Introduction to Quantum Information Science
Homework 10

Due Wednesday, November 17 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.

Solution: Large Q is necessary so that we get the destructive interference that makes sampling y that are not multiples of Q/s unlikely.

For example, consider if we chose $Q = 32$ and $x = 2$ when factoring $N = 21$. In this case, $s = 6$. The state of the $|r\rangle$ register after applying Hadamards and the query is

$$|\psi\rangle = \frac{1}{\sqrt{5}}(|4\rangle + |10\rangle + |16\rangle + |22\rangle + |28\rangle).$$

(Note that we are in the "unlucky" case where s does not divide Q, so we would need continued fractions.) We have that $y = 10$ is not a multiple of $Q/s = 16$, so we do not want to observe it. But the probability of obtaining $y = 10$ is

$$|\langle 10| F_Q |\psi\rangle|^2 = \frac{1}{5 \cdot 32} \left| \sum_{\ell=0}^{L-1=4} e^{2\pi i 6\ell(10/32)} \right|^2 \approx 0.015$$

which is no longer astronomically unlikely.

More details: One of the reasons we don't get the desired interference patterns is that in our original analysis of Shor's algorithm, when we analyzed the sum of terms up to $\ell = L - 1$, like above, we used the bound $\frac{Q}{s} - 1 \leq L \leq \frac{Q}{s} + 1$ and made the approximation $L - 1 \approx \frac{Q}{s}$. This approximation is less accurate when Q is smaller, since $\frac{Q}{s}$ becomes coarser. In particular, if Q is at most a constant times N, then it's possible Q is at most a constant times s (s is upper bounded by N), so $\frac{Q}{s} \pm 1$ is a constant, so the relative error of $L - 1$ vs $\frac{Q}{s}$ is a constant, which adds up quickly as N grows and more terms are added to the sums. Whereas, if Q is at about N^2, then the relative error of $L - 1$ vs $\frac{Q}{s}$ scales like $\frac{1}{N}$, so the total error stays small.

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.

Solution: If this happens, then the state $|\psi\rangle$ we obtain after measuring the second register will not contain a periodic superposition.

For example, if f is a constant function, then measuring the output register yields a uniform superposition over all inputs, which gives no information about the period.

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.

Solution: Observe that in $\mathbb{Z}_p$ if p is an odd prime, 1 has two square roots: $\pm 1 \pmod p = \{1, p-1\}$. But if $p=2$, then these coincide! If $N=qp$ where p,q are odd primes, then 1 has several more square roots, also known as 'false witnesses'.

Suppose $N=2p$ for prime p. For any number x, we want s such that $x^s = 1 \pmod N$. This means $x^{s/2} = \sqrt{1} \pmod N$, which always equals 1 or $N-1=2p-1$ in the multiplicative group. So, one of $x^{s/2}\pm 1$ must be congruent to 0 in the multiplicative group, meaning it's a multiple of N. The reduction of factoring to period finding only works when neither $(x^{s/2}+1), (x^{s/2}-1)$ is a multiple of N.

For example if $N=14$:

$$\mathbb{Z}_N = \{3,5,9,11,13\} \quad \rightarrow \quad 3^6 = 1, 5^6 = 1, 9^3 = 1, 11^3 = 1, 13^2 = 1$$
$$3^{6/2} \rightarrow 12, \mathbf{14}; \quad 5^{6/2} \rightarrow 12, \mathbf{14}; \quad 13^{2/2} \rightarrow 12, \mathbf{14}$$

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 $b < 1/\sqrt{2\epsilon}$.

