CSE439, Fall 2024 Problem Set 5 Due Fri. 11/15, 11:59pm

The **Second Prelim Exam** will be on **Thursday, Nov. 21** *in class period*. It will cover material up through section 14.7, although only up through 14.4 is reflected in past coverage and this problem set. This is the last graded homework before the exam, though there may be ungraded practice problems on the Spectral Theorem (theorem 14.1 in section 14.6 and its continuation as theorem 18.1 on pages 206–207) and/or the CHSH game (section 14.7). For next week, please read chapter 14 up through section 14.7 and the one theorem from chapter 18, as already stated on *Piazza*.

———————*-Assignment 5, due Fri. 11/15 "midnight stretchy" on CSE Autolab*———————-

(1) Exercise 10.6 on page 105, described this way: Let $f(x) = y$ be a function with arguments x and values y that are modulo $M = 2^m$. Suppose there is an unknown value k such that whenever $x_2 - x_1$ is a multiple of 2^k, $f(x_2) = f(x_1)$, and moreover, the function f takes on 2^k distinct values. Give a quantum algorithm that computes the value of k in expected time $m^{O(1)}$. (Note that the text says "...in $n^{O(1)}$ time," which intends to mean "in polynomial time" but the relevant complexity parameter is m, not $n = 2^n$ as stated there. Note that the given conditions of Shor's algorithm do not apply since M is not a product of two odd primes; this is intended to channel Simon's algorithm but with the twist of f being more than 2-to-1. Think of the arguments as m-bit binary strings and what $x_2 - x_1$ being a multiple of 2^k means then. 30 pts. total)

(2) Consider *Blum integers* $M = pq$ where the primes p and q are both congruent to 3 modulo 4. The smallest such numbers are $21 = 3 \cdot 7$, $33 = 3 \cdot 11$, $57 = 3 \cdot 19$ and (more interesting since 3 is not involved) $77 = 7 \cdot 11$. In many cases, the numbers $a < M$ that work have the property:

a is a quadratic residue mod p or a quadratic residue mod q, but not both.

Being a quadratic residue mod p means that there is an x such that $x^2 \equiv a$ modulo p. Exactly half the numbers in $1..p-1$ are quadratic residues, and similarly for q. Moreover, this bumps up to say that exactly half of the numbers $a < M$ that are relatively prime to M have the above-stated property. Thus if those numbers always worked in Shor's algorithm, we would have a very simple way to prove the claim that the part of the success probability governed by the choice of a is at least 0.5

Find, however, a number $a < 77$ that has this property and has even period r, but is not "helpful"' in the text's sense that r is a multiple of $p-1$ or of $q-1$. (That is, find a such that its period r is not a multiple of either $p-1$ or $q-1$. The term "helpful" comes from the blog post referenced at the end of chapter 12, but it is the same as the precondition for the properties called $A(r,p,q)$ and $B(r,p,q)$ in section 12.3, as expressed by the words "...provided we come upon a multiple r of $p-1$ or $q-1$.") For a hint, try making a congruent to $+1$ and/or -1 modulo the primes. And finally compute $X = a^{r/2}$ and observe that $\gcd(X-1, 77)$ and $\gcd(X+1, 77)$ yield factors after all.

(This goes to show why we've not been able to find a really simple exposition of the classical part of Shor's algorithm. This example is a little trivial, but the smallest cases I judge to be really nontrivial are for $p = 31$, $q = 43$ making $M = 1,333$ (with unhelpful period $r = 70$). That's ten times higher than the biggest M that can be run without overloading our department's machine `metallica` for intensive computing. You are welcome to try out $M = 77$ and your a on my code `qci` in `/projects/regan/QCSAT`—scroll up to see if it worked on the first try and also what value xy got measured, was it trivial? 18 pts. total)

(3) Lipton-Regan text, problem 13.7 in chapter 13. An important point is that the Grover oracle $\mathbf{U}_G$ for a particular graph G is given separately and has all the needed information about G. The oracle is also *compact* in the following sense: it uses only ℓ qubits, where $L = 2^\ell$ is the next power of 2 above the number of potential solutions. Here the number of potential solutions is the binomial coefficient $\binom{n}{3}$ (which $\sim \frac{1}{6}n^3$), since any trio of nodes could be a triangle in G.

Explain how using just $\mathbf{U}_G$ on ℓ qubits, you can find a triangle (provided one exists) with high probability in the time specified. The word "about" means the time can be technically $\tilde{O}(n^{3/2})$, where the tilde means that factors of $\log n$ are ignored. You may assume that $\mathbf{U}_G$ is already coded via quantum gates (Toffoli gates are good enough since they can simulate NAND) and can ignore how many gates or how much time it took to build it—you can treat it as a "black box." So you need not fuss over details of $\mathbf{U}_G$ and may suppose that whatever the set S of actual triangles in G, $\mathbf{U}_G$ gives you reflection around the "miss vector" $\mathbf{m}_S$. Much of this is just digesting key details of Chapter 13—including a brief recap of section 13.3 since you don't know $|S|$—with the point being how and why it works out to time $\tilde{O}(n^{3/2})$. (12 pts. total)

[For some further chitchat: A classical algorithm has to be given G not $\mathbf{U}_G$. It can brute-force search for triangles in time $\tilde{O}(n^3)$ by trying each trio of nodes. There is another way by taking the $n \times n$ adjacency matrix A of G and computing its "Boolean square" $A^{[2]}$ under the rule that any sum greater than 1 counts as 1. Then G has a triangle if and only if $A + A^{[2]}$ has an entry 2 somewhere. This can be done in the time for $n \times n$ matrix multiplication, which is currently $\tilde{O}(n^{2.37155\ldots})$. Whether this can be done in time $O(n^2)$—which is linear in the max number of edges in the graph—is a major open question in complexity theory, but it can't be less classically. Thus the back-story of this problem is that it comes closest to saying Grover's algorithm can save time at polynomial-in-n rather than exponential-in-n scales. But this is still ignoring the time needed to create $\mathbf{U}_G$ to begin with.]

(4) Lipton-Regan text, problem 14.4 in chapter 14. (If you only have the first edition, where chapter 14 is the same as the present chapter 16 on quantum walks, please let me know.) This should include a check that $\theta = \frac{\pi}{4}$, $\varphi = 0$ in Bloch sphere coordinates is the same one-qubit state vector as $[\cos(\frac{\pi}{8}), \sin(\frac{\pi}{8})]$ in Cartesian coordinates. (18 pts. total, for 78 on the set)