Introduction to Quantum Information Science
Homework 10

Due Wednesday, November 20 at 11:59 PM

Note: You should explain your reasoning, i.e. show your work, for all problems. You do not need to show us every step of each calculation, but every answer should include an explanation *written with words* of what you did.

Shor's practice problem In past years, we've asked students to walk through Shor's algorithm to factor $N = 21$. This year, we'll do it in recitation instead. It's not required, but we suggest you try it out yourself.

1. Shor's Algorithm—Anything That Can Go Wrong Will Go Wrong

a) [2 Points] What can go wrong in Shor's algorithm if Q is not taken to be sufficiently large? Demonstrate with an example, using a specific N, Q, and calculations.

b) [3 Points] What can go wrong if the function f satisfies that if s divides $p - q$ then $f(p) = f(q)$, but it's not an "if and only if" (i.e., we could have $f(p) = f(q)$ even when s doesn't divide $p - q$)? Note that this does not actually happen for the function in Shor's algorithm, but it could happen when attempting period finding on an arbitrary function. Illustrate with an example, describing a specific function.

c) [3 Points] What can go wrong in Shor's algorithm if the integer N to be factored is even (that is, one of the prime factors, p and q, is equal to 2)? Illustrate with an example.

2. Continued fractions In the continued fraction step of Shor's algorithm, we need the following key fact: if a given real number x is sufficiently close to a rational number a/b with a "conspicuously small denominator", then that rational number is unique.

a) [5 Points] Prove that, indeed, there can be at most one rational a/b, with a and b coprime positive integers, that's at most ϵ away from x and that satisfies $b < 1/\sqrt{2\epsilon}$.

b) [1 Points] Explain how this relates to the choice, in Shor's algorithm, to choose Q to be quadratically larger than the integer N that we're trying to factor.
Hint: Recall that the achievable precision ϵ goes inversely with the dimension Q of the Fourier transform.

3. Shor's, Generalized Suppose we use Shor's algorithm to factor $N = 105$ into $3 \cdot 5 \cdot 7$. (Yes, N is now a product of 3 primes!) Suppose also that we make the choices $x = 2$ and $Q = 60000$.

a) [1 Point] What is the order of the multiplicative group $\mathbb{Z}_N^\times$?

b) [1 Points] What is the period of the function $f(r) = x^r (\mathrm{mod} N)$?

c) [2 Points] Suppose we factor $x^s - 1$ into $x^{s/2} - 1$ and $x^{s/2} + 1$, and then take the gcd of both factors with N itself. Which prime factors of N, if any, would be "peeled off" this way?

d) [2 Points] After we apply the QFT to the $|r\rangle$ register and then measure that register, what are the possible results that we could observe?

4. Breaking Diffie-Hellman In the following problem we'll be stepping through the adaptation of Shor's period finding algorithm to breaking Diffie-Hellman public-key encryption. The Diffie-Hellman encryption scheme is based on the conjectured hardness of the Discrete Logarithm Problem.

The Discrete Logarithm Problem (i.e. the problem you need to solve to break the encryption) is as follows: Given p be a prime number, α be an element of the multiplicative group $\mathbb{Z}_p^\times$, and g be a generator of $\mathbb{Z}_p^\times$ — that is, an element such that all other members of $\mathbb{Z}_p^\times$ can be found by taking powers of $g \mod p$, find an integer a such that $g^a = \alpha \mod p$.

a) [4 Points] The first step we need to accomplish is a reduction of the Discrete Logarithm Problem to Period Finding. To do so, given some instance of Discrete Logarithm, we'll introduce a new function $f : \mathbb{Z}_R \times \mathbb{Z}_R \to \mathbb{Z}_p^\times$ where $f(x_1, x_2) = \alpha^{x_1} g^{x_2} \mod p$ and where $R = |\mathbb{Z}_p^\times|$.
Show that this function is periodic in x_1 and x_2. In other words, show there exists a pair of integers (l, m) such that $f(x_1, x_2) = f(x_1 + l, x_2 + m)$.
How would knowledge of this period allow us to solve the Discrete Logarithm Problem?
Is this function efficiently computable? If so, how would one efficiently compute it?

b) [1 Point] Next we'll step through the adaptation of Shor's Period Finding algorithm to find the period of the function f defined above. Assume our state is initialized in the superposition:

$$|\psi\rangle = \frac{1}{R} \sum_{x_1, x_2 = 0}^{R-1} |x_1\rangle |x_2\rangle |0\rangle$$

We then apply an XOR query to f writing the result into the final register. What is the state of the system following the query?

c) [2 Points] Suppose we now measure the output register and observe the value g^c for some (unknown) integer c. What state do the input registers collapse to? Rearrange your answer so that it is in terms of x_1 but not x_2.

d) [2 Points] We now apply the inverse Quantum Fourier Transform, $F_R^\dagger |x\rangle = \frac{1}{\sqrt{R}} \sum_{y=0}^{R-1} \omega^{-xy} |y\rangle$, to both of the input registers. What is the resulting state?

e) [2 Points] Finally, we measure the input registers. Which pairs $|y_1'\rangle |y_2'\rangle$ could be measured with nonzero probability? Given one such pair, how do we solve the original instance of Discrete Logarithm?