Quantum Cryptanalysis

Shor Algorithm and Grover Algorithm

Hao Chung (鍾豪)
National Taiwan University

Aug. 2, 2018

Self Introduction

台大電機碩士準畢業生

2016 暑期密碼學課程學生

2017 暑期密碼學助教

研究主題：Quantum key distribution (量子密鑰分發)

Quantum Cryptanalysis

Grover Algorithm
Shor Algorithm

Crypto

Quantum Cryptography

Quantum Key Distribution

Post-quantum Cryptography

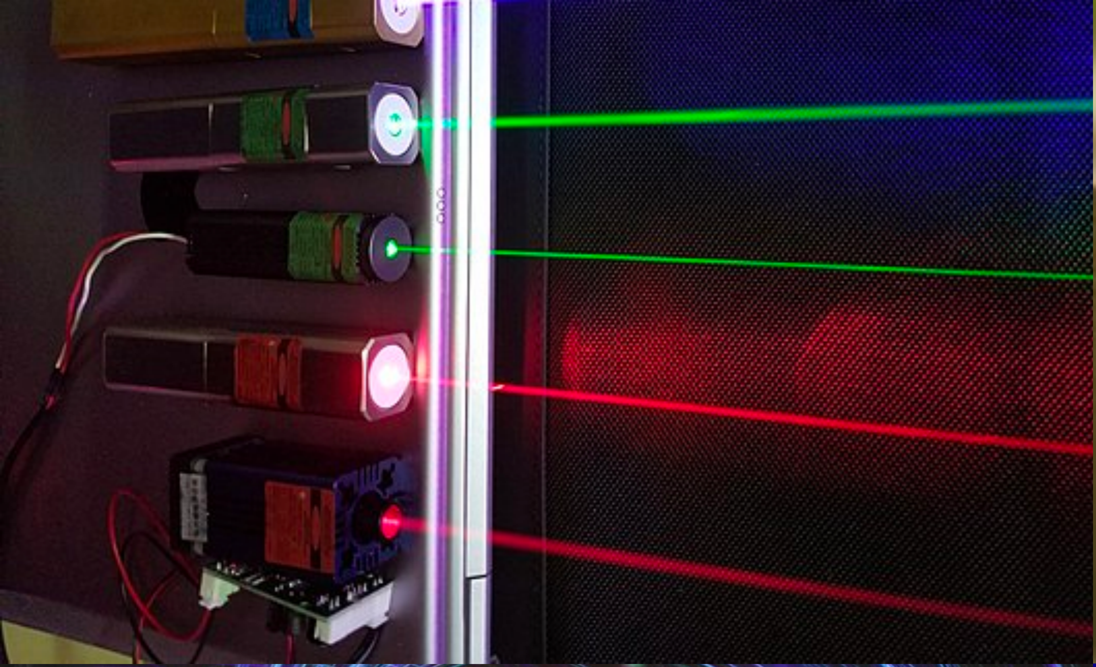
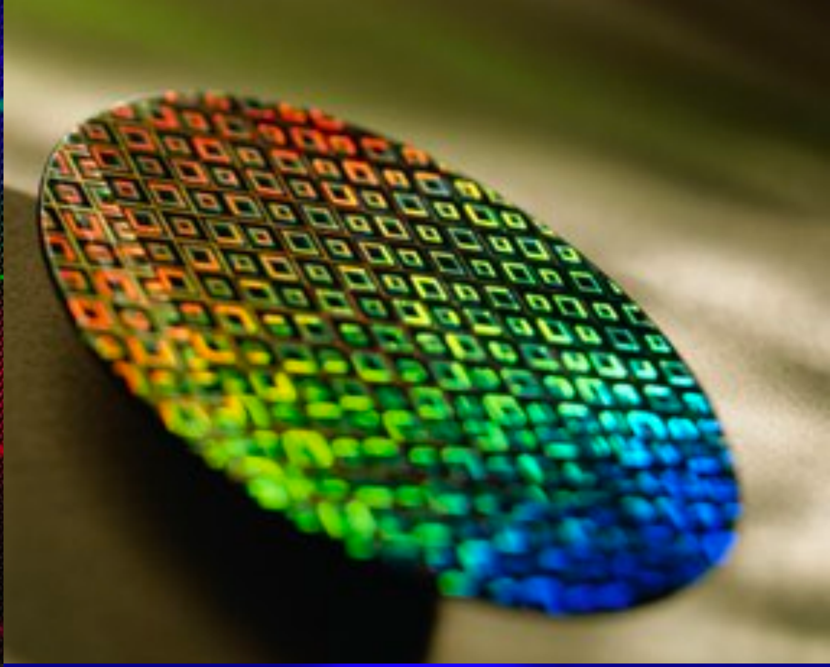
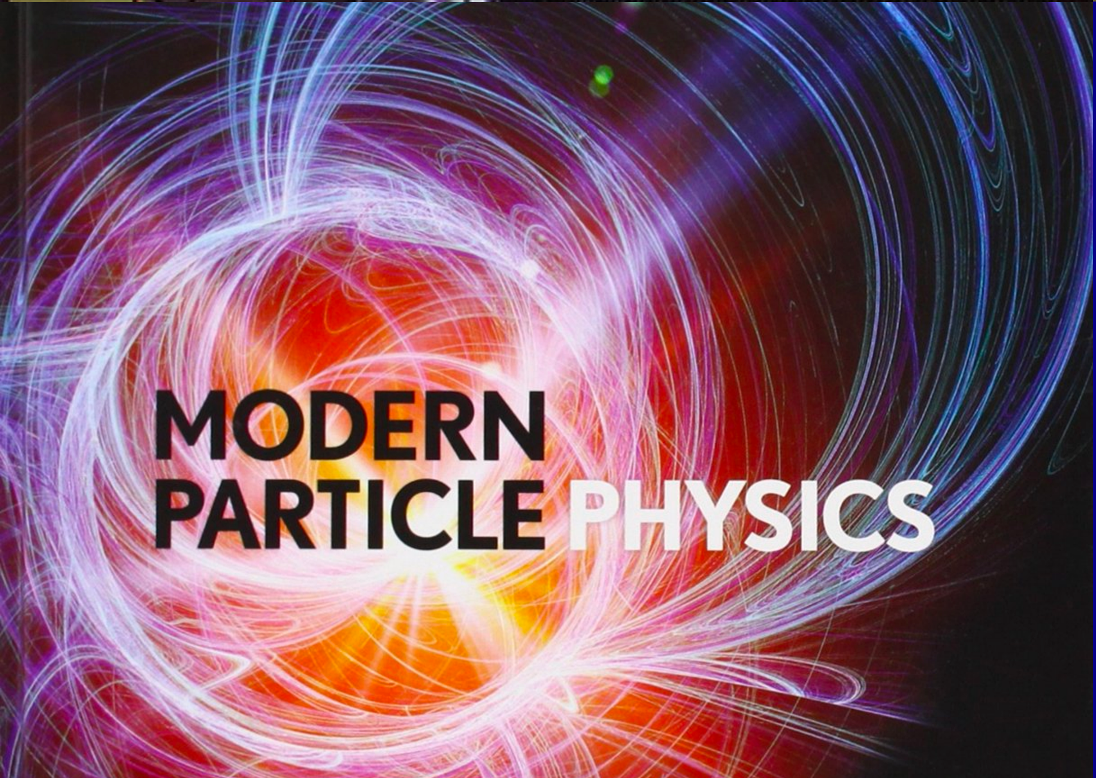
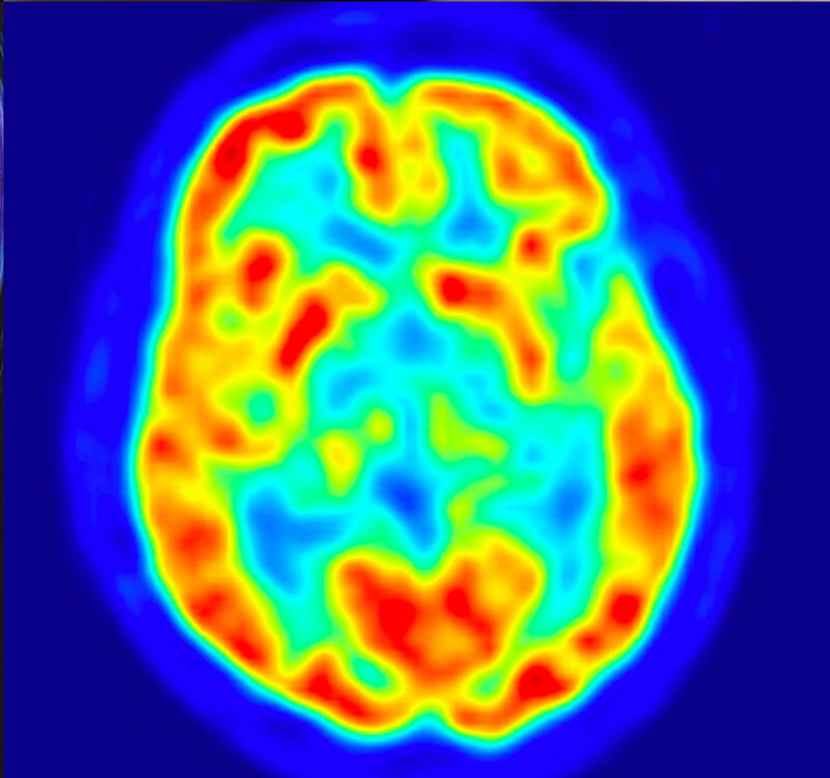
Outline

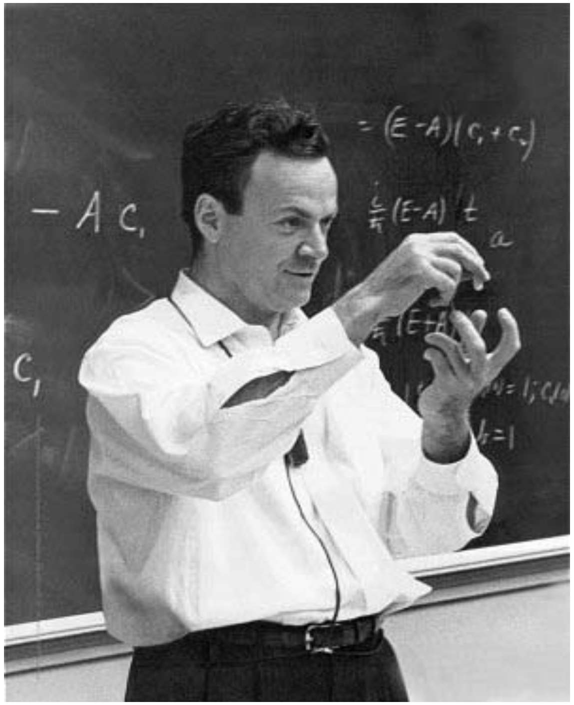
1. Introduction to quantum computing
2. Grover Algorithm
3. Shor Algorithm

What is QUANTUM?

