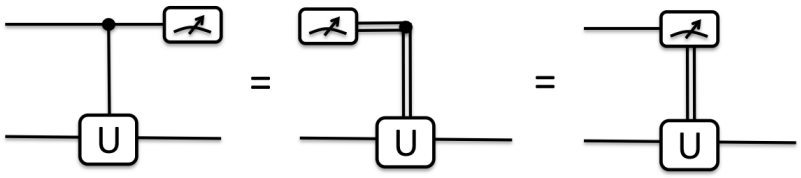
Exercises 4: Quantum Algorithms (theory chapters 4, 5, 6 and 7)

1.- Measurements, controls, and the measured quantum Fourier transform:

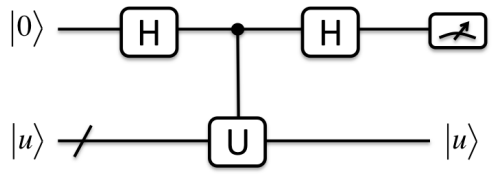
(a) A consequence of the principle of deferred measurement (see chapter on quantum circuits) is that measurements conmute with quantum gates when the qubit being measured is a control qubit, that is



(Recall that the double lines represent classical bits in the diagram). Prove the first equality. The rightmost circuit is simply a convenient notation to depict the use of a measurement result to classically control a quantum gate.

(b) Suppose the quantum Fourier transform is performed as the last step of a quantum computation, followed by a measurement in the computational basis. Use the previous result to show that the combination of quantum Fourier transform and measurement is equivalent to a circuit made only of *one* qubit gates and measurements, with classical control, and no two-qubit gates.

2.- Kitaev's phase estimation algorithm: Consider the quantum circuit



where $|u\rangle$ is an eigenstate of U with eigenvalue $e^{2\pi i\alpha}$. Show that the top qubit is measured to be 0 with probability $p \equiv \cos^2(\pi\alpha)$. Since the state $|u\rangle$ is unaffected by the circuit, it may be reused; if U can be replaced by U^k, where k is an arbitrary integer under your control, show that by repeating this circuit and increasing k appropriately, you can efficiently obtain as many bits of p as desired, and thus, of α. This type of algorithms, which estimate the eigenvalue of an unitary operator for a given eigenvector, are called *phase estimation algorithms*, and are important in a wide variety of contexts.

3.- Very large entanglement is necessary for exponential speed-up:

(a) Consider a quantum circuit with $2n$ qubits, where the initial state is a product state of all the qubits, e.g. $|\psi\rangle = |0\rangle^{\otimes 2n}$. Moreover, the quantum circuit consists only of one-qubit gates. Show that the number of real parameters necessary to describe classically the quantum state of the system at any step in the quantum circuit is, at most, $6n$. This scaling is *polynomial in the size of the system*, and therefore *efficient*.

(b) Next, consider a quantum circuit with $2n$ qubits where the quantum state at every step can always be written as a tensor product of states involving, at most, $\log n$ qubits. Show that this time the number of real parameters necessary to describe the system at every step is, at most, $2n(n-1)/\log n$. This scaling is again efficient, and can be handled classically with low effort.

(c) Show that for an entangled quantum state of $\log n$ qubits, the Schmidt rank with respect to any bipartition is, at most, $\sqrt{n}$, and therefore the entanglement entropy of any bipartition is bounded by $S \leq (1/2)\log n$.

(d) The quantum state in Shor's quantum factoring algorithm, immediately after the modular exponentiation operation, is given by

$$\frac{1}{2^{n/2}} \sum_{q=0}^{2^n-1} |q\rangle |a^q \mathrm{mod} N\rangle \ , \tag{1}$$

where the first ket corresponds to the source qubits, and the second to the target qubits. Compute the reduced density matrix of the target qubits, and show that the Schmidt rank of the bipartition between the target and source qubits is $O(r)$, r being the period of the modular exponentiation function. Classically hard instances of the order-finding problem are those where $r = O(N) = O(2^n)$. In such cases, the entanglement entropy between source and target is bounded by $S \leq O(n)$. Compared to the previous sections, this implies an exponentially larger amount of entanglement in the system, which is not necessarily described efficiently by classically means.

4.- Grover's algorithm for a small database: Consider an unstructured search problem with $N = 4$ elements in the database and $M = 1$ marked element.

(a) How many queries to the database are needed, classically, to find the marked item on average? and in the worst case?

(b) How many queries to the database are needed, using Grover's quantum search algorithm, to find the marked item and with which probability?

(c) Repeat all the above for the case of $N = 10$ and $M = 3$, where the aim is to find any of the marked elements.