An Introduction to Quantum Computing

Lecture 10:

Order Finding - Towards Shor's Algorithm (II)

Paolo Zuliani

Dipartimento di Informatica
Università di Roma "La Sapienza", Rome, Italy

SAPIENZA
UNIVERSITÀ DI ROMA

Agenda

- Integer division
- Order-finding Problem
- Quantum Algorithm for Integer Factoring (Peter Shor, 1994)

Integer (Euclidean) Division

Proposition

Given two integers n, p ($p \neq 0$) there exist unique integers q, r with $0 \leqslant r < |p|$ such that

$$n = p \times q + r$$

We say that q is the *quotient* and r is the *remainder (modulo)*.

Integer (Euclidean) Division

Proposition

Given two integers n, p $(p \neq 0)$ there exist unique integers q, r with $0 \leqslant r < |p|$ such that

$$n = p \times q + r$$

We say that q is the *quotient* and r is the *remainder (modulo)*.

Examples:

$$n = 31, p = 7 \qquad 31 = 4 \times 7 + 3$$

$$n = 73, p = 8 \qquad 73 = 9 \times 8 + 1$$

Order-finding Problem

Let x, N two integers with $x < N$ and **coprime**, *i.e.*, $\gcd(x, N) = 1$.

Definition

The **order** of x modulo N is the *least* integer r such that

$$x^r = 1 \bmod N$$

Order-finding Problem

Let x, N two integers with $x < N$ and **coprime**, *i.e.*, $\gcd(x, N) = 1$.

Definition

The **order** of x modulo N is the *least* integer r such that

$$x^r = 1 \bmod N$$

Definition (Order-finding Problem)

Given $x < N$ coprimes, find r.

Order-finding Problem

Let x, N two integers with $x < N$ and **coprime**, *i.e.*, $\gcd(x, N) = 1$.

Definition

The **order** of x modulo N is the *least* integer r such that

$$x^r = 1 \bmod N$$

Definition (Order-finding Problem)

Given $x < N$ coprimes, find r.

Examples:

$$x = 4, N = 7 \qquad r = 3 \text{ (because } 4^3 = 64 = 9 \times 7 + 1)$$

$$x = 4, N = 11 \qquad r = 5 \text{ (because } 4^5 = 1024 = 93 \times 11 + 1)$$

Order-finding Algorithms: Complexity

Classical: no algorithm (yet) with polynomial complexity in the input length ($\log N$).

Quantum: *poly*($\log N$) algorithm exists! [Quantum Phase Estimation.]

Quantum Order-finding

Problem: Find least r such that $x^r = 1 \mod N$, with $x < N$ and *coprime*.

Quantum Order-finding

Problem: Find least r such that $x^r = 1 \bmod N$, with $x < N$ and *coprime*.

Solution: use QPE with

$$\boxed{U_x \left|y\right\rangle = \left|xy \bmod N\right\rangle}$$

for $y \in \{0,1\}^L$ and $L = \lceil \log N \rceil$. [If $y > N$, then U_x does nothing, *i.e.*, it maps y to y.]

Quantum Order-finding

Problem: Find least r such that $x^r = 1 \bmod N$, with $x < N$ and *coprime*.

Solution: use QPE with

$$\boxed{U_x |y\rangle = |xy \bmod N\rangle}$$

for $y \in \{0, 1\}^L$ and $L = \lceil \log N \rceil$. [If $y > N$, then U_x does nothing, *i.e.*, it maps y to y.]

Proposition

$U_x |y\rangle = |xy \bmod N\rangle$ *is unitary.*

Quantum Order-finding

Problem: Find least r such that $x^r = 1 \bmod N$, with $x < N$ and *coprime*.

Solution: use QPE with

$$\boxed{U_x |y\rangle = |xy \bmod N\rangle}$$

for $y \in \{0,1\}^L$ and $L = \lceil \log N \rceil$. [If $y > N$, then U_x does nothing, *i.e.*, it maps y to y.]

Proposition

$U_x |y\rangle = |xy \bmod N\rangle$ *is unitary.*

We need to prove $U_x U_x^\dagger = U_x^\dagger U_x = I$, with:

$$U_x = |xy \bmod N\rangle\langle y| \qquad U_x^\dagger = |y\rangle\langle xy \bmod N|$$

Let us prove $U_x^\dagger U_x = I$.