Max Planck (1858-1947)

$$E = nh\nu$$




MODERN
PARTICLE PHYSICS




Richard Feynman (1918-1988)

therefore, the problem is, how can we simulate the quantum mechanics? There are two ways that we can go about it. We can give up on our rule about what the computer was, we can say: Let the computer itself be built of quantum mechanical elements which obey quantum mechanical laws. Or

Quantum State

In quantum computing, we use Dirac notation "$| \cdot \rangle$" to represent a state.

For example, a state of a coin could be

$$|\mathrm{Head}\rangle \text{ and } |\mathrm{Tail}\rangle.$$

Or, a state of a die could be

$$|1\rangle, |2\rangle, |3\rangle, |4\rangle, |5\rangle \text{ and } |6\rangle.$$

A **qubit** is a quantum object that has two states, usually written as

$$|0\rangle \text{ and } |1\rangle.$$

Superposition

Classical Coin

$\frac{1}{2}$: Head

$\frac{1}{2}$: Tail

Quantum Coin

$$\frac{1}{\sqrt{2}}|\mathrm{Head}\rangle + \frac{1}{\sqrt{2}}|\mathrm{Tail}\rangle$$

Superposition

What is the difference between **classical** states and **quantum** states?

A classical bit should **either** be 0 **or** be 1.

A qubit can be superposition of both:

$$\alpha|0\rangle + \beta|1\rangle.$$

- When we measure it, we get

$$\begin{cases} 0 \text{ with probability } |\alpha|^2; \\ 1 \text{ with probability } |\beta|^2. \end{cases}$$

- Since the sum of the probability must be one,

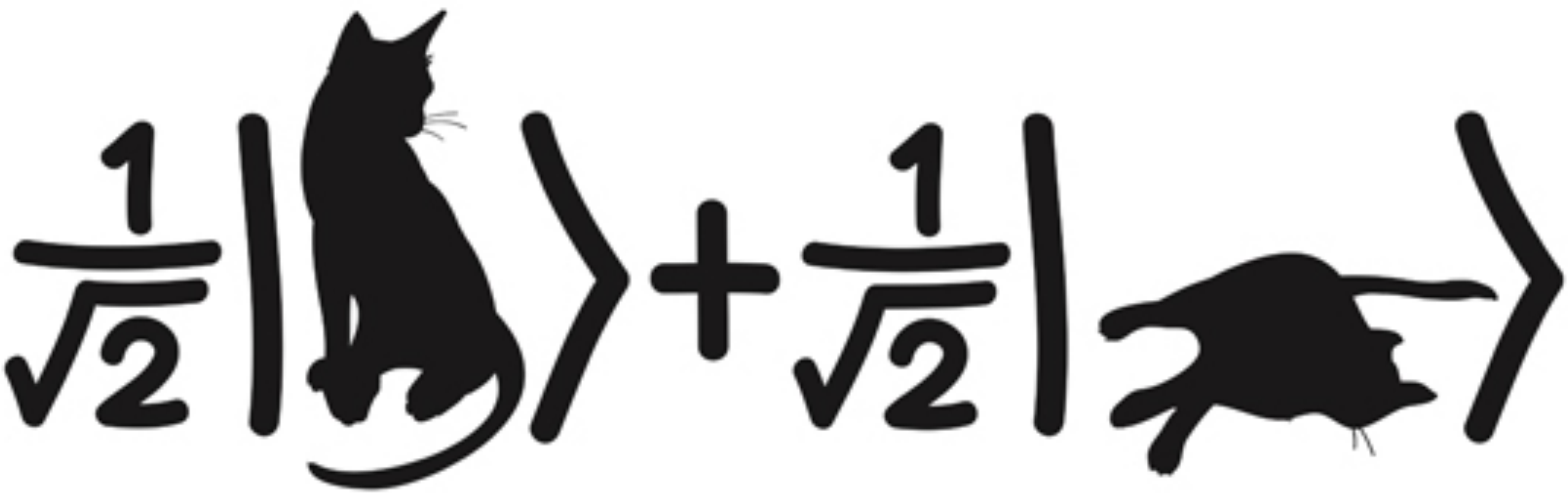
$$|\alpha|^2 + |\beta|^2 = 1.$$

Example (Fair Quantum Die)

What is the state of a fair quantum die before we measure it?

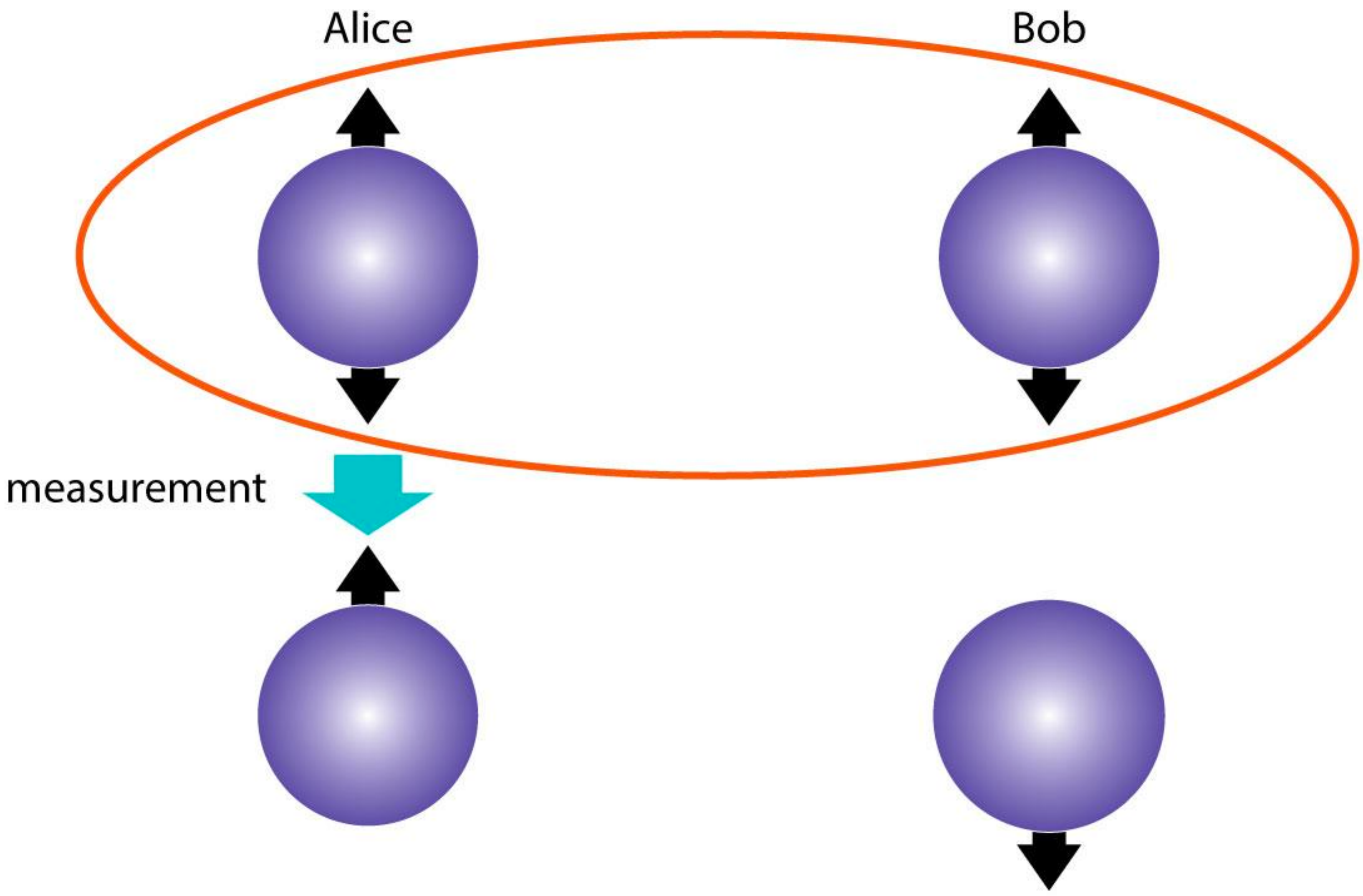
$$\frac{1}{\sqrt{6}}|1\rangle + \frac{1}{\sqrt{6}}|2\rangle + \frac{1}{\sqrt{6}}|3\rangle + \frac{1}{\sqrt{6}}|4\rangle + \frac{1}{\sqrt{6}}|5\rangle + \frac{1}{\sqrt{6}}|6\rangle.$$

Superposition



Entanglement

Entanglement



Composite System

What happens if we have more qubits?

For two qubits, we can write two-qubit system as

$$a_1|00\rangle + a_2|01\rangle + a_3|10\rangle + a_4|11\rangle,$$

where $|a_1|^2 + |a_2|^2 + |a_3|^2 + |a_4|^2 = 1.$

In general, if we have N qubits, the system is

$$\sum_{x=1}^{2^N} a_x|x\rangle\,,$$

where $\sum_{x=1}^{2^N} |a_x|^2 = 1\,.$

Independent State

If we have two qubits:

$$(\alpha_1|0\rangle + \beta_1|1\rangle)(\alpha_2|0\rangle + \beta_2|1\rangle).$$

The composite system follows distributive law:

$$\alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle.$$

For example, condition on the 1st qubit is 0, the residue state is

$$|0\rangle\left(\frac{\alpha_1\alpha_2|0\rangle + \alpha_1\beta_2|1\rangle}{\sqrt{|\alpha_1|^2}}\right) = |0\rangle(\alpha_2|0\rangle + \beta_2|1\rangle).$$

Entanglement

Consider the following function U such that

$$U|x\rangle = |x\rangle|\neg x\rangle.$$

If the input is $|0\rangle$, the output is $|0\rangle|1\rangle$.

If the input is $|1\rangle$, the output is $|1\rangle|0\rangle$.

What happens if the input is $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$?

$$U\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) = \frac{1}{\sqrt{2}}|0\rangle|1\rangle + \frac{1}{\sqrt{2}}|1\rangle|0\rangle.$$

Entanglement

For the state

$$\frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle,$$

can we write it as a product state

$$(\alpha_1|0\rangle + \beta_1|1\rangle)(\alpha_2|0\rangle + \beta_2|1\rangle)?$$

No! If we measure one of the qubits, the coefficients of the other qubit will change.

We say these two qubits are **entangled**.

Mathematical Formalism

Postulate 1: A quantum system is described a **unit vector** in the Hilbert space.

- Hilbert space is defined as an inner product space over $\mathbb{C}$.

For a single qubit, we write $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$.

In general,

$$\alpha|0\rangle + \beta|1\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}.$$

Example (EPR pair)

The state in the previous slide is the famous Einstein-Podolsky-Rosen (EPR) pair:

$$\frac{|01\rangle + |10\rangle}{\sqrt{2}} = \begin{bmatrix} 0 \\ 1/\sqrt{2} \\ 1/\sqrt{2} \\ 0 \end{bmatrix}.$$

Mathematical Formalism

Postulate 2: Quantum operation in a closed system is described by a unitary operator U.

