Shor's Algorithm

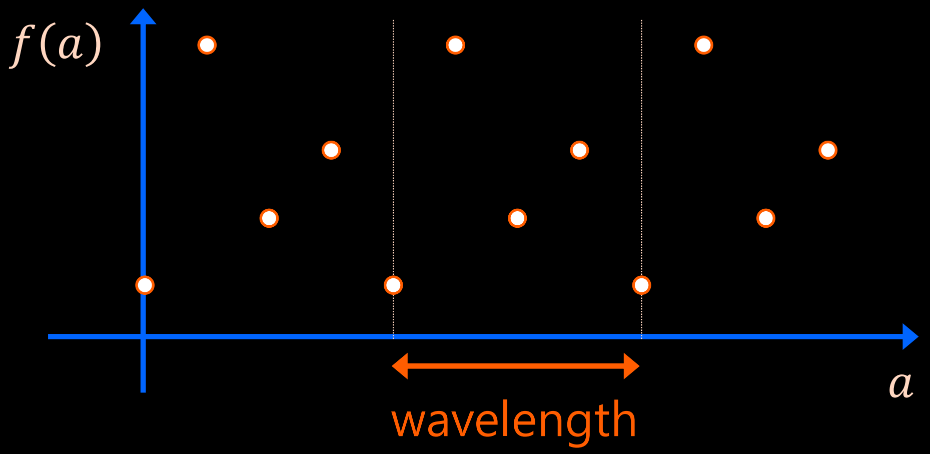
Sungmin Kim
Yonsei Theory Study Group

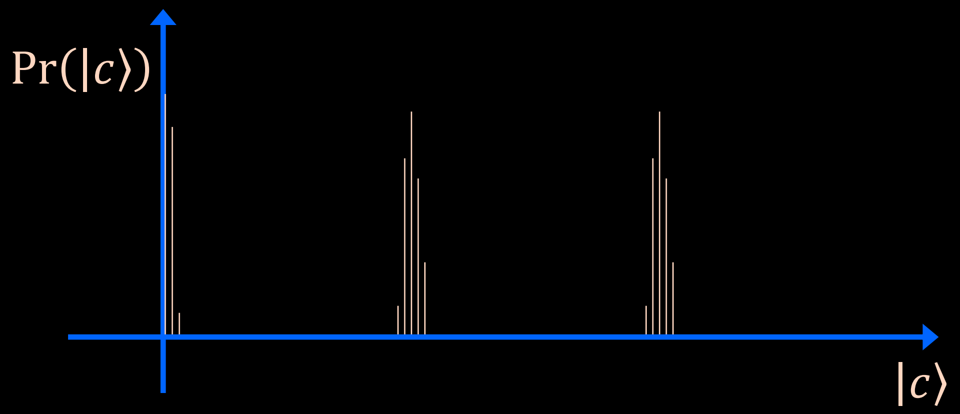
23' Oct. 04

Quantum Computing Recap

Quantum Fourier transformation

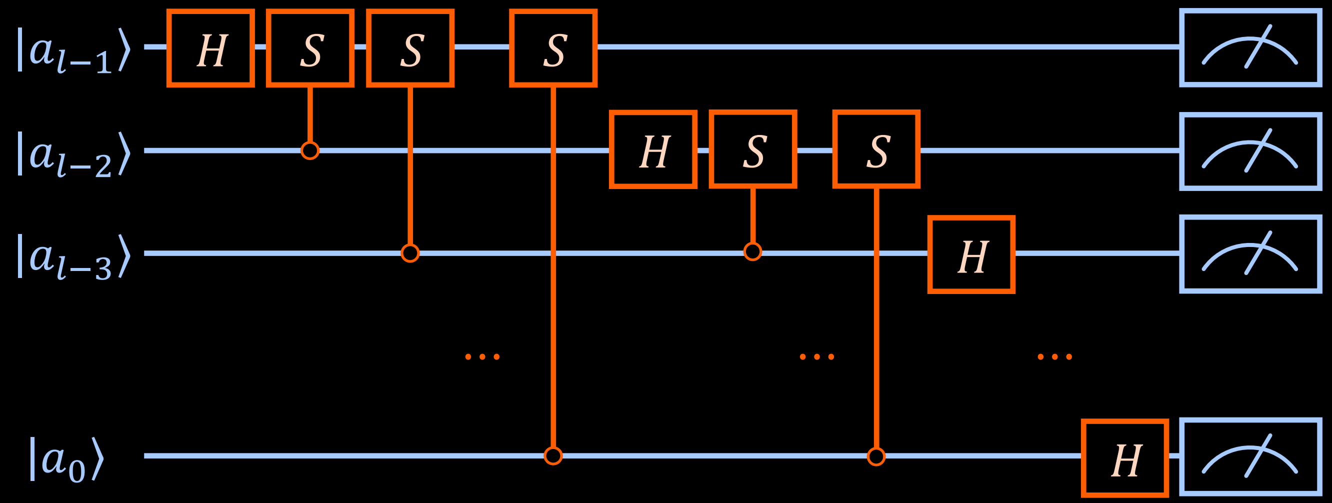
- Given superposition of a's entangled with function:
- computes quantum state w/ probability distribution:





Quantum Computing Recap

Quantum Fourier transformation implementation



- H (Hadamard) gate

$$\begin{array}{c|cc|} & |0\rangle & |1\rangle \\ |0\rangle & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ |1\rangle & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{array}$$

- S gate

$$\begin{array}{c|cccc|} & |00\rangle & |01\rangle & |10\rangle & |11\rangle \\ |00\rangle & 1 & 0 & 0 & 0 \\ |01\rangle & 0 & 1 & 0 & 0 \\ |10\rangle & 0 & 0 & 1 & 0 \\ |11\rangle & 0 & 0 & 0 & e^{i\pi/2^{k-j}} \end{array}$$

Recall

- Let $q = 2^l$ for some integer l
- Transform state $|a\rangle$ to state

$$\frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} |c\rangle \exp(2\pi i a c/q)$$

- Need $O(l^2)$ gates

Preliminaries

- [Knuth'81] We can obtain $\mathrm{GCD}(x, y)$ for integers x, y in $O(\log \min\{x, y\})$ time.
- [Bernstein'98] We can decide if integer x is a prime power in $(\log x)^{1+o(1)}$ time.
- [Chinese remainder] For k pairwise coprime integers $n_1, n_2, \dots, n_k$ where $N = \prod n_i$,
  there is exactly one solution for the system
  $x \equiv a_i \pmod{n_i}$ for all $i = 1,2, \dots, k$,
  $0 \leq x < N$.
- [Euler's formula] $e^{i\theta} = \cos\theta + i\sin\theta$.
- [Complex norms] $|z_1||z_2| = |z_1 z_2|$ for complex numbers z_1, z_2.
- [Hardy and Wright'79] We can quickly make a fraction expansion of a number for a given base.
- [Euler's totient function] $\phi(r) = \#$ of numbers coprime to r between 1 and r.

Problem: Integer Factorization

Prob Given an integer N, return two integers $n_1, n_2 \geq 2$ such that $n_1 n_2 = N$.

Alg Traditional $\sqrt{N}$ algorithm

for $i \leftarrow 2,3,\ldots,\sqrt{N}$ do
    if i divides N then
        return $N/i, i$
return false

- General Number Field Sieve (GNFS)

$$\exp\left(\left(\sqrt[3]{\frac{64}{9}} + o(1)\right)(\ln n)^{\frac{1}{3}}(\ln\ln(n))^{\frac{2}{3}}\right) \text{ time}$$

(best known deterministic)

- Shor's Algorithm

Shor's Algorithm: Overview

Def For integers x and n, the order of x in the multiplicative group $\bmod n$ is the least integer r such that $x^r \equiv 1 \pmod{n}$.

Integer Factorization

$x, n \rightarrow$ order of x

Shor's Algorithm: Non-Quantum Part

Alg Factorization [Miller'76]

if N is even or a prime power, easily factorize N

repeat:

    pick a random number $1 < x < N$

    if $\mathrm{GCD}(x, N) \neq 1$

        $g \leftarrow \mathrm{GCD}(x, N)$

        return $\langle g, N/g \rangle$

    $r \leftarrow$ order of $x \pmod{N}$

    if r is even and $x^{r/2} \not\equiv -1 \pmod{N}$

        $g \leftarrow \mathrm{GCD}\left(x^{r/2} - 1, N\right)$

        return $\langle g, N/g \rangle$

until confident

return prime

Shor's Algorithm: Non-Quantum Part

Alg | **Factorization [Miller'76]**

if N is even or a prime power, easily factorize N

repeat:

  pick a random number $1 < x < N$

  if $\mathrm{GCD}(x, N) \neq 1$

    $g \leftarrow \mathrm{GCD}(x, N)$

    return $\langle g, N/g \rangle$

  $r \leftarrow$ order of $x \pmod{N}$

  if r is even and $x^{r/2} \not\equiv -1 \pmod{N}$

    $g \leftarrow \mathrm{GCD}\left(x^{r/2} - 1, N\right)$

    return $\langle g, N/g \rangle$

until confident

return prime

Recall

- [Knuth'81] We can obtain $\mathrm{GCD}(x, y)$ for integers x, y in $O(\log \min\{x, y\})$ time.
- [Bernstein'98] We can decide if integer x is a prime power in $(\log x)^{1+o(1)}$ time.