Quantum Order-finding

$$U_x^\dagger U_x = \sum_y |y\rangle\langle xy \bmod N| \sum_z |xz \bmod N\rangle\langle z| = \sum_{y,z} |y\rangle \langle xy \bmod N|xz \bmod N\rangle \langle z|$$

Quantum Order-finding

$$\begin{aligned}
U_x^\dagger U_x &= \sum_y |y\rangle\langle xy \bmod N| \sum_z |xz \bmod N\rangle\langle z| = \sum_{y,z} |y\rangle \langle xy \bmod N|xz \bmod N\rangle \langle z| \\
&= \sum_{y=z} |y\rangle\langle z| + \sum_{y\neq z} |y\rangle \langle xy \bmod N|xz \bmod N\rangle \langle z|
\end{aligned}$$

Quantum Order-finding

$$
\begin{aligned}
U_x^\dagger U_x &= \sum_y |y\rangle\langle xy \bmod N| \sum_z |xz \bmod N\rangle\langle z| = \sum_{y,z} |y\rangle \langle xy \bmod N|xz \bmod N\rangle \langle z| \\
&= \sum_{y=z} |y\rangle\langle z| + \sum_{y\neq z} |y\rangle \langle xy \bmod N|xz \bmod N\rangle \langle z| \\
&= I + \sum_{y\neq z \geqslant N} |y\rangle \langle xy \bmod N|xz \bmod N\rangle \langle z| + \sum_{y\neq z<N} |y\rangle \langle xy \bmod N|xz \bmod N\rangle \langle z|
\end{aligned}
$$

Quantum Order-finding

$$
\begin{aligned}
U_x^\dagger U_x &= \sum_y |y\rangle\langle xy \bmod N| \sum_z |xz \bmod N\rangle\langle z| = \sum_{y,z} |y\rangle \langle xy \bmod N|xz \bmod N\rangle \langle z| \\
&= \sum_{y=z} |y\rangle\langle z| + \sum_{y\neq z} |y\rangle \langle xy \bmod N|xz \bmod N\rangle \langle z| \\
&= I + \sum_{y\neq z\geqslant N} |y\rangle \langle xy \bmod N|xz \bmod N\rangle \langle z| + \sum_{y\neq z<N} |y\rangle \langle xy \bmod N|xz \bmod N\rangle \langle z| \\
&= I + \sum_{y\neq z\geqslant N} |y\rangle \langle y|z\rangle \langle z| + \sum_{y\neq z<N} |y\rangle \langle xy \bmod N|xz \bmod N\rangle \langle z|
\end{aligned}
$$

Quantum Order-finding

$$
\begin{aligned}
U_x^\dagger U_x &= \sum_y |y\rangle\langle xy \bmod N| \sum_z |xz \bmod N\rangle\langle z| = \sum_{y,z} |y\rangle \langle xy \bmod N|xz \bmod N\rangle \langle z| \\
&= \sum_{y=z} |y\rangle\langle z| + \sum_{y\neq z} |y\rangle \langle xy \bmod N|xz \bmod N\rangle \langle z| \\
&= I + \sum_{y\neq z\geqslant N} |y\rangle \langle xy \bmod N|xz \bmod N\rangle \langle z| + \sum_{y\neq z<N} |y\rangle \langle xy \bmod N|xz \bmod N\rangle \langle z| \\
&= I + \sum_{y\neq z\geqslant N} |y\rangle \langle y|z\rangle \langle z| + \sum_{y\neq z<N} |y\rangle \langle xy \bmod N|xz \bmod N\rangle \langle z| \qquad (\langle y|z\rangle = \delta_{yz})
\end{aligned}
$$

Quantum Order-finding

$$
\begin{aligned}
U_x^\dagger U_x &= \sum_y |y\rangle\langle xy \bmod N| \sum_z |xz \bmod N\rangle\langle z| = \sum_{y,z} |y\rangle \langle xy \bmod N|xz \bmod N\rangle \langle z| \\
&= \sum_{y=z} |y\rangle\langle z| + \sum_{y\neq z} |y\rangle \langle xy \bmod N|xz \bmod N\rangle \langle z| \\
&= I + \sum_{y\neq z\geqslant N} |y\rangle \langle xy \bmod N|xz \bmod N\rangle \langle z| + \sum_{y\neq z<N} |y\rangle \langle xy \bmod N|xz \bmod N\rangle \langle z| \\
&= I + \sum_{y\neq z\geqslant N} |y\rangle \langle y|z\rangle \langle z| + \sum_{y\neq z<N} |y\rangle \langle xy \bmod N|xz \bmod N\rangle \langle z| \qquad (\langle y|z\rangle = \delta_{yz}) \\
&= I + \sum_{y\neq z<N} |y\rangle \langle xy \bmod N|xz \bmod N\rangle \langle z|
\end{aligned}
$$

