Shor's Algorithm
CS 294-4 (Quantum Computation) Lecture 6

Lecturer: Prof Umesh Vazirani Scribe: Arindam Chakrabarti

October 11, 2002

Introduction

Now that we have talked about Quantum Fourier Transforms and discussed some of their properties, let us see an application area for these ideas. We will talk about Shor's algorithm for finding prime factors of large integers.

The problem statement is as follows: Given an integer N, find prime numbers p_i and integers e_i such that

$$N = p_1^{e_1} \times p_2^{e_2} \times \ldots \times p_k^{e_k}$$

Here's how Shor's algorithm solves the problem: Given N, split it into integers N_1 and N_2 such that $N = N_1 \times N_2$. After a linear number (in size of the input, i.e. $\log N$) of such steps, we are guaranteed to reach prime factors.

Recall that the numbers $\{x \bmod N : \gcd(x,N) = 1\}$ forms a group under multiplication modulo N. The **order finding problem** is: given x and N such that $\gcd(x,N) = 1$, find $\mathrm{order}(x) =$ minimum positive r such that $x^r \equiv 1 \bmod N$.

Theorem 1 *If N is odd and x is random mod N such that $\gcd(x,N) = 1$, then with probability at least $\frac{1}{2}$, $\mathrm{order}(x) = r$ is even and $x^{\frac{r}{2}} \neq \pm 1 \bmod N$.*

Here is how to split N using order finding:

- Pick x at random from $[0, N-1]$.
- If $\gcd(x,N) \neq 1$ then $\gcd(x,N)$ is a proper divisor of N.
- Otherwise, if N is even then 2 is a proper divisor of N.
- Otherwise, let $r = \mathrm{order}(x)$. If r is even,

$$\begin{aligned} N &\mid x^r - 1 \\ N &\mid (x^{r/2}+1)(x^{r/2}-1) \end{aligned}$$

If $x^{r/2} \neq \pm 1 \mod N$ then

$$N \nmid x^{r/2} \pm 1$$

$\therefore \gcd(x^{\frac{r}{2}+1}, N)$ is a proper divisor of N.

How do we efficiently find order(x) ? Here is how Shor does it:

1. Let Q be sufficiently large, and in $O(N^{O(1)})$. Shor uses two registers:
   - register 1 stores a number mod $Q = 2^q$
   - register 2 stores a number mod N
2. The registers are initially in the state $|0\rangle \otimes |0\rangle$.
3. On applying the Fourier Transform modulo Q to register 1 we get the state

$$\frac{1}{\sqrt{Q}} \Sigma_a |a\rangle \otimes |0\rangle$$

4. Consider $f(a) = x^a \mod N$, a function that is easy to compute classically (can be computed in $\log a$ multiplications using repeated squaring), and has r as its smallest period. Figure 1 shows such a function graphically. Note that f is distinct on $[0, r-1]$ since otherwise it would have a smaller period. Applying function f to the contents of register 1 and storing the result in register 2, we get

$$\frac{1}{\sqrt{Q}} \Sigma_a |a\rangle |f(a)\rangle$$

5. Now we measure the second register. When we measure, we must get some value; let it be $f(k)$, where k is uniformly random over $[0, r-1]$. Then all superposed states inconsistent with the measured value must disappear.

   So, the state of the two registers must be given by (ignoring fencepost errors)

$$\frac{1}{\sqrt{\frac{Q-k}{r}}} \Sigma_{j=0}^{\lfloor \frac{Q-k}{r} \rfloor} |jr+k\rangle |f(k)\rangle$$

6. Thus we have set up a periodic superposition of period r

$$\frac{1}{\sqrt{(\lfloor \frac{Q-k}{r} \rfloor)}} \times \Sigma_{j=0}^{\lfloor \frac{Q-k}{r} \rfloor} |jr+k\rangle$$

   in register 1.

   Now we can drop the second register. The first register has a periodic superposition whose period is the value we wanted to compute in the first place. How do we get that period ?

   Can we get anywhere by measuring the first register ? It's no good, because all we will get is a random point, with no correlation across independent trials (because k is random). Here's what Shor does next.

