CS 294-2 Shor's Factoring Algorithm 10/5/04
Fall 2004 Lecture 9

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

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

Let us make two simplifications of the problem without loosing generality: Firstly, given N, it is enough to split it into integers N_1 and N_2 such that $N = N_1 \times N_2$. It is easy to see that after a linear number (in size of the input, i.e. $\log N$) of such steps, we are guaranteed to reach prime factors. Secondly, assume that N is a product of two primes, $N = p \times q$, where $p, q \in \mathbb{P}$.

Classically, naive algorithm for the factoring problem works in time $O(\sqrt{N})$. The fastest known algorithm for this problem is Field Sieve algorithm that works in time $2^{O(\sqrt[3]{logN})}$.

In fact, Shor showed that we can do better with quantum computer.

Theorem 9.1: *There exists quantum algorithm that solves the factoring problem with bounded error probability in polynomial time.*

The rest of the paper is a proof of this theorem. Specifically, the factoring problem turns out to be equivalent to the order-finding problem (defined below), because from a fast algorithm for order-finding problem we can get a fast algorithm for factoring problem. The section 2 shows the reduction of factoring to order-finding and the section 3 shows a fast quantum algorithm for order-finding.

2 The reduction of factoring to order-finding

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

The reduction of factoring to order-finding follows from Lemma 9.1 and Lemma 9.3.

Lemma 9.1: *Given a composite number N and x, s.t. x is a nontrivial square root of* 1 *over N (that is,* $x^2 \equiv 1(mod\ N)$*, and neither* $x \equiv 1(mod\ N)$ *nor* $x \equiv -1(mod\ N)$*), we can efficiently compute a nontrivial factor of N.*

Proof:From $x^2 \equiv 1(mod\ N)$ follows that $x^2 - 1 \equiv (x-1) \times (x+1) \equiv 0(mod\ N)$. Since neither $x \equiv 1(mod\ N)$ nor $x \equiv -1(mod\ N)$ we know that $1 < x < N-1$, so one of $gcd(x-1, N)$ and $gcd(x+1, N)$ is a nontrivial factor of N. Since there exist a fast algorithm for computing gcd (Euclid's algorithm), the efficiency easy follows. □

Example: Let $N = 15$. Then $4^2 \equiv 1(mod\ N)$ and $4 \not\equiv \pm 1(mod\ N)$. Both $gcd(4-1, 15) = 3$ and $gcd(4+1, 15) = 5$ are nontrivial factors of 15.

Lemma 9.2: *Let p be an odd prime and let x be uniformly random element s.t.* $0 \le x < p$*. Then* $ord(x)$ *is even with probability at least one-half.*

Proof:By Fermat's little theorem we know that for every $x : x^{p-1} \equiv 1(mod\ p)$. It is well known that multiplicative group modulo prime number is a cyclic group, that means, there is an element g which generates all elements of group in the sense that any element can be written $x \equiv g^k (mod\ p)$ for some k. Since x is chosen uniformly at random, k is odd with probability one-half. Further assume that k is odd. Since $x \equiv g^k (mod\ p)$ it turns out that

$$x^{ord(x)} \equiv g^{k\ ord(x)} \equiv 1 (mod\ p).$$

Now we can deduce that $p-1 | k\ ord(x)$. Since p is odd, $p-1$ is even, and k is odd, $ord(x)$ has to be even. $\square$

Lemma 9.3: *Let $N = p \times q$, $p, q \in \mathbb{P}$ is composite odd number and x is taken uniformly at random from $0..N-1$. If $\gcd(x,N) = 1$ then with probability at least $\frac{3}{8}$ $\mathrm{ord}(x) = r$ is even and $x^{\frac{r}{2}} \neq \pm 1 (\mathrm{mod}\ N)$.*

Proof:

By the Chinese remainder theorem, choosing x uniformly at random from $0..N-1$ is the same as choosing x_1 uniformly at random from $0..p-1$ and independently x_2 uniformly at random from $0..q-1$. Order for those numbers also are related. Let $r_1 = ord(x_1)$ and $r_2 = ord(x_2)$. It is easy to see that both $r_1 | r$ and $r_2 | r$.

Firstly, let us prove that the probability that r is even is at least 3/4. Since N is odd, p and q are odd primes. Thus r_1 is even when x_1 is odd and r_2 is even when x_2 is odd. Since r is even when either r_1 is even or r_2 is even, and x_1 and x_2 are chosen uniformly at random, the probability that r is even is at least $3/4$ from Lemma 2.

Secondly, let us prove that the probability that $x^{\frac{r}{2}} \equiv \pm 1 (\mathrm{mod}\ N)$ is at most one-half when r is even. Note that $x^r \equiv 1 (mod\ p)$ and $x^r \equiv 1 (mod\ p)$ and there are only two square roots of 1 modulo prime number, namely ± 1. By Chinese reminder theorem it follows that there are only four roots of 1 modulo N. Only two of them makes $x^{\frac{r}{2}} \neq \pm 1 (\mathrm{mod}\ N)$.

