Quantum Attack on Cryptography
Shor's and Grover's Algorithm

Hao Chung

National Taiwan University

r05921076@ntu.edu.tw

August 15, 2017

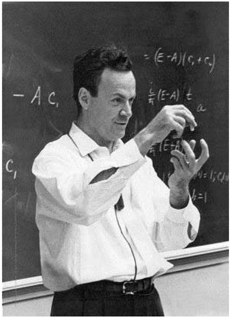
Overview

Outline

1. Introduction to Quantum Computing
2. Shor's Algorithm
3. Grover Search Algorithm
4. Recent Progress on Quantum Computer

The beginning of quantum computing

- Simulating physics with computers
  - In 1982, Feynman proposed the idea of creating machines based on the laws of quantum mechanics instead of the laws of classical physics
- Why quantum can do better than classical?
  - Superposition
  - Entanglement



Quantum State

In quantum computing, we use Dirac notation "$|\cdot\rangle$" to represent a state. For example, a state of a coin could be

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

Quantum State

In quantum computing, we use Dirac notation "$|\cdot\rangle$" to represent a state. For example, a state of a coin could be

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

Or, a state of a die could be

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

Quantum State

In quantum computing, we use Dirac notation "$|\cdot\rangle$" to represent a state. For example, a state of a coin could be

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

Or, a state of a die could be

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

If you are the Shrodingers cat, then

$$|\text{Alive Cat}\rangle \text{ and } |\text{Dead Cat}\rangle .$$

Quantum State

In quantum computing, we use Dirac notation "$|\cdot\rangle$" to represent a state. For example, a state of a coin could be

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

Or, a state of a die could be

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

If you are the Shrodingers cat, then

$$|\text{Alive Cat}\rangle \text{ and } |\text{Dead Cat}\rangle .$$

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

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

Superposition

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

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:

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

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 0 with probability $|\alpha|^2$ and get 1 with probability $|\beta|^2$.

Since the sum of the probability must be one,

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

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 0 with probability $|\alpha|^2$ and get 1 with probability $|\beta|^2$.

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?

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 0 with probability $|\alpha|^2$ and get 1 with probability $|\beta|^2$.

Since the sum of the probability must be one,

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

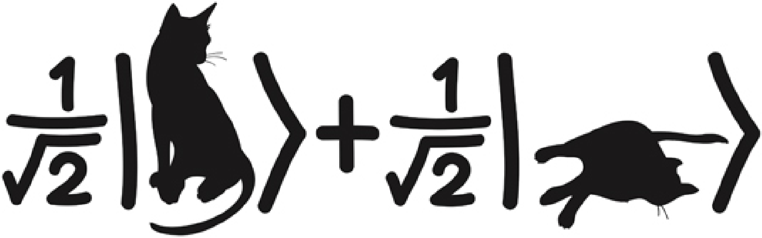
Example (Fair Quantum Die)

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

Answer:

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

Superposition



Composite System

What happens if we have two qubits?

Composite System

What happens if we have two qubits?
Assume we have a two qubits system:

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

By distributive law, we have

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

Composite System

What happens if we have two qubits?
Assume we have a two qubits system:

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

By distributive law, we have

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

For convenience, we write the state as

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

Composite System

What happens if we have two qubits?
Assume we have a two qubits system:

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

By distributive law, we have

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

For convenience, we write the state as

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

Of course, the sum of probability should be one ☺:

$$|\alpha_1\alpha_2|^2 + |\alpha_1\beta_2|^2 + |\beta_1\alpha_2|^2 + |\beta_1\beta_2|^2 = 1.$$

Composite System

What happens if we measure the first qubit?

Composite System

What happens if we measure the first qubit?
For the state

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

the probability of getting 0 at first qubit is $|\alpha_1\alpha_2|^2 + |\alpha_1\beta_2|^2 = |\alpha_1|^2$, which is the same as we only focus on the first qubit.

Composite System

What happens if we measure the first qubit?
For the state

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

the probability of getting 0 at first qubit is $|\alpha_1\alpha_2|^2 + |\alpha_1\beta_2|^2 = |\alpha_1|^2$, which is the same as we only focus on the first qubit.
After measurement, the residue state is

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

where $\sqrt{|\alpha_1\alpha_2|^2 + |\alpha_1\beta_2|^2} = \alpha_1$ is the normalized factor.