Quantum Order-finding

$$
\begin{aligned}
U_x^\dagger U_x &= \sum_y |y\rangle\langle xy \bmod N| \sum_z |xz \bmod N\rangle\langle z| = \sum_{y,z} |y\rangle \langle xy \bmod N|xz \bmod N\rangle \langle z| \\
&= \sum_{y=z} |y\rangle\langle z| + \sum_{y\neq z} |y\rangle \langle xy \bmod N|xz \bmod N\rangle \langle z| \\
&= I + \sum_{y\neq z\geqslant N} |y\rangle \langle xy \bmod N|xz \bmod N\rangle \langle z| + \sum_{y\neq z<N} |y\rangle \langle xy \bmod N|xz \bmod N\rangle \langle z| \\
&= I + \sum_{y\neq z\geqslant N} |y\rangle \langle y|z\rangle \langle z| + \sum_{y\neq z<N} |y\rangle \langle xy \bmod N|xz \bmod N\rangle \langle z| \qquad (\langle y|z\rangle = \delta_{yz}) \\
&= I + \sum_{y\neq z<N} |y\rangle \langle xy \bmod N|xz \bmod N\rangle \langle z| \\
&= I \qquad (\text{if } x \text{ is coprime with } N \text{ then } xy \equiv xz \bmod N \;\text{ iff }\; y \equiv z \bmod N, \text{and } y, z < N)
\end{aligned}
$$

Exercise: prove $U_x U_x^\dagger = I$.

Quantum Order-finding

What are U_x's eigenvectors and eigenvalues?

Quantum Order-finding

What are U_x's eigenvectors and eigenvalues?

Proposition

For any $0 \leqslant s \leqslant r-1$ *(*r *is the order of* $x \bmod N$*) the vector*

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi i s k/r} \left|x^k \bmod N\right\rangle$$

is an eigenvector of the previously defined U_x.

Quantum Order-finding

What are U_x's eigenvectors and eigenvalues?

Proposition

For any $0 \leqslant s \leqslant r-1$ *(*r *is the order of* $x \bmod N$*) the vector*

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi i s k / r} \left| x^k \bmod N \right\rangle$$

is an eigenvector of the previously defined U_x.

Let's prove it.

We need to find $\lambda \in \mathbb{C}$ such that $U_x |u_s\rangle = \lambda |u_s\rangle$.

Quantum Order-finding

$$
\begin{aligned}
U_x |u_s\rangle &= U_x \left(\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi isk/r} |x^k \bmod N\rangle \right) \\
&= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi isk/r} U_x |x^k \bmod N\rangle
\end{aligned}
$$

Quantum Order-finding

$$
\begin{aligned}
U_x \left| u_s \right\rangle &= U_x \left(\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi i s k / r} \left| x^k \bmod N \right\rangle \right) \\
&= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi i s k / r} U_x \left| x^k \bmod N \right\rangle \\
&= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi i s k / r} \left| x(x^k \bmod N) \bmod N \right\rangle
\end{aligned}
$$

Quantum Order-finding

$$
\begin{aligned}
U_x \left| u_s \right\rangle &= U_x \left(\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi i s k / r} \left| x^k \bmod N \right\rangle \right) \\
&= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi i s k / r} U_x \left| x^k \bmod N \right\rangle \\
&= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi i s k / r} \left| x (x^k \bmod N) \bmod N \right\rangle \\
&= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi i s k / r} \left| x^{k+1} \bmod N \bmod N \right\rangle
\end{aligned}
$$

Quantum Order-finding

$$
\begin{aligned}
U_x \left| u_s \right\rangle &= U_x \left(\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi i s k / r} \left| x^k \bmod N \right\rangle \right) \\
&= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi i s k / r} U_x \left| x^k \bmod N \right\rangle \\
&= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi i s k / r} \left| x(x^k \bmod N) \bmod N \right\rangle \\
&= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi i s k / r} \left| x^{k+1} \bmod N \bmod N \right\rangle \\
&= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi i s k / r} \left| x^{k+1} \bmod N \right\rangle
\end{aligned}
$$

