Shor's Algorithm
Part 2

Andreas Klappenecker
Given: integer $n$ and an integer $c$ coprime to $n$

Let $q$ be a power of 2 such that $n^2 \leq q = 2^l < 2n^2$.

We use two registers, each with $l = \log_2 q$ bits.

The state space is $\mathbb{C}^q \otimes \mathbb{C}^q$
$B_{x^a} = \begin{cases} 
C^q \otimes C^q \\ |a\rangle \otimes |y\rangle 
\end{cases} \rightarrow C^q \otimes C^q \\
|a\rangle \otimes |y \oplus x^a \mod n\rangle$
Analysis

The initial state is $|0\rangle \otimes |0\rangle$.

After applying Hadamard gates, we get

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

Applying the black box function yields

$$\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle \otimes |x^a \pmod{n}\rangle.$$ 

The Boolean function depends on $n$ and $x$. It can be constructed in poly time.
Analysis

\[ \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle \otimes |x^a \text{ (mod } n)\rangle. \]

Applying the Fourier transform yields

\[ \frac{1}{q} \sum_{a=0}^{q-1} \sum_{c=0}^{q-1} \exp(2\pi iac/q) |c\rangle \otimes |x^a \text{ (mod } n)\rangle. \]
Analysis

\[ \frac{1}{q} \sum_{a=0}^{q-1} \sum_{c=0}^{q-1} \exp\left(\frac{2\pi i ac}{q}\right)|c\rangle \otimes |x^a \pmod{n}\rangle. \]

We now measure.
Let’s assume that \( x \) has order \( r \) mod \( n \). Then

\[
\Pr[\text{observe } (c, x^k \pmod{n})] = \left| \frac{1}{q} \sum_{a: x^a \equiv x^k} \exp\left(\frac{2\pi i ac}{q}\right) \right|^2
= \left| \frac{1}{q} \sum_{b=0}^{\left[\frac{(q-k-1)}{r}\right]} \exp\left(2\pi i (br + k)c/q\right) \right|^2
\]

\( 0 \leq k < r \)
Analysis

\[
\Pr[\text{observe } (c, x^k \mod n)] = \left| \frac{1}{q} \sum_{b=0}^{\lfloor (q-k-1)/r \rfloor} \exp(2\pi i (br + k)c/q) \right|^2
\]

\[
= \frac{1}{q^2} \left| \sum_{b=0}^{\lfloor (q-k-1)/r \rfloor} \exp(2\pi i bcr/q) \right|^2
\]

The powers of \( \exp(2\pi i cr/q) \) nearly cancel out unless \( cr/q \) is close to an integer. This is called destructive interference.
Destructive Interference

\[ \exp(2\pi i \frac{b\text{c}}{q}) \] for various \( b \)
when \( \frac{c}{q} \) is not close to an integer

\[ \exp(2\pi i \frac{b\text{c}}{q}) \] for various \( b \)
when \( \frac{c}{q} \) is close to an integer
Destructive Interference

\[ \exp(2\pi i \frac{bc r}{q}) \text{ for various } b \]
when \( cr/q \) is not close to an integer

\[ \exp(2\pi i \frac{bc r}{q}) \text{ for various } b \]
when \( cr/q \) is close to an integer
Destructive Interference

\[ \exp(2\pi i \frac{bcr}{q}) \text{ for various } b \]
when \( cr/q \) is not close to an integer

\[ \exp(2\pi i \frac{bcr}{q}) \text{ for various } b \]
when \( cr/q \) is close to an integer
Destructive Interference

\[ \exp(2\pi i \frac{bcr}{q}) \text{ for various } b \]
when \( cr/q \) is not close to an integer

\[ \exp(2\pi i \frac{bcr}{q}) \text{ for various } b \]
when \( cr/q \) is close to an integer
Destructive Interference

\[ \exp(2\pi i \frac{bcr}{q}) \text{ for various } b \]
when \( \frac{cr}{q} \) is not close to an integer

\[ \exp(2\pi i \frac{bcr}{q}) \text{ for various } b \]
when \( \frac{cr}{q} \) is close to an integer
Destructive Interference

\[ \exp(2\pi i b r/q) \text{ for various } b \]

when \( cr/q \) is not close to an integer

\[ \exp(2\pi i b r/q) \text{ for various } b \]

when \( cr/q \) is close to an integer
Destructive Interference

$\exp(2\pi i \frac{b c r}{q})$ for various $b$
when $c r/q$ is not close to an integer

$\exp(2\pi i \frac{b c r}{q})$ for various $b$
when $c r/q$ is close to an integer
Destructive Interference

\[ \exp(2\pi i \frac{bcr}{q}) \] for various \( b \) when \( cr/q \) is not close to an integer

\[ \exp(2\pi i \frac{bcr}{q}) \] for various \( b \) when \( cr/q \) is close to an integer
Destructive Interference

\[ \exp(2\pi i \frac{bcr}{q}) \text{ for various } b \]
when \( cr/q \) is not close to an integer

\[ \exp(2\pi i \frac{bcr}{q}) \text{ for various } b \]
when \( cr/q \) is close to an integer
Destructive Interference

\[ \exp(2\pi i \frac{bc r}{q}) \text{ for various } b \]
when \( cr/q \) is not close to an integer

\[ \exp(2\pi i \frac{bc r}{q}) \text{ for various } b \]
when \( cr/q \) is close to an integer
Destructive Interference

\[\exp(2\pi i \frac{bc}{q}) \text{ for various } b\] when \(\frac{cr}{q}\) is not close to an integer

\[\exp(2\pi i \frac{bc}{q}) \text{ for various } b\] when \(\frac{cr}{q}\) is close to an integer
Destructive Interference

$\exp(2\pi i \frac{bc r}{q})$ for various $b$
when $cr/q$ is not close to an integer

$\exp(2\pi i \frac{bc r}{q})$ for various $b$
when $cr/q$ is close to an integer
Learning from Observations

In general, \( rc \mod q \) lies in the large interval \([-q/2, q/2]\).

If \( rc \mod q \) in \([-r/2, r/2]\) then \( \Pr[\text{observe } (c, x^k \mod n)] \geq 1/3r^2 \)

\( rc \mod q \) in \([-r/2,r/2]\) means that there exists an integer \( d \) s.t.

\[-r/2 \leq rc - dq \leq r/2\]

Dividing by \( rq \) yields

\[|c/q - d/r| \leq 1/2q \quad (*)\]

Since \( q > n^2 \) there is at most one fraction \( d/r \) with \( r < n \) satisfying \((*)\)
Continued Fractions

Since we know c and q, we obtain the fraction d/r in lowest terms by rounding c/q to the nearest fraction having a denominator smaller than n.

We can find this fraction by using the continued fraction expansion of c/q. This can be done by a variation of the Euclidean algorithm.
Loose Ends

We remains to show that

- the Fourier transform can be computed in $O((\log q)^2)$ time.
- the modular exponentiation can be computed in poly time
- the continued fraction can yield the result

Assuming these results, we obtained a polynomial time algorithm to factor a given composite integer $n$. 