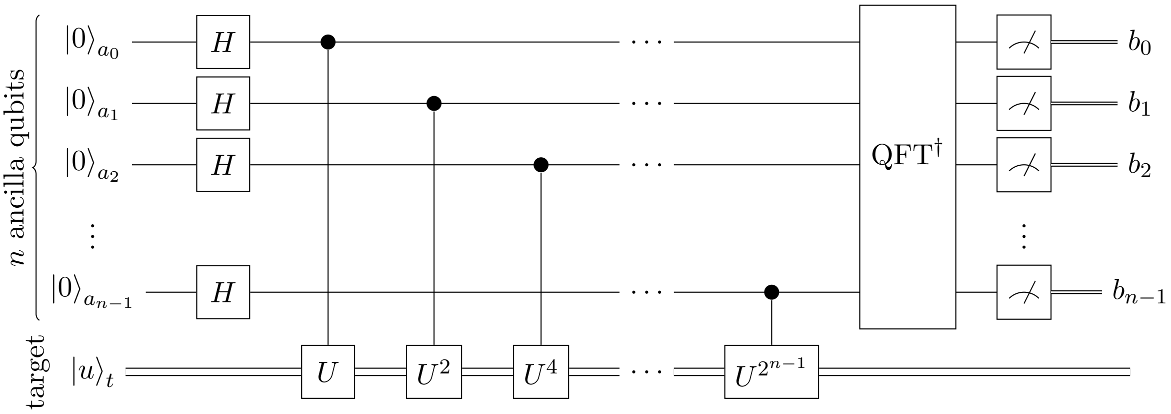
Exercise 1. *Phase estimation*

In the lecture we have seen that the quantum Fourier transform allows us to find the period of a function efficiently. Another important procedure that is enabled by the quantum Fourier transform is *phase estimation.* In the task of phase estimation the goal is to determine the eigenvalue $e^{2\pi i\varphi}$ of a unitary operator U corresponding to a given eigenstate $|u\rangle$. In order to do so, one needs oracles that perform controlled-U^{2^j} operations, where j is an integer ranging from 0 to an upper limit $n-1$. The integer n counts the number of ancillary qubits needed to perform the circuit and is a measure for the accuracy with which φ can be estimated.



The above circuit achieves phase estimation efficiently through the final measurement whose outcome is taken as an approximation $\tilde{\varphi}$ to the phase φ by means of $\varphi \approx \tilde{\varphi} = \frac{1}{2^n}\sum_{0\le j<n} 2^j b_j$.

(a) Use the fact that C-$U^k \frac{1}{\sqrt{2}}\left(|0\rangle_{a_j} + |1\rangle_{a_j}\right)\otimes|u\rangle_t = \frac{1}{\sqrt{2}}\left(|0\rangle_{a_j} + e^{2\pi i\varphi k}|1\rangle_{a_j}\right)\otimes|u\rangle_t$ to express the state of the ancilla qubits before the Fourier transform in the basis $\{|l\rangle_a\}_{l=0}^{N-1}$, where $N=2^n$ and l is binarily encoded in the ancilla qubits. (C-U^k denotes the controlled application of U^k.)
Hint: For example, if $n=4$ and $l=5$, the binary encoding would be $|5\rangle_a = |0\rangle_{a_3}\otimes|1\rangle_{a_2}\otimes|0\rangle_{a_1}\otimes|1\rangle_{a_0}$, i.e. the ancillary qubit a_{j-1} stores the j^{th} digit of the binary representation of k.

(b) Assume $\varphi = \frac{l}{2^n}$ for some integer l, $0\le l<2^n$. Show that the state of the ancillary qubits after the inverse Fourier transform is just $|l\rangle_a$.
Hint: The inverse Fourier transform QFT† acts as $|k\rangle \mapsto \frac{1}{\sqrt{N}}\sum_j e^{-\frac{2\pi i kj}{N}}|j\rangle$.