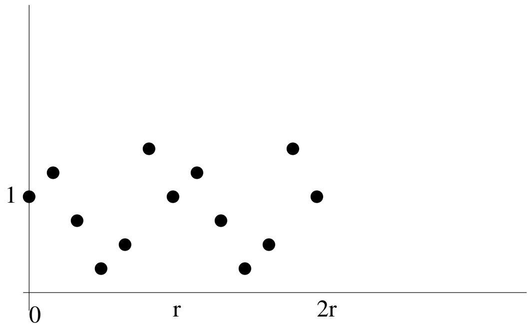

Figure 1: Function with smallest period r

7. Fourier sample modulo Q:
   Since the next step is Fourier sampling, we can drop the shift value k by the properties of Fourier Transforms discussed earlier in this lecture. This allows us to drop k. Dropping k from

$$\frac{1}{\sqrt{(Q/r)}}\Sigma_{j=0}^{\lfloor\frac{Q-k}{r}\rfloor}|jr+k\rangle|f(k)\rangle$$

   gives us

$$\frac{1}{\sqrt{(Q/r)}}\Sigma_{j=0}^{Q/r}|jr\rangle$$

   Applying the Fourier sample to the above state gives us

$$\Sigma_{l=0}^{Q-1}\alpha_l|l\rangle$$

   where

$$\alpha_l = \frac{1}{\sqrt{Q}} \times \frac{1}{\sqrt{(Q/r)}}\Sigma_{j=0}^{Q/r}e^{\frac{2\pi irl}{Q}j}$$

   Let

$$\beta = e^{\frac{2\pi irl}{Q}j}$$

   This stands for a vector on the complex plane. The sum

$$\Sigma_{j=0}^{Q/r}e^{\frac{2\pi irl}{Q}j}$$

   is a geometric series with common ratio β. Now, there are two possibilities:

   (a) The terms of the series fan out less than or equal to an angle π on the complex plane. This happens when β makes a small angle with the real line. Then as shown in Figure 2 half of the terms in the above series make an angle less than or equal to $\frac{\pi}{4}$ with the resultant of the vector addition of the terms in the series. Then each such term contributes a fraction at least

$$\cos\frac{\pi}{4} \quad = \quad \frac{1}{\sqrt{2}}$$

of its length to the resultant vector. So the magnitude of the resultant is at least

$$\frac{1}{2}\times\frac{1}{\sqrt{2}}\times\frac{Q}{r}\times\frac{1}{\sqrt{Q}}\times\frac{1}{\sqrt{(Q/r)}}=\frac{1}{2^{3/2}}\times\frac{1}{\sqrt{r}}$$

(b) The other case is when β makes a large angle with the real line. Then the sum is very close to 0, because the contributions of vectors in different directions cancel each other out, as shown in Figure 3.

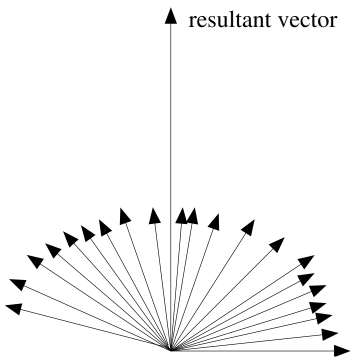

Figure 2: β makes small angle with real line

The first case happens when l satisfies the condition

$$-\frac{r}{2} \quad \leq lr \bmod Q \leq \quad \frac{r}{2}$$

so that powers of β fan out in directions making angles 0 to

$$\frac{Q}{r}\times\frac{r}{2}\times\frac{2\pi i}{Q} \quad = \quad \pi$$

with the X-axis. How many values of l satisfy this constraint ?

If $\gcd(r,Q)=1$ then $r^{-1} \bmod\ Q$ exists. Thus as l varies in the range $[0,Q-1]$, lr must take values forming a permutation of $\{0,1,2,\ldots Q-1\}$. Thus, as Figure 4 shows, at least r values of lr lie in the range $[Q-r/2,r/2]$.

If $\gcd(r,Q)\neq 1$, then $lr \bmod\ Q$ is distributed as shown in Figure 5. In this case, at least $r/2$ values of lr lie in a range $[Q-r/2,r/2]$ of size r.

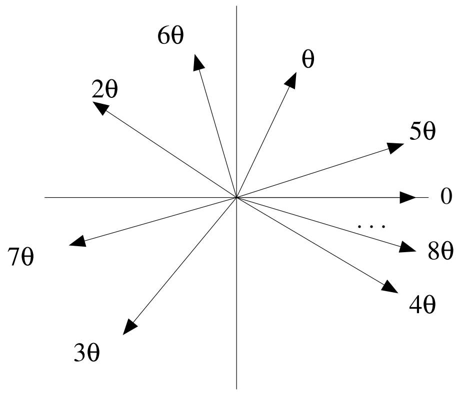

Figure 3: β makes large angle with real line

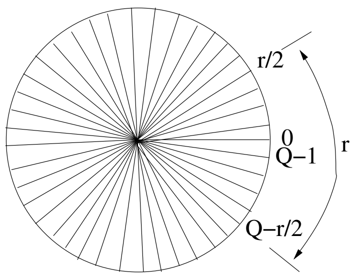

Figure 4: At least r values of lr satisfy the constraint

Thus, in any case, at least $r/2$ values of l satisfy the condition

$$-\frac{r}{2} \leq lr \bmod Q \leq \frac{r}{2}$$

Each of them has amplitude at least

$$\frac{1}{2^{3/2}} \times \frac{1}{r^{1/2}}$$

Thus the probability of sampling such an l is at least

$$\frac{r}{2} \times \left(\frac{1}{2^{3/2}} \times \frac{1}{r^{1/2}}\right)^2 \geq \frac{1}{16}$$

So with probability more than $\frac{1}{16}$ we will sample an l such that

$$-\frac{r}{2} \leq lr \bmod Q \leq \frac{r}{2}$$

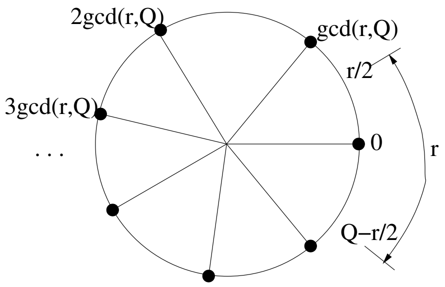

Figure 5: At least $r/2$ values of lr satisfy the constraint in the worst case

i.e.

$$|lr - kQ| \leq \frac{r}{2}$$

for some integer k; equivalently,

$$|\frac{l}{Q} - \frac{k}{r}| \leq \frac{1}{2Q}$$

Thus, $\frac{l}{Q}$ is an $\frac{1}{2Q}$-approximation of the rational $\frac{k}{r}$ with denominator $r < N$ ($r < N$ since $x^r = 1 \mod N$). We can measure l, and we know Q. The ratio $\frac{l}{Q}$, when reduced to lowest terms, leads to a rational $\frac{a}{b}$, say, which is a $\frac{1}{Q}$-good approximation to $\frac{k}{r}$.

This suggests a way to make a good approximation, by simply choosing Q to be much larger than N. How much larger than N does Q need to be, for us to evaluate r accurately ?

Example 1 *(Continued Fractions) Let us try to approximate* π *to the first two decimal places with a rational number. We know that*

$$\begin{aligned}
\pi &= 3.14\ldots \\
&= 3 + \frac{14}{100} \\
&= 3 + \frac{1}{\frac{100}{14}} \\
&= 3 + \frac{1}{7 + \frac{2}{14}} \\
&\approx 3 + \frac{1}{7} \\
&= \frac{22}{7}
\end{aligned}$$

If we decided to approximate π to four decimal places, we would have

$$\begin{aligned}
\pi &= 3.1415\ldots \\
&= 3+\frac{1415}{10000} \\
&= 3+\frac{1}{\frac{10000}{1415}} \\
&= 3+\frac{1}{7+\frac{95}{1415}} \\
&= 3+\frac{1}{7+\frac{1}{\frac{1415}{95}}} \\
&= 3+\frac{1}{7+\frac{1}{14+\frac{85}{95}}} \\
&\approx 3+\frac{1}{7+\frac{1}{14}} \\
&= \frac{311}{99}
\end{aligned}$$

Definition 1 *(Continued Fractions) A real number α can be approximated by a set of integers a_0, a_1, $\ldots$, a_n as $CF_n(\alpha) = a_0 + \frac{1}{a_1+\frac{1}{a_2+\ldots}} = \frac{P_n}{Q_n}$, where P_n and Q_n are integers.*

Theorem 2 *$CF_n(\alpha)$ is the best rational approximation of α with denominator $\leq Q_n$.*

Theorem 3 *If α is rational then it occurs as one of the approximations $CF_n(\alpha)$.*

Since k is randomly chosen from the range $[0, r-1]$, with probability at least $\frac{1}{\log k}$, k and r are co-prime. In that case if $a \neq k$ and $b \neq r$, then

$$|\frac{a}{b} - \frac{k}{r}| \geq \quad \frac{1}{br} \quad \geq \frac{1}{N^2}$$

Thus, if we have $\frac{a}{b}$ to be a $\frac{1}{2N^2}$-approximation to $\frac{k}{r}$, then we can conclude that $a = k$ and $b = r$. Thus, we have found r, since b is known.

Thus, to be able to find r (with probability $\frac{1}{\log k}$), we need to have $\frac{1}{2Q} \leq \frac{1}{2N^2}$, or $Q \approx N^2$. In that case, using Theorem 1 we see that Shor's algorithm splits N with probablity $\frac{1}{2logk}$.