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

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 $(\mathbb{Z}/P\mathbb{Z})^\times$.

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

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

In order to check whether the computer is in a solution state, the impatient runner must first make a copy of the output bit into another register using the quantum FANOUT gate which sends $|0\rangle|0\rangle \rightarrow |0\rangle|0\rangle$ and $|1\rangle|0\rangle \rightarrow |1\rangle|1\rangle$. Next, he checks whether this state is in a solution state by measuring in the $|\alpha\rangle, |\beta\rangle$ basis.