- An operator U is unitary if for all $|v\rangle \in V$, operator U satisfies

$$\| U|v\rangle \| = \| |v\rangle \|.$$

Example (NOT gate)

Let $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. Then,

$$X|0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle.$$

X gate is the NOT gate in quantum computing.

Quantum Parallelism

A single quantum computer can compute multiple computations **simultaneously** by the effect of superposition.

For example,

$$U_f\ (|x\rangle|0\rangle)\ =\ |x\rangle\,|f(x)\rangle$$

$$|\psi\rangle = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}(|x\rangle|0\rangle)$$

$$U_f\ |\psi\rangle = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}(|x\rangle|{\color{red}f(x)}\rangle)$$

It seems that $\sum_{x=0}^{2^n-1}|f(x)\rangle$ can be computed in one operation.

Quantum Parallelism

Example (Modular Exponential)

Let $f_{a,N}(x) = a^x \bmod N$, and U_f is an unitary operator corresponding to $f_{a,N}(x)$.

Now we have $a = 7, N = 15$ and

$$|\psi\rangle = \frac{1}{2}(|0\rangle + |1\rangle + |2\rangle + |3\rangle).$$

Then,

$$U_f(|\psi\rangle|0\rangle) = \frac{1}{2}(|0\rangle|1\rangle + |1\rangle|7\rangle + |2\rangle|4\rangle + |3\rangle|13\rangle).$$

The example shows that we somehow can compute $7^0, 7^1, 7^2, 7^3 \pmod{15}$ simultaneously.

The problem is “how we extract the answer?”

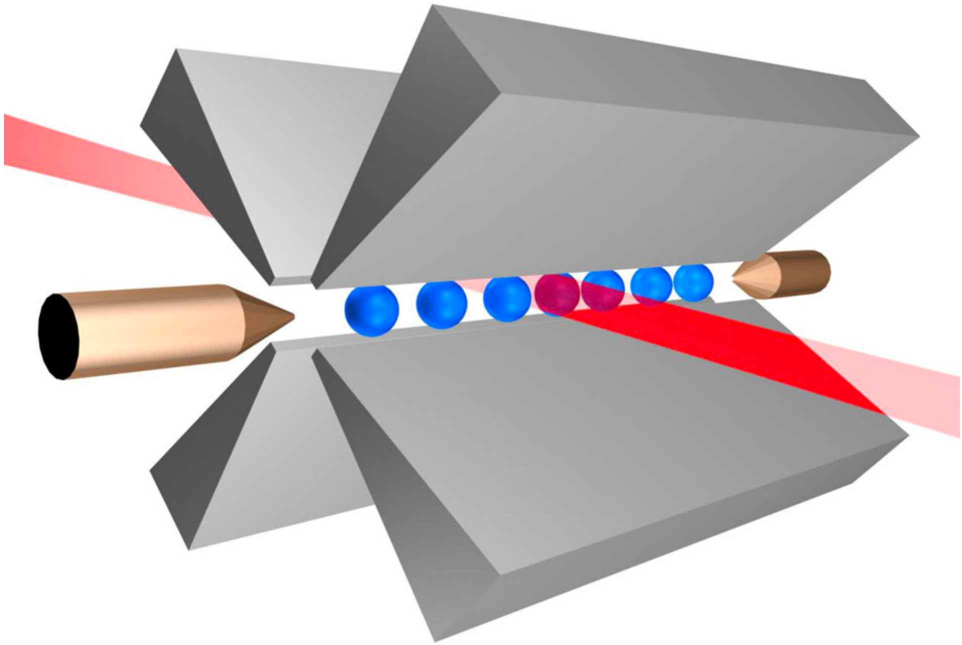
Summary

量子態可由一個「單位向量」表示，
而量子運算可由一個unitary 矩陣表示

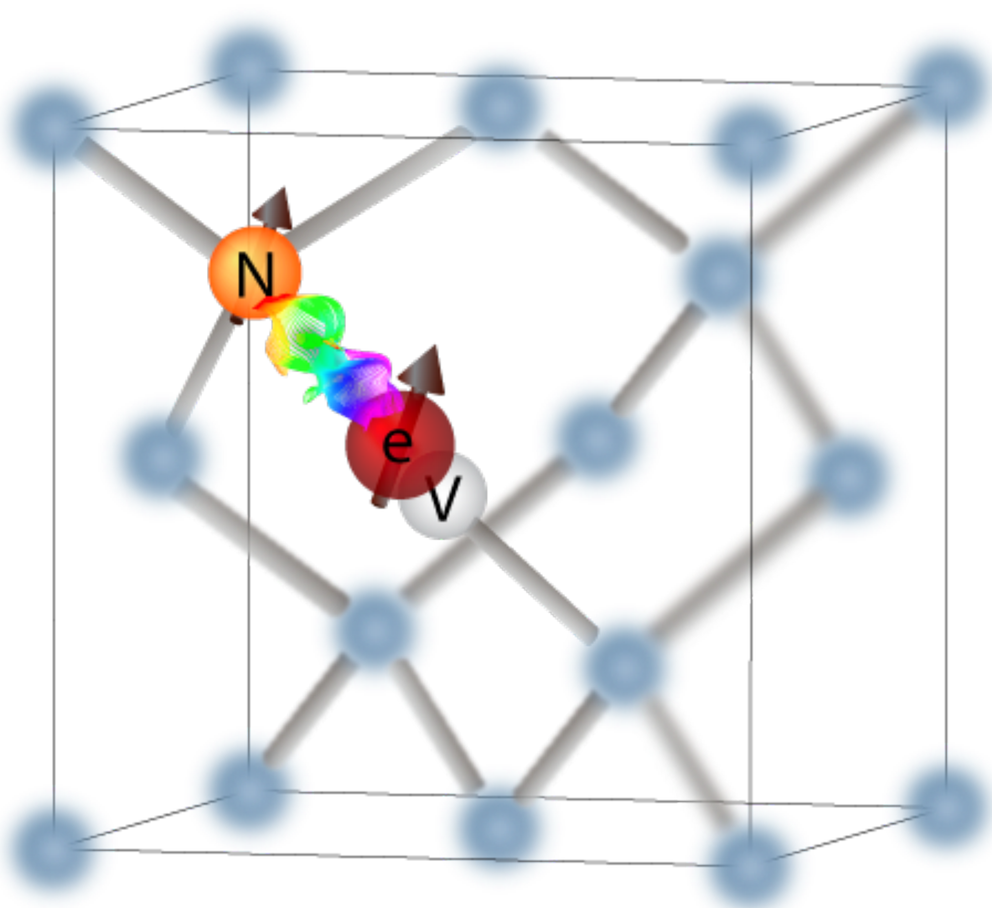
「量子平行」是利用疊加的特性，
達到一次操作即可同時計算多個疊加態

大多數量子演算法的設計巧妙在於
「如何操控係數，使我們測量到需要的結果」

Quantum Computer --- Ion Trap



Quantum Computer --- Solid State Based



Outline

1. Introduction to quantum computing
2. Grover Algorithm
3. Shor Algorithm

Needle-in-a-Haystack

Suppose you have N envelopes. One of them has money inside but others are empty.

How many trials do you need to do for finding money?

- Worst case: $N-1$ times.
- In average: $N/2$ times.

Classically, we need to try $O(N)$ times.

Grover suggests an algorithm for such problem only takes $O(\sqrt{N})$ operations.

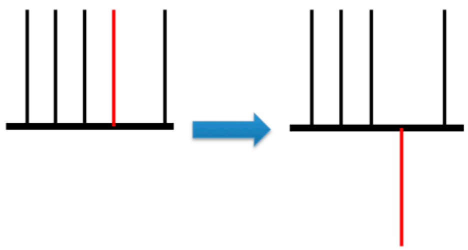
Needle-in-a-Haystack

Grover Algorithm

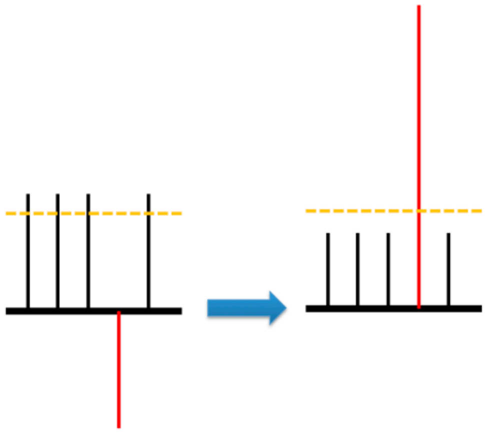
Idea: Maximize the amplitude of the right answer in a superposed state.

One Grover iteration consists of two steps:

Phase inversion



Inversion about mean



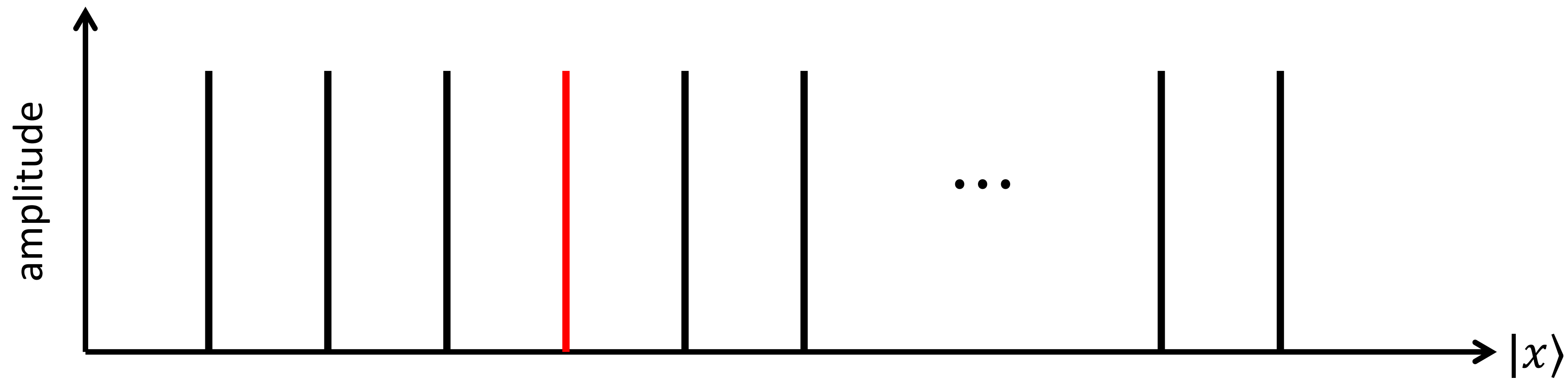
One Grover algorithm only need $O(\sqrt{N})$ Grover iterations.

