Shor's algorithm

Ryuhei Mori

Tokyo Institute of Technology

12, Nov., 2021

Integer factoring and primality test

- PRIMALITYTEST:
  Input: $N \in \mathbb{N}$
  Output: YES if N is a prime number, NO if N is a composite number.

- INTEGERFACTORING:
  Input: $N \in \mathbb{N}$
  Output: $a \in \mathbb{N}$ satisfying $a \neq 1, N$ and a divides N.

Does there exist an algorithm with time complexity $O((\log N)^c)$?

It is known that $\textsc{PrimalityTest} \in \mathrm{P}$ [Agrawal, Kayal, Saxena, 2004].
It is believed that $\textsc{IntegerFactoring} \notin \mathrm{BPP}$.
It is known that $\textsc{IntegerFactoring} \in \mathrm{BQP}$. [Shor 1994]

Nontrivial square root of 1

$$x^2 = 1 \mod N$$

$$\begin{aligned} & x^2 = 1 \mod N \\ \iff & (x-1)(x+1) = 0 \mod N \end{aligned}$$

If N is a prime number, $x = \pm 1$ are only solution.

If there exists a nontrivial square root of 1, then N must be composite number.

If we find a nontrivial square root x of 1, we can also find a nontrivial factor of N by $\gcd(x \pm 1, N)$.

Fermat little theorem

Theorem (Fermat little theorem)

If p is a prime number, any integer a that is not a multiple of p,

$$a^{p-1} = 1 \mod p.$$

Proof.

The map

$$x \longmapsto ax \mod p$$

is a bijection on $\{1, \dots, p-1\}$. Hence,

$$\prod_{x=1}^{p-1} x = \prod_{x=1}^{p-1} (ax) \mod p$$
$$\iff 1 = a^{p-1} \mod p.$$

$\square$

Fermat test

```
function FERMAT(N)
    loop    k times
        a ← a random integer in [2, N − 2]
        if a^(N−1) ≠ 1  mod N then
            return NO
        end if
    end loop
    return YES
end function
```

Carmichel numbers ($561 = 3 \cdot 11 \cdot 17$, $1105 = 5 \cdot 13 \cdot 17, \cdots$) passes the Fermat test for all a coprime with N.

Finding the nontirivial square root of 1

We assume that $a^{N-1} = 1 \mod N$ for some integer $a \in [2, N-2]$,

Let u and d be an integer and an odd integer, respectively, satisfying $N - 1 = 2^u d$.

a^d	a^{2d}	$a^{2^2 d}$	$\cdots$	$a^{2^{k-1} d}$	$a^{2^k d}$	$\cdots$	$a^{2^{u-1} d}$	$a^{2^u d}$
$*$	$*$	$*$	$\cdots$	$z \neq 1$	1	$\cdots$	1	1

z is a square root of 1 modulo N.

Miller–Rabin primality test

```
function MILLER–RABIN(N)
    Let u and d be an integer and an odd integer, respectively,
satisfying N = 2^u d + 1
    loop    k times
        a ← a random integer in [2, N − 2]
        x ← a^d mod N
        if x = 1  or  x = N − 1 then continue
        end if
        loop    u − 1 times
            x ← x^2 mod N
            if x = N − 1 then break
            end if
        end loop
        if x ≠ N − 1 then return NO
        end if
    end loop
    return YES
end function
```

Why Miller–Rabin algorithm doesn't solve INTEGERFACTORING

In fact, the Miller–Rabin test outputs NO with probability $1 - 1/4^k$ for composite N.

The Miller–Rabin algorithm seems to find a nontrivial square root of 1, which means that we can also find a nontrivial factor of N, right ?

NO!

a^d	a^{2d}	$a^{2^2 d}$	$\cdots$	$a^{2^u d}$
$*$	$*$	$*$	$\cdots$	$\neq 1$

Shor's algorithm

function $\textsc{Shor}(N\text{: An odd integer})$
    if $N = a^b$ for some $a \geq 1$ and $b \geq 2$ **then**
        return a
    end if
    loop
        $a \leftarrow$ a random integer in $[2, N-2]$.
        $b \leftarrow \gcd(a, N)$.
        if $b \neq 1$ **then return** b
        end if
        $r \leftarrow \textsc{OrderFinding}(a, N)$.
        if r is odd **then continue**
        end if
        if $a^{r/2} \neq N-1$ **then**
            return $\gcd(a^{r/2}+1, N)$
        end if
    end loop
end function

Eigenvalues of the unitary operator

Let r be the order of a modulo N, which is a smallest positive integer satisfying

$$a^r = 1 \mod N.$$

For a that is coprime with N, define the unitary operator U_a by

$$U_a |x\rangle = \begin{cases} |ax \bmod N\rangle & \text{if } x < N \\ |x\rangle & \text{Otherwise.} \end{cases}$$

Here, $U_a^r = I$. This means that all eigenvalues of U_a are in the form $e^{2\pi i \frac{s}{r}}$ for $s \in \{0, 1, 2, \ldots, r-1\}$.

