*An equation for me has no meaning, unless it expresses a thought of God.*
*– Srinivasa Ramanujan*

# Problem Set 5

**PCMI USS, Summer 2023**

1. In Grover, we argued that the map $U = 2|\psi\rangle\langle\psi| - I$ is a reflection and therefore unitary. Express $U$ in math notation (yellow) and show that $U$ is in fact unitary. Style points if you can also prove this this in Dirac notation.

2. (**Single-query Grover**)

   (a) Consider Grover's problem of identifying $a \in \{0, \ldots, N-1\}$. Suppose that you are only given one classical query to the oracle. With what probability can you correctly identify the answer $a$?

   (b) Now suppose instead that you are given only one quantum query? With what probability can you determine $a$? How does this probability compare with your answer to (a)?

   (c) Now suppose you are given $k$ classical queries, where $k > 1$, but still pretty small (compared with $\sqrt{N}$, say.) With what probability can you identity $a$ correctly? Now analyze $k$ quantum queries; i.e, say you do $k$ Grover iterations and then measure. With approximately what probability do you get the correct value of $a$?

   (d) Your friend Jeff is excited by the answers to (a), (b), and (c). "Dude, I'm so jazzed that a single quantum query does *waaay* better than a single classical query. I even used this to discover a cool new quantum search algorithm. Like, you want to see it?" Jeff goes on to explain that you can just repeatedly do a single quantum query followed by a measurement. "Each time, the correct answer is more likely than any other answer, so if you run single-query Grover enough times, then the result you see most often has just *got* to be the correct value of $a$." How well can you get Jeff's idea to perform? That is, roughly how many times must you run single-query Grover to have a good shot of being able to determining $a$ correctly? Are things any better if you repeatedly run $k$-query Grover?

3. Imagine that you try to run Grover's algorithm, but you've been tricked: in violation of the promise of there being a correct answer $a$, there is, in fact, no correct answer.

   (a) Classically, is it possible to discover that you've been tricked? With how many queries?

   (b) Now consider the quantum version. Assuming there is no correct answer, describe the action of the oracle. If you run Grover's algorithm as usual, what state will you have just before you measure? What will be the result of your measurement?

(c) Can you think of a protocol to protect against such trickery? That is, assuming there is a single correct answer $a$ or no correct answer, is there a protocol that with high probability correctly outputs the value $a$ or outputs "No answer."

4. (**Grover with multiple correct answers**) In our analysis of Grover's problem, we assumed that there was only one correct answer. Now, let's assume that there are $K$ correct answers. You know the value of $K$, and you wish to find and output one of these $K$ answers.

   (a) Before reading on, think as much as possible about setting up and solving this problem. When you are so-inclined, read the remaining parts of this problem, which suggest notation and other ideas about how to approach this problem.

   (b) We'll let $f : \{0, \ldots, N-1\} \to \{0, 1\}$. denote our mystery function. Let $S_0 = f^{-1}(0)$ be the preimage of 0 (the nonanswers), and $S_1 = f^{-1}(1)$ be the preimage of 1 (the answers). We assume that $|S_1| = K > 0$ and the goal is to output an element $a \in S_1$. Any $x \in \{0, \ldots, N-1\}$ can be queried and is responded to with $f(x)$. Analyze the classical query complexity of this problem. Don't be super precise unless you want to be.

   (c) We'll use the phase kick-back trick, so quantum oracle $\mathcal{O}_f$ will act on a basis of $\mathcal{H} = \mathbf{C}^N$ by
   $$|x\rangle \longmapsto (-1)^{f(x)}|x\rangle.$$
   Explain why this is the correct equation, or at least understand why.

   (d) Let $|g\rangle$ (for good) be the equal superposition of all basis states corresponding to the answers, and $|b\rangle$ (for bad) be the superposition of all the nonanswer basis states. Write a formula for $|g\rangle$ and $|b\rangle$. Make sure you have normalized correctly. What is $\langle g|b\rangle$?

   (e) Let $|\psi\rangle$ be the equal superposition of all $N$ basis states. Show that $|\psi\rangle$ lies in the 2-dimensional plane $P$ spanned by $|g\rangle$ and $|b\rangle$. What is the angle between $|\psi\rangle$ and $|b\rangle$? Draw a picture.

   (f) Consider our favorite operator $U = 2|\psi\rangle\langle\psi| - I$. Show that $U$ maps $P$ into $P$.

   (g) Does $\mathcal{O}_f$ also map $P$ into $P$?

   (h) Give geometric descriptions of how the operators $U$, $\mathcal{O}_f$ and $U\mathcal{O}_f$ act on $P$.

   (i) Suppose you start with the equal superposition state $|\psi\rangle$, and perform $U\mathcal{O}_f$ repeatedly. Describe what happens geometrically.

   (j) Now give a quantum algorithm for finding a correct answer. Approximately how many queries does your algorithm make? With approximately what probability does your algorithm succeed?

5. (**Rigorous Grover**) In analyzing Grover, we relied heavily on geometric arguments.

   (a) Examine the analysis again. How rigorous do you think the whole argument is?

   (b) Make the argument more rigorous by analytically applying $U\mathcal{O}_a$ to the state $\cos\gamma|\varphi\rangle + \sin\gamma|a\rangle$. (The geometry tells you what the result should be, so you can use that as a guide in your proof.)