(c) Assume now that $\varphi = \frac{l+\delta}{2^n}$, with $-\frac{1}{2}\le\delta<\frac{1}{2}$. Show that the probability to measure a state $|j\rangle$ with $|j-l|>p\,(\operatorname{mod} N)$ is at most $\frac{1}{2(p-1)}$.
Hint: The coefficients of the pre-measurement state expressed in the basis $\{|l\rangle_a\}_{l=0}^{N-1}$ can be computed as a geometric sum. Then, use $|1-\exp i\theta|\le 2$ and $|1-\exp i\theta|\ge\frac{2|\theta|}{\pi}\ \forall\ |\theta|\le\pi$.

(d) Describe what measurement outcomes you would expect if the target Hilbert space starts out in a superposition $\frac{1}{\sqrt{2}}(|u\rangle_t + |v\rangle_t)$, where $|u\rangle_t$ and $|v\rangle_t$ are eigenvectors belonging to different eigenvalues.

Exercise 2. ***Shor's algorithm from phase estimation***

We will now explore the relation between period finding and phase estimation. The former can be reduced to the latter in some special but relevant cases.

The key element to Shor's algorithm as we encountered it in the lecture was a method to find the *period* of the function $f(x) = a^x \,(\mathrm{mod}\, M)$, with $0 < a < M$ and a and M co-prime (whether they are can be tested efficiently using Euclid's algorithm). For such a and M one defines the *order* of a to be the least positive integer r s.t. $a^r = 1 \,(\mathrm{mod}\, M)$.

(a) In the order finding problem one wants to determine the order of some specified a w.r.t. a given M, promised that a and M are co-prime (otherwise it may happen that there is no positive solution to $a^r = 1 \,(\mathrm{mod}\, M)$). Show that the order of a is equal to the period of the f defined above.

This implies that efficient order finding allows to efficiently factor numbers (by Shor). Now we go on to understand how phase estimation enables order finding. Let $m = \lceil \log M \rceil$ be the number of qubits needed to encode the number M and define the operation U as

$$U\,|x\rangle = \begin{cases} |xa \,(\mathrm{mod}\, M)\rangle & \text{if } x < M, \\ |x\rangle & \text{otherwise.} \end{cases} \tag{1}$$

acting on the space of m qubits where we again work in the computational basis $\{|x\rangle\}_{x=0}^{2^m-1}$ as in Ex. 1(a).

(b) Show that U is a unitary operation.
Hint: It will be important that a and M are co-prime.

(c) Let r be the order of a (and by Ex. 2(a) the period of f). Then $\exp\left(\frac{2\pi i s}{r}\right)$, $0 \leq s < r$, are eigenvalues of U. Find the corresponding eigenvectors $|u_s\rangle$.
Comment: Not all eigenvalues of U are of this form but we are only interested in those because they encode relevant information about r.

Hence, if we can do phase estimation for some of the eigenstates $|u_s\rangle$ we can determine r with high probability. Summing up the argument, we have seen that phase estimation for U enables order finding for a, which enables period finding for f, which in turn enables factoring via Shor's algorithm.
However, it is not as easy as that. We have observed above that in order to estimate a phase efficiently we need to be able to apply controlled-U^{2^j} operations for different j and prepare an eigenstate $|u_s\rangle$, or a superposition of them. So we can only conclude that phase estimation allows efficient factoring if we can efficiently provide these two things. The former task can be achieved by modular exponentiation.[1] The latter is more tricky because preparing a single eigenstate would require the knowledge of r.

(d) Show that $|1\rangle$ lies in the span of $\{|u_s\rangle\}_{s=0}^{r-1}$ and find its decomposition in terms of the $|u_s\rangle$. Why does this solve the problem of preparing a suitable input state to phase estimation?
Hint: Use Ex. 1(d) to argue in the answer of the last question.

[1] The interested reader can find more information about modular exponentiation and a possible way of implementing it in Box 5.2 in Nielsen & Chuang. A thorough discussion of it goes beyond the scope of this lecture (and thus in particular of this sheet).