Name: **Huan Q. Bui**
Course: **8.370 - QC**
Problem set: **#8**
Due: Wednesday, Nov 16, 2022
Collaborators/References: Piazza

1. A generator g of the multiplicative group modulo P is a number such that $g^{P-1} = 1 \mod P$, but $gk \neq 1 \mod P$ 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.

While not explicit, the phrasing of the problem implies that P is prime: since the order of a generator g of $(\mathbb{Z}/P\mathbb{Z})^\times$ is the order of the group, $P-1$, we must have $\phi(P) = P-1$, which is true in general if P is prime. Now, I'm not sure why we have to use the discrete log algorithm here, especially since we do not know of *a* generator g for the multiplicative group modulo P to begin with. Instead, given some element $h \in (\mathbb{Z}/P\mathbb{Z})^\times$, we can use the **period-finding algorithm** to efficiently compute the order r of h. Once done, we simply compare r to the order of $(\mathbb{Z}/P\mathbb{Z})^\times$, which is $\phi(P) = P-1$. If $r = P-1$ then h is a generator of $(\mathbb{Z}/P\mathbb{Z})^\times$. Otherwise, h is not a generator of $(\mathbb{Z}/P\mathbb{Z})^\times$.

Okay but what if we absolutely have to use the discrete logarithm algorithm?

2. The Principle of Deferred Measurement

Suppose the state of the system after the first set of unitaries is

$$|\Psi\rangle = |0\rangle_1 |\alpha_0\rangle_2 |\psi_0\rangle + |1\rangle_1 |\alpha_1\rangle_2 |\psi_1\rangle .$$

Then after the measurement and possibly the unitary gate U on the second qubit, the state of the system is

$$|\Psi'\rangle = |j\rangle_1 U^j \left|\alpha_j\right\rangle_2 \left|\psi_j\right\rangle$$

where $j \in \{0, 1\}$ is the measurement outcome. After the last set of unitaries $\mathcal{U}$, the state of the system is

$$|\Psi''\rangle = |j\rangle_1 \mathcal{U} U^j \left|\alpha_j\right\rangle_2 \left|\psi_j\right\rangle .$$

If the measurement outcome is $j = 0$ then we have

$$|\Psi''\rangle_{j=0} = |0\rangle_1 \mathcal{U} |\alpha_0\rangle_2 |\psi_0\rangle .$$

Else if $j = 1$:

$$|\Psi''\rangle_{j=1} = |1\rangle_1 \mathcal{U} U |\alpha_1\rangle_2 |\psi_1\rangle .$$

In the second case, the state of the system after first state of unitaries is the same as before. So we look at the system after the controlled-unitary U:

$$|\Phi'\rangle = |0\rangle_1 |\alpha_0\rangle_2 |\psi_0\rangle + |1\rangle_1 U |\alpha_1\rangle_2 |\psi_1\rangle .$$

Now we apply the second set of unitaries $\mathcal{U}$. By linearity we have

$$|\Phi''\rangle = |0\rangle_1 \mathcal{U} |\alpha_0\rangle_2 |\psi_0\rangle + |1\rangle_1 \mathcal{U} U |\alpha_1\rangle_2 |\psi_1\rangle$$

Now we measure the first qubit. Let the measurement outcome be j, then the state of the system is

$$|\Phi''\rangle_j = |0\rangle_1 \mathcal{U} |\alpha_0\rangle_2 |\psi_0\rangle \delta_{j,0} + |1\rangle_1 \mathcal{U} U |\alpha_1\rangle_2 |\psi_1\rangle \delta_{j,1}.$$

In particular, if $j = 0$ then

$$|\Phi''\rangle_{j=0} = |0\rangle_1 \mathcal{U} |\alpha_0\rangle_2 |\psi_0\rangle$$

Else if $j = 1$ then

$$|\Phi''\rangle_{j=1} = |1\rangle_1 \mathcal{U} U |\alpha_1\rangle_2 |\psi_1\rangle$$

which is exactly what we have before.

3. Impatient runner of Grover's algorithm...

Let k be such that $K < k < 2K$. And let S denotes the space of solutions. By definition, $|S| = M$. The state of the computer after k Grover iterations is

$$G^k |\psi\rangle = \cos\left(\frac{2k+1}{2}\theta\right)|\alpha\rangle + \sin\left(\frac{2k+1}{2}\theta\right)|\beta\rangle .$$

Here

$$|\alpha\rangle = \frac{1}{\sqrt{N-M}}\sum_{x\notin S}|x\rangle \quad \text{and} \quad |\beta\rangle = \frac{1}{\sqrt{M}}\sum_{x\in S}|x\rangle \quad \text{and} \quad \cos\frac{\theta}{2} = \sqrt{\frac{N-M}{N}}$$

Now, the impatient experimenter checks whether this state is in a solution state by measuring in the $|\alpha\rangle, |\beta\rangle$ basis. The probability that he finds the state to be in the solution space is

$$p = \sin^2\left(\frac{2k+1}{2}\theta\right).$$

If he finds that the state is in the solution space then he stops. Else, he repeats the process. Under the assumption that $M \ll N$ and the additional assumption that $K\theta \ll \pi/2$, we make small-angle approximation on p to obtain

$$p \approx \left(\frac{2k+1}{2}\theta\right)^2.$$

Now $\theta = 2\,\mathrm{acos}\left(\sqrt{(N-M)/N}\right)$. Since $M \ll N$, we can expand this in terms of (small) M/N to get

$$\theta \sim \sqrt{\frac{M}{N}} + \frac{(M/N)^{3/2}}{6} + O((M/N)^{5/2})$$

With this, we have

$$p \approx \left(\frac{2k+1}{2}\right)^2 \frac{M}{N}.$$

Suppose the experimenter measures $j-1$ failures before seeing the first success at the jth measurement. Then the probability for this event is

$$\Pr(X = j) = (1-p)^{j-1}p$$

The expected value for the random variable X, which is the expected number of trials before the first success, is thus

$$E[X] = \frac{1}{p} = \frac{N}{M}\left(\frac{2}{2k+1}\right)^2.$$

Since $K < k < 2K$, the experimenter has to try $\boxed{O(N/MK^2)}$ times.