CSE439, Fall 2025 Problem Set 5 Due Thu. 11/6, 11:59pm

The **Second Prelim Exam** is set for **Thursday, November 20** in class period. It will be "cumulative"—meaning concepts from all of the course may be drawn on—but will focus on Chapters 8—13 and Chapter 14 up through section 14.6, as (to be) refercted in assignments 4–6. This is a short assignment, really "5A," and an assignment to be given next week will be numbered 6 but really be "5B" relative to last year. The assignments will be due on **Thursdays** again.

Reading: For next week, read Chapter 13 on Grover's Algorithm **and** Chapter 14 up through section 14.4. Note that the first pages of chapter 13 hark back to section 6.5, so please (re-)read that too—we previously only skimmed it in section 5.4 before covering section 5.5. We've actually used some of the earliest material in chapter 14, but we will focus on the nature of qubits, pure versus mixed states, and the Bloch Sphere.

———————-*Assignment 5, due Thu. 11/6 "midnight stretchy" on CSE Autolab*———————-

(1) Text, exercise 11.3 on page 117, but *modified* this way: Let M, a, f_a, r, and Q be as in the presentation of Shor's Algorithm. Now let ϕ stand for Boolean formulas with n variables, which we'll call $u_1, \ldots, u_n$, where n is such that $N = 2^n$ is the least power of 2 above M. Note that if $M = 21$ then $N = 32$, so $n = 5$; moreover $Q = 512$ but $N^2 = 1,024$. Let us *redefine* $Q = N^2$ in cases like this, so $Q = N^2 = 2^{2n}$ holds in all cases—this change matters very little in the analysis of Shor's algorithm given in lecture.

Given any number $x \in [0, \ldots, Q-1]$, we can identify x with a binary string of length $2n$. When we write $\phi(x)$, we mean taking the n *lowest-order* bits, assigning them to the variables $u_1, \ldots, u_n$, and outputting the number 1 if the result is true, 0 for false. Note that the function $\phi(x)$ has a period of length N since we use only the n low-order bits, but it might have shorter periods—indeed, it could be constant-0 or constant-1. Now define

$$f'_a(x) = f_a(x) + \phi(x) \pmod{M} = a^x + \phi(x) \pmod{M}.$$

(a) Show that f'_a has a period P that satisfies $r \leq P < Q$ (where r means the true minimum period of f_a).

(b) What is the period if $\phi(x)$ is the constant-0 function, which is the same as the formula ϕ being **unsatisfiable**? Likewise if ϕ is the constant-1 function—meaning ϕ is a **tautology**—and does the injectivity condition hold in these cases?

(c) Does the injectivity condition hold if ϕ is not constant? Say why or why not. (By the way, whether ϕ is "balanced" is not relevant here.)

(d) Explain why it is feasible to design the quantum circuits in Shor's algorithm to handle f'_a much the same way they operate on f_a.

Now we pick up the question in the text's problem: show that if Shor's algorithm applied to f'_a would be able to calculate the period P with the same nearly-constant probability as for

f_a, then we would get a quantum polynomial time algorithm for telling whether any given ϕ is (un-)satisfiable. Or whether ϕ is a tautology, which is the same as $\neg\phi$ being unsatisfiable. Those problems are **NP-hard**, so we would get the consequence that the complexity class NP is contained within BQP. This consequence is generally **not** believed—so we should suspect some reason why Shor's Algorithm fails to work in these cases.

The text question is set up to blame the failure of the injectivity condition. But—in this particular setup—is that really the whole story? What other condition about the magnitude of the period vis-à-vis M and Q might be needed—and most in particular, how might its violation deceive us in the outcomes of the algorithm? (This question is somewhat open-ended—I actually surprised myself by how close it comes—but the grading scheme starts of concretely with 4×6 points for parts (a)–(d). Then 18 more points for the final discussion to make 42 points total, but extra credit might be possible.)

(2) Take $M = 35$. Find the periods r_a of f_a for all $a \leq 17$ that are relatively prime to M. (Yes, this will involve a lot of calculator-punching. It is "good for you"—e.g. as a stress-reliever if the Bills-Chiefs game or the ICCF Women's Cricket World Cup final on Sunday are close.) For each one, say whether $X = a^{r_a/2}$ exists without being $-1 = 34 \bmod 35$, and if so, whether $\gcd(X - 1, 35)$ or $\gcd(X + 1, 35)$ gives you one of the factors. (18 points total, for 66 on the set)