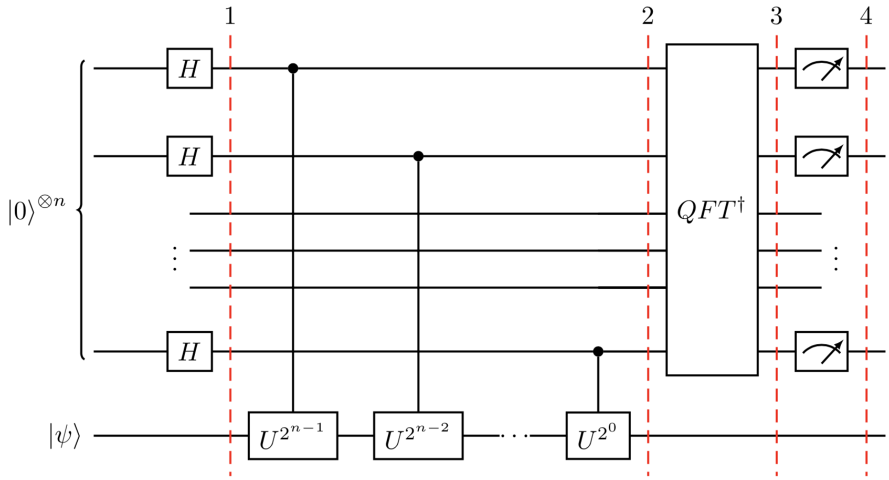
1. Show that QFT_N is unitary.
2. In this exercise we will show how to compute QFT_N for $N = 2^n$ with a gateset composed of H, $SWAP$[1] and the controlled version of one-qubit gates of the form
$$R_s = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^s} \end{pmatrix}.$$
   (a) Show that for every string $x \in \{0,1\}^n$, we have that $QFT_N|x\rangle$ is equal to
$$\left(\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi ik/2}|1\rangle\right)\right) \otimes \left(\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi ik/2^2}|1\rangle\right)\right) \otimes ... \otimes \left(\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi ik/2^n}|1\rangle\right)\right). \quad (1)$$
   (b) What is the output of the following circuit on input $|x\rangle$. [2]



   (c) What is the difference between the answer of Exercise 2b and Equation 1?
   (d) Can you propose a quantum circuit to compute QFT_N?
   (e) **Pour aller plus loin...** Show that R_s can be approximated using H, R_1, R_2 and R_3.
3. Let U be an m-qubit unitary and $|\psi\rangle$ is an m-qubit quantum state such that $U|\psi\rangle = e^{2\pi i\theta}|\psi\rangle$ for some $\theta = [0,1)$ (i.e. $|\psi\rangle$ is an eigenvector of U with eigenvalue $e^{2\pi i\theta}$). In this exercise we show that using QFT, we can estimate the eigenvalue $e^{i\theta}$ (or equivalently, that we can compute θ). For simplicuty, we assume that θ can be computed with n bits of precision (meaning that $2^n\theta$ is an integer number).
   (a) Show that $U^j|\psi\rangle = e^{2\pi i\theta j}|\psi\rangle$.

[1] Remember that $SWAP$ is the two-qubit gate such that $SWAP|a\rangle|b\rangle = |b\rangle|a\rangle$.
[2] In this picture, the gates are described using circles instead of rectangles, but that is just a different notation.

(b) Compute the state of the following computation at phases 1,2,3 and 4.



Shor's algorithm

4. Let us consider the function $f = 7^x \pmod{10}$.

   (a) What is the period of this function?

   (b) Compute the state corresponding to each step of the period finding algorithm with $q = 128$. Give an example of measurement outcome ℓ that would allow you to compute the period (i.e. $\frac{\ell}{q} = \frac{k}{r}$ in its lowerst terms).