Problem 1

Imagine that a new theory appears that extends Quantum Mechanics. According to this new theory (named Beyond Quantum Theory, or BQT) one can build a computing device that extends the Circuit Model of Quantum computation. Let BQTP the class of "easy" problems for this computation model. Assuming that one can prove $BQTP = P$, what can we say about the relation between BQP (the class of "easy" problems for a Quantum computer) and P? And what if we prove that $BQTP \neq P$?

[illegible]
BQTP $\geq$ P

Problem 2

For the Deutsch algorithm, show that after the evaluation of the oracle for a binary input x , the resulting state can be written as

$$U_f : |x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \to |x\rangle(|f(x)\rangle - |1 \oplus f(x)\rangle)$$
$$= |x\rangle(-1)^{f(x)} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle),$$

Problem 3

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 $\cos 3A = 4\cos^3 A - 3\cos A$)

Problem 4

The order finding routine of Shor's algorithm for factoring uses the operator

$$U_{x,N}|y\rangle = |xy(modN)\rangle$$

The eigenstates of this operator are the states

$$|u_s\rangle = \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1} exp[\frac{-2\pi isk}{r}]|x^k(modN)\rangle$$

Show that:

$$\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|u_s\rangle = |1\rangle$$

(*Hint*: Use $\sum_{s=0}^{r-1} exp(-2\pi isk/r) = r\delta_{k0}$)