Quantum Order-finding

$$= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi i s k / r} \left| x^{k+1} \bmod N \right\rangle$$

Quantum Order-finding

$$= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi isk/r} \left| x^{k+1} \bmod N \right\rangle$$

$$= \frac{1}{\sqrt{r}} e^{2\pi is/r} e^{-2\pi is/r} \sum_{k=0}^{r-1} e^{-2\pi isk/r} \left| x^{k+1} \bmod N \right\rangle$$

Quantum Order-finding

$$= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi i s k / r} \left| x^{k+1} \bmod N \right\rangle$$

$$= \frac{1}{\sqrt{r}} e^{2\pi i s / r} e^{-2\pi i s / r} \sum_{k=0}^{r-1} e^{-2\pi i s k / r} \left| x^{k+1} \bmod N \right\rangle$$

$$= \frac{1}{\sqrt{r}} e^{2\pi i s / r} \sum_{k=0}^{r-1} e^{-2\pi i s (k+1) / r} \left| x^{k+1} \bmod N \right\rangle$$

Quantum Order-finding

$$= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi i s k/r} \left| x^{k+1} \bmod N \right\rangle$$

$$= \frac{1}{\sqrt{r}} e^{2\pi i s/r} e^{-2\pi i s/r} \sum_{k=0}^{r-1} e^{-2\pi i s k/r} \left| x^{k+1} \bmod N \right\rangle$$

$$= \frac{1}{\sqrt{r}} e^{2\pi i s/r} \sum_{k=0}^{r-1} e^{-2\pi i s(k+1)/r} \left| x^{k+1} \bmod N \right\rangle$$

$$= \frac{1}{\sqrt{r}} e^{2\pi i s/r} \sum_{k=0}^{r-1} e^{-2\pi i s k/r} \left| x^{k} \bmod N \right\rangle \qquad \text{(previous sum “wraps” around last term)}$$

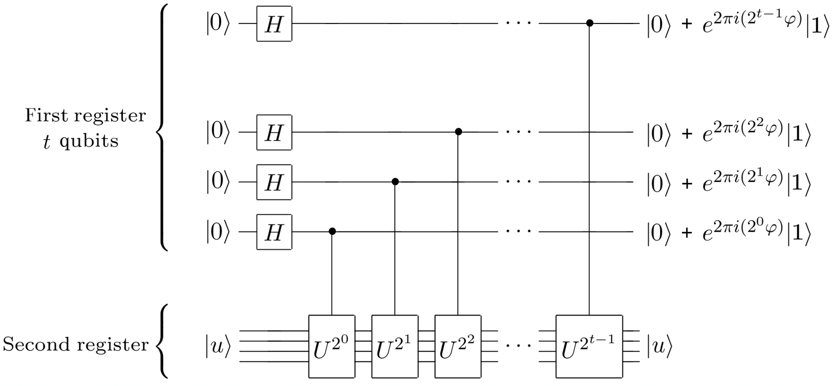
Quantum Order-finding

$$
\begin{aligned}
&= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi isk/r} \left| x^{k+1} \bmod N \right\rangle \\
&= \frac{1}{\sqrt{r}} e^{2\pi is/r} e^{-2\pi is/r} \sum_{k=0}^{r-1} e^{-2\pi isk/r} \left| x^{k+1} \bmod N \right\rangle \\
&= \frac{1}{\sqrt{r}} e^{2\pi is/r} \sum_{k=0}^{r-1} e^{-2\pi is(k+1)/r} \left| x^{k+1} \bmod N \right\rangle \\
&= \frac{1}{\sqrt{r}} e^{2\pi is/r} \sum_{k=0}^{r-1} e^{-2\pi isk/r} \left| x^{k} \bmod N \right\rangle \qquad \text{(previous sum “wraps” around last term)} \\
&= e^{2\pi is/r} \left| u_s \right\rangle
\end{aligned}
$$

Therefore, $|u_s\rangle$ is an eigenvector of U_x with eigenvalue $e^{2\pi is/r}$.

Quantum Order-finding

Using QPE we can compute with *high accuracy* the phase of $e^{2\pi i s/r}$, *i.e.*, s/r.