$\square$

It is easy to see from Lemma 9.1 and Lemma 9.3 that if someone computs $ord()$ function for us, we can find prime factors of N classicaly. By checking answer (easy can be done efficiently) and repeating several times we can increase the probability of success.

3 Shor's order-finding algorithm

How do we efficiently find $\mathrm{ord}(x) = r$? Here is how Shor's quantum algorithm does it. The next subsection will describe algorithm and will analyze it in a simplified case.

3.1 The simplified case

Let Q be sufficiently large, s.t. $Q \gg N^2$. Let us assume now that $r|Q$. Case where $r \nmid Q$ algorithm is similar, just analysis is somewhat more complicate.

The algorithm uses two registers:

- register 1 stores a number mod $Q = 2^q$,
- register 2 stores a number mod N,

and has several steps.

1. The registers are initially in the state $|0\rangle \otimes |0\rangle$.
2. On applying the Fourier Transform modulo Q to register 1 we get the state

$$\frac{1}{\sqrt{Q}} \sum_{a=0}^{Q-1} |a\rangle \otimes |0\rangle$$

3. Consider $f(a) = x^a \bmod N$, a function that is easy to compute classically (can be computed in $\log a$ multiplications using repeated squaring, $x^2 = x \times x$, $x^4 = x^2 \times x^2$, $x^8 = x^4 \times x^4$, ...), 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

$$\frac{1}{\sqrt{Q}} \sum_{a=0}^{Q-1} |a\rangle |f(a)\rangle$$

4. Now we measure the second register. When we measure, we must get some value; let it be $f(l)$, where l 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

$$\frac{1}{\sqrt{\frac{Q}{r}}} \sum_{j=0}^{\frac{Q}{r}-1} |jr+l\rangle |f(l)\rangle$$

5. Thus we have set up a periodic superposition of period r 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 l is random). Here's what Shor's algorithm does next.

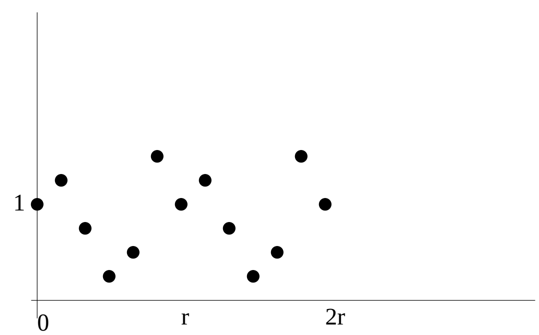

Figure 1: Function with smallest period r

   Fourier sample modulo Q:
   Since the next step is Fourier sampling, we can drop the shift value l by the properties of Fourier Transforms discussed in the previous lecture. This allows move l to phase. Applying the Fourier sample to state

$$\frac{1}{\sqrt{\frac{Q}{r}}} \sum_{j=0}^{\frac{Q}{r}-1} |jr+l\rangle$$

   gives us

$$\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \omega^{kl} |k\frac{Q}{r}\rangle$$

   where ω is a primitive qth root of unity,

$$\omega = e^{\frac{2\pi i}{Q}}.$$

6. Let us measure register 1. The measurement gives us $k\frac{Q}{r}$, where k is random variable uniformly from 0..r-1. It is easy to see that with big probability $gcd(k, \frac{Q}{r}) = 1$. If so, then by computing $gcd(k\frac{Q}{r}, Q)$ we get $\frac{Q}{r}$. Since we know Q, from $\frac{Q}{r}$ it is straightforward to compute r.

3.2 The general case

In the previous lecture we made assumption that $r|Q$. It is very strong assumption because we do not know any algorithm for computing such Q given x. Now we will show that the algorithm works correctly with constant probability even if $r \nmid Q$.

Now, in the 4th step, after applying the first measurement, we get state

$$\frac{1}{\sqrt{\lfloor \frac{Q}{r} \rfloor}} \sum_{j=0}^{\lfloor \frac{Q}{r} \rfloor - 1} |jr + l\rangle$$

This is no longer a coset of a subgroup, so earlier reasoning does not apply. Nevertheless, we will take a Fourier transform anyway, and we will show that we get constructive interference primarily at the points close to multiples of $\frac{Q}{r}$. In fact, we will be close enough to essentially "round" to the nearest multiple, and this will allow us to calculate r with some reasonable probability.

Applying a Fourier transform to the expression above, we get

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

where

$$\alpha_l = \frac{1}{\sqrt{Q}} \times \frac{1}{\sqrt{\lfloor \frac{Q}{r} \rfloor}} \sum_{j=0}^{\lfloor \frac{Q}{r} \rfloor - 1} (\omega^{rl})^j.$$

Notice that if *rl mod Q* is small, then terms in the sum cover only a small angle in the complex plane, and hence, the magnitude of the sum is almost the sum of the magnitudes. Next lemmas makes it precise.

