ELEN 162
A. I. Zecevic

Project 1

1. Suppose that there is a 10 bit binary security key that must be entered before you can access some sensitive information that you need. You don't know what this key is, but you do have access to a quantum operator $\hat{U}_f$ that will transform function

$$\Psi_x = \psi_{x_1} \otimes \psi_{x_2} \otimes \ldots \otimes \psi_{x_{10}} \tag{1}$$

into

$$\hat{U}_f \Psi_x = -\Psi_x \tag{2}$$

if $x = x_1 x_2 \ldots x_{10}$ corresponds to the correct bit combination. For all other values of x, $\hat{U}_f$ will leave function Ψ_x unchanged. Your task in this problem will be to use operator $\hat{U}_f$ to determine the security key as efficiently as possible.

   (a) The "brute force" approach to this problem would be to randomly choose a state Ψ_x, and check if applying operator $\hat{U}_f$ changes its sign. What is the probability that this strategy will be successful after the first try? How many attempts would you have to make in the worst case scenario?

   (b) An alternative (and far more sophisticated) approach would be to use operator $\hat{U}_f$ in conjunction with Grover's algorithm. If we were to do so, how many particles would we need, and what input state Ψ should we choose as our starting point? Show how can such a state be produced using standard quantum gates.

   (c) For each of the first 50 steps of Grover's algorithm, calculate the probability that the measured state Ψ_x will match the security key. You can represent your results by plotting the probability as a function of the number of steps.

   (d) Using the results obtained in part (c), determine the minimal number of steps after which the probability of registering the correct state Ψ_x is greater than 50%. After how many steps will this probability exceed 90%, and when will it attain its maximal value?

   (e) Is this a "traditional" iterative method, where the result continues to improve as the number of iterations increases? Explain.

2. In this problem (as well as in Problems 3 and 4) we will be interested in computing the prime factors of $N = 39$ using the quantum order finding algorithm.

   (a) How many elements will group Z_N^* have in this case? Determine the order modulo 39 for each of these numbers, and identify those for which r is even and satisfies

$$x^{r/2} + 1 \neq 0 \pmod{39} \tag{3}$$

   Note: You can use any publicly available order finding calculator for this problem, since N is not a large number.

(b) Based on your answer in part (a), compute the probability that you will randomly choose a number $x \in Z_{39}^*$ whose order is even and satisfies condition (1).

3. For any $x \in Z_N^*$ that meets the conditions described in Problem 2, the quantum order finding algorithm approximates a randomly selected eigenvalue of function

$$\Phi_s = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-\frac{2\pi i s k}{r}} \Psi_{x^k \bmod N} \tag{4}$$

Each of these eigenvalues has the form $\lambda = e^{2\pi i \omega}$ where

$$\omega = s/r \quad (0 \leq s \leq r-1) \tag{5}$$

and r represents the order of x modulo N.

(a) If $\tilde{\omega}$ represents the approximation of ω produced by the order finding algorithm, how accurate must this approximaion be to correctly determine r for any $x \in Z_N^*$ when $N = 39$? Express your answer in terms of the number of bits in $\tilde{\omega}$ and ω that must be identical. If you want to ensure that such a match will occur with a probability of at least 99%, what is the minimal number of qubits that you will need?

(b) Suppose that you have a 20 qubit quantum computer at your disposal, and that you randomly picked $x = 11$ from set Z_{39}^*. Suppose further that the measured state is

$$\Psi_x = \psi_{x_1} \otimes \psi_{x_2} \otimes \ldots \otimes \psi_{x_{20}} \tag{6}$$

and that the obtained values for $\{x_1, x_2, \ldots, x_{20}\}$ produce

$$\tilde{\omega} = 0.x_1 x_2 \ldots x_{20} = 0.10010101010100110110 \tag{7}$$

as the estimate for ω (in binary form). Use continued fraction expansion to determine which eigenvalue of Φ_s was approximated by this algorithm, and check whether condition

$$\left| \tilde{\omega} - \frac{s}{r} \right| \leq \frac{1}{2r^2} \tag{8}$$

has been met.

(c) Use the value of r that you computed in part (b) to find the prime factors of $N = 39$.

(d) What would have happened if the estimated eigenvalue corresponded to $s = 3$? Would you be able to compute the order of $x = 11$ in this case as well? Explain.

(e) Based on your answer for part (d), how many eigenvalues from the set

$$\{\frac{1}{r}, \frac{2}{r}, \ldots, \frac{r-1}{r}\} \tag{9}$$

will actually be useful to us in calculating the order of $x = 11$? List all of them explicitly.

4. Suppose that you are now given a 10 qubit quantum computer (instead of a 20 qubit one), and that you are still interested in computing the prime factors of $N = 39$. Let us further assume that you randomly picked $x = 11$ once again, and that you happened to approximate the *same* eigenvalue of Φ_s as in Problem 3. This time around, the measured state is

$$\Psi_x = \psi_{x_1} \otimes \psi_{x_2} \otimes \ldots \otimes \psi_{x_{10}} \tag{10}$$

and the obtained values for $\{x_1, x_2, \ldots, x_{10}\}$ produce

$$\tilde{\omega} = 0.x_1 x_2 \ldots x_{10} = 0.1001110011 \tag{11}$$

as the estimate for ω.

   (a) Show that in this case we can guarantee that the first 4 bits of ω and $\tilde{\omega}$ will match with a probability of 99%.

   (b) Perform the continued fraction expansion of $\tilde{\omega}$, and show that it does *not* produce the correct order for $x = 11$. Explain why this is so.

5. Suppose that you have intercepted a message that was encrypted using the RSA algorithm. You know the public key (which is $N = 391$ and $b = 31$ in this case), and the message is $y = 132$.

   (a) Determine the prime factors of N using the quantum order finding algorithm. In doing so, assume that you randomly chose $x = 5$ from set Z^*_{391}. Once you obtain the order r, show that $x^{r/2} + 1$ is not divisible by 391. **Note:** You can use the same order calculator as in Problem 2 to find r.

   (b) Use the answer that you obtained in part (a) to decrypt the message, and identify the number x that the sender wanted to share with his intended recipient.