Quantum Order-finding: Quantum Circuit

Two problems with QPE:

1. We need controlled-U operations (*modular exponentiation* – non-trivial, but can be done with $O(L^3)$ gates)

Quantum Order-finding: Quantum Circuit

Two problems with QPE:

1. We need controlled-U operations (*modular exponentiation* – non-trivial, but can be done with $O(L^3)$ gates)
2. We must prepare $|u_s\rangle$ in the lower quantum register of the QPE circuit. However, it can be shown that:

$$|1\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle$$

   where $|1\rangle$ is an L-qubit state.

Let us prove problem 2.

Quantum Order-finding: Quantum Circuit

$$\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|u_s\rangle = \frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}e^{-2\pi isk/r}\left|x^k \bmod N\right\rangle = \frac{1}{r}\sum_{s,k=0}^{r-1}e^{-2\pi isk/r}\left|x^k \bmod N\right\rangle$$

Quantum Order-finding: Quantum Circuit

$$\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|u_s\rangle = \frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}e^{-2\pi isk/r}\left|x^k \bmod N\right\rangle = \frac{1}{r}\sum_{s,k=0}^{r-1}e^{-2\pi isk/r}\left|x^k \bmod N\right\rangle$$

$$= \frac{1}{r}\sum_{s=0}^{r-1}|1\rangle + \frac{1}{r}\sum_{s=0,k=1}^{r-1}e^{-2\pi isk/r}\left|x^k \bmod N\right\rangle$$

Quantum Order-finding: Quantum Circuit

$$\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|u_s\rangle = \frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}e^{-2\pi isk/r}\,|x^k \bmod N\rangle = \frac{1}{r}\sum_{s,k=0}^{r-1}e^{-2\pi isk/r}\,|x^k \bmod N\rangle$$

$$= \frac{1}{r}\sum_{s=0}^{r-1}|1\rangle + \frac{1}{r}\sum_{s=0,k=1}^{r-1}e^{-2\pi isk/r}\,|x^k \bmod N\rangle$$

$$= |1\rangle + \frac{1}{r}\sum_{k=1}^{r-1}|x^k \bmod N\rangle\sum_{s=0}^{r-1}e^{-2\pi isk/r}$$

Quantum Order-finding: Quantum Circuit

$$\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|u_s\rangle = \frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}e^{-2\pi isk/r}\,|x^k \bmod N\rangle = \frac{1}{r}\sum_{s,k=0}^{r-1}e^{-2\pi isk/r}\,|x^k \bmod N\rangle$$

$$= \frac{1}{r}\sum_{s=0}^{r-1}|1\rangle + \frac{1}{r}\sum_{s=0,k=1}^{r-1}e^{-2\pi isk/r}\,|x^k \bmod N\rangle$$

$$= |1\rangle + \frac{1}{r}\sum_{k=1}^{r-1}|x^k \bmod N\rangle\sum_{s=0}^{r-1}e^{-2\pi isk/r}$$

$$= |1\rangle + \frac{1}{r}\sum_{k=1}^{r-1}|x^k \bmod N\rangle\sum_{s=0}^{r-1}(e^{-2\pi ik/r})^s$$

Quantum Order-finding: Quantum Circuit

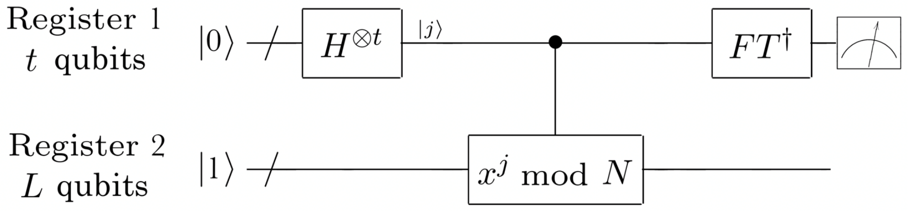
$$
\begin{aligned}
\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|u_s\rangle &= \frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}e^{-2\pi isk/r}\,|x^k \bmod N\rangle = \frac{1}{r}\sum_{s,k=0}^{r-1}e^{-2\pi isk/r}\,|x^k \bmod N\rangle \\
&= \frac{1}{r}\sum_{s=0}^{r-1}|1\rangle + \frac{1}{r}\sum_{s=0,k=1}^{r-1}e^{-2\pi isk/r}\,|x^k \bmod N\rangle \\
&= |1\rangle + \frac{1}{r}\sum_{k=1}^{r-1}|x^k \bmod N\rangle\sum_{s=0}^{r-1}e^{-2\pi isk/r} \\
&= |1\rangle + \frac{1}{r}\sum_{k=1}^{r-1}|x^k \bmod N\rangle\sum_{s=0}^{r-1}(e^{-2\pi ik/r})^s \qquad \text{(geometric sum)} \\
&= |1\rangle + \frac{1}{r}\sum_{k=1}^{r-1}|x^k \bmod N\rangle\,\frac{1-(e^{-2\pi ik/r})^r}{1-e^{-2\pi ik/r}}
\end{aligned}
$$

