C S 358H: Intro to Quantum Information Science

Sayam Sethi

November 2024

Contents

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

Question 1.1

Question. *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.*

Proof. If Q is not taken to be sufficiently large then the error term might be large and we will be unable to narrow down the fraction c/s after measurement. For instance, consider the example $N = 21$ $(p = 7, q = 3), Q = 32, x = 2$. The period of x^r is $s = 6$, which is $p - 1 = 7 - 1$. For simplicity let's assume we measure $y = 1$ in the ancilla register. The state we end up with is:

$$\begin{aligned} |\psi\rangle &= \frac{1}{\sqrt{6}} \left(|0\rangle + |6\rangle + |12\rangle + |18\rangle + |24\rangle + |30\rangle\right) \\ \implies F_Q(|\psi\rangle) &= \frac{1}{\sqrt{6}} \sum_{l=0}^{l=5} \left(\frac{1}{\sqrt{32}} \sum_{k=0}^{31} \left(\omega^k\right)^{6l} |k\rangle \right) \\ &= \frac{1}{\sqrt{192}} \sum_{k=0}^{31} \left(\sum_{l=0}^{l=5} \omega^{6lk} \right) |k\rangle \end{aligned} \tag{1}$$

Now, since we measure some integer that is of the form $c \cdot Q/s + \epsilon = c \cdot 16/3 + \epsilon$. Let us consider the first integer solution $c = 1$, we have the result as $16/3 + \epsilon$. The closest integer to this is 5, therefore, let us try to solve for c/s using 5 as the measurement result:

$$\frac{5}{32} = \frac{1}{6 + \frac{2}{5}} \approx \frac{1}{6} \tag{2}$$

However, it is also possible to measure 6 with somewhat high probability. In that case, we will get:

$$\frac{6}{32} = \frac{3}{16} = \frac{1}{5 + \frac{1}{3}} \approx \frac{1}{5} \tag{3}$$

This will lead us to believe $s = LCM(6, 5) = 30$, which is incorrect. Therefore, we need to take Q to be sufficiently large to avoid such errors. □

Question 1.2

Question. *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.*

Proof. If we have values p, q such that $f(p) = f(q)$ but $p - q$ is not a multiple of the period of the function, then we will have extraneous terms in the superposition and we will be unable

to find the period of the function using QFT. Consider the following function:

$$f(x) = \begin{cases} |x-2|, & \text{if } 0 \leq x < 4 \\ f(x-4), & \text{otherwise} \end{cases} \tag{4}$$

Note that the above function is defined on whole numbers. It is easy to see that the period of the function is $s = 4$, however, we also have $f(1 + c \cdot 2) = f(1) = 1$. Now, if we measure $y = 1$ in the ancilla register and perform Shor's algorithm, we will end up with the period of $s' = 2$, which is incorrect.
The above function does not provide a concrete solution since if we run the algorithm again, measuring the ancilla registers will give $0, 2$ with probabilities close to $1/4$ each. However, we can construct a different function that amplifies this problem:

$$f(x) = \begin{cases} 0, & \text{if } x = 0 \bmod 2^m \\ 1, & \text{if } x = 2^{m-1} \bmod 2^m \\ 2, & \text{otherwise} \end{cases} \tag{5}$$

The period of the above function is 2^m, however, the probability of measuring $y = 0, 1$ is only of the order of $1/2^{m-1}$ and this reduces as m is increased. Therefore, we will get a period of 1 with high probability which is incorrect. □

Question 1.3

Question. *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.*

Proof. If N is even, we will always get the period as $s = \varphi(N)$ and therefore, we will be unable to identify one of the two prime factors. In other words, the algorithm will reject every $x \in \mathbb{Z}_N^\times$ since one of $x^{s/2} \pm 1$ will be a multiple of N. For example consider the case when $N = 10 = 2 \times 5$ and we have $\mathbb{Z}_N^\times = \{1, 3, 7, 9\}$. All elements in this set have their period $s = q - 1 = 4$ and we have $3^{s/2} + 1 = 10$, $7^{s/2} + 1 = 50$, $9^{s/2} - 1 = 80$. In all cases, we get a factor that is a multiple of $N = 10$, leading us to discard the solution. Therefore, Shor's algorithm fails.
However, note that in this case we get $s = \varphi(N)$ always instead of getting a factor of $\varphi(N)$ as the period (for all $x \in \mathbb{Z}_N^\times$), therefore we can use the solution from Question 4 of HW 9 to still factor N (if we still insist on not noticing that N is even and trivially has 2 as a factor). □

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.