Grover Iteration

First, we prepare a superposed state

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=1}^{N} |x\rangle.$$

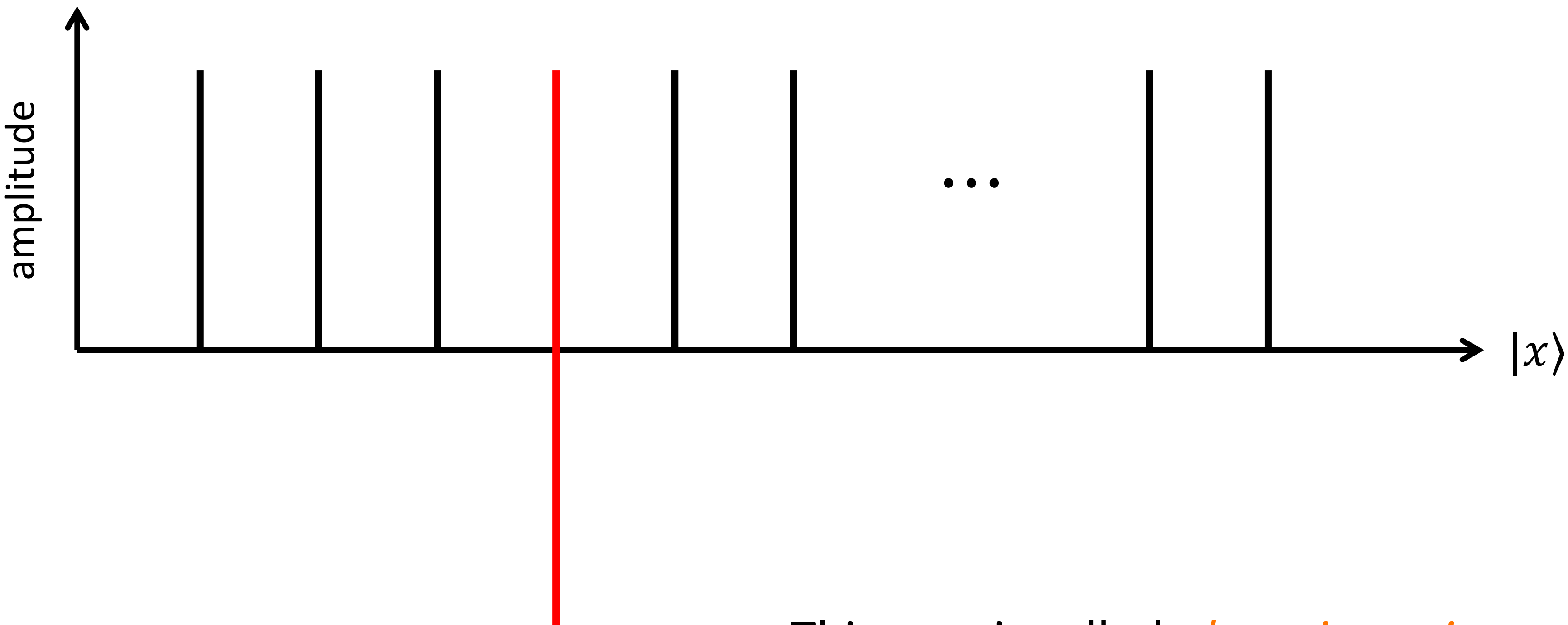
Assume the red one is the right answer we want to obverse.



Grover Iteration

We inverse the amplitude of the right answer,

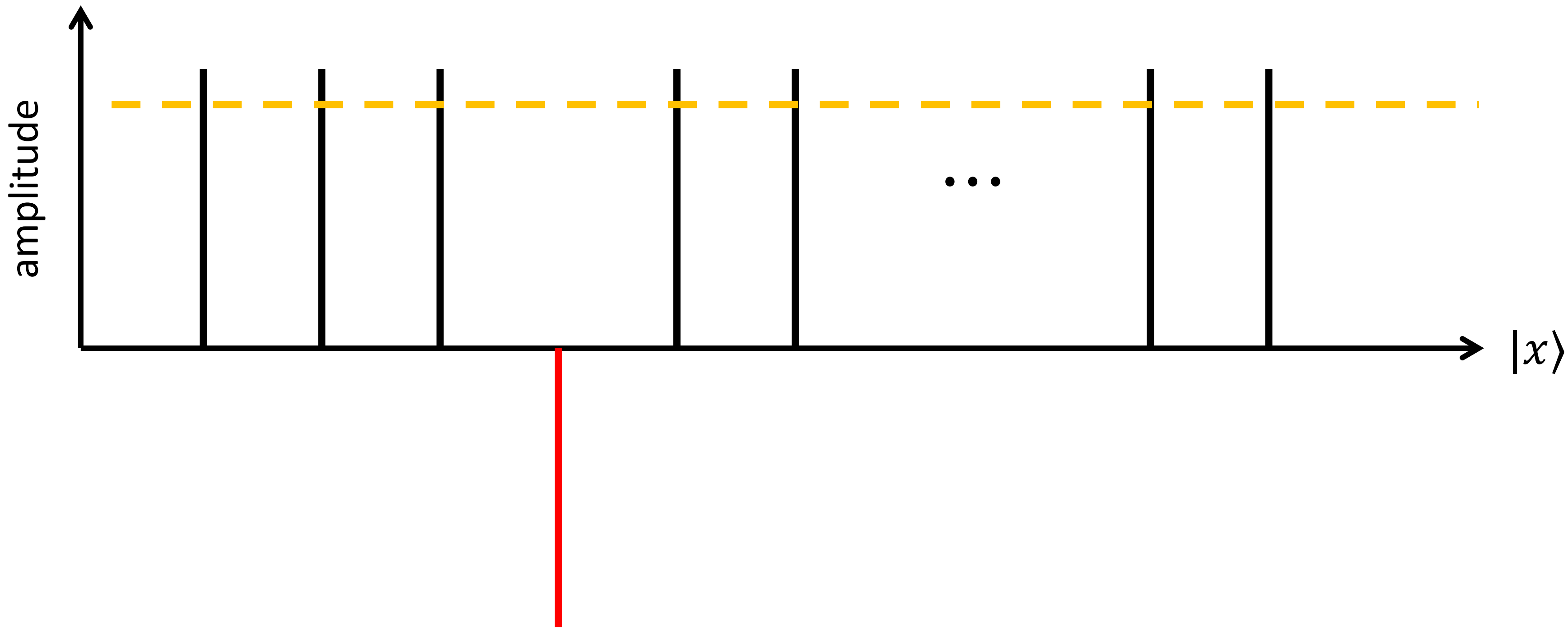
$$\frac{1}{\sqrt{N}}|x\rangle \to \frac{-1}{\sqrt{N}}|x\rangle.$$



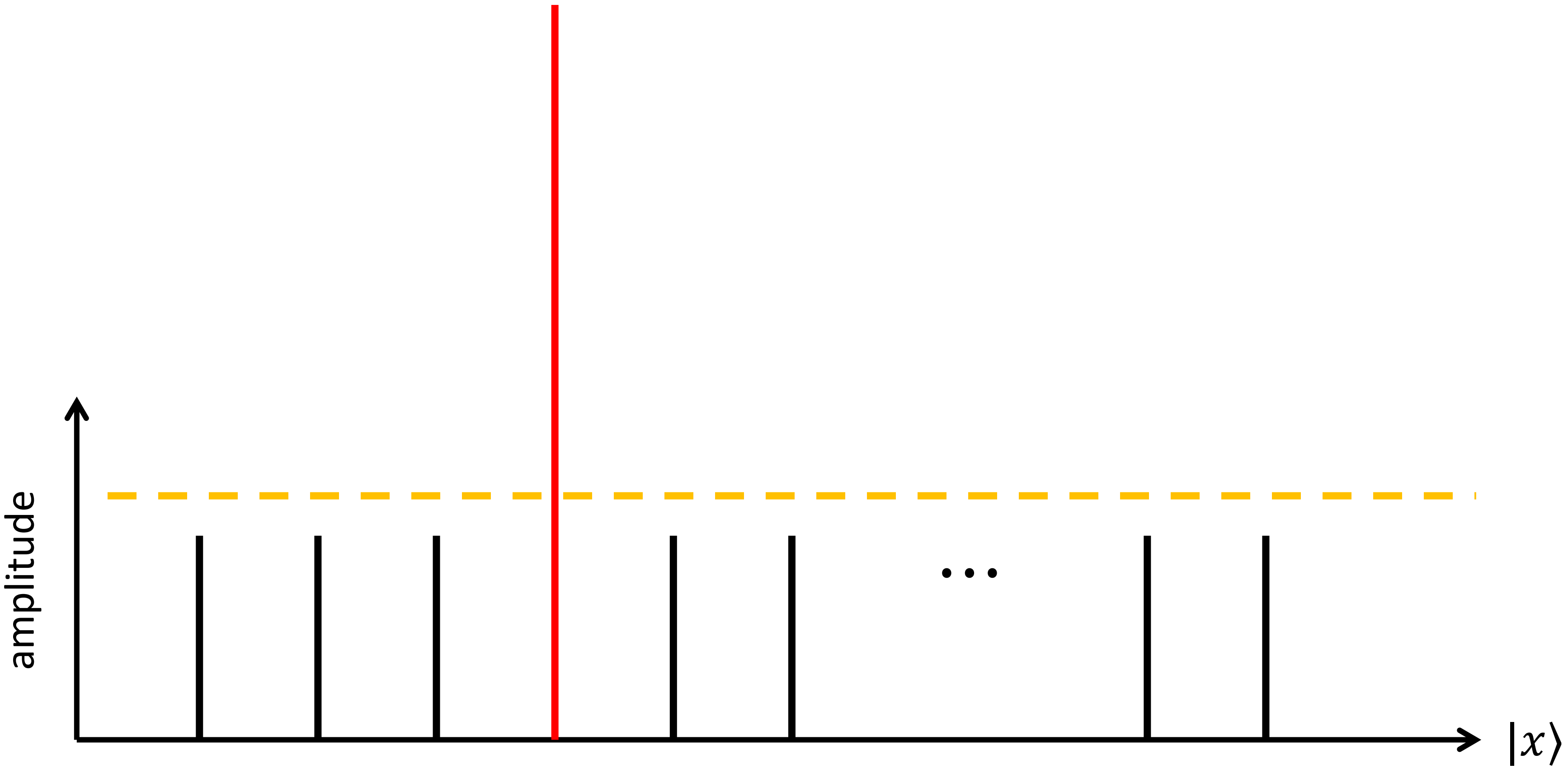
This step is called *phase inversion*.

Grover Iteration

The orange line is the average of all amplitudes.



Grover Iteration



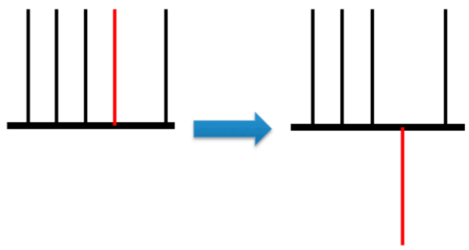
This step is called *inversion about mean*.