Lemma 9.4: *If* $-\frac{r}{2} \leq lr \bmod Q \leq \frac{r}{2}$ *for some lr then* $|\alpha_l| \geq \frac{1}{2^{2/3}} \times \frac{1}{\sqrt{r}}$.

Proof:

Let

$$\beta = e^{\frac{2\pi i r l}{Q} j} = \omega^{rl}.$$

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

$$\sum_{j=0}^{\lfloor \frac{Q}{r} \rfloor - 1} \beta^j$$

is a geometric series with common ratio β.

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

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

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

$$\frac{1}{2} \times \frac{1}{\sqrt{2}} \times \frac{Q}{r} \times \frac{1}{\sqrt{Q}} \times \frac{1}{\sqrt{\lfloor \frac{Q}{r} \rfloor}} = \frac{1}{2^{3/2}} \times \frac{1}{\sqrt{r}}$$

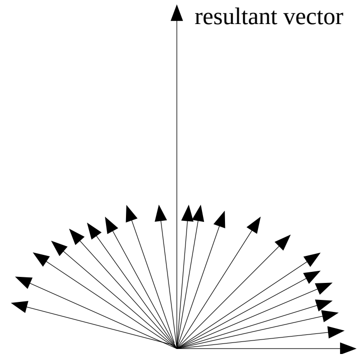

Figure 2: β makes small angle with real line

□

Lemma 9.5: $-\frac{r}{2} \leq lr \bmod Q \leq \frac{r}{2}$ *with probability* $\Theta(1)$.

Proof:

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 3 shows, at least r values of lr lie in the range $[Q-r/2, r/2]$.

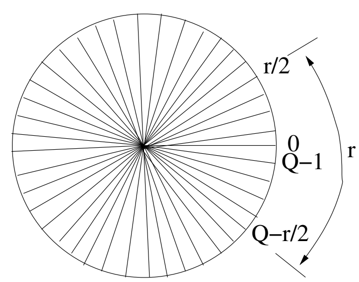

Figure 3: At least r values of lr satisfy the constraint

If $\gcd(r,Q) \neq 1$, then $lr \bmod Q$ is distributed as shown in Figure 4. In this case, at least $r/2$ values of lr lie in a range $[Q-r/2, r/2]$ of size r.

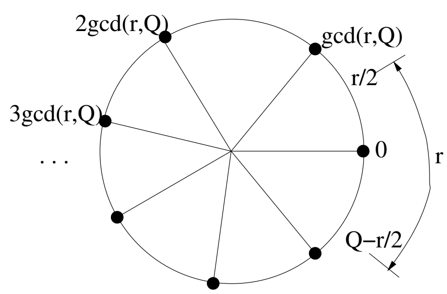

Figure 4: At least $r/2$ values of lr satisfy the constraint in the worst case

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

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

From Lemma 9.4 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

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

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

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

□

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

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

i.e.

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

for some integer k; equivalently,

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

Thus, $\frac{l}{Q}$ is an $\frac{1}{2Q}$-approximation of the rational $\frac{k}{r}$. 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 $\frac{1}{2Q}$-good approximation to $\frac{k}{r}$.

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. Thus by computing $\frac{k}{r}$ we can compute r as well.

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?

The answer is given by Lemma 9.7 using continued fractions in the next subsection. We just compute continued fractions until precision is at least $\frac{1}{2Q}$. Assume, that the approximation is some rational number $\frac{k'}{r'}$. If $r = r'$ then we succeed otherwise

$$\left|\frac{k}{r} - \frac{k'}{r'}\right| \geq \frac{1}{rr'} \geq \frac{1}{N^2}.$$

It is contradiction because both $\frac{k}{r}$ and $\frac{k'}{r'}$ is $\frac{1}{2Q} \leq \frac{1}{2N^2}$ close to $\frac{a}{b}$. Therefore $r = r'$.

3.3 Continued Fractions

The idea of continued fractions is to approximate real numbers using finite number of integers.

Definition 9.1 (Continued Fractions): A real number α can be approximated by a set of positive integers a_0, $a_1, \ldots, a_n$ as $CF_n(\alpha) = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\cdots + \frac{1}{a_n}}}} = \frac{P_n}{Q_n}$, where P_n and Q_n are integers.

Example: 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

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

The following two lemmas are well known facts about continued fractions that we will leave without a proof.

Lemma 9.6: *$CF_n(\alpha)$ is the best rational approximation of α with denominator $\leq Q_n$.*

Lemma 9.7: *If α is rational then it occurs as one of the approximations $CF_n(\alpha)$.*

Moreover, it is easy to see that continued fractions are easy to compute for any rational number.