Entanglement

For the state

$$\frac{1}{\sqrt{2}}|00\rangle + 0|01\rangle + 0|10\rangle + \frac{1}{\sqrt{2}}|11\rangle,$$

can we write it as a product state with some coefficients

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

Entanglement

For the state

$$\frac{1}{\sqrt{2}}|00\rangle + 0|01\rangle + 0|10\rangle + \frac{1}{\sqrt{2}}|11\rangle,$$

can we write it as a product state with some coefficients

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

NO! It means that 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 on $\mathbb{C}$.

For a single qubit, we write $|0\rangle = \binom{1}{0}, |1\rangle = \binom{0}{1}$. In general,

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

Example (EPR pair)

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

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} = \begin{array}{cl} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} & \begin{array}{l} 00 \\ 01 \\ 10 \\ 11 \end{array} \end{array}.$$

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

- An operator U in vector space V 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,

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

X gate is the NOT gate in quantum computing.

Quantum Parallel

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

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

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

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

The problem is we only can find out one of the result from measurement.

- The Nature knows all the result but only tells us one!

Quantum Parallel

Example (Modular Exponential)

Let $f_{a,N}(x) = a^x \mathit{mod}\, N$, and U_f is an unitary operator corresponding to $f_{a,N}$.
Now we have $a = 7, N = 15$ and $|\psi\rangle = \frac{1}{2}(|0\rangle + |1\rangle + |2\rangle + |3\rangle)$.
Then,
$U_f(|\psi\rangle |0\rangle) = \frac{1}{2}(|0\rangle |1\rangle + |1\rangle |7\rangle + |2\rangle |4\rangle + |3\rangle |13\rangle)$.

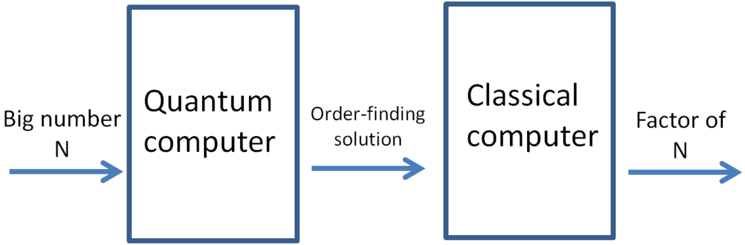
The example shows that we somehow can compute $7^0, 7^1, 7^2, 7^3\ (\mathit{mod}\, 15)$ simultaneously. The problem is "how we extract the answer?"

In the following slides, we will see that how different quantum algorithms deal with this problem.

Outline

Shor's algorithm has two parts:

- Classical part: reduce factoring to order-finding problem
- Quantum part: order-finding problem



Order-finding Problem

Order-finding problem

For $a \in \mathbb{Z}_N^*$, the order of a in $\mathbb{Z}_N^*$ (or the order of a modulo N) is the smallest positive integer r such that

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

The order-finding problem is given a positive integer $N \geq 2$ and an element $a \in Z_N^*$, try to find the order of a in Z_N^*.

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

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

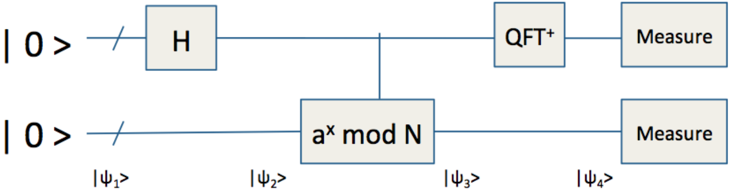
It cannot happen that $N \mid (a^{r/2} - 1)$, because this would mean that r was not the order of a. If $N \nmid (a^{r/2} + 1)$, then $gcd(N, a^{r/2} + 1)$ is a non-trivial factor for N.

Theorem

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

$$Pr[r \text{ is even} \wedge N \nmid (a^{r/2} + 1)] \geq \frac{1}{2}.$$

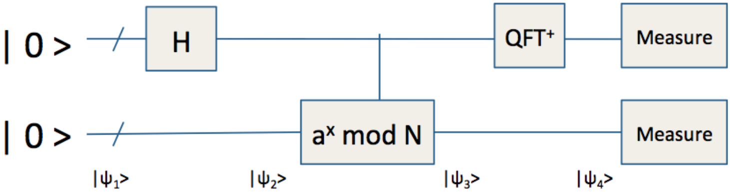
Order-finding Problem



$$|\psi_1\rangle = |0\rangle\,|0\rangle$$
$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle\,|0\rangle$$
$$|\psi_3\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle\,|a^x \text{mod N}\rangle$$
$$|\psi_4\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} QFT^\dagger(|x\rangle)\,|a^x \text{mod N}\rangle$$

- $QFT^\dagger(|x\rangle) = \sum_{t=0}^{N} e^{ixt/N}\,|t\rangle$

Order-finding Problem



When measuring the second register and get some value "u", the first register will collapse to the pre-image of u, i.e. $\{i \,|\, f(i) = u\}$. Since modular exponential is a periodic function, where the period is the order of a.