By quantum phase estimation for U_a, an approximation of $\frac{s}{r}$ can be computed efficiently.

From $0.b_n b_{n-1} \cdots b_1 \approx \frac{s}{r}$, we can extract the denominator r if s is comprime with r.

Eigenvectors of the unitary operator

For $s \in \{0, 1, \dots, r-1\}$,

$$|\psi_s\rangle := \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} e^{-2\pi i \frac{sj}{r}} |a^j \bmod N\rangle .$$

$$\begin{aligned}
U_a |\psi_s\rangle &= \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} e^{-2\pi i \frac{sj}{r}} |a^{j+1} \bmod N\rangle \\
&= e^{2\pi i \frac{s}{r}} \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} e^{-2\pi i \frac{s(j+1)}{r}} |a^{j+1} \bmod N\rangle \\
&= e^{2\pi i \frac{s}{r}} \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} e^{-2\pi i \frac{sj}{r}} |a^j \bmod N\rangle \\
&= e^{2\pi i \frac{s}{r}} |\psi_s\rangle .
\end{aligned}$$

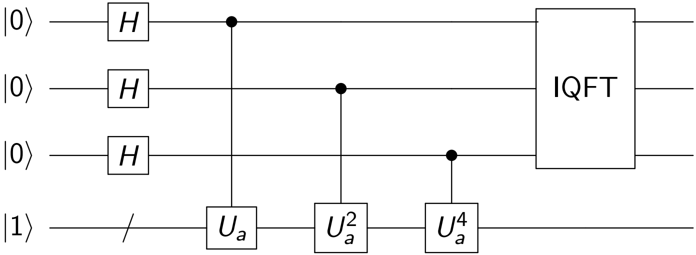
The uniform sperposition of the eigenvectors

For $s \in \{0, 1, \dots, r-1\}$,

$$|\psi_s\rangle := \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} e^{-2\pi i \frac{sj}{r}} \left| a^j \bmod N \right\rangle .$$

$$\begin{aligned}
\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |\psi_s\rangle &= \frac{1}{r} \sum_{s=0}^{r-1} \sum_{j=0}^{r-1} e^{-2\pi i \frac{sj}{r}} \left| a^j \bmod N \right\rangle \\
&= \sum_{j=0}^{r-1} \left(\frac{1}{r} \sum_{s=0}^{r-1} e^{-2\pi i \frac{sj}{r}} \right) \left| a^j \bmod N \right\rangle \\
&= |1\rangle
\end{aligned}$$

Quantum phase estimation



For uniformly chosen $s \in \{0, 1, \dots, r-1\}$, we obtain an approximation of s/r.

Continued fraction

$$\theta = \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cdots}}}}$$

Theorem

Suppose s/r is a rational number satisfying

$$\left| \frac{s}{r} - \theta \right| \leq \frac{1}{2r^2}.$$

Then, s/r is a convergent of the continued fraction for θ.

The probability that we can calculate r from s/r

For uniformly chosen $s \in \{0, 1, \dots, r-1\}$, we obtain an approximation of s/r.

From the denominators d_1 and d_2 of the irreducible fractions of s_1/r and s_2/r, we can calculate r by $\mathrm{lcm}(d_1, d_2)$.

$$
\begin{aligned}
\Pr(\mathrm{lcm}(d_1, d_2) \neq r) &= \Pr_{s_1, s_2 \in \{0, \dots, r-1\}}(\gcd(s_1, s_2, r) \neq 1) \\
&= \Pr_{s_1, s_2 \in \{1, \dots, r\}}(\gcd(s_1, s_2, r) \neq 1) \\
&\leq \Pr_{s_1, s_2 \in \{1, \dots, r\}}(\gcd(s_1, s_2) \neq 1) \\
&\leq \sum_{p\text{: prime}} \Pr_{s_1, s_2 \in \{1, \dots, r\}}(p \mid s_1, p \mid s_2) \\
&\leq \sum_{p\text{: prime}} \frac{1}{p^2} \leq 0.4523
\end{aligned}
$$

Assignments

1. Show all eigenvectors and corresponding eigenvalues of $2^{\lceil \log N \rceil} \times 2^{\lceil \log N \rceil}$ matrix U_a.