1: (30 points) Consider the circuit below, composed of Hadamard and CNOT gates. What is the state of the system after all the gates have been applied?

Answer; It starts out as $|\,000\rangle$. After the first Hadamard, we get $\frac{1}{\sqrt{2}}(|\,0\rangle+|\,1\rangle)\,|\,00\rangle$. The first CNOT gate makes this $\frac{1}{\sqrt{2}}(|\,00\rangle+|\,11\rangle)\,|\,0\rangle$. The second CNOT gate makes this $\frac{1}{\sqrt{2}}(|\,000\rangle+|\,111\rangle)$. The three Hadamards then give $\frac{1}{\sqrt{2}}(|\,000\rangle+|\,011\rangle+|\,101\rangle+|\,110\rangle)$.

2: Suppose that for some large prime p we are given the state

$$\frac{1}{\sqrt{p-1}}\sum_{x=1}^{p-1}|\,x\rangle\,|\,ax+b \bmod p\rangle$$

where we do not know a or b.

2a: (20 points) Explain how we can use a quantum computer to find a with high probability. (In this problem, you need not explicitly give a circuit for the quantum Fourier transform mod p or for reversible classical computation.)

Answer: We take a QFT of *both* registers. We then get

$$\frac{1}{p\sqrt{p-1}}\sum_{s=0}^{p-1}\sum_{t=0}^{p-1}\sum_{x=1}^{p-1}|\,s\rangle\,|\,t\rangle\,e^{2\pi i(xs+(ax+b)t)/p}$$

We can factor out the $e^{2\pi ibt/p}$ term. The probability of observing $|\,s\rangle\,|\,t\rangle$ is then the square of

$$\frac{1}{p\sqrt{p-1}}\sum_{x=1}^{p-1}e^{2\pi ix(s+at)/p}.$$

The sum (without the prefactor) is either $p-1$ or 1, depending on whether $s+at=0$.

If the sum is $p-1$, the probability of observing a particular s,t pair with this sum is $\frac{p-1}{p^2}$, and when we sum over all possible such s,t pairs, we get $\frac{p-1}{p}$. If $s\neq 0$ in such a pair, we can obtain a by division.

If the sum is 1, the probability of observing such a pair is $\frac{1}{p^2(p-1)}$, and multiplying by all the $(p-1)p$ possible such pairs, we get $\frac{1}{p}$. In this case, division will give us the wrong answer.

We thus get the right answer with probability roughly $1-\frac{2}{p}$

Answer: 2b: (10 points) Show how we can use quantum computing to find b with high probability.

We can convert this to the question in part 2a. First, take the inverse of x. This gives

$$\frac{1}{\sqrt{p-1}}\sum_{x=1}^{p-1}\left|\,x^{-1}\right\rangle\,|\,ax+b \bmod p\rangle$$

Second, multiply the first register into the second register (which we can do since $x^{-1} \neq 0$). This gives

$$\frac{1}{\sqrt{p-1}} \sum_{x=1}^{p-1} |\, x^{-1} \rangle \, |\, a + bx^{-1} \bmod p \rangle \, .$$

Now, changing x^{-1} to y, we obtain the same state as in part (a), with the variables a and b reversed:

$$\frac{1}{\sqrt{p-1}} \sum_{y=1}^{p-1} |\, y \rangle \, |\, a + by \bmod p \rangle \, .$$

3: (30 points) Suppose we have a quantum algorithm which applies U_1, U_2, U_3, ..., U_n to the initial state. Let us start with state $|\, \psi \rangle$. Let us call the state of the system after k steps $|\, \psi_k \rangle$. Thus,

$$|\, \psi_k \rangle = U_k U_{k-1} \ldots U_2 U_1 \, |\, \psi \rangle$$

After the kth step, someone comes and applies a projective measurement to the first qubit using the basis $|\, 0 \rangle \, , |\, 1 \rangle$. The rest of the algorithm, consisting of the applications of the unitaries U_{k+1}, ..., U_n, proceeds normally. Suppose that the probability of the measurement outcome $|\, 0 \rangle$ is at least $1 - \epsilon$ for $\epsilon = 0.0001$. Prove that if the measurement outcome is $|\, 0 \rangle$, the final state is not very different from $|\, \psi_n \rangle$.

Answer: Let's assume the probability is exactly $1 - \epsilon$ for simplicity. At the kth step, since we know the outcome $|\, 0 \rangle$ has probability $1 - \epsilon$, the state must be of the form (for some $|\, \phi_0 \rangle$ and $|\, \phi_1 \rangle$ on the second through last qubits.

$$U_k \ldots U_1 \, |\, \psi \rangle = \sqrt{1-\epsilon} \, |\, 0 \rangle \, |\, \phi_0 \rangle + \sqrt{\epsilon} \, |\, 1 \rangle \, |\, \phi_1 \rangle$$

Now, after it is measured, the state is

$$|\, 0 \rangle \, |\, \phi_0 \rangle$$

We want the distance between these two states. By the triangle inequality, this is less than

$$\big| \, |\, 0 \rangle \, |\, \phi_0 \rangle - \sqrt{1-\epsilon} \, |\, 0 \rangle \, |\, \phi_0 \rangle \, \big| + \big| \, \sqrt{1-\epsilon} \, |\, 0 \rangle \, |\, \phi_0 \rangle - U_k \ldots U_1 \, |\, \psi \rangle \, \big| \, .$$

Both these terms are easy to estimate.

4: Suppose you are given one of the two states

$$|\, \psi_1 \rangle = \tfrac{1}{\sqrt{10}} (3 \, |\, 0 \rangle + |\, 1 \rangle) \qquad |\, \psi_2 \rangle = \tfrac{1}{\sqrt{10}} (3 \, |\, 0 \rangle - |\, 1 \rangle)$$

and you are offered a bet. You can guess which one it is; if you guess right, you are given \$1, but if you guess wrong, you lose \$3. One strategy you could use is unambiguous state discrimination; in this case, you will never guess wrong, but you may not always be able to make a guess. From your homework, the probability of not guessing in this case is $\langle \psi_1 | \psi_2 \rangle = \frac{8}{10}$, so if you use this strategy, you will make an average of \$.20 per quantum state.

4a: (10 points) Suppose you decide you always want to make a guess. In this case, you should make the measurement which gives you the highest probability of guessing the state correctly. What is the measurement? With what probability do you get the right state? How much money do you make per quantum state in this case? (4b and c next page)

Recall we are betting on the two states

$$|\,\psi_1\rangle = \tfrac{1}{\sqrt{10}}(3\,|\,0\rangle + |\,1\rangle) \qquad |\,\psi_2\rangle = \tfrac{1}{\sqrt{10}}(3\,|\,0\rangle - |\,1\rangle)$$

Winning gives you \$1, and losing costs you \$3. Now, let's try to calculate the maximum return per quantum state. The optimal measurement will be a POVM which has elements $E_1 = |\,v_1\rangle\langle v_1\,|$, $E_2 = |\,v_2\rangle\langle v_2\,|$ and $E_3 = |\,v_3\rangle\langle v_3\,|$. We can take $|\,v_1\rangle = \frac{1}{\sqrt{2}}(a\,|\,0\rangle + |\,1\rangle)$ and $|\,v_2\rangle = \frac{1}{\sqrt{2}}(a\,|\,0\rangle - |\,1\rangle)$, for some positive $a \leq 1$.

4b: (10 points) What is $|\,v_3\rangle$? Explain (you need not be rigorous) why the optimal measurement will have this form.

4c: (10 points) What is the a which maximizes the expected return per quantum state, and what is that return?