Grover Algorithm

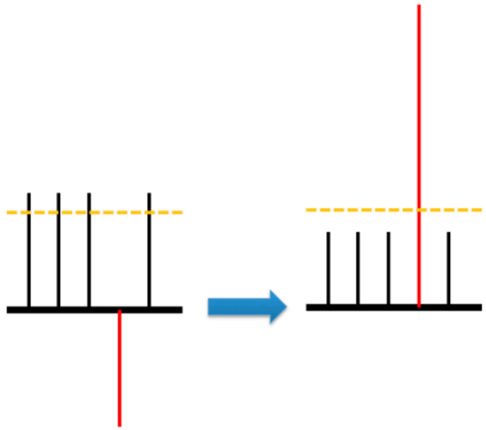
If we run $O(\sqrt{N})$ Grover iterations, the red line will goes close to 1.

One Grover iteration consists of two steps:

Phase inversion



Inversion about mean



Phase Inversion

Assume we have a classical function

$$f(x) = \begin{cases} 1, \text{if } x \text{ is the answer we want} \\ 0, \text{otherwise.} \end{cases}$$

Let U_f be a operator such that

$$U_f|x\rangle|q\rangle = |x\rangle|q \oplus f(x)\rangle,$$

which can be viewed as applying NOT gate on the desired state.

Magically, if we set $|q\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$, we have

$$U_f|x\rangle|q\rangle = |x\rangle\frac{|1\rangle - |0\rangle}{\sqrt{2}} = -|x\rangle|q\rangle,$$

which is the phase inversion we want.

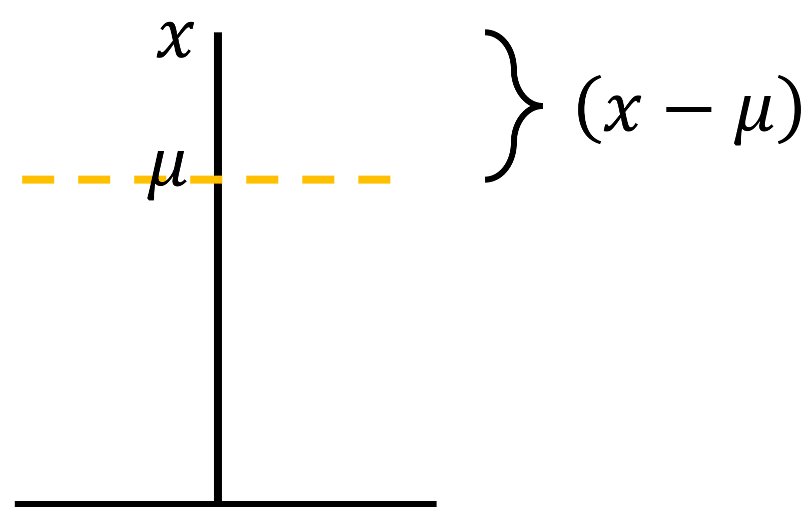
Inversion about Mean

Q: If μ is the average, how can we inverse x about μ?

A: Because $(x-\mu)$ is the difference between them,

$$\mu - (x-\mu) = 2\mu - x$$

attains our goal.



Inversion about Mean

To compute the average, we assign

$$A = \begin{bmatrix} \frac{1}{2^n} & \frac{1}{2^n} & \cdots & \frac{1}{2^n} \\ \frac{1}{2^n} & \frac{1}{2^n} & \cdots & \frac{1}{2^n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{2^n} & \frac{1}{2^n} & \cdots & \frac{1}{2^n} \end{bmatrix},$$

where it makes

$$A \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_{2^n} \end{bmatrix} = \begin{bmatrix} \mu \\ \mu \\ \vdots \\ \mu \end{bmatrix}.$$

Then $(2A - I)$ is the operator of inversion about mean.

Example

Example (Grover iteration)

First, we prepare a superposed state and the red one is the amplitude we want to enhance.

$$|\psi_1\rangle = \begin{bmatrix}\frac{1}{\sqrt{8}} & \frac{1}{\sqrt{8}} & \frac{1}{\sqrt{8}} & \frac{1}{\sqrt{8}} & \frac{1}{\sqrt{8}} & \frac{1}{\sqrt{8}} & \frac{1}{\sqrt{8}} & \frac{1}{\sqrt{8}}\end{bmatrix}.$$

Then, we inverse the amplitude of the target.

$$|\psi_2\rangle = \begin{bmatrix}\frac{1}{\sqrt{8}} & \frac{1}{\sqrt{8}} & \frac{1}{\sqrt{8}} & \frac{1}{\sqrt{8}} & \frac{1}{\sqrt{8}} & \frac{-1}{\sqrt{8}} & \frac{1}{\sqrt{8}} & \frac{1}{\sqrt{8}}\end{bmatrix}.$$

The average of these numbers is $\frac{7\cdot\frac{1}{\sqrt{8}}-\frac{1}{\sqrt{8}}}{8} = \frac{3}{4\sqrt{8}}$, so after inversion about mean, we have

$$|\psi_3\rangle = \begin{bmatrix}\frac{1}{2\sqrt{8}} & \frac{1}{2\sqrt{8}} & \frac{1}{2\sqrt{8}} & \frac{1}{2\sqrt{8}} & \frac{1}{2\sqrt{8}} & \frac{5}{2\sqrt{8}} & \frac{1}{2\sqrt{8}} & \frac{1}{2\sqrt{8}}\end{bmatrix}.$$

Example

Example (Grover iteration)

If we do another Grover iteration, we get

$$|\psi_4\rangle = \begin{bmatrix} \frac{-1}{4\sqrt{8}} & \frac{-1}{4\sqrt{8}} & \frac{-1}{4\sqrt{8}} & \frac{-1}{4\sqrt{8}} & \frac{-1}{4\sqrt{8}} & \frac{11}{4\sqrt{8}} & \frac{-1}{4\sqrt{8}} & \frac{-1}{4\sqrt{8}} \end{bmatrix}.$$

Note that $\frac{11}{4\sqrt{8}} = 0.97227$. The probability of getting right answer is

$$\left|\frac{11}{4\sqrt{8}}\right|^2 \approx 0.9453.$$

We can find the desired answer with probability 95% only using two iterations!

Grover Algorithm on Cryptography

If we have a plaintext-ciphertext pair (m, c), then we can design the "envelope" as

$$f(x) = \begin{cases} 1, c = Enc_x(m); \\ 0, \text{otherwise.} \end{cases}$$

Assume we want to break AES-128. About 2^{64} Grover iterations could find the correct key with high probability.

Outline

1. Introduction to quantum computing

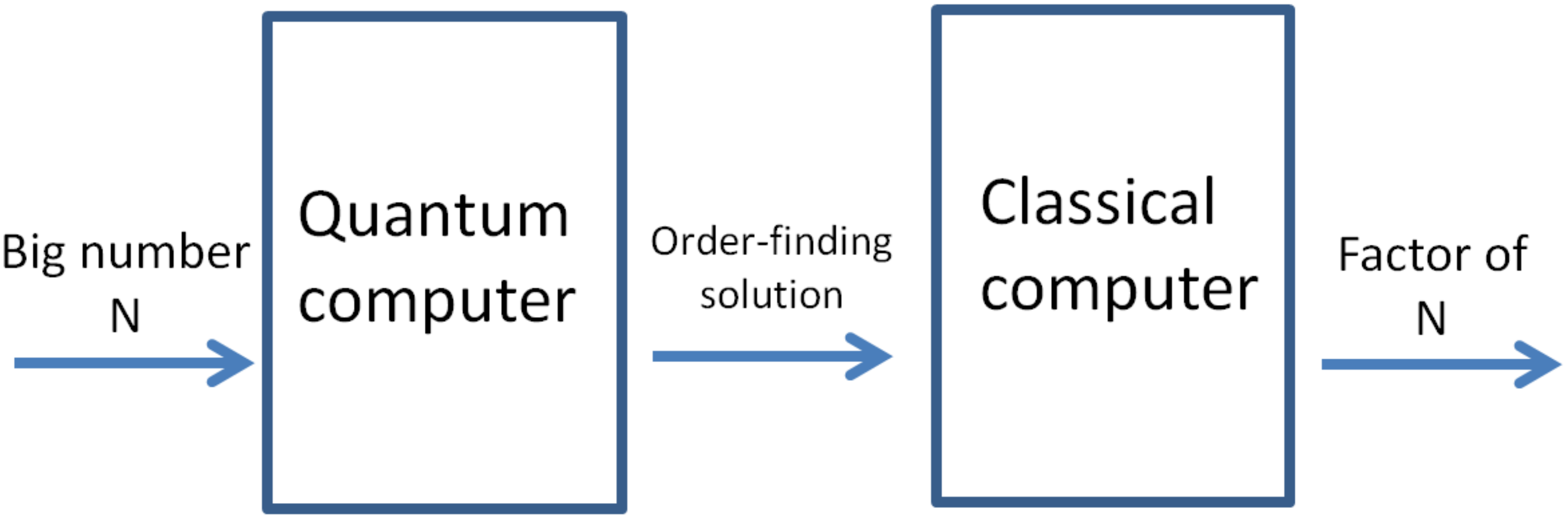
2. Grover Algorithm

3. Shor Algorithm

Shor Algorithm

Input: an odd composite number N

Output: a non-trivial factorization of N **with some probability**



Order-finding Problem

Given a and N, find the smallest positive integer r such that

$$a^r \equiv 1 \; mod \; N.$$

For example, if $a = 7, N = 15$:

7^0 mod 15 = 1

7^1 mod 15 = 7

7^2 mod 15 = 4

7^3 mod 15 =13

7^4 mod 15 = 1

so, the order r is 4.

Reduce Factoring to Order-finding Problem

If we have

$$a^r \equiv 1 \, (mod \; N),$$

then

$$N \mid a^r - 1.$$

If r is even, we have

$$N \mid (a^{r/2} - 1)(a^{r/2} + 1).$$

It cannot happen that $N \mid (a^{r/2} - 1)$, because this would mean that r was not the order of a. If $N \not| (a^{r/2} + 1)$, then $gcd(N, a^{r/2} + 1)$ is a non-trivial factor for N.

Theorem

If a is chosen randomly from Z_N^*, and r is the order of a, then

$$Pr[r \text{ is even} \wedge N \not| (a^{r/2} + 1)] \geq \frac{1}{2}.$$

Note that $f_{a,N}(x) = a^x \bmod N$ is a periodic function.