Solution: Suppose that there are two rational numbers $a_1/b_1, a_2/b_2$ with $a_1, b_1, a_2, b_2 \in \mathbb{Z}_+$ s.t. $b_1 < 1/\sqrt{2\epsilon}$ and $b_1 < 1/\sqrt{2\epsilon}$. We want to show that under these conditions a_1/b_1 and a_2/b_2 must actually correspond to the same number, i.e.:

$$\left|\frac{a_1}{b_1} - \frac{a_2}{b_2}\right| = 0$$

From the triangle inequality and the fact that both numbers are within ϵ of x we have:

$$\left|\frac{a_1}{b_1} - \frac{a_2}{b_2}\right| \leq \left|\frac{a_1}{b_1} - x\right| + \left|\frac{a_2}{b_2} - x\right| \leq 2\epsilon$$

$$\left|\frac{a_1}{b_1} - \frac{a_2}{b_2}\right| = \frac{|b_2 a_1 - a_2 b_1|}{b_1 b_2}$$

From our conditions on b_1 and b_2 we have:

$$\frac{1}{b_1 b_2} > 2\epsilon$$

This gives

$$2\epsilon|b_2a_1 - a_2b_1| < \frac{|b_2a_1 - a_2b_1|}{b_1b_2}$$

Chaining the inequalities we find

$$2\epsilon|b_2a_1 - a_2b_1| < 2\epsilon$$

Since a_1, b_1, a_2, b_2 are all positive integers this implies that the term in the absolute value must be zero for the inequality to hold. Setting it equal to zero and rearranging we find that $a_1/b_1 = a_2/b_2$

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.

Solution: In Shor's algorithm, after we make a measurement and observe a number k, we know that with high probability $\frac{k}{Q}$ is "close" to some multiple of $\frac{1}{s}$. Suppose that rational number is $\frac{c}{s}$ for some integer c. Our goal is to apply continued fractions to k/Q and find $\frac{c}{s}$, since after we repeat this several times, $\text{lcm}\left(\frac{c_1}{s}, \frac{c_2}{s}, \frac{c_3}{s}, \dots\right) = s$ with high probability.

When we say "close", we mean

$$\left|\frac{k}{Q} - \frac{c}{s}\right| \leq \frac{\epsilon}{Q},$$

where we chose some constant ϵ earlier in Shor's algorithm. Let $x := \frac{k}{Q}$. So, the distance from x to $\frac{c}{s}$ is at most $\frac{\epsilon}{Q}$. By our result from part (a), there's at most one rational number that close to x such that the denominator is less than

$$\frac{1}{\sqrt{2\epsilon/Q}} = \frac{\sqrt{Q}}{\sqrt{2\epsilon}}.$$

Since $s \leq N$ and $Q \geq N^2$, we see that our desired rational number $\frac{c}{s}$ is satisfies this condition. Therefore, $\frac{c}{s}$ is only "close" rational number with a "small" denominator and we should be able to find it with continued fractions.

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 $\mathbb{Z}_N^\times$?

Solution: For N which has prime factors each with multiplicity exactly 1, the solution is $(p_1 - 1)(p_2 - 1)(p_3 - 1)\dots$ (the more general case of Euler's totient function is a bit more complicated).

Here, that means the order is $(3 - 1)(5 - 1)(7 - 1) = 48$.

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

Solution: We can brute-force this by just testing different values of r until x^r "wraps around" and equals 0 (mod N). We see $r = 0 \mapsto x^r = 1$, and checking $r = 1, 2, \dots$, we eventually find $r = 12 \mapsto x^r = 4096 = 4095 + 1 = 1 \pmod N$. The answer is 12.

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?

Solution: $2^6 - 1 = 63$ and $2^6 + 1 = 65$. Then, following the standard classical postprocessing for Shor's algorithm, we would compute $\gcd(63, 105) = \cdots = 21$ and compute $\gcd(65, 105) = \cdots = 5$.

Now, we add a step that we skipped when we assumed N had exactly 2 prime factors. We check whether the divisors we just computed are prime (efficiently via primality testing). We find that 5 is prime, so we can "peel it off" and reduce our problem to factoring $105/5 = 21$ (getting 21 here and 21 previously is a coincidence).

