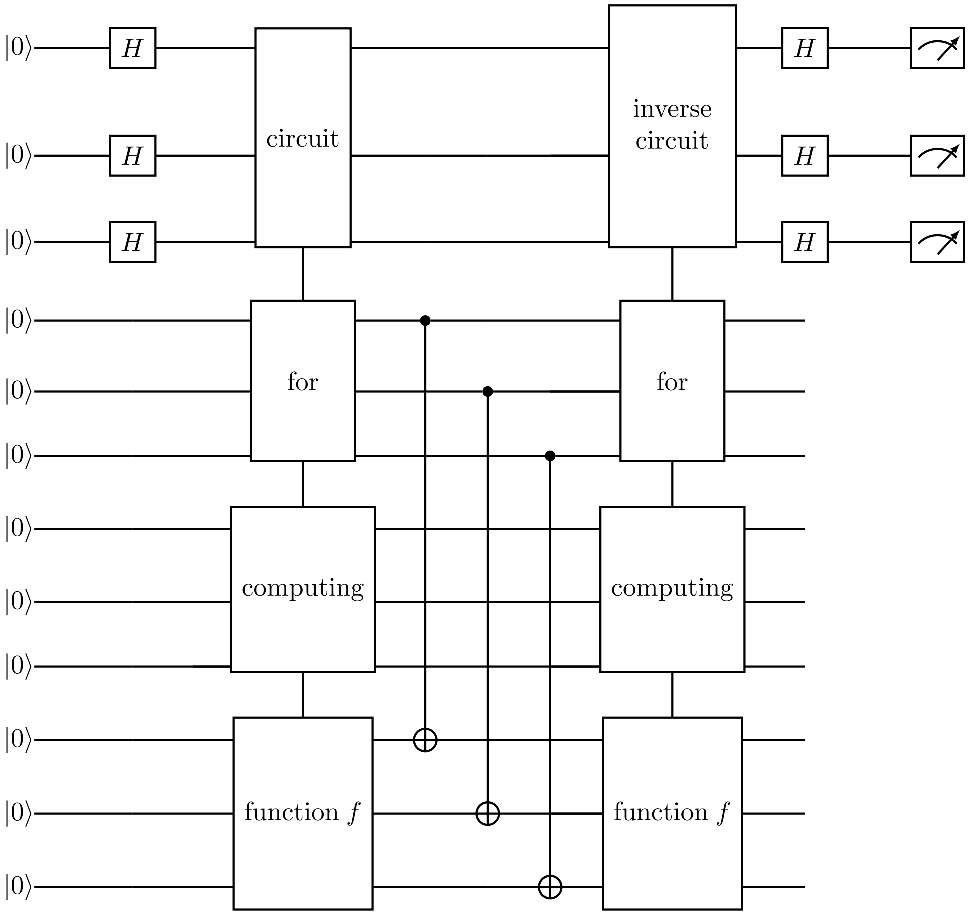
Homework 6 Clarification

2. If you don't erase the workbits in a quantum computer, it can cause your algorithm to get incorrect results. Here is an example.

   Consider Simon's algorithm. Suppose you want to test Simon's algorithm experimentally to prove that it works. Obviously, you're not going to implement an oracle in one step. You'll implement your oracle by some quantum circuit that might require extra workbits, and in the intermediate stages of your implementation, these workbits might fill up with junk bits.

   The right way of doing this uses the following circuit:



   Here, you compute the function $f(x)$, which possibly gives you some junk in the work bits, you copy the result $f(x)$ into the fourth register, and then you uncompute the function $f(x)$ by reversing the circuit that computed it.

After the Hadamard gates, your quantum computer is in the state

$$\sum_{x=0}^{2^L-1} |x\rangle\,|0\rangle\,|0\rangle\,|0\rangle\,.$$

After the circuit for x, your quantum computer is in the state

$$\sum_{x=0}^{2^L-1} |x\rangle\,|f(x)\rangle\,|\mathrm{junk}_x\rangle\,|0\rangle\,.$$

After the CNOTs, your quantum computer is in the state

$$\sum_{x=0}^{2^L-1} |x\rangle\,|f(x)\rangle\,|\mathrm{junk}_x\rangle\,|f(x)\rangle\,.$$

And after the inverse function, your quantum computer is in the state

$$\sum_{x=0}^{2^L-1} |x\rangle\,|0\rangle\,|0\rangle\,|f(x)\rangle\,.$$

where applying the Hadamard transform will result in Simon's algorithm.

My question is: why do you need to reverse the function? Suppose you just leave out the circuit that uncomputes $f(x)$. Does Simon's algorithm still work? Why or why not? To make the problem easier, you may assume that for x and y with $x \oplus c = y$, you have $|\mathrm{junk}_x\rangle \neq \left|\mathrm{junk}_y\right\rangle$.