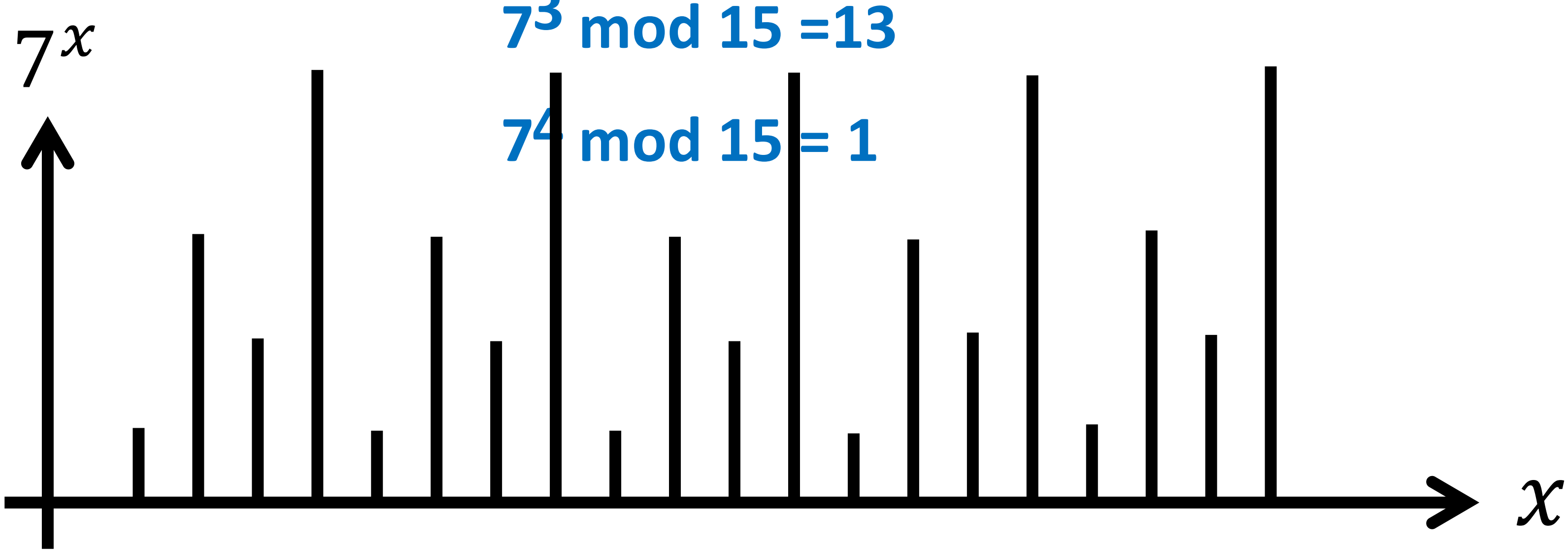
7^0 mod 15 = 1

7^1 mod 15 = 7

7^2 mod 15 = 4

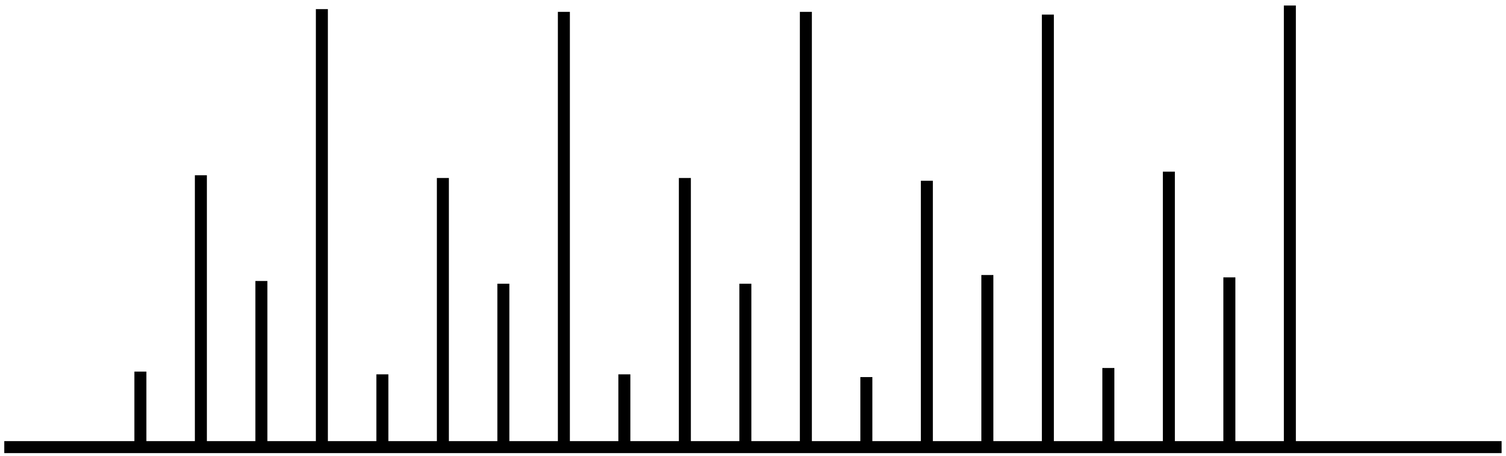
7^3 mod 15 =13

7^4 mod 15 = 1



Quantum Part

Note that $f_{a,N}(x) = a^x \bmod N$ is a periodic function.



We can find the period by quantum Fourier transform (QFT).

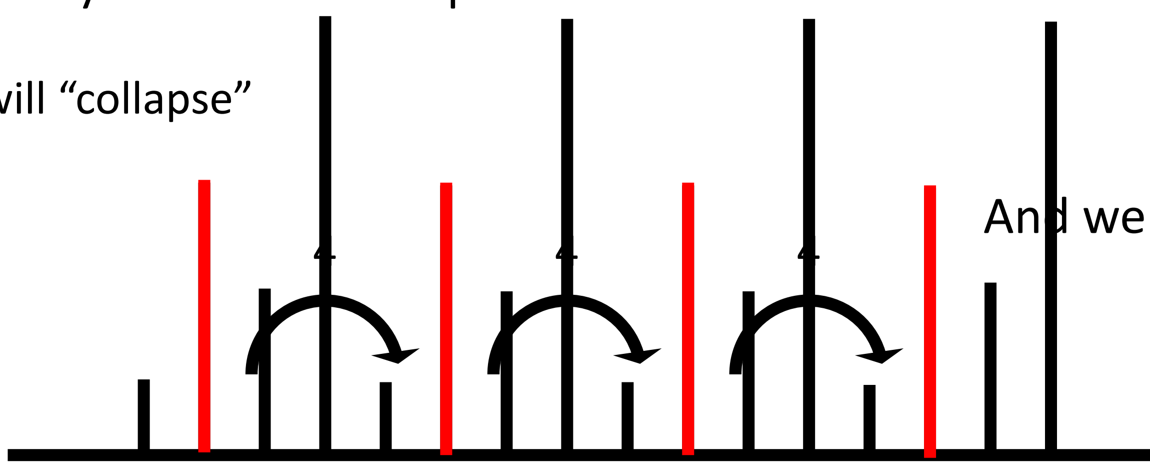
Quantum Circuit

After modular exponential, we have

$$
\begin{aligned}
&\frac{1}{4}(|0\rangle + |4\rangle + |8\rangle + |12\rangle)\,|1\rangle \\
+&\frac{1}{4}(|1\rangle + |5\rangle + |9\rangle + |13\rangle)\,|7\rangle \\
+&\frac{1}{4}(|2\rangle + |6\rangle + |10\rangle + |14\rangle)\,|4\rangle \\
+&\frac{1}{4}(|3\rangle + |7\rangle + |11\rangle + |15\rangle)\,|13\rangle
\end{aligned}
$$

If we measure the second register and get $|7\rangle$, then the first register will only remain the red part.

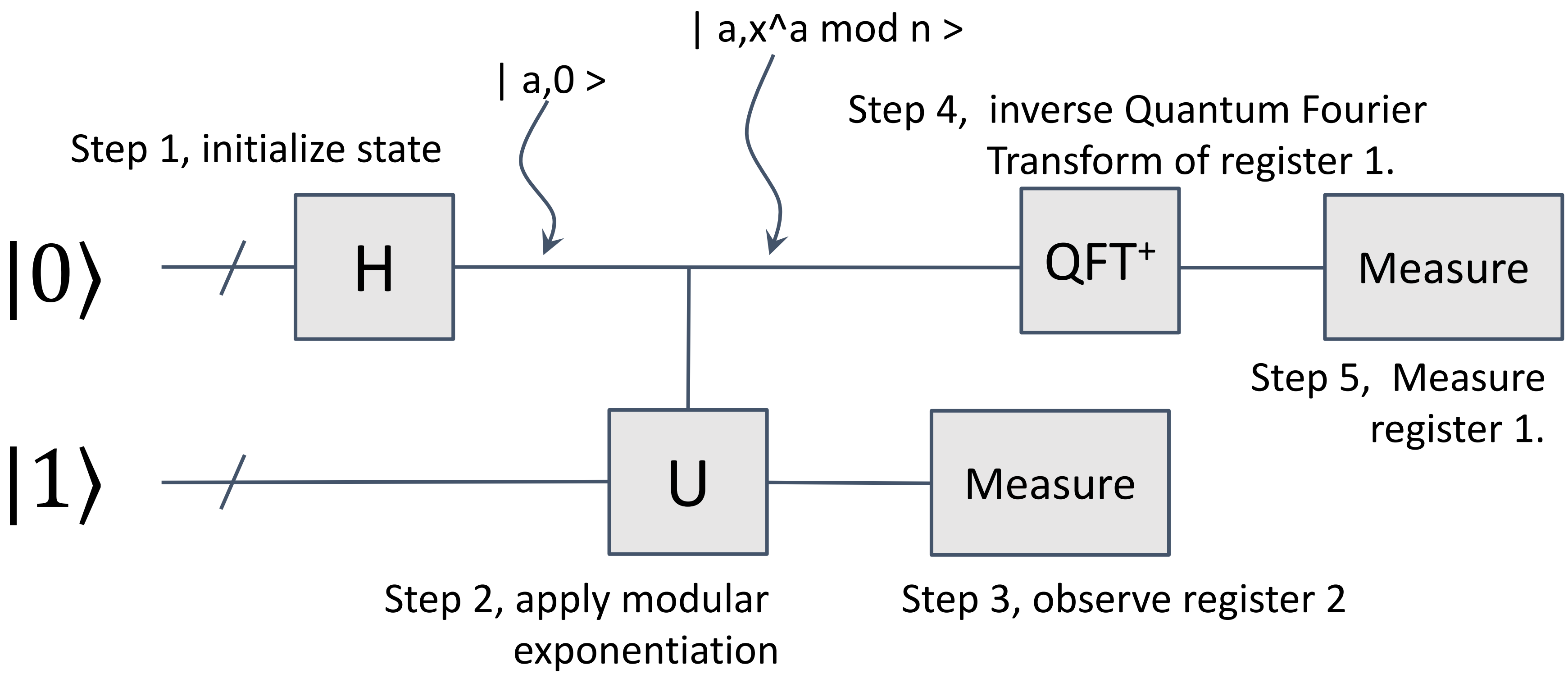
Other parts will "collapse"



And we find the period "4."