Assume N is not prime

$$N = \prod p_i^{a_i}$$

for $i \geq 2$, primes $p_1, \dots, p_i$,

and integers $a_1, \dots, a_i \geq 1$.

Shor's Algorithm: Non-Quantum Part

Alg — Factorization [Miller'76]

```
if N is even or a prime power, easily factorize N
repeat:
    pick a random number 1 < x < N
    if GCD(x, N) ≠ 1
        g ← GCD(x, N)
        return ⟨g, N/g⟩
    r ← order of x (mod N)
    if r is even and x^{r/2} ≢ −1 (mod N)
        g ← GCD(x^{r/2} − 1, N)
        return ⟨g, N/g⟩
until confident
return prime
```

Assume N is not prime

$$N = \prod p_i^{a_i}$$

for $i \geq 2$, primes $p_1, \ldots, p_i$, and integers $a_1, \ldots, a_i \geq 1$.

- How can we be sure?
- If $\mathrm{GCD}(x, N) \neq 1$, we're happy ☺
- What can we do if $\mathrm{GCD}(x, N) = 1$?
- Use x to create another candidate

Shor's Algorithm: Non-Quantum Part

By def r is the least integer such that $x^r \equiv 1 \pmod{N}$.

$$x^r - 1 = QN$$

If r is even, i.e.,

$$x^r - 1 = x^{2r'} - 1 = \left(x^{r'} + 1\right)\left(x^{r'} - 1\right)$$

Note that,

$$\mathrm{GCD}\left(x^{r'} - 1, N\right) \neq N$$

Therefore, N is composite if:

$$\mathrm{GCD}\left(x^{r'} + 1, N\right) \neq N$$

Shor's Algorithm: Non-Quantum Part

Alg Factorization [Miller'76]

if N is even or a prime power, easily factorize N
repeat:
  pick a random number $1 < x < N$
  if $\mathrm{GCD}(x, N) \neq 1$
    $g \leftarrow \mathrm{GCD}(x, N)$
    return $\langle g, N/g \rangle$
  $r \leftarrow$ order of $x \pmod N$
  if r is even and $x^{r/2} \not\equiv -1 \pmod N$
    $g \leftarrow \mathrm{GCD}\left(x^{r/2} - 1, N\right)$
    return $\langle g, N/g \rangle$
until confident
return prime

assume $\mathrm{GCD}(x, N) = 1$

Assume N is not prime

$$N = \prod p_i^{a_i}$$

$$r_i = \text{order of } x \left(\mathrm{mod}\ p_i^{a_i}\right)$$

Failure

- if r is odd

  $\mathrm{LCM}(r_i) = r \equiv 1 \pmod 2$

  $\therefore r_i \equiv 1 \pmod 2$ for all i
- if $x^{r/2} \equiv -1 \pmod N$

  $r_i = 2^m q_i,\ q_i \equiv 1 \pmod 2$

  for all i and some integer $m \geq 1$
- $r_i = 2^m q_i,\ q_i \equiv 1 \pmod 2,\ m \geq 0$

Shor's Algorithm: Non-Quantum Part

Alg Factorization [Miller'76]

if N is even or a prime power, easily factorize N
repeat:
  pick a random number $1 < x < N$
  if $\mathrm{GCD}(x, N) \neq 1$
    $g \leftarrow \mathrm{GCD}(x, N)$
    return $\langle g, N/g \rangle$
  $r \leftarrow$ order of $x \pmod N$
  if r is even and $x^{r/2} \not\equiv -1 \pmod N$
    $g \leftarrow \mathrm{GCD}\left(x^{r/2} - 1, N\right)$
    return $\langle g, N/g \rangle$
until confident
return prime

Test fails when

$$r_i = 2^m q_i,\ q_i \equiv 1 \pmod 2,\ m \geq 0$$

Recall

- [Chinese remainder] There is exactly one solution for the system
  $x \equiv a_i \pmod{n_i}$ for all $i = 1,2, \dots, k$,
  $0 \leq x < N$.
- choosing $x \in [2, N-1]$ U.A.R.
  $\Leftrightarrow$ (large N)
  choosing r_i's $\in \left[0, p_i^{a_i}\right]$ U.A.R.
- $\mathrm{Prob(failure)} = \sum_m \prod_i \mathrm{Prob}(r_i \equiv 2^m q_i)$

$$< \frac{1}{2^{\#\text{prime factors} - 1}} \leq \frac{1}{2}$$

Shor's Algorithm: Non-Quantum Part

Alg — Factorization [Miller'76]

if N is even or a prime power, easily factorize N
repeat:
    pick a random number $1 < x < N$
    if $\mathrm{GCD}(x, N) \neq 1$
        $g \leftarrow \mathrm{GCD}(x, N)$
        return $\langle g, N/g \rangle$
    $\boxed{r \leftarrow \text{order of } x \ (\mathrm{mod}\ N)}$
    if r is even and $x^{r/2} \not\equiv -1 \ (\mathrm{mod}\ N)$
        $g \leftarrow \mathrm{GCD}\left(x^{r/2} - 1, N\right)$
        return $\langle g, N/g \rangle$
until confident
return prime

