You have 60 minutes. No notes, books, computers, phones, etc. are allowed.

You may cite any definitions and theorems discussed in class, homework, or project work. You do not have to re-derive that material. You should not use material, that we haven't studied, without developing it first.

If a problem is ambiguous, then ask for clarification. If it remains unclear, then explain your interpretation in your answer. Never interpret a problem in a manner that renders the problem trivial.

Show all of your work, in as organized a manner as possible. Incorrect answers with solid work often earn partial credit. Correct answers without explanatory work rarely earn full credit.

Good luck. :)

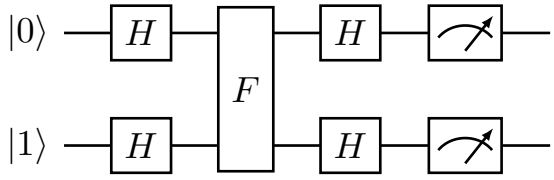
A. We have defined a *state* to be a unit vector, with the caveat that two unit vectors, that are global phase changes of each other, are really the same state. We have defined a *gate* to be a unitary matrix. Should that definition also come with a caveat?

B. Recall that the two-qbit CNOT gate corresponds to the one-bit identity function $f(\alpha) = \alpha$. So, if we feed $|\alpha\rangle \otimes |0\rangle$ into CNOT, we get

$$\text{CNOT} \cdot (|\alpha\rangle \otimes |0\rangle) = |\alpha\rangle \otimes |0 \oplus f(\alpha)\rangle = |\alpha\rangle \otimes |\alpha\rangle.$$

This seems to be a way around the no-cloning theorem. Discuss.

C. The circuit below is a modified version of Deutsch's algorithm. Does it still solve Deutsch's problem, or does it solve another problem, or does it do nothing of value?



D. Here's a quantum cryptosystem similar to that of Bennett (1992). Two friends, Ariko and Babatope, repeat the following core protocol many times to build a one-time pad.

First, Ariko flips a coin to choose a classical state $|\alpha\rangle = |0\rangle$ or $|\alpha\rangle = |1\rangle$. Ariko flips another coin to choose a gate $U = I$ or $U = H$. Ariko sends $|\psi\rangle = U|\alpha\rangle$ to Babatope.

Second, Babatope receives $|\psi\rangle$. He flips a coin to choose a gate $V = I$ or $V = H$. Babatope computes $|\beta\rangle = \text{measure}(V|\psi\rangle)$.

Third, Ariko tells Babatope what U is, and Babatope tells Ariko what V is. If $U \neq V$, then the procedure fails; they start over at the beginning. If $U = V$, then the procedure succeeds; Ariko and Babatope both know the random bit value $|\alpha\rangle = |\beta\rangle$.

Now suppose that Einar eavesdrops. As the qbit carrying $|\psi\rangle$ passes by, he measures that qbit. Later, he learns whether $U = V$.

So here's my question: Can Ariko and Babatope detect Einar's eavesdropping? (Your response should include calculations that compare and contrast this situation with that of Bennett (1992). Use the back of this sheet?)