1. A generator g of the multiplicative group modulo P is a number such that $g^{P-1} = 1(\text{mod } P)$, but $g^k \neq 1(\text{mod } P)$ for any $1 < k < P-1$. As far as I know, we know of no classical algorithms, even probabilistic ones, for testing whether g is a generator mod P.

   Show how you can use the discrete log algorithm to test whether something is a generator g modulo P. (At least with a high probability of success.)

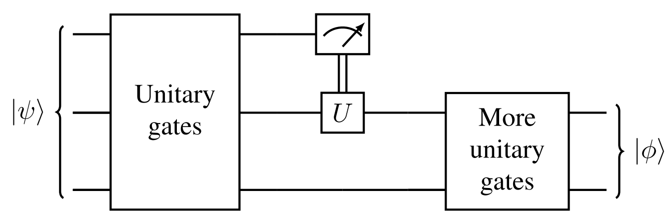
   Solution: There are multiple ways to do this problem, and full credit should be given to all valid solutions.

   Suppose we choose a random x mod P. What is the chance that it is not in the subgroup generated by g? The chance is at least $\frac{1}{2}$, because Lagrange's theorem says that the size of a subgroup divides the size of the group.

   Another way of seeing this is: we know that $g^{P-1} \equiv 1$ (mod P) Since g is not a generator, we know that $g^{\frac{P-1}{k}} \equiv 1$ (mod P). So there are only $\frac{P-1}{k}$ powers of g, and the probability that a random number between 1 and $P-1$ is not a power of g (mod P) is $\frac{k-1}{k}$, which is at most $\frac{1}{2}$. So with probability at least $\frac{1}{2}$, the discrete log algorithm will never work when applied to a find the discrete log of h with respect to g mod P. This will tell you that g is not a generator.

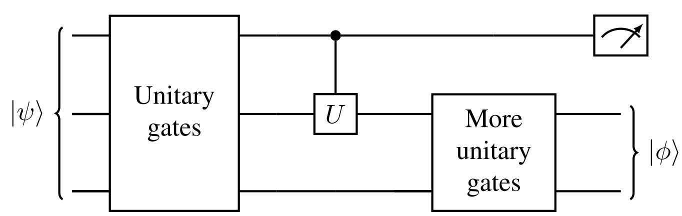
2. *The Principle of Deferred Measurement*

   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:



   Solution: Suppose we have a chance of probability p of measuring $|0\rangle$ state and probability q of measuring $|1\rangle$ when we make the measurement. Then the state right before the measurement must be

$$\sqrt{p}\,|0\rangle\,|\chi_0\rangle + \sqrt{q}\,|1\rangle\,|\chi_1\rangle\,.$$

And if we let the "more unitary gates" implement the transformation U to the system, we see that $U|\chi_0\rangle - |\phi_0\rangle$ and $U|\chi_1\rangle = |\phi_1\rangle$, where $|\phi_0\rangle$ and $|\phi_1\rangle$ are the states of the output when we measured $|0\rangle$ and $|1\rangle$, respectively. Now, applying U to the state of the system when we delay the measurement, we get

$$\sqrt{p}\,|0\rangle\,U\,|\chi_0\rangle + \sqrt{q}\,|1\rangle\,U\,|\chi_1\rangle\,,$$

and the delayed measurement gives us a 0 and $U|\chi_0\rangle = |\phi_0\rangle$ with probability p, and and a 1 and $U|\chi_1\rangle = |\phi_1\rangle$ with probability 1, the same probabilities and the same outcomes as if we hadn't delayed the measurement.

3. 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.

   Solution: In this problem, we assume that $M << N$, and K is a constant. Recall that in Grover's algorithm, our state lives in the $|\alpha\rangle\,, |\beta\rangle$ plane, where $|\alpha\rangle$ is the non-solutions state and $|\beta\rangle$ is the solutions state. If the angle between the uniform superposition state and $|\alpha\rangle$ is $\theta/2 \approx \sqrt{\frac{M}{N}}$, then each iteration of the Grover step rotates our state $|\psi\rangle$ by $2\theta \approx 2\sqrt{\frac{M}{N}}$ radians.

   The key to this question is that when we don't know the value of M, we don't know what's the right number of steps to run this Grover step. A correct strategy, as discussed in lecture, is to first try running 5-10 steps and measure, then try running 10-20 steps and measure, then try 20-40 steps and so on. This strategy guarantees that we will succeed in expected $O(\sqrt{\frac{N}{M}})$ steps. However, if we are impatient and only tries one interval, namely the $[K, 2K]$ interval, then if K is not a good choice, we will have low probability of success in every iteration.

   More precisely, suppose we ran cK Grover steps, then the probability of measuring $|\beta\rangle$ is

$$\sin(cK\sqrt{\frac{M}{N}})^2 \approx O(K^2M/N).$$

   Therefore, the expected number of iterations is $O(N/K^2M)$, which means the expected number of Grover steps is $O(N/KM)$. If K is a constant, then we need to run for $O(N/M)$ steps, which is much worse than the exponential approach.