CS 294-2	Quantum Factoring Algorithm	2/14/04
Spring 2007		Lecture 8

In this lecture, we develop many tools that will be part of the quantum factoring algorithm. The problem of quantum factoring reduces to a sequence of steps:

1. Finding a nontrivial square root of N (mod N)
2. Computing the order of an element (mod N)
3. Finding the period of a periodic superposition

We will start from the last step and work backwards.

1 Properties of Quantum Fourier Transform

Previously we discussed the construction of the Quantum Fourier Transform circuit. We will now look at some interesting properties that will help us in presenting interesting applications.

Recall that the Quantum Fourier Transform takes an input superposition

$$|\alpha\rangle = \sum_{x=0}^{N-1} \alpha_x |x\rangle$$

and outputs

$$|\hat{\alpha}\rangle = \sum_{y=0}^{N-1} \hat{\alpha}_y |y\rangle$$

where

$$\hat{\alpha}_y = \sum_{x=0}^{N-1} \alpha_x \frac{\omega^{xy}}{\sqrt{N}}, \omega = e^{\frac{2\pi i}{N}}$$

We now present some useful properties of the Quantum Fourier Transform.

Property 1: Shifting the indices

Consider the superposition $|\alpha_{+j}\rangle = \sum_{x=0}^{N-1} \alpha_x |x+j\rangle(\bmod N)$. Then, using this as input to our QFT yields $\hat{\alpha}_{+j}\rangle = \sum_{y=0}^{N-1} \omega^{jk} \hat{\alpha}_y |y\rangle$. Note that this modifies only the phase so that the measurement probabilities don't change, since $|\omega^{jy}| = 1$ This is very easy to check using the formula given above:

$$|\hat{\alpha}_{+j}\rangle = \sum_{x=0}^{N-1} \alpha_x \frac{\omega^{(x+j)y}}{\sqrt{N}} |x\rangle = \sum_{y=0}^{N-1} \omega^{jk} \hat{\alpha}_y |y\rangle$$

Property 2: Periodic superpositions

Suppose we have $r|M$, and a periodic superposition

$$|P_r\rangle = \sqrt{\frac{r}{M}} \sum_{k=0}^{M/r-1} |kr\rangle$$

Claim: the output of the QFT yields

$$|P_{M/r}\rangle = \sqrt{\frac{1}{r}} \sum_{k=0}^{r-1} |kM/r\rangle$$

Again, we can verify this property using the formula above:

$$\sqrt{\frac{r}{M}}\sum_{k=0}^{M/r-1}|kr\rangle = \sum_y \hat{\alpha}_y|y\rangle$$
$$\hat{\alpha}_y = \sqrt{\frac{r}{M}}\sum_{k=0}^{M/r-1}\omega^{kry}$$

There are two cases for y:

1. Case 1: y is a multiple of $\frac{M}{r}$.

   In this case, then $\omega^{kry} = \omega^{kr\frac{M}{r}j} = 1$ for all j (ω is an m-th root of unity). So $\hat{\alpha}_y = \frac{\sqrt{r}}{M}\frac{M}{r} = \frac{1}{\sqrt{r}}$.

   Note that there are r multiples of M/r. The sum of the magnitudes squared for these values of y is 1. This implies that for other y $\hat{\alpha}_y = 0$.

2. Case 2: y is not a multiple of $\frac{M}{r}$.

   We already showed that $\hat{\alpha}_y$ must be 0 from the previous case. But we can also give an intuition for why this is the case. Note that $\omega^{ry}, \omega^{2ry}, \ldots$ will be evenly spaced vectors of unit length around the origin. Thus the $\hat{\alpha}_y$, the sum of these complex numbers, is 0.

2 Period Finding

Now, applying what we know about the two properties, we present the following problem related to period finding, which is used in the factoring algorithm. Given the following periodic superposition with a shift, $\sqrt{\frac{r}{M}}\sum_{k=0}^{M/r-1}|kr+l\rangle$ we want to be able to determine r. Since l is arbitrary, we cannot simply measure the superposition. Instead, we want to apply the QFT modulo M. By the first property, the shifting factor l drops out, and by the second property, we get another periodic superposition, $|P_{M/r}\rangle$ with period M/r. Now, since M is known, we can perform a measurement to gather information about r. The idea is to use Quantum Fourier Sampling to sample the superposition many times, say m times, and calculate the GCD of the results. This will get us closer to the period after each sample, since every state is a multiple of the period.

Now we ask what the chance of finding the correct period after m samples. If after m samples, suppose we have not found the desired period M/r, and instead we have the j-th multiple of M/r. This means that in every of the m samples, we measured a multiple of jM/r. There are $M/(jM/r) = r/j$ multiples of jM/r, and since there are r multiples total, the probability of seeing a multiple of jM/r is $1/j$. Therefore,

$$\text{Pr[GCD = multiple of jM/r]} = (1/j)^m \leq (1/2)^m$$

and the error,

$$\text{Pr[GCD} > M/r \text{ after m samples]} \leq M(1/2)^m$$

So we need O($\log M$) measurements to guarantee a solution.