Overall

- $l \triangleq$ # of iterations
- if N is prime, always correct
- if N is composite, incorrect with probability at most $1/2^l$
- Running time in $O\big(l(\log N + q)\big)$

Running time of quantum submodule

To Quantum Part >>

Shor's Algorithm: Quantum Part

Alg — Order-Finding Quantum Algorithm

$q \leftarrow$ smallest power of 2 with $q \geq N^2$

repeat:

  make uniform superposition in register 1:

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

  compute $|x^a \pmod{N}\rangle$ in register 2

  perform Fourier transform in register 1

  $c \leftarrow$ observation result

  $d/r \leftarrow$ round c/q to nearest frac w/ $r < N$

until we are confident

return r

Shor's Algorithm: Quantum Part

Alg — Order-Finding Quantum Algorithm

$q \leftarrow$ smallest power of 2 with $q \geq N^2$

repeat:

  make uniform superposition in register 1:

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

  compute $|x^a \pmod N\rangle$ in register 2

  perform Fourier transform in register 1

  $c \leftarrow$ observation result

  $d/r \leftarrow$ round c/q to nearest frac w/ $r < N$

until we are confident

return r

Use two quantum registers

- Register 1: value computation
- Register 2: condition checking
- Both ranges include states from 0 to $N-1$
- Need at least N^2 states when concatenated

Shor's Algorithm: Quantum Part

Alg Order-Finding Quantum Algorithm

$q \leftarrow$ smallest power of 2 with $q \geq N^2$
repeat:
  make uniform superposition in register 1:

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

  compute $|x^a \pmod{N}\rangle$ in register 2
  perform Fourier transform in register 1
  $c \leftarrow$ observation result
  $d/r \leftarrow$ round c/q to nearest frac w/ $r < N$
until we are confident
return r

How?

- Uniform superposition with Hadamard gate
- $|x^a \pmod{N}\rangle$ with conditioned gates

$|x^a \pmod{N}\rangle$ implementation

Pw $\leftarrow$ 1
for $i = 0, 1, \ldots, \log q - 1$:
  if $|a\rangle[i] = 1$:
    $\boxed{\text{Pw} \leftarrow \text{Pw} \times x^{2^i}}$

Shor's Algorithm: Quantum Part

Alg — Order-Finding Quantum Algorithm

$q \leftarrow$ smallest power of 2 with $q \geq N^2$

repeat:

  make uniform superposition in register 1:

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

  compute $|x^a \pmod{N}\rangle$ in register 2

  perform Fourier transform in register 1

How?

- Uniform superposition with Hadamard gate
- $|x^a \pmod{N}\rangle$ with conditioned gates

$|x^a \pmod{N}\rangle$ implementation

Pw $\leftarrow 1$

for $i = 0, 1, \ldots, \log q - 1$:

  if $|a\rangle[i] = 1$:

    Pw $\leftarrow$ Pw $\times\, x^{2^i}$

Shor's Algorithm: Quantum Part

Alg — **Order-Finding Quantum Algorithm**

$q \leftarrow$ smallest power of 2 with $q \geq N^2$

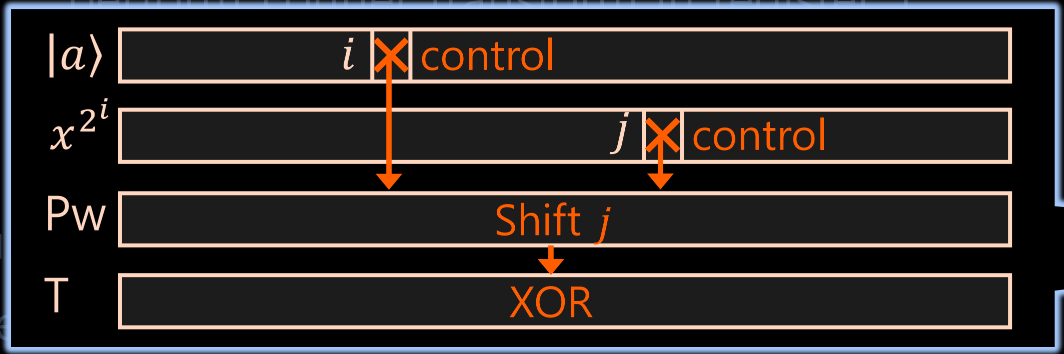
repeat:

make uniform superposition in register 1:

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

compute $|x^a \pmod N\rangle$ in register 2

perform Fourier transform in register 1



How?

