Introduction to Quantum Computing

Yuxiang Peng

Institute for Interdisciplinary Information Science
Tsinghua University

January 25, 2019

Contents

UTR#3: Quantum Break

- It provides you with a lot of arrays a with a length of 2^n.
- For each a, there are only two non-zero entry x, y. (with the same value)
- We know that $x \oplus y$ is a constant. The task is to find it out.
- Each time the worker works on one particular array.
- Several interactive functions:
- 1. query(): Randomly return a label v with probability $\frac{a[v]^2}{\sum_i a[i]^2}$. Then this array is disposed, and the worker turns to another array.
- 2. manipulate(A, i): For each k such that the i-th bit is 0, act a linear mapping A to $a[k], a[k+2^i]$.
- (The problem is slightly modified.)

Training Team Problemset: Unnamable

- You need to find out a complex number x whose norm is 1.
- You are provided with an array with a length of 2^n. Initially, the only non-zero term is a_0.
- Several interactive functions:
- 1. CU(d, k): For each i such that the d-th bit is 1, multiply a phase x^k to $a[i]$.
- 2. CR(d_1, d_2, A): For each i such that the d_1-th bit and d_2-th bit is 1, act a linear mapping A to $a[i-2^{d_2}]$, $a[i]$.
- 3. QR(): Randomly return a label v with probability $\frac{|a[v]|^2}{\sum_i |a[i]|^2}$.
- (The problem is slightly modified.)

One Small Step for Classical Bit

One giant leap for information

- A classical bit: 0, 1
- Discrete representation.
- Usually be realized by voltage difference.

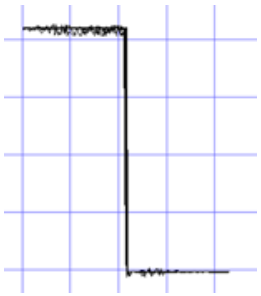

Figure: Voltage changes from 5V to 0V

- What if there are intermediate states?
- Are there such examples?

Insights from Optics

Polarization of light beam

- Physicists tell us light beams have different polarization angles.

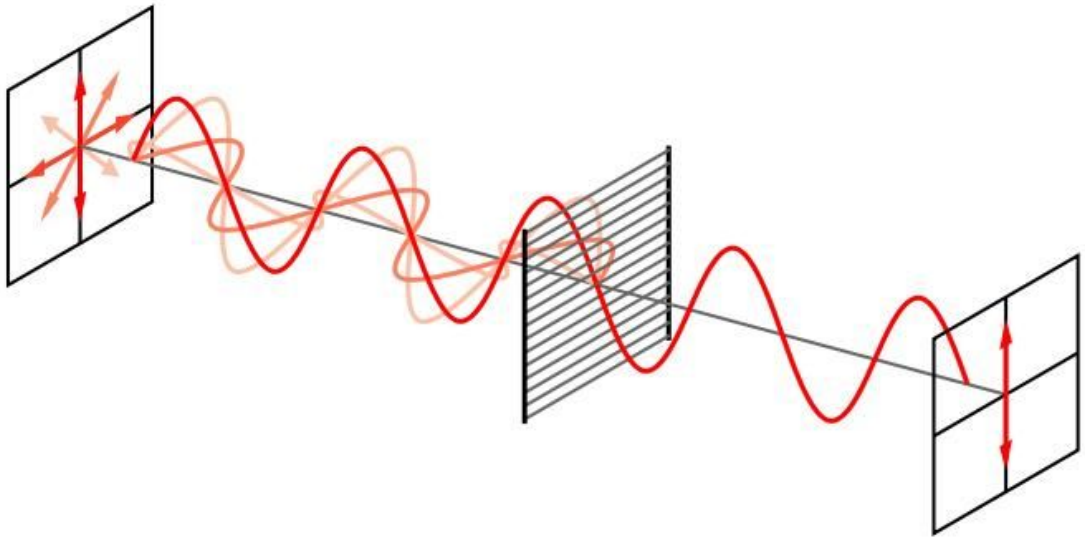

Figure: Polarizations of light and the effect of polaroid

- It is easy to understand in wave form.