Question 2.1

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

Proof. We will prove this by contradiction. Suppose that we have two rationals a_1/b_1 and a_2/b_2 such that both are at most ϵ away from x and $b_i < 1/\sqrt{2\epsilon}$ for $i \in \{1, 2\}$. WLOG, we can assume that $a_1/b_1 < a_2/b_2$. Then, we have that

$$\begin{aligned} & \frac{a_2}{b_2} - \frac{a_1}{b_1} \leq (x + \epsilon) - (x - \epsilon) \\ \implies & \frac{a_2 b_1 - a_1 b_2}{b_1 b_2} \leq 2\epsilon \\ \implies & \frac{1}{2\epsilon} \leq \frac{a_2 b_1 - a_1 b_2}{2\epsilon} \leq b_1 b_2, \text{ since } a_2 b_1 - a_1 b_2 \geq 1 \end{aligned} \tag{6}$$

From Equation 6 we have that at least one of b_1 or b_2 is $\geq 1/\sqrt{2\epsilon}$, which contradicts the hypothesis. Hence, there can be at most one rational a/b that is at most ϵ away from x and that satisfies $b < 1/\sqrt{2\epsilon}$. □

Question 2.2

Question. *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.*

Proof. The ϵ in Shor's algorithm is of the form ε/Q (using notation from the class). From the condition discussed in Question 2.1, we want:

$$\begin{aligned} & s < \frac{1}{\sqrt{2\epsilon}} \\ \implies & s < \frac{1}{\sqrt{2\varepsilon/Q}} \\ \implies & s\sqrt{2\varepsilon} < \sqrt{Q} \\ \implies & s^2 2\varepsilon < Q \\ \implies & s^2 \cdot O(1) < Q, \text{ since } \varepsilon = O(1) \\ \implies & Q = O(N^2), \text{ since } s = O(N) \end{aligned} \tag{7}$$

Therefore, to ensure that we have at most one possible fraction, we need to choose a Q that is quadratically larger than N. □

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 $Q = 60000$.

Question 3.1

Question. *What is the order of the multiplicative group $\mathbb{Z}_N^\times$?*

Proof. The order of the multiplicative group $\mathbb{Z}_N^\times$ is $\varphi(N)$ which can be computed as $(3-1) \cdot (5-1) \cdot (7-1) = 2 \cdot 4 \cdot 6 = 48$. □

Question 3.2

Question. *What is the period of the function $f(r) = x^r \pmod N$?*

Proof. We have $2^{12} = 4096 = 1 \bmod 105$. This is the smallest power of 2 that leaves a remainder of 1 when divided by 105. Therefore, the period of $f(r)$ is 12. □

Question 3.3

Question. *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?*

Proof. $x^{s/2} - 1 = 63$ and $x^{s/2} + 1 = 65$. Taking GCDs, we get $\gcd(63, 105) = 21$ and $\gcd(65, 105) = 5$. Therefore, we get 5 as one of the prime factors. Now we can solve for the other prime factors after dividing N with 5. We can then run Shor's again to factor $N/5 = 21$ to then get 3 and 7 as the prime factors. □

Question 3.4

Question. *After we apply the QFT to the $|r\rangle$ register and then measure that register, what are the possible results that we could observe?*

Proof. WLOG let us assume we measured $y = 1$ (since the measurement result on the ancilla

just adds a global phase in the form of the initial value of $|r\rangle$) we will have the state:

$$\begin{aligned}
|\psi\rangle &= \frac{1}{\sqrt{L}} \sum_{l=0}^{L-1} |12l\rangle \text{ , where } L = \left\lfloor \frac{Q}{12} \right\rfloor = 5000 = \frac{Q}{12} \\
\implies F_Q |\psi\rangle &= \frac{1}{\sqrt{QL}} \sum_{k=0}^{Q-1} \left(\sum_{l=0}^{L-1} \left(\omega^{12k}\right)^l \right) |k\rangle \\
&= \frac{1}{\sqrt{QL}} \sum_{k=0}^{Q-1} \left(\sum_{l=0}^{L-1} \left(e^{\frac{2\pi i k}{L}}\right)^l \right) |k\rangle \\
&= \sqrt{\frac{L}{Q}} \sum_{k \bmod L = 0} |k\rangle \text{ , since the sum is zero when } e^{\frac{2\pi i k}{L}} \neq 1
\end{aligned} \tag{8}$$

Therefore, we measure an integer that is a multiple of $L = Q/s = 5000$, i.e., $|m\rangle = c \cdot 5000$, for $0 \leq c < 12$. □

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 $g^a = \alpha \mod p$.

Question 4.1

Question. *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. It is easy to see that the function is periodic in x_1 and x_2 since we know from Fermat's little theorem that $x^{p-1} = 1 \bmod p$. Therefore, we have $f(x_1, x_2) = f(x_1 + (p-1), x_2) = f(x_1, x_2 + (p-1)) = f(x_1 + (p-1), x_2 + (p-1))$. Note that $p-1$ is the smallest period for x_2 since g is a generator of $\mathbb{Z}_p^\times$, however, there may be a smaller period for x_1 which will be a factor of $p-1$.
However, note that the above period is not the *best* possible period, i.e., since the period is computed modulo $p-1$ (we know it repeats every $p-1$), we can find the period of the function as follows:

$$\begin{aligned} f(x_1, x_2) &= f(x_1 + l, x_2 + m) \\ \implies \alpha^{x_1} g^{x_2} &= \alpha^{x_1 + l} g^{x_2 + m} \bmod p \\ \implies \alpha^l g^m &= 1 \bmod p \\ \implies g^{al+m} &= 1 \bmod p \\ \implies al + m &= c(p-1) \text{ for some integer } c \end{aligned} \tag{9}$$

$$\text{Since we want to find the smallest period, we set } l = 1, c = 1$$

$$\implies m = p - 1 - a$$

Therefore from Equation 9, we have the smallest period is $(1, p-1-a)$. Any other period that we get will be a multiple of this period modulo $p-1$.
We can use this period to find the discrete log after we find the period by finding $a = p-1-m$. The function is efficiently computable since we already know α, g and we can compute the powers modulo p by performing binary exponentiation. Therefore, the computation time will be $O(\log(x_1 x_2))$. □

Question 4.2

Question. *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. The state of the system after the query is given by:

$$|\psi\rangle = \frac{1}{R}\sum_{x_1,x_2=0}^{R-1} |x_1\rangle\,|x_2\rangle\,|f(x_1,x_2)\rangle = \frac{1}{R}\sum_{x_1,x_2=0}^{R-1} |x_1\rangle\,|x_2\rangle\,|\alpha^{x_1} g^{x_2} \bmod p\rangle \tag{10}$$

□

Question 4.3

Question. *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. If we observe some state g^c in the ancilla register, we have $ax_1 + x_2 = c \bmod (p-1)$ (from Equation 9 and Equation 10). WLOG, we can choose $c < p-1$. Therefore, the state of the input registers will collapse to:

$$|\psi\rangle = \frac{1}{\sqrt{R}}\sum_{x_1=0}^{R-1} |x_1\rangle\,|c + (p-1-a)x_1 \bmod (p-1)\rangle = \frac{1}{\sqrt{R}}\sum_{x_1=0}^{R-1} |x_1\rangle\,|c + (p-1-a)x_1 \bmod R\rangle \tag{11}$$

□

Question 4.4

Question. *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. The state we end up with on applying $F_R^\dagger \otimes F_R^\dagger$ to the state in Equation 11 is:

$$
\begin{aligned}
(F_R^\dagger \otimes \mathbf{I})\,|\psi\rangle &= \frac{1}{\sqrt{R}} \sum_{x_1=0}^{R-1} \left(\frac{1}{\sqrt{R}} \sum_{y=0}^{R-1} \omega^{-x_1 y}\,|y\rangle \right) |c + (p-1-a)x_1 \bmod R\rangle \\
\implies (\mathbf{I} \otimes F_R^\dagger)(F_R^\dagger \otimes \mathbf{I})\,|\psi\rangle &= \frac{1}{R} \sum_{x_1=0}^{R-1} \left(\sum_{y=0}^{R-1} \omega^{-x_1 y}\,|y\rangle \right) \left(\frac{1}{\sqrt{R}} \sum_{z=0}^{R-1} \omega^{-(c+(p-1-a)x_1 \bmod R)z}\,|z\rangle \right) \\
\implies (F_R^\dagger \otimes F_R^\dagger)\,|\psi\rangle &= \frac{1}{\sqrt{R^3}} \sum_{y=0}^{R-1} \sum_{z=0}^{R-1} \left(\sum_{x_1=0}^{R-1} \omega^{-x_1 y - cz + ((p-1-a)x_1)z} \right) |y\rangle\,|z\rangle \text{ , since } \omega^R = 1 \\
&= \frac{1}{\sqrt{R^3}} \sum_{y=0}^{R-1} \sum_{z=0}^{R-1} \omega^{-cz} \left(\sum_{x_1=0}^{R-1} \left(\omega^{z(p-1-a)-y} \right)^{x_1} \right) |y\rangle\,|z\rangle \\
&= \frac{1}{\sqrt{R^3}} \sum_{z=0}^{R-1} \omega^{-cz} R\,|z(p-1-a) \bmod R\rangle\,|z\rangle \\
&\left(\text{since } \sum_{\beta=0}^{R-1} (\omega^\gamma)^\beta = 0 \text{ when } \gamma \neq 0 \bmod R \right) \\
&= \frac{1}{\sqrt{R}} \sum_{z=0}^{R-1} \omega^{-cz}\,|z(p-1-a) \bmod R\rangle\,|z\rangle
\end{aligned}
\tag{12}
$$

□

Question 4.5

Question. *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. From Equation 12, we will measure a state $|y_1'\rangle\,|y_2'\rangle$ such that $y_1 = y_2(p-1-a) \bmod R$. Now, since we know R, we can find $y_2^{-1} \bmod R$ (if it exists). Therefore, we will obtain $p-1-a$ and we know $p-1$. Thus, we can compute a, which is the solution to the discrete log problem. Note that we will have $\varphi(R)$ possible different values of y_2 that have an inverse and this happens with high probability ($= \varphi(R)/R$). So if we fail to find an inverse, we can just repeat to get a $y_2 \in \mathbb{Z}_R^\times$. □