- Uniform superposition with Hadamard gate
- $|x^a \pmod N\rangle$ with conditioned gates

$|x^a \pmod N\rangle$ implementation

Pw $\leftarrow$ 1
for $i = 0,1,\dots,\log q - 1$:
  if $|a\rangle[i] = 1$:
    T $\leftarrow$ 0
    for $j = 0,1,\dots,\log q - 1$:
      if $x^{2^i}[j] = 1$:
        add $2^j \times$ Pw to T
    Pw $\leftarrow$ T

Shor's Algorithm: Quantum Part

Alg — Order-Finding Quantum Algorithm

$q \leftarrow$ smallest power of 2 with $q \geq N^2$

repeat:

  make uniform superposition in register 1:

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

  compute $|x^a \pmod{N}\rangle$ in register 2

  perform Fourier transform in register 1

u

re

- Intuition: multiplication w/ base 2
- Total of $O\left((\log N)^2\right)$ gates

$$\begin{array}{rcc} & a & b \\ \times & c & d \\ \hline & ad & bd \\ + \; ac & bc & \\ \hline & \mathrm{T} & \end{array}$$

How?

- Uniform superposition with Hadamard gate
- $|x^a \pmod{N}\rangle$ with conditioned gates

$|x^a \pmod{N}\rangle$ implementation

Pw ← 1
for $i = 0, 1, \ldots, \log q - 1$:
  if $|a\rangle[i] = 1$:
    T ← 0
    for $j = 0, 1, \ldots, \log q - 1$:
      if $x^{2^i}[j] = 1$:
        add $2^j \times$ Pw to T
    Pw ← T

Shor's Algorithm: Quantum Part

Alg — Order-Finding Quantum Algorithm

$q \leftarrow$ smallest power of 2 with $q \geq N^2$

repeat:

  make uniform superposition in register 1:

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

  compute $|x^a \pmod N\rangle$ in register 2

  perform Fourier transform in register 1

  $c \leftarrow$ observation result

  $d/r \leftarrow$ round c/q to nearest frac w/ $r < N$

until we are confident

return r

Before

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

Transform state $|a\rangle$ to state

$$\frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} \exp(2\pi i a c/q)\, |c\rangle$$

After

$$\frac{1}{q} \sum_{a=0}^{q-1} \sum_{c=0}^{q-1} \exp(2\pi i a c/q)|c\rangle\, |x^a \pmod N\rangle$$

Shor's Algorithm: Quantum Part

Current quantum state

$$\frac{1}{q}\sum_{a=0}^{q-1}\sum_{c=0}^{q-1}\exp(2\pi iac/q)|c\rangle\,|x^a \pmod N\rangle$$

The probability of observing state $|c, x^k \pmod N\rangle$

- By definition of quantum state

$$\left|\frac{1}{q}\sum_{a:x^a\equiv x^k}\exp\left(\frac{2\pi ac}{q}\right)\right|^2$$

Shor's Algorithm: Quantum Part

Current quantum state

$$\frac{1}{q}\sum_{a=0}^{q-1}\sum_{c=0}^{q-1}\exp(2\pi iac/q)|c\rangle\,|x^a \pmod N\rangle$$

The probability of observing state $|c, x^k \pmod N\rangle$

- By definition of quantum state

$$\left|\frac{1}{q}\sum_{a:x^a\equiv x^k}\exp\left(\frac{2\pi ac}{q}\right)\right|^2$$

- Let $a = br + k$ for integer b

$$\left|\frac{1}{q}\sum_{b=0}^{\lfloor (q-k-1)/r \rfloor}\exp(2\pi i(br+k)c/q)\right|^2$$

Shor's Algorithm: Quantum Part

Current quantum state

$$\frac{1}{q}\sum_{a=0}^{q-1}\sum_{c=0}^{q-1}\exp(2\pi iac/q)|c\rangle\,|x^a \pmod N\rangle$$

The probability of observing state $\left|c, x^k \pmod N\right\rangle$

$$= \left|\cos\left(\frac{2\pi kc}{q}\right) + i\sin\left(\frac{2\pi kc}{q}\right)\right|^2 = 1$$

- Recall $|z_1||z_2| = |z_1 z_2|$:

$$\left|\exp\left(\frac{2\pi ikc}{q}\right)\right|^2 \left|\frac{1}{q}\sum_{b=0}^{\lfloor (q-k-1)/r \rfloor} \exp(2\pi ibrc/q)\right|^2$$