We can find the period by Fourier transform.

Remark: the probability that the circuit output an even order of a is $\Omega(\frac{1}{\log \log N})$.

Example

Example

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

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

Next, compute the modular exponential and yield

$$|\psi'\rangle = \tfrac{1}{4}(|0\rangle\,|1\rangle + |1\rangle\,|7\rangle + \ldots + |15\rangle\,|13\rangle)$$
$$= \tfrac{1}{4}\Big((|0\rangle + |4\rangle + |8\rangle + |12\rangle)\,|1\rangle$$
$$+(|1\rangle + |5\rangle + |9\rangle + |13\rangle)\,|7\rangle$$
$$+(|2\rangle + |6\rangle + |10\rangle + |14\rangle)\,|4\rangle$$
$$+(|3\rangle + |7\rangle + |11\rangle + |15\rangle)\,|13\rangle\Big)$$

Example

Example (con'd)

The quantum Fourier transform yields

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

When measuring the first register, we can get the even order with probability $\Omega(\frac{1}{\log\log 15})$.

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

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 on a quantum computer, it takes only one day to factor the number.

Outline

Motivation of Grover Search Algorithm

Envelope Problem: 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?

Motivation of Grover Search Algorithm

Envelope Problem: 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:

Motivation of Grover Search Algorithm

Envelope Problem: 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.

Motivation of Grover Search Algorithm

Envelope Problem: 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:

Motivation of Grover Search Algorithm

Envelope Problem: 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.

Motivation of Grover Search Algorithm

Envelope Problem: 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.
- Even you allow the probability of failure P_f (a constant), you still need to try $O(N)$ times.

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

Grover Algorithm

One important design technique for quantum algorithm is preparing a superposed state that exploits quantum parallelism and try to maximize the amplitude of the right answer.

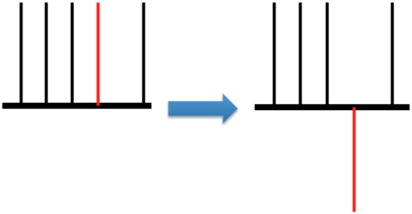
Grover algorithm is a beautiful example for demonstrating this technique. One Grover iteration consists of two steps:

1. Phase inversion
2. Inversion about mean

After many iterations, we can get the result with high probability.

Phase inversion

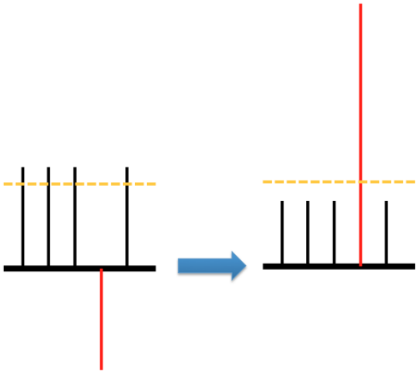
- First, we prepare a superposed state $|\psi\rangle = \sum_{x=0}^{N} \frac{1}{\sqrt{N}} |x\rangle$
- Assume the red one is the right answer we want to obverse
- Second, we inverse the amplitude of the right answer, i.e. $\frac{1}{\sqrt{N}} |x\rangle \to -\frac{1}{\sqrt{N}} |x\rangle$



Grover Algorithm Overview

Inversion about mean

- Orange dotted line represents the average of all the amplitude
- Since the red one has negative amplitude, the average will slightly lower than most amplitude.
- If we inverse each amplitude about the mean, the amplitude of the right answer will grow about three times high.



Phase Inversion

Assume we have a classical boolean function $f(x)$ such that

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

Phase Inversion

Assume we have a classical boolean function $f(x)$ such that

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

Let U_f be an unitary 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 would 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: $(x-\mu)$ is the difference between them. $\mu-(x-\mu)=2\mu-x$ attains our goal.

