Problem 1

QMA is informally the class of problems that can be efficiently checked on a Quantum Computer given a "witness" quantum state related to the answer to the problem. Also, the $k-$Hamiltonian problem has been shown to be $QMA-$complete for different values of k. BQP is the class of problems polynomially solvable by a Quantum Computer.

Comment whether these relations are true or false, and why:

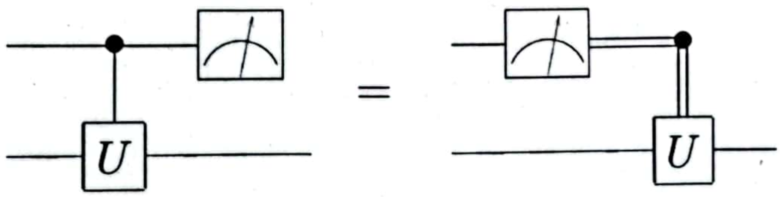
- $BQP \subseteq QMA$
- $NP \subseteq QMA$

Can we then say something about the relation between NP and BQP

Problem 2

The Quantum Fourier transform can be completely performed using a single Qubit. To do so, one has to use an strategy of measurements and classical control over successive single Quantum gates.

Show that measurements commute with quantum gates when the qubit being measured is a control qubit, as shown in the diagram (Recall that the double lines represent classical bits):



Problem 3

Given $t = 3$, $x = 7$ and $N = 15$, write explicitly the outcome state $|\Psi\rangle$ after the modular exponentiation operation for the period finding routine (*Reminder:* $\sum_{i=0}^{2^t-1} |i\rangle|x^i modN\rangle$). With this calculation you have direct access to the period r, which you have to use to obtain the factors of N using $gcd(x^{\frac{r}{2}} \pm 1, N)$.

Problem 4

In the graphical representation of the search (Grover) algorithm with a single solution, one can show that the state is a rotation on the plane defined by $|\alpha\rangle$ and $|\beta\rangle$, where

$$|\alpha\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq Solution} |x\rangle$$
$$|\beta\rangle = |solution\rangle$$

The Grover Operator is $G = (2|\Psi\rangle\langle\Psi| - I)O$, with $|\Psi\rangle = \cos\frac{\theta}{2}|\alpha\rangle + \sin\frac{\theta}{2}|\beta\rangle$, and $O(a|\alpha\rangle + b|\beta\rangle) = a|\alpha\rangle - b|\beta\rangle$. Show that after one iteration of the algorithm:

$$G|\Psi\rangle = \cos\frac{3\theta}{2}|\alpha\rangle + \sin\frac{3\theta}{2}|\beta\rangle$$

(*Hint*: Use $\sin 3A = 3\sin A - 4\sin^3 A$, and $\cos 3A = 4\cos^3 A - 3\cos A$)