- Let $a = br + k$ for integer b

$$\left|\frac{1}{q}\sum_{b=0}^{\lfloor (q-k-1)/r \rfloor} \exp(2\pi i(br+k)c/q)\right|^2$$

Shor's Algorithm: Quantum Part

Current quantum state

$$\frac{1}{q}\sum_{a=0}^{q-1}\sum_{c=0}^{q-1}\exp(2\pi iac/q)|c\rangle\,|x^a \pmod N\rangle$$

The probability of observing state $|c, x^k \pmod N\rangle$

- By definition of quantum state

If we let $rc = dq + R$:

$$\begin{aligned}&\exp(2\pi ibrc/q)\\&= \exp(2\pi ibR/q)\exp(2\pi ibd)\\&= \exp(2\pi ibR/q)(\cos 2\pi bd + i\,sin 2\pi bd)\end{aligned}$$

Note that $2bd$ is an even integer:

$$= \exp(2\pi ibR/q)(1 + i\cdot 0)$$

- Recall $|z_1||z_2| = |z_1 z_2|$:

$$\left|\exp\left(\frac{2\pi ikc}{q}\right)\right|^2\left|\frac{1}{q}\sum_{b=0}^{\lfloor (q-k-1)/r\rfloor}\exp(2\pi ibrc/q)\right|^2$$

- Let $R: R \equiv rc \pmod q, R \in \left(-\frac{q}{2}, \frac{q}{2}\right]$

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

Shor's Algorithm: Quantum Part

Current quantum state

$$\frac{1}{q}\sum_{a=0}^{q-1}\sum_{c=0}^{q-1}\exp(2\pi iac/q)|c\rangle\,|x^a\ (\mathrm{mod}\ N)\rangle$$

The probability of observing state $|c, x^k\ (\mathrm{mod}\ N)\rangle$

- Approximate to integral:

$$\left|\frac{1}{q}\sum_{b=0}^{\lfloor (q-k-1)/r\rfloor}\exp(2\pi ibR/q)\right|^2 = \frac{1}{r}\int_0^{\frac{r}{q}\left\lfloor\frac{q-k-1}{r}\right\rfloor}\exp\left(2\pi i\frac{R}{r}u\right)du + O\left(\frac{\left\lfloor\frac{(q-k-1)}{r}\right\rfloor}{q}\left(\exp\left(\frac{2\pi iR}{q}\right)-1\right)\right)$$

$$\approx \frac{1}{r}\int_0^1 \exp\left(2\pi i\frac{R}{r}u\right)du + O\left(\frac{1}{q}\right)$$

Minimized when $\frac{R}{r} = \pm\frac{1}{2}$,
value at minimum $= \frac{4}{\pi^2 r^2} \approx \frac{1}{3r^2}$

Shor's Algorithm: Quantum Part

Alg — Order-Finding Quantum Algorithm

$q \leftarrow$ smallest power of 2 with $q \geq N^2$

repeat:

  make uniform superposition in register 1:

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

  compute $|x^a \pmod N\rangle$ in register 2

  perform Fourier transform in register 1

  $c \leftarrow$ observation result

  $d/r \leftarrow$ round c/q to nearest frac w/ $r < N$

until we are confident

return r

Cont.

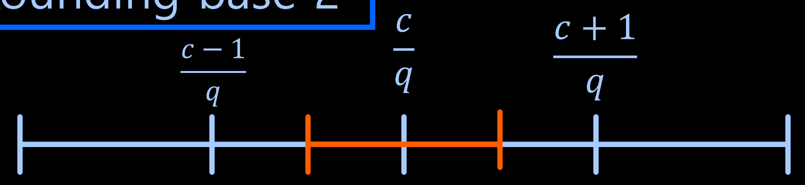
- The probability of $|c, x^k \pmod N\rangle$ at least $\frac{1}{3r^2}$ in range

$$-\frac{r}{2} < R \leq \frac{r}{2}$$

- Let $rc = dq + R$:

$$\left|\frac{c}{q} - \frac{d}{r}\right| \leq \frac{1}{2q}$$

Rounding base 2



d/r in here

Shor's Algorithm: Quantum Part

Alg — **Order-Finding Quantum Algorithm**

$q \leftarrow$ smallest power of 2 with $q \geq N^2$

repeat:

  make uniform superposition in register 1:

  compute $|x^a \pmod N\rangle$ in register 2

  perform Fourier transform in register 1

  $c \leftarrow$ observation result

  $d/r \leftarrow$ round c/q to nearest frac w/ $r < N$

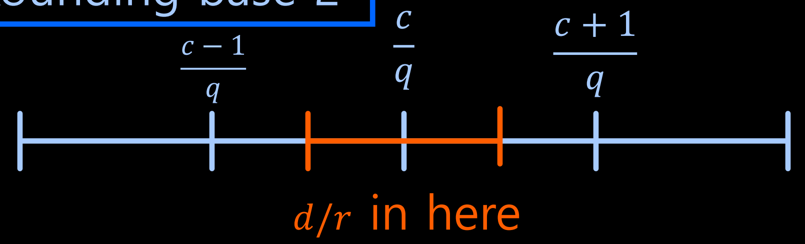
until we are confident

return r

Q. How many states $|c, x^k \pmod N\rangle$ can we compute r this way?

Solve with fast fraction expansion

Rounding base 2



Cont.

- Assume ∃2+ fractions with $r < N$

$$\frac{d_1}{r_1} - \frac{d_2}{r_2} = \frac{d_1 r_2 - d_2 r_1}{r_1 r_2} \geq \frac{1}{r_1 r_2} > \frac{1}{N^2}$$

- We chose $q > N^2$

$$\frac{1}{N^2} > \frac{1}{q}$$

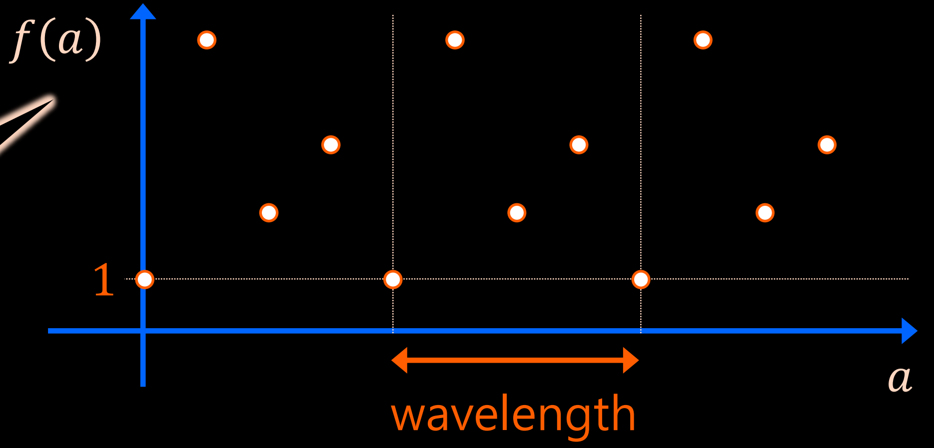
- Only one fraction with $r < N$ inside orange!

Shor's Algorithm: Non-Quantum Part

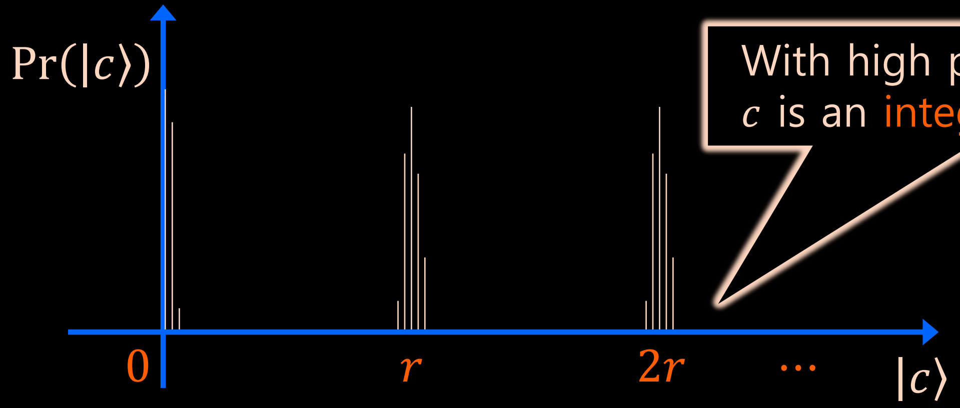
Recall::Quantum Fourier transformation

- Given superposition of a's entangled with function:

$f(a) = x^a \pmod N$ is periodic injective



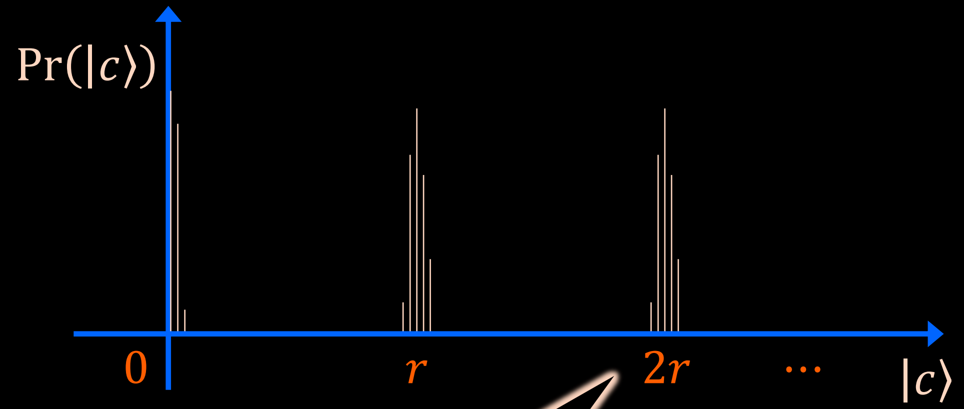
- computes quantum state w/ probability distribution:



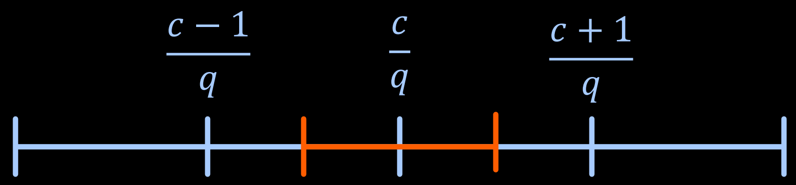
With high probability, c is an integral multiple of r

Shor's Algorithm: Non-Quantum Part

Recall::Quantum Fourier transformation



With high probability,
c is an integral multiple of r



At most one d/r in here

- q: fixed, know
- r: fixed, don't know, coprime w/ d
- c: not fixed, observe
- d: at most one for each (q, r, c)

How many states $|c, x^k \pmod{N}\rangle$?

$$(\#d\text{'s coprime w/ } r) \cdot \left(\#x^k \pmod{N}\right) = \phi(r) \cdot r$$

Shor's Algorithm: Quantum Part

Alg — Order-Finding Quantum Algorithm

$q \leftarrow$ smallest power of 2 with $q \geq N^2$

repeat:

    make uniform superposition in register 1:

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

    compute $|x^a \pmod N\rangle$ in register 2

    perform Fourier transform in register 1

    $c \leftarrow$ observation result

    $d/r \leftarrow$ round c/q to nearest frac w/ $r < N$

until we are confident

return r

We have

- Obtain correct r for $r\phi(r)$ choices of $|c, x^k \pmod N\rangle$
- The probability of each $|c, x^k \pmod N\rangle$ at least $\frac{1}{3r^2}$
- Obtain correct r with probability at least

$$\frac{r\phi(r)}{3r^2} > \frac{\delta}{3 \log \log r}$$

for some constant δ

- Repeat $O(\log \log r)$ times to be sure

Shor's Algorithm: Quantum Part

Alg — Order-Finding Quantum Algorithm

$q \leftarrow$ smallest power of 2 with $q \geq N^2$

repeat:

  make uniform superposition in register 1:

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

  compute $|x^a \pmod{N}\rangle$ in register 2

  perform Fourier transform in register 1

  $c \leftarrow$ observation result

  $d/r \leftarrow$ round c/q to nearest frac w/ $r < N$

until we are confident

return r

Overall

- $O(\log\log r)$ iterations
- $|x^a \pmod{N}\rangle$ and QFT both use $O((\log N)^2)$ gates
- overall # gates and running time polynomial in $\log N$

Shor's Algorithm: Non-Quantum Part

Alg | **Factorization [Miller'76]**

if N is even or a prime power, easily factorize N

repeat:

    pick a random number $1 < x < N$

    if $\mathrm{GCD}(x, N) \neq 1$

        $g \leftarrow \mathrm{GCD}(x, N)$

        return $\langle g, N/g \rangle$

    $\boxed{r \leftarrow \text{order of } x \pmod{N}}$

    if r is even and $x^{r/2} \not\equiv -1 \pmod{N}$

        $g \leftarrow \mathrm{GCD}\left(x^{r/2} - 1, N\right)$

        return $\langle g, N/g \rangle$

until confident

return prime

Overall

- $l \triangleq$ # of iterations
- if N is prime, always correct
- if N is composite, incorrect with probability at most $1/2^l$
- Running time in $O\big(l(\log N + q)\big)$

Running time of quantum submodule polynomial in $\log N$

From Quantum Part

References

- D. E. Knuth. *The art of computer programming, vol. 2: seminumerical algorithms, second edition.* Addison-Wesley, 1981.
- D. J. Bernstein. *Detecting perfect powers in essentially linear time*. Mathematics of Computation, 1998.
- P. W. Shor. *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*. SIAM Journal on Computing, 1997.
- G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers, fifth edition*. Oxford University Press, 1979.