Show it in graph

Quantum Circuit



Time complexity

Assume we want to factor a n-bit number N:

- Modular exponential: $\Theta(n^3)$
- QFT: $\Theta(n^2)$
- Succeed probability: $\Omega(\frac{1}{\log n})$

Thus, the total time complexity is $O(n^3 \log n)$.

Example (RSA-2048)

To factor a 2048-bit number, we need roughly $2048^3 \cdot \log 2048 \sim 10^{11}$ operations. If we assume each operation takes 1 microsecond (μs) on a quantum computer, it takes only one day to factor the number.

Shor Algorithm on Elliptic Curves

Shor's discrete logarithm quantum algorithm for elliptic curves

John Proos and Christof Zalka

Department of Combinatorics and Optimization
University of Waterloo, Waterloo, Ontario
Canada N2L 3G1
e-mail: japroos@math.uwaterloo.ca zalka@iqc.ca

Shor algorithm

Phase Estimation → Order-Finding → Factoring

Phase Estimation

Given a unitary matrix U and a vector $|v\rangle$, find the phase of eigenvalue θ such that

$$U|v\rangle = e^{2\pi i\theta}|v\rangle.$$

Order-Finding

Given a and N, find the smallest positive integer r such that

$$a^r \equiv 1 \; mod \; N.$$

Factoring

Given a integer N, find a non-trivial factor of N.

Phase Estimation

Because unitary matrices preserve the length, so its eigenvalue must have the form of $e^{2\pi i\theta}$.

Definition (Phase Estimation)

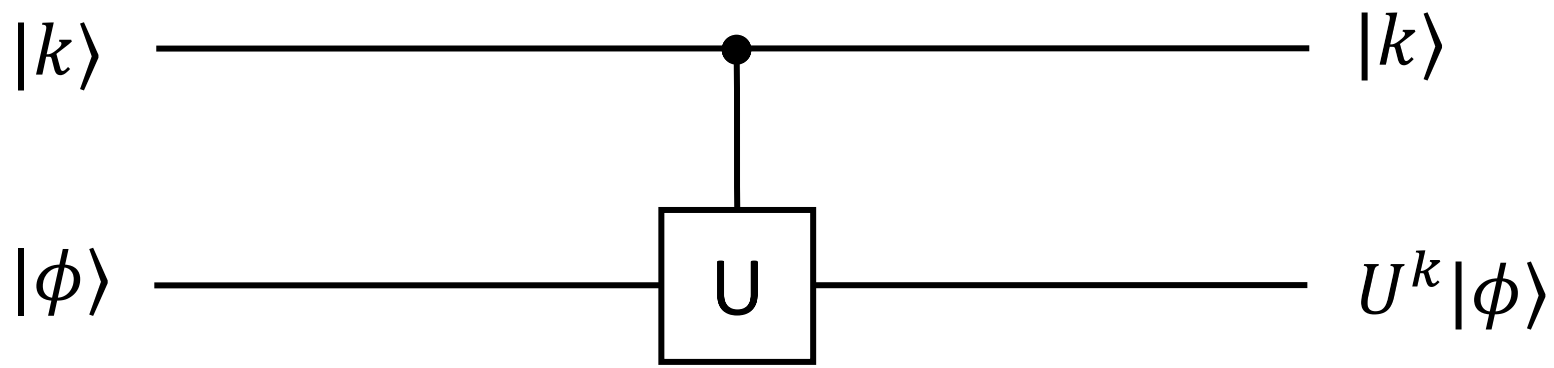
Given a unitary matrix U and its eigenvector $|v\rangle$, find the phase of eigenvalue $\theta \in [0,1)$ such that

$$U|v\rangle = e^{2\pi i\theta}|v\rangle.$$

Phase Estimation

Given a unitary operator U and an integer k. Let $|\phi\rangle$ be an eigenstate of U.

Consider the following circuit:

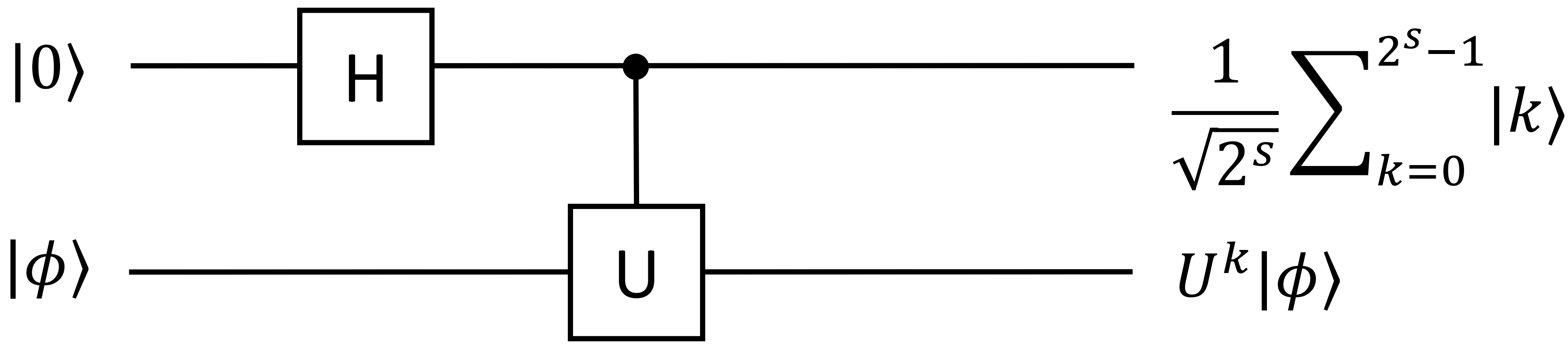


If U is a unitary matrix, we have

$$U^k|\phi\rangle = e^{2\pi i\theta k}|\phi\rangle.$$

Phase Estimation

If we make the first register in a superposed state:

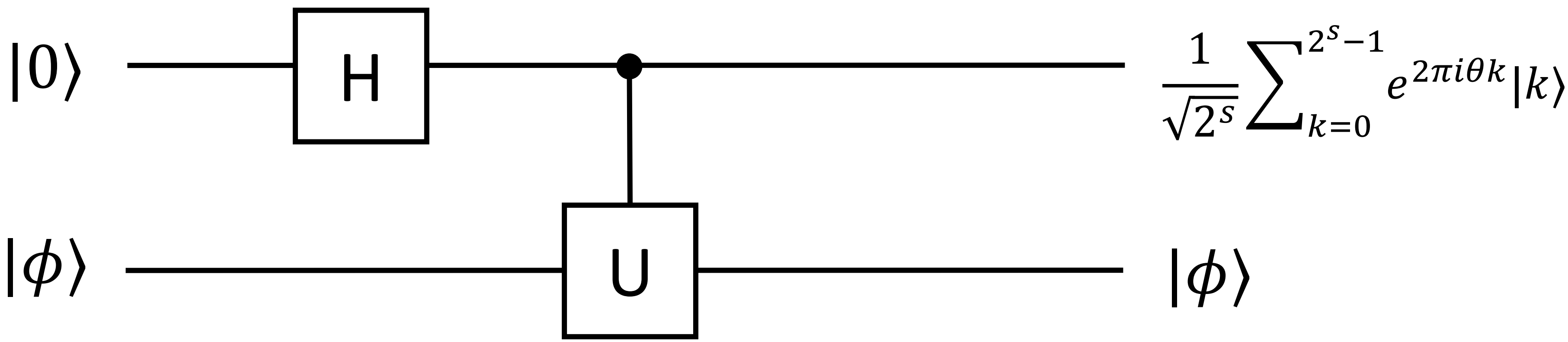


Because $U^k|\phi\rangle = e^{2\pi i\theta k}|\phi\rangle$, we have

$$\frac{1}{\sqrt{2^s}}\sum_{k=0}^{2^s-1}|k\rangle\left(e^{2\pi i\theta k}|\phi\rangle\right) = \frac{1}{\sqrt{2^s}}\sum_{k=0}^{2^s-1}e^{2\pi i\theta k}|k\rangle\,|\phi\rangle.$$

Phase Estimation

If we make the first register in a superposed state:



Because they are in the product state (1st and 2nd are independent), we can just focus on the first register.

We have

$$\frac{1}{\sqrt{2^s}}\sum_{k=0}^{2^s-1} e^{2\pi i\theta k}|k\rangle\,|\phi\rangle = \left(\frac{1}{\sqrt{2^s}}\sum_{k=0}^{2^s-1} e^{2\pi i\theta k}|k\rangle\right)\otimes|\phi\rangle.$$

Phase Estimation

Suppose θ happens to have a form of $\theta = \frac{j}{2^s}$, for some integer $j \in \{0, \dots, 2^s - 1\}$.

Then,

$$\frac{1}{\sqrt{2^s}} \sum_{k=0}^{2^s-1} e^{2\pi i j k / 2^s} |k\rangle = \frac{1}{\sqrt{2^s}} \sum_{k=0}^{2^s-1} \omega^{jk} |k\rangle = |\phi_j\rangle,$$

where $\omega = e^{2\pi i / 2^s}$.

It can be shown that $\{|\phi_0\rangle, \dots, |\phi_{2^s-1}\rangle\}$ forms an orthonormal basis.

That is,

$$\langle \phi_j | \phi_{j'} \rangle = \begin{cases} 1, \text{if } j = j'; \\ 0, \text{if } j \neq j'. \end{cases}$$

Phase Estimation

There is a unitary matrix F satisfies $F|j\rangle = |\phi_j\rangle$.

That is, the j^{th} column of F is $|\phi_j\rangle = \frac{1}{\sqrt{2^s}}\sum_{k=0}^{2^s-1}\omega^{jk}|k\rangle$.

Write it in the matrix form, we have

$$F = \frac{1}{\sqrt{2^s}}\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{2^s-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(2^s-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{2^s-1} & \omega^{2(2^s-1)} & \cdots & \omega^{(2^s-1)^2} \end{bmatrix},$$

which is exactly the discrete Fourier transform.

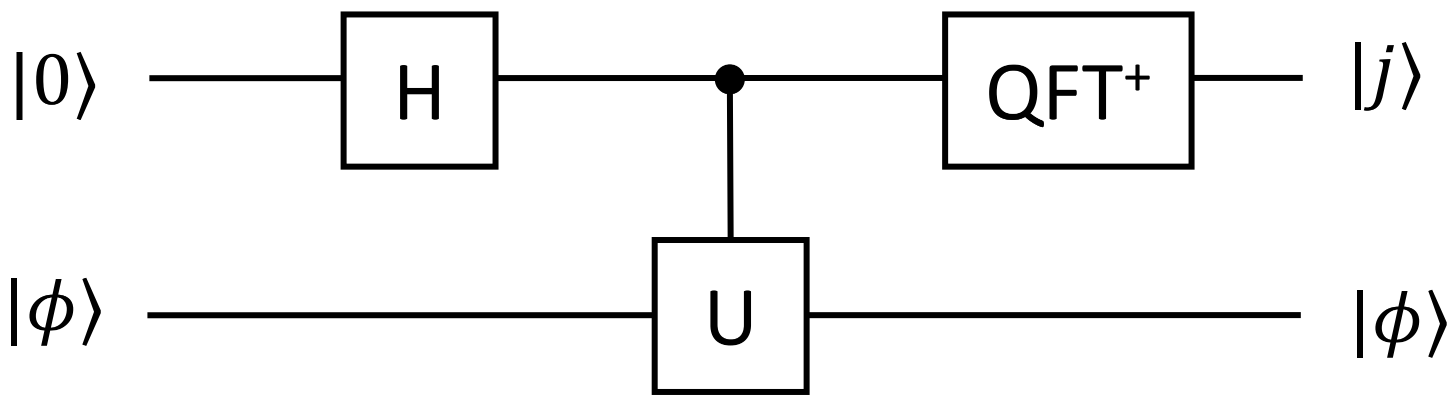
In quantum computing, we call it "quantum Fourier transform."