Insights from Optics

Polarization of light beam

- For a light beam polarized in 45 degrees to horizontal direction.

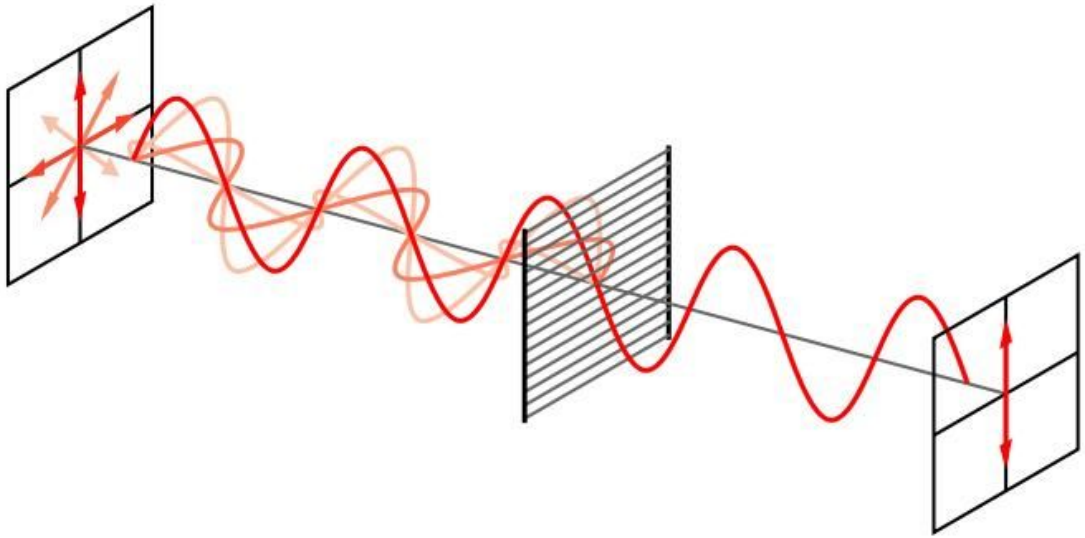

Figure: Polarizations of light and the effect of polaroid

- Passing through a horizontal polaroid leads to half the energy.
- The polarization angle turns to horizontal.
- It is easy to understand because of wave decomposition.

Insights from Optics

Wave-particle duality

- A quantum view.
- Physicists tell us the unity of wave and particle.
- So is the light:
  Wave form: light wave.
  Particle form: photon.
- What is polarizations in photon form?

Insights from Optics

View of photons

- The 45° polarized light contains only one kind of photons.
- These photons should be in an intermediate state.
- Half energy: for single photon, it has 50% chance to pass through the polaroid.
- And the polarization angle changes to horizontal.

Qubit: Quantum Bit

Introduction

- Notation 'ket':
$$|0\rangle, |1\rangle.$$
- In linear algebra:
$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$
- We use them to represent the horizontal and vertical directions.
- The 45° polarized photon:
$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle).$$
- Passing through a horizontal polaroid: it has $|\frac{1}{\sqrt{2}}|^2 = 50\%$ to act like $|1\rangle$.

Qubit: Quantum Bit

Formalization

- n dimensional Hilber space: $\mathcal{H}_n$.
- Computation basis:

$$(\{|0\rangle, |1\rangle, \ldots, |n-1\rangle\}),$$

with

$$|j\rangle = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix},$$

whose j-th entry is 1.

Qubit: Quantum Bit

Formalization

- Notation 'bra':

$$\langle\varphi| = |\varphi\rangle^\dagger,$$

  where † means the conjugated transpose.