Quantum Order-finding: Quantum Circuit

$$
\begin{aligned}
\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|u_s\rangle &= \frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}e^{-2\pi isk/r}\,|x^k \bmod N\rangle = \frac{1}{r}\sum_{s,k=0}^{r-1}e^{-2\pi isk/r}\,|x^k \bmod N\rangle \\
&= \frac{1}{r}\sum_{s=0}^{r-1}|1\rangle + \frac{1}{r}\sum_{s=0,k=1}^{r-1}e^{-2\pi isk/r}\,|x^k \bmod N\rangle \\
&= |1\rangle + \frac{1}{r}\sum_{k=1}^{r-1}|x^k \bmod N\rangle\sum_{s=0}^{r-1}e^{-2\pi isk/r} \\
&= |1\rangle + \frac{1}{r}\sum_{k=1}^{r-1}|x^k \bmod N\rangle\sum_{s=0}^{r-1}(e^{-2\pi ik/r})^s \qquad \text{(geometric sum)} \\
&= |1\rangle + \frac{1}{r}\sum_{k=1}^{r-1}|x^k \bmod N\rangle\,\frac{1-(e^{-2\pi ik/r})^r}{1-e^{-2\pi ik/r}} = |1\rangle \qquad (e^{-2\pi ik}=1)
\end{aligned}
$$

Quantum Order-finding: Quantum Circuit

Thus, by using QPE we can get an estimate of s/r for any s.



Quantum Order-finding

Hold on! We can get an accurate estimate for s/r, but we actually want r.

Quantum Order-finding

Hold on! We can get an accurate estimate for s/r, but we actually want r.

r can be extracted by the *continued fractions* algorithm $[O(L^3)]$:

$$r = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \frac{1}{a_M}}}}$$

where $a_0, a_1, \ldots, a_M$ are positive integers. [r can be recovered from the $a_0, a_1, \ldots, a_M$.]

Yesterday: Brief Recap

1. Eigenvalues of unitary operators can be written as $e^{2\pi i\varphi}$, where φ is the *phase* (a real number).

Yesterday: Brief Recap

1. Eigenvalues of unitary operators can be written as $e^{2\pi i\varphi}$, where φ is the *phase* (a real number).
2. One can (efficiently) find φ using the Quantum Phase Estimation algorithm, which in turn exploits the QFT.

Yesterday: Brief Recap

1. Eigenvalues of unitary operators can be written as $e^{2\pi i\varphi}$, where φ is the *phase* (a real number).
2. One can (efficiently) find φ using the Quantum Phase Estimation algorithm, which in turn exploits the QFT.
3. The order-finding problem: Find least integer r such that $x^r = 1 \bmod N$, with integers $x < N$ and *coprime* (no common factors).

Yesterday: Brief Recap

1. Eigenvalues of unitary operators can be written as $e^{2\pi i\varphi}$, where φ is the *phase* (a real number).
2. One can (efficiently) find φ using the Quantum Phase Estimation algorithm, which in turn exploits the QFT.
3. The order-finding problem: Find least integer r such that $x^r = 1 \bmod N$, with integers $x < N$ and *coprime* (no common factors).
4. Solving order-finding "quantumly": define a suitable unitary operator that encodes the sought order r in the phase of an eigenvalue.

Yesterday: Brief Recap

1. Eigenvalues of unitary operators can be written as $e^{2\pi i\varphi}$, where φ is the *phase* (a real number).
2. One can (efficiently) find φ using the Quantum Phase Estimation algorithm, which in turn exploits the QFT.
3. The order-finding problem: Find least integer r such that $x^r = 1 \bmod N$, with integers $x < N$ and *coprime* (no common factors).
4. Solving order-finding "quantumly": define a suitable unitary operator that encodes the sought order r in the phase of an eigenvalue.
5. Use QPE to compute the phase and the continued fractions algorithm to extract the order r from the phase.

Integer Factoring

Theorem (Fundamental Theorem of Arithmetic (Euclid, 300BC (!)))