Note that to generalize this to even more than three prime factors, we might have found that neither of the two divisors was prime, and we would factor them.

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?

Solution: Here, we are in the "lucky" case where the period s divides Q. Following the analysis from the lecture notes, we have a uniform superposition over all $k \leq Q$ such that $Q|ks$, i.e. $60000|12k$. This happens for $k = 0$, for $k = 60000 \div 12 = 5000$, and for all multiples of 5000 up to Q, of which there are 12. We might observe any of these k.

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?

Solution: Our function is given by

$$f(x_1, x_2) = \alpha^{x_1} g^{x_2} \bmod p.$$

Recall that $\alpha = g^a$. As such this function is equal to:

$$f(x_1, x_2) = g^{ax_1 + x_2}$$

We now want to find integers (l, m) such that $f(x_1, x_2) = f(x_1 + l, x_2 + m)$.

$$g^{ax_1 + x_2} = g^{a(x_1 + l) + (x_2 + m)} \to ax_1 + x_2 = ax_1 + al + x_2 + m$$

If we let $m = -al$ then we can see that this is satisfied. As such, the function is periodic with period $(l, -al)$ for any integer l.

Given the value of this period we can take the ratio in order to find a.

This function is just modular exponentiation and can be efficiently computed using repeated squaring.

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?

Solution:

$$|\psi\rangle = \frac{1}{R}\sum_{x_1,x_2=0}^{R-1} |x_1\rangle\,|x_2\rangle\,|f(x_1,x_2)\rangle = \frac{1}{R}\sum_{x_1,x_2=0}^{R-1} |x_1\rangle\,|x_2\rangle\,\left|g^{ax_1+x_2}\right\rangle$$

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.

Solution: The state of the input registers collapses to all of the values of x_1 and x_2 consistent with seeing g^c. In other words, all of the values of x_1 and x_2 satisfying $ax_1 + x_2 = c$. We can rearrange this to get $x_2 = c - ax_1$

$$\frac{1}{R}\sum_{x_1,x_2=0}^{R-1} |x_1\rangle\,|x_2\rangle\,\left|g^{ax_1+x_2}\right\rangle \to \frac{1}{\sqrt{R}}\sum_{x_1=0}^{R-1} |x_1\rangle\,|c-ax_1\rangle\,|g^c\rangle$$

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?

Solution: We can drop the output register now, since we don't need it anymore.

$$\frac{1}{\sqrt{R}}\sum_{x_1=0}^{R-1} |x_1\rangle\,|c-ax_1\rangle \to \frac{1}{R^{3/2}}\sum_{x_1=0}^{R-1} \omega^{-x_1y_1}\omega^{-(c-ax_1)y_2}\,|x_1\rangle\,|c-ax_1\rangle$$

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?

Solution: The amplitude on the $|y_1'\rangle\,|y_2'\rangle$ state is given by:

$$\frac{1}{R^{3/2}}\sum_{x_1=0}^{R-1} \omega^{-x_1y_1'}\omega^{-(c-ax_1)y_2'} = \frac{1}{R^{3/2}}\sum_{x_1=0}^{R-1} \omega^{-x_1y_1'}\omega^{-cy_2'}\omega^{ax_1y_2'}$$

We can drop the $\omega^{-cy_2'}$ term since it just adds an overall phase which doesn't affect the probability. As we saw with Shor's factoring algorithm we now have a sum of roots of unity. In order to have constructive interference we need to have the exponent of ω cancel. In other words:

$$ax_1y_2 - x_1y_1 = 0 \mod R \to ay_2 = y_1 \mod R.$$

With this condition, we get a final state of the form:

$$|ay_2\rangle\,|y_2\rangle$$

In order to solve the original Discrete Logarithm problem we just need to multiply ay_2 by y_2^{-1}. This is contingent on y_2 being in the multiplicative group so that we're guaranteed y_2^{-1} exists, but it can be shown this happens with high probability.