- Inner product of $|\varphi\rangle$ and $|\psi\rangle$:

$$\langle\psi|\varphi\rangle.$$

Qubit: Quantum Bit

Pure states

- A pure state $|\varphi\rangle$ satisfies:

$$\begin{aligned} \||\varphi\rangle\| &= \sqrt{\langle\varphi|\varphi\rangle} = 1, \\ |\varphi\rangle &\in \text{span}(|0\rangle, |1\rangle, \ldots, |n-1\rangle). \end{aligned}$$

- Notice that, if coefficients are multiplied by $e^{i\theta}$, the behaviors of quantum states are the same.
- Hence we could ignore the global phase.
- Pure state remains pure under linear operations:

$$|\varphi\rangle = a_1|\psi_1\rangle + a_2|\psi_2\rangle + \cdots + a_k|\psi_k\rangle.$$

- This is the superposition of quantum states.

Mutually unbiased basis in $\mathcal{H}_2$

- Two special basis other than the Z basis ($\{|0\rangle, |1\rangle\}$ basis).
- The X basis:

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

- The Y basis:

$$|i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), \quad |-i\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle).$$

- Notice that any two vectors above from different basis has inner product result $|\langle\psi|\varphi\rangle| = \frac{1}{\sqrt{2}}$. (It is $\frac{1}{\sqrt{n}}$ in $\mathcal{H}_n$.)
- We call them mutually unbiased basis.

Bloch Sphere

- Why are they named X, Y, Z basis?
- Bloch sphere:

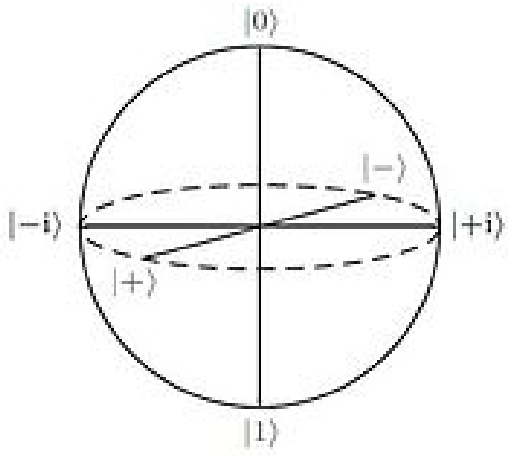

Figure: The Bloch sphere.

- All the pure states in $\mathcal{H}_2$ lie on the surface.

Tensor Product

- We could write $|\varphi\rangle \otimes |\psi\rangle = |\varphi\rangle|\psi\rangle$ to represent the unity of two seperate state $|\varphi\rangle$ and $|\psi\rangle$.
- Similarly, for two operators U, V seperately acting on two states, we could write a joint operator $U \otimes V$ to represent it.
- Mathematically, we have:

$$C = A \otimes B = \begin{pmatrix} a_{0,0}B & \cdots & a_{0,m-1}B \\ \vdots & \ddots & \vdots \\ a_{n-1,0}B & \cdots & a_{n-1,m-1}B \end{pmatrix}.$$

- In computational basis, we could write:

$$|0\rangle \otimes |0\rangle = |00\rangle.$$

Superposition

Quantum randomness resources

- The superposition of quantum state:

$$|\varphi\rangle = a_1|\psi_1\rangle + a_2|\psi_2\rangle + \cdots + a_k|\psi_k\rangle.$$

- Here a are complex coefficients.
- If the $|\psi\rangle$s are orthogonal, and we measure $|\varphi\rangle$ in $\{|\psi_1\rangle, |\psi_2\rangle, \cdots, |\psi_k\rangle\}$ basis:
- The probability of resulting in $|\psi_j\rangle$ is $|a_j|^2$.
- The formalization of measurement will be given later.

Density Matrix and Mix State

Exploring the Bell state

- A special two-qubit state: Bell state

$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

- If we measure it in computational basis:
  50% chance: $|00\rangle$.
  50% chance: $|11\rangle$.
- Now we assume Alice possesses the qubit 1, and Bob possesses the qubit 2.
- We also assume they are distant. (i. e. Alice is a human, and Bob is a Trisolarian.)
- When Alice measures the qubit 1:
  50% chance: Alice has $|0\rangle \Rightarrow$ Bob has $|0\rangle$.
  50% chance: Alice has $|1\rangle \Rightarrow$ Bob has $|1\rangle$.
- But