Thus, in vector representation, inversion about mean can be done by

$$(2A-I)\left|x\right\rangle, \text{ where } A=\begin{pmatrix} \frac{1}{2^n} & \frac{1}{2^n} & \cdots & \frac{1}{2^n} \\ \frac{1}{2^n} & \frac{1}{2^n} & \cdots & \frac{1}{2^n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{2^n} & \frac{1}{2^n} & \cdots & \frac{1}{2^n} \end{pmatrix}.$$

Remark: It can be showed that $(2A-I)$ is an unitary operator:
Since $(2A-I)$ is a real symmetric matrix, $(2A-I)=(2A-I)^\dagger$.

$$(2A-I)(2A-I)=4A^2-4A+I=4A-4A+I=I$$

Example

Example (Grover iteration)

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

$$|\psi_1\rangle = [\frac{1}{\sqrt{8}}, \frac{1}{\sqrt{8}}, \frac{1}{\sqrt{8}}, \frac{1}{\sqrt{8}}, \frac{1}{\sqrt{8}}, \frac{1}{\sqrt{8}}, \frac{1}{\sqrt{8}}, \frac{1}{\sqrt{8}}]$$

Then, we inverse the amplitude of the target.

$$|\psi_2\rangle = [\frac{1}{\sqrt{8}}, \frac{1}{\sqrt{8}}, \frac{1}{\sqrt{8}}, \frac{1}{\sqrt{8}}, \frac{1}{\sqrt{8}}, \frac{-1}{\sqrt{8}}, \frac{1}{\sqrt{8}}, \frac{1}{\sqrt{8}}]$$

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

$$|\psi_3\rangle = [\frac{1}{2\sqrt{8}}, \frac{1}{2\sqrt{8}}, \frac{1}{2\sqrt{8}}, \frac{1}{2\sqrt{8}}, \frac{1}{2\sqrt{8}}, \frac{5}{2\sqrt{8}}, \frac{1}{2\sqrt{8}}, \frac{1}{2\sqrt{8}}]$$

Example (con'd)

If we do another Grover iteration, we get

$$|\psi_4\rangle = [\frac{-1}{4\sqrt{8}}, \frac{-1}{4\sqrt{8}}, \frac{-1}{4\sqrt{8}}, \frac{-1}{4\sqrt{8}}, \frac{-1}{4\sqrt{8}}, \frac{-1}{4\sqrt{8}}, \frac{11}{4\sqrt{8}}, \frac{-1}{4\sqrt{8}}, \frac{-1}{4\sqrt{8}}]$$

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

$$|\frac{11}{4\sqrt{8}}|^2 = 0.9453.$$

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

It can be showed that operating Grover iteration $O(\sqrt{N})$ times can attends the maximum probability to get the right answer.

Note that $f(x)$ could be "any" boolean function that can be implemented in quantum circuit. Thus, if you have plaintext-ciphertext pair, Grover algorithm could leads to quadratic speed up.

Example (AES-128)

Assume we want to break AES-128.
If we have a plaintext-ciphertext pair (m, c), then we can have a function $f(x)$ such that output 1 when $c = Enc_x(m)$. About 2^{64} Grover iterations could find the correct key with high probability.

Outline

Universal Set

A set of unitary operators is called universal set if all the unitary operator can be made up of the members of the set.

Theorem (Universal Set)

$\{X, Z, H, T, CNOT\}$ *forms an universal set.*

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{pmatrix}, CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

51-qubit vs 2000-qubit?

IBM Just Made a 17 Qubit Quantum Processor, Its Most Powerful One Yet

MEREDITH RUTLAND BAUER
May 17 2017, 10:13pm

51-qubit vs 2000-qubit?

IBM Just Made a 17 Qubit Quantum Processor, Its Most Powerful One Yet

MEREDITH RUTLAND BAUER
May 17 2017, 10:13pm

TECHNOLOGY

First 51-Qubit Quantum Computer Using Cold Atoms Announced In Moscow

BY **HIMANSHU GOENKA** ON 07/21/17 AT 6:17 AM

51-qubit vs 2000-qubit?

IBM Just Made a 17 Qubit Quantum Processor, Its Most Powerful One Yet

MEREDITH RUTLAND BAUER
May 17 2017, 10:13pm

TECHNOLOGY

First 51-Qubit Quantum Computer Using Cold Atoms Announced In Moscow

BY HIMANSHU GOENKA ON 07/21/17 AT 6:17 AM

SEP 27, 2016

D-Wave Systems Previews 2000-Qubit Quantum System

Comparison between Different Implementation