Exercise sheet 4

1. **Hidden slope**

   For a prime p and two numbers a, b, with $1 < a, b < p$, consider the quantum state

   $$\frac{1}{\sqrt{p}} \sum_{j=0}^{p-1} |j \pmod p\rangle \, |aj + b \pmod p\rangle$$

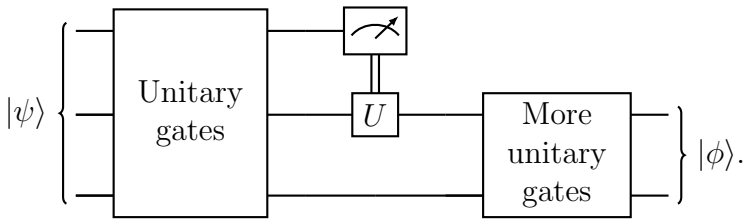
   Hint: there are two techniques that we've seen in class that you might use to attack parts (a) and (b). One is the quantum Fourier transform and the other is phase estimation. One of these techniques works substantially better than the other.

   (a) Show that if you are given one copy of this quantum state, then with a quantum computer, you can find a with high probability (i.e., with probability going to 1 as p goes to ∞).

   (b) Show that you can also find b with high probability (i.e., with probability going to 1 as p goes to ∞).

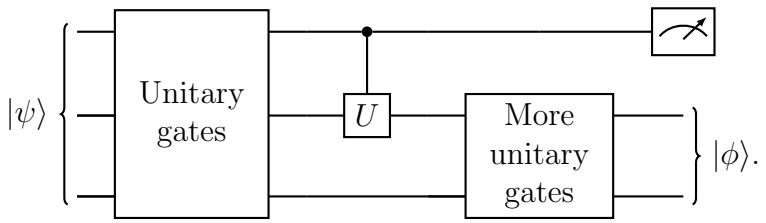
   (c) Show that no quantum algorithm can identify a with probability 1.

2. **The Principle of Deferred Measurement** Suppose you have the quantum circuit below:



   In the middle of this circuit, we measure a qubit, and use it as a classical control for a unitary gate that applies U if the measurement result is 1 and applies I if the result is 0.

   Show that we this circuit gives the same outcomes with the same probabilities if instead we apply a quantum C-U gate and wait and measure the qubit at the end:



3. **A watched pot doesn't get a quadratic speedup** Suppose an impatient person is running Grover's algorithm, and roughly every K steps checks to see whether the state is a solution state with a projective measurement. (They don't actually measure which state the computer is in, but just measure whether it is in a marked site.) Assume that they check the solution after a random number of steps between K and $2K$. Will they eventually find a solution state? Approximately how long will it take? Assume there are M solution states out of N states.