Now more generally, we may have a period r that does not divide M neatly. There is still a way to find the period of such a superposition. Suppose we are given the superposition

$$|P_r\rangle = \frac{1}{\sqrt{s}}\sum_{k=0}^{s-1}|kr\rangle$$

where r does not divide M. If we take the QFT of this superposition, we will get some other superposition $\sum_l \hat{\alpha}_l|l\rangle$. By the formula for QFT, we find that

$$\hat{\alpha}_l = \frac{1}{\sqrt{sM}}\sum_{k=0}^{s-1}\omega^{krl}$$

Intuitively, we want to find the values of l for which the amplitudes ω^{krl} "line up" in the complex plane. Previously, when the period divided M exactly, all the amplitudes for multiples of M/r "lined up" at 1. It turns out that over $r/2$ values "almost line up." We present the following claim:

Claim: There are greater than $r/2$ values of l such that $|lr \bmod M| \leq r/2$, and for these values of l, $\hat{\alpha}_l \geq \frac{C}{\sqrt{r}}$ for some constant C.

Thus, we can find such values of l with constant probability.

Proof:

First we show that values of l satisfying the inequality above have amplitudes greater than $C/\sqrt{r}$ ($\hat{\alpha}_l \geq C/\sqrt{r}$) for some constant C. Recall that $\hat{\alpha}_l = \frac{1}{\sqrt{sM}} \sum_{k=0}^{s-1} \omega^{krl}$.

Without loss of generality, we consider the case where lr is "positive" (between 0 and $r/2$), and the other case is treated identically. Then because $rl \leq r/2$ and $k \leq s$, we have that the values ω^{krl} are in the upper-half quadrants of the complex plane, starting from 0 and fanning out until $\omega^{rs/2}$, which is "before" $\omega^{M/2}$. If we sum these vectors, then the resultant vector bisects the angle between 1 and $\omega^{(s-1)rl}$. Note that we can lower-bound the magnitude of the result by considering the bisector angle, α: The contribution from each individual vector to the resultant vector is at least $\cos\alpha$. Thus,

$$|\hat{\alpha}_l| \geq \cos\alpha \frac{1}{\sqrt{sM}} s = \cos\alpha \sqrt{\frac{s}{M}} = \sqrt{\frac{\cos\alpha}{r}}$$

so that a measurement will produce l within a constant probability.

The argument that there are greater than $r/2$ values such that $|lr \bmod M| \leq r/2$ is left to the reader.

$\square$

Finally, we want to be able to recover r from this fact. We know that we can recover l satisfying the property that $|lr \bmod M| \leq r/2$ with constant probability. Rearranging this inequality, we have that

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

Since we know what l/M is, we can exploit properties of rational numbers and continued fractions to give us r from k/r.

For the next part, we assume that $M > 2r^2$ (M can be chosen to be as large as we like to satisfy this). Let's examine the rationals p/q such that $q \leq r$, and ask how close it is to k/r. Note that in the 'worst' case,

$$\left| \frac{p}{q} - \frac{k}{r} \right| \geq \frac{1}{qr} \geq \frac{1}{r^2}$$

However, the value we know about, l/M is closer to k/r.

Thus, if we use l/M as a continued fraction approximation to k/r, we will be able to extract r easily, as k/r would appear as part of the continued fraction (see section on continued fractions below).

2.1 Continued Fractions

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

Definition 8.1 (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 8.1: *$CF_n(\alpha)$ is the best rational approximation of α with denominator $\leq Q_n$.*

Lemma 8.2: *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.

3 Quantum Factoring

We now know enough information to present the Quantum Factoring algorithm. First, we show that factoring a number N reduces to finding a non-trivial square root of 1 (mod N). Let R be a nontrivial square root of 1 (mod N). This means that $R^2-1|N$, or $(R-1)$ and $(R+1$ are factors of N.

To find a non-trivial square root, we simply pick a random number x (mod N) and compute its order r, or the minimum non-zero r such that $x^r \equiv 1$ (mod N). Then, we can take $y = x^{r/2}$ as a non-trivial square root, given that x is not trivial.

Example: Let $N = 15$. Then let's suppose we picked $x = 7$. Then $x = 7, x^2 = 4, x^3 = 13, x^4 = 1$, so x has order 4. Now, taking $y = x^{r/2} = 4$, notice that $y-1 = 3$ and $y+1 = 5$ are both factors of 15.

To compute the order, note that we can use a quantum circuit to simulate the calculation of the function $f(a) = x^a$ (mod N), which is k-to-one. Let (mod M) be the domain of the function, and assume $M \gg N^2$.

By picking a random element in the range of f, we can used the machinery in the previous sections to find the period. Let's note a few assumptions we have made.

1. Continued fractions. This is known to be fast to compute.
2. GCD. This is also fast, using Euclid's algorithm.
3. Modular exponentiation. This is also fast using repeated squaring.

All three of these functions can be simulated in a quantum circuit.

The entire quantum circuit set-up has two quantum registers (r_1, r_2), and performs the following steps:

1. Initially, $r_1 = r_2 = |0\dots 0\rangle$.
2. Apply Hadamard basis to $r1$ to generate a superposition of all possible input strings.
3. Feed r_1, r_2 so we can calculate $x^a \pmod N$. (output has $x, a, x^a \pmod N$)
4. Measure r_2, to set up a periodic superposition in r_1.
5. QFT and measure r_1 to compute the order.
6. Use continued fractions to get r.
7. Finally, compute $x^{r/2} \pm 1$

Note that because of randomized nature of part of the algorithm, we may need to repeat this procedure many times. Everything needs to satisfy the right conditions in order for the result to be valid. Still, under repeated measurement, we can bound the error tightly.