Any integer N can be written uniquely as:

$$N = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots p_m^{\alpha_m}$$

where $p_1, p_2, \ldots, p_m$ are primes *and $\alpha_1, \alpha_2, \ldots, \alpha_m$ are positive integers.*

Integer Factoring

Theorem (Fundamental Theorem of Arithmetic (Euclid, 300BC (!)))

Any integer N can be written uniquely as:

$$N = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots p_m^{\alpha_m}$$

where $p_1, p_2, \ldots, p_m$ are primes *and $\alpha_1, \alpha_2, \ldots, \alpha_m$ are positive integers.*

Definition (Integer Factoring Problem)

Given N, find the factors $p_1, p_2, \ldots, p_m$ (and the powers $\alpha_1, \alpha_2, \ldots, \alpha_m$).

Next, we reduce factoring to order-finding.

Factoring via Order-Finding

Two key theorems:

Theorem

Suppose N is an L-bit composite number, and x is a non-trivial solution to the equation $x^2 = 1 \bmod N$ for $1 \leqslant x \leqslant N$ (i.e., neither $x = 1 \bmod N$ nor $x = N - 1 = -1 \bmod N$). Then at least one of $\gcd(x-1, N)$ and $\gcd(x+1, N)$ is a non-trivial factor of N that can be computed using $O(L^3)$ operations.

"a non-trivial solution to $x^2 = 1 \bmod N$ can be (efficiently) turned into a factor of N"

Factoring via Order-Finding

Theorem

Suppose $N = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots p_m^{\alpha_m}$ is the prime factorization of an odd composite positive integer N. Let x be an integer chosen uniformly at random between 1 and $N-1$, and coprime to N. Let r be the order of $x \bmod N$. Then

$$\mathit{Prob}(r \text{ is even and } x^{r/2} \neq -1 \bmod N) \geqslant 1 - 2^{-m}$$

"with probability at least 50% the order r of x is even and $x^{r/2}$ is not a trivial solution of $x^2 = 1 \bmod N$"

Quantum Factoring: Shor's Algorithm

Algorithm 1: Reduction of factoring to order-finding

Input: A composite number N

Output: A non-trivial factor of N

```
if N is even then
    return 2;
```

Quantum Factoring: Shor's Algorithm

Algorithm 2: Reduction of factoring to order-finding

Input: A composite number N

Output: A non-trivial factor of N

if N *is even* **then**
  return *2*;

`// there is an efficient classical algorithm for this`

if $N = a^b$ *for* $a \geqslant 1$ *and* $b \geqslant 2$ **then**
  return a;

Quantum Factoring: Shor's Algorithm

Algorithm 3: Reduction of factoring to order-finding

Input: A composite number N
Output: A non-trivial factor of N

```
if N is even then
    return 2;
// there is an efficient classical algorithm for this
if N = a^b for a ⩾ 1 and b ⩾ 2 then
    return a;
x ← rand(1 ... N − 1);
if gcd(x, N) > 1 then
    return gcd(x, N);
```

Quantum Factoring: Shor's Algorithm

Algorithm 4: Reduction of factoring to order-finding

Input: A composite number N

Output: A non-trivial factor of N

```
if N is even then
    return 2;
// there is an efficient classical algorithm for this
if N = a^b for a ≥ 1 and b ≥ 2 then
    return a;
x ← rand(1 ... N − 1);
if gcd(x, N) > 1 then
    return gcd(x, N);
r ← order of x mod N ;            // use quantum order-finding algorithm
```

Quantum Factoring: Shor's Algorithm

Algorithm 5: Reduction of factoring to order-finding

Input: A composite number N
Output: A non-trivial factor of N

if N *is even* **then**
  return *2*;

`// there is an efficient classical algorithm for this`

if $N = a^b$ *for* $a \geqslant 1$ *and* $b \geqslant 2$ **then**
  return a;

$x \leftarrow \text{rand}(1 \ldots N-1)$;
if $\gcd(x, N) > 1$ **then**
  return $\gcd(x, N)$;

$r \leftarrow$ order of $x \bmod N$; `// use quantum order-finding algorithm`

if r *is even and* $x^{r/2} \neq -1 \bmod N$ **then**
  compute $\gcd(x^{r/2} - 1, N)$ and $\gcd(x^{r/2} + 1, N)$ and return the one that is a non-trivial factor
else
  abort