MIT 8.370 Pset 8

Vassilios Kaxiras

November 19, 2021

Solution (1)**.** Suppose we can compute the discrete log problem, finding x for $g^x = h \mod p$ given h and a generator g.
So, if we are given g, we can choose a random h between 1 and $p-1$, and run the discrete log algorithm to obtain x. If g is a generator, we will succeed. If g is not a generator, it generates a subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$, and by Lagrange's Theorem this subgroup can have size at most half of $(\mathbb{Z}/p\mathbb{Z})^\times$. Thus no matter what the discrete log algorithm outputs in this case, at least half the time we will get an incorrect value, because at least half of the values of h will have no solution to $g^x = h$. It is easy to check if $g^x = h$ once you have x, so we can run n trials of this procedure, randomly picking an h and trying to find its discrete log. If we find an x for every one of the n values of h we choose, we can conclude that g is a generator, and we will be wrong with probability

$$\leq \frac{1}{2^n} \tag{1}$$

if we find a wrong x at any step, then we immediately know g is not a generator.
On the other hand, g is a generator if and only if the period of g^i is $p-1$. So, we can apply phase estimation and calculate the period r of g^i, and then conclude it is a generator if $r = p-1$.

Solution (2)**.** Denote the first unitary gates that act on all three qubits as U_0. Denote the controlled gate as U_1 (labelled U in the diagram), and denote U_2 as the gates applied to only the second and third qubits after U_1.
The state before the U_1 step can be written as

$$U_0|\psi\rangle = a_0|0\rangle|\phi_0\rangle + a_1|1\rangle|\phi_1\rangle \tag{2}$$

where $|\phi_0\rangle, |\phi_1\rangle$ are states of the second and third qubits.
If we measure sooner rather than later, we will have two results. If we measure 0, U_1 will not be applied and we will end up with the state

$$|0\rangle(U_2|\phi_0\rangle) \tag{3}$$

this has probability $|a_0|^2$.
If we measure 1, we will apply U_1 and obtain the state

$$|1\rangle(U_2(U_1 \otimes I)|\phi_1\rangle) \tag{4}$$

with probability $|a_1|^2$.
Now, if we measure later, we first apply a controlled U_1 gate on the first two qubits, followed by U_2 on the last two:

$$(I \otimes U_2)(CU_1 \otimes I)U_0|\psi\rangle = a_0|0\rangle(U_2|\phi_0\rangle) + a_1|1\rangle(U_2(U_1 \otimes I)|\phi_1\rangle) \tag{5}$$

if we now measure, we immediately see that we get the same results for the same probabilities.

Solution (3)**.** Suppose this person is measuring in the $|\alpha\rangle, |\beta\rangle$ basis, where $|\alpha\rangle$ comprises of all the unmarked states, and $|\beta\rangle$ comprises of all the marked states. This way the person measures the state as marked or not. If they fail, and measure unmarked, the state will collapse to $|\alpha\rangle$. So, after each failure, they restart the algorithm at $|\alpha\rangle$. If we presume $M \ll N$, then we can approximate the algorithm as starting at $|\alpha\rangle$ on the first try as well (even though it actually starts at $|\psi\rangle = \sqrt{\frac{N-M}{N}}|\alpha\rangle + \sqrt{\frac{M}{N}}|\beta\rangle$). After each try, the state is moved an angle θ counterclockwise in the $|\alpha\rangle$ - $|\beta\rangle$ plane, where

$$\sin(\theta/2) = \sqrt{\frac{M}{N}} \tag{6}$$

thus the probability of measuring $|\beta\rangle$ after K steps is

$$\sin^2(K\theta) \tag{7}$$

so the number of tries, N, that it will take the person to succeed is a random variable with the First Success distribution, which means eventually the person will succeed, but on average it will take

$$\boxed{\frac{K}{\sin^2(K\theta)} \approx \frac{N}{4KM}} \tag{8}$$

total steps (tries times K), where we have included an approximation for $K\theta \ll 1$.

Solution (4)**.** (a) We see

$$O_x|\psi\rangle = \sqrt{\frac{N-M}{N}}|\alpha\rangle + e^{i\theta}\sqrt{\frac{M}{N}}|\beta\rangle = |\psi\rangle + (e^{i\theta}-1)\sqrt{\frac{M}{N}}|\beta\rangle \tag{9}$$

So one iteration, we have the state

$$G|\psi\rangle = ((1-e^{i\theta})|\psi\rangle\langle\psi| - I)\left(|\psi\rangle + (e^{i\theta}-1)\sqrt{\frac{M}{N}}|\beta\rangle\right) \tag{10}$$

If we want to be entirely in the $|\beta\rangle$ state after this one iteration, since $|\psi\rangle$ contains non-zero $|\alpha\rangle$ dependence, we must have that the coefficient in front of $|\psi\rangle$ above is 0, since that is the origin of all $|\alpha\rangle$ dependence. Thus the coefficient of $|\beta\rangle$ must have norm 1:

$$1 = \left|(e^{i\theta}-1)\sqrt{\frac{M}{N}}\right|^2 = \frac{M}{N}(2-2\cos\theta) \tag{11}$$

since $0 \leq 2 - 2\cos\theta \leq 4$, we have

$$\boxed{\frac{N}{M} \leq 4} \tag{12}$$

(b) If we can get $\frac{M}{N} \geq \frac{1}{4}$, then since we know N, M we can find the θ' necessary to complete the algorithm in one step from that point:

$$\theta' = \cos^{-1}\left(1 - \frac{N}{2M}\right) \tag{13}$$

so we can modify the standard Grover algorithm to perform as many iterations as we need to get to a state that has effective M' such that we meet the above bound. Specifically, since after k iterations of the standard algorithm we are in the state

$$\sin\left((2k+1)\frac{\theta}{2}\right)|\alpha\rangle + \cos\left((2k+1)\frac{\theta}{2}\right)|\beta\rangle \tag{14}$$

where

$$\sin(\theta/2) = \sqrt{\frac{M}{N}} \tag{15}$$

We want to perform k steps such that

$$\sin\left((2k+1)\frac{\theta}{2}\right) = \sqrt{\frac{M'}{N}} \geq \sqrt{\frac{1}{4}} = \frac{1}{2} \implies (2k+1)\frac{\theta}{2} \geq \frac{\pi}{6} \implies k \geq \frac{\pi}{6\theta} - \frac{1}{2} \tag{16}$$

so given N, M, we perform $k = \lceil \frac{\pi}{6\theta} - \frac{1}{2} \rceil$ steps of the regular Grover algorithm, and then calculate

$$\theta' = \cos^{-1}\left(1 - \frac{N}{2M'}\right) = \cos^{-1}\left(1 - \frac{1}{2\sin^2\left((2k+1)\frac{\theta}{2}\right)}\right) \tag{17}$$

and perform one step of the modified Grover algorithm with phase θ'.