Phase Estimation

Thus, if we apply inverse quantum Fourier transform (F^{-1}) to the first register, we get $|j\rangle$.

If we measure it, we get j and $\theta = \frac{j}{2^s}$ is our desired phase estimation.

The whole circuit for phase estimation is



Phase Estimation

How about θ is not in the form of $\frac{j}{2^s}$?

It turns out that the state after QFT$^+$ is

$$\frac{1}{2^s}\sum_{k=0}^{2^s-1}\sum_{j=0}^{2^s-1} e^{2\pi i(k\theta-kj/2^s)}|j\rangle = \sum_{j=0}^{2^s-1}\left(\frac{1}{2^s}\sum_{k=0}^{2^s-1} e^{2\pi ik(\theta-j/2^s)}\right)|j\rangle.$$

The probability of measuring j is

$$p_j = \left|\frac{1}{2^s}\sum_{k=0}^{2^s-1} e^{2\pi ik\left(\theta-\frac{j}{2^s}\right)}\right|^2.$$

Reduce Order-Finding to Phase Estimation

To solve order-finding problem, we consider the following unitary operator

$$U_a|y\rangle = |ay \pmod N\rangle.$$

Let r be the order of a in $\mathbb{Z}_N^*$. Then the following vector is an eigenvector of U_a

$$|\psi_0\rangle = \frac{1}{\sqrt{r}}(|1\rangle + |a\rangle + |a^2\rangle + \cdots + |a^{r-1}\rangle),$$

because $U_a|\psi_0\rangle = \frac{1}{\sqrt{r}}(|a\rangle + |a^2\rangle + \cdots + |a^{r-1}\rangle + |a^r\rangle)$

$$= \frac{1}{\sqrt{r}}(|a\rangle + |a^2\rangle + \cdots + |a^{r-1}\rangle + |1\rangle)$$

$$= |\psi_0\rangle.$$

Reduce Order-Finding to Phase Estimation

Let $\omega_r = e^{2\pi i/r}$.

In general, the eigenvectors of U_a have the form of

$$|\psi_t\rangle = \frac{1}{\sqrt{r}}\left(|1\rangle + \omega_r^{-t}|a\rangle + \omega_r^{-2t}|a^2\rangle + \cdots + \omega_r^{-t(r-1)}|a^{r-1}\rangle\right),$$

since

$$U_a|\psi_t\rangle = \omega_r^t|\psi_t\rangle.$$

Then, phase estimation can help us find

$$\theta = \frac{t}{r}.$$

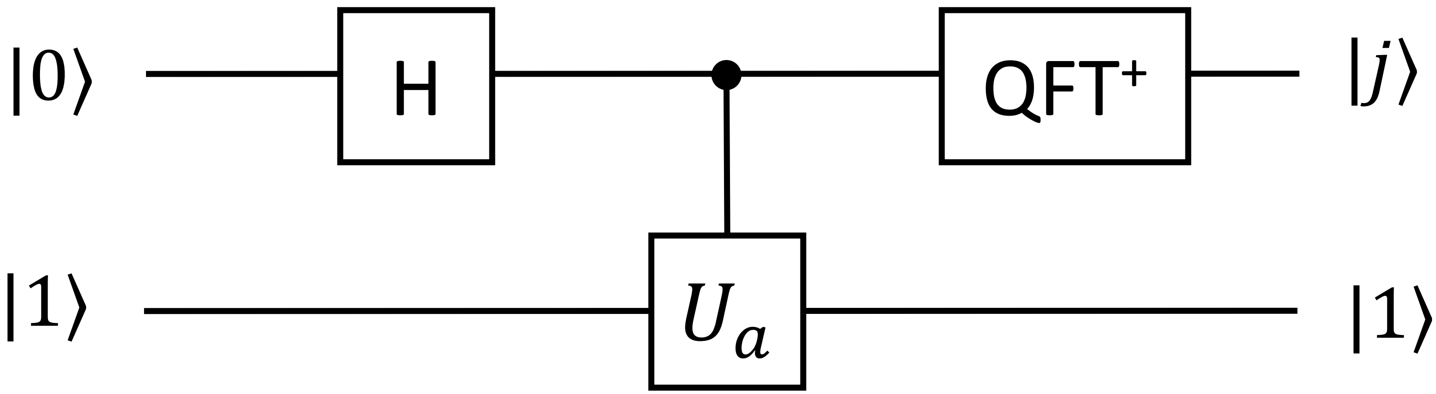
Reduce Order-Finding to Phase Estimation

$$|\psi_t\rangle = \frac{1}{\sqrt{r}}\left(|1\rangle + \omega_r^{-t}|a\rangle + \omega_r^{-2t}|a^2\rangle + \cdots + \omega_r^{-t(r-1)}|a^{r-1}\rangle\right)$$

How do we prepare $|\psi_t\rangle$ if we do not know r?

Fortunately, we have

$$\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}|\psi_t\rangle = \frac{1}{r}\sum_{k=0}^{r-1}\sum_{l=0}^{r-1}\omega_r^{-kl}|a^l\rangle = |a^0\rangle = |1\rangle.$$



Reduce Order-Finding to Phase Estimation

How do we find r if we only know

$$\frac{j}{2^s} \approx \frac{t}{r}?$$

We know We do not know

Fortunately, we can do it by continued fraction, because the following theorem.

Theorem

Suppose $\frac{t}{r}$ is a rational number such that $\left|\frac{j}{2^s} - \frac{t}{r}\right| \leq \frac{1}{2r^2}$. Then $\frac{t}{r}$ is a *convergent* of the continued fraction for $\frac{j}{2^s}$.

Continued Fraction

The continued fraction of a number s is

$$s = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\cdots + \cfrac{1}{a_N}}}}}.$$

In this case, we can express arbitrary number s as a sequence of positive integers $(a_0, a_1, \cdots, a_N)$.

Continued Fraction

Example (continued fraction of ${}^{31}/_{13}$)

First, we split $\frac{31}{13}$ into integer part and fraction part,

$$\frac{31}{13} = 2 + \frac{5}{13}.$$

Then, inverse the fraction part and get

$$\frac{31}{13} = 2 + \frac{1}{\frac{13}{5}} = 2 + \frac{1}{2 + \frac{3}{5}}.$$

Similarly,

$$\frac{31}{13} = 2 + \frac{1}{2 + \frac{1}{\frac{5}{3}}} = 2 + \frac{1}{2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2}}}}.$$

Thus, $(2,2,1,1,2)$ is the continued fraction expansion of $\frac{31}{13}$.

Continued Fraction

The i^{th} convergent of a continued fraction $(a_0, a_1, \cdots, a_N)$ is the number that $(a_0, a_1, \cdots, a_i)$ represents.

Let p_i denote the i^{th} convergent of $(a_0, a_1, \cdots, a_N)$.

Then,

$$p_0 = a_0.$$

$$p_1 = a_0 + \frac{1}{a_1}.$$

$$p_2 = a_0 + \frac{1}{a_1 + \frac{1}{a_2}}.$$

$$\vdots$$

Example

Example (Shor Algorithm for Factoring)

Assume we want to factor 15. We choose $a = 7$. The first step is to prepare a superposition state

$$|\psi_1\rangle = \frac{1}{4}\sum_{x=0}^{15}|x\rangle|0\rangle\,.$$

Next, we compute the modular exponential and get

$$\begin{aligned}|\psi_2\rangle &= \frac{1}{4}(|0\rangle|1\rangle + |1\rangle|7\rangle + \cdots + |15\rangle|13\rangle)\\ &= \frac{1}{4}\{(|0\rangle + |4\rangle + |8\rangle + |12\rangle)|1\rangle\\ &\quad +(|1\rangle + |5\rangle + |9\rangle + |13\rangle)|7\rangle\\ &\quad +(|2\rangle + |6\rangle + |10\rangle + |14\rangle)|4\rangle\\ &\quad +(|3\rangle + |7\rangle + |11\rangle + |15\rangle)|13\rangle\}.\end{aligned}$$

Example

Example (Shor Algorithm for Factoring)

The quantum Fourier transform yields

$$
\begin{aligned}
\frac{1}{4}\{&(|0\rangle + |4\rangle + |8\rangle + |12\rangle)|1\rangle \\
&+(|0\rangle + i|4\rangle - |8\rangle - i|12\rangle)|7\rangle \\
&+(|0\rangle - |4\rangle + |8\rangle - |12\rangle)|4\rangle \\
&+(|0\rangle - i|4\rangle - |8\rangle + i|12\rangle)|13\rangle\}
\end{aligned}
$$

If we measure the first register, we can get $0,4,8$ or 12 with the same probability.

If the measurement result is 4 or 12, we can get the correct order by condinued fraction.

How many qubits do we need?

Theorem

Suppose $\frac{t}{r}$ is a rational number such that $\left|\frac{j}{2^s} - \frac{t}{r}\right| \leq \frac{1}{2r^2}$. Then $\frac{t}{r}$ is a convergent of the continued fraction for $\frac{j}{2^s}$.

Note that we do not know r in advance.

However, r must be smaller than N, the integer we want to factor. So

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

If $\frac{j}{2^s}$ can accurate to $\log 2N^2$ bits, the theorem applies.

How many qubits do we need?

Assume we want to factor a n-bit number N.

The 1st register need $\log 2N^2 = 2n + 1$ qubits.

The 2nd register needs to compute $a^x \bmod N$, so it needs n qubits to save a^x.

Because the 1st register needs $2n$ qubits and the 2nd register needs n qubits, **we need $3n$ qubits in total.**

Summary

Assume we want to factor a n-bit number N.

Time Complexity	$O(n^3 log\, n)$
Number of qubits	$3n$

Suggested Reading

- Quantum Computing: John Watrous' Lecture Notes
- Shor and Grover Algorithm: John Watrous' Lecture Notes

- Suggested reading for quantum key distribution (QKD):
  1. 我的科普文章

     (https://medium.com/@chunghaoblog/qkd-c6b82a9b04e0)
  2. 科普影片 (https://youtu.be/6H_9l9N3IXU)
  3. 量子計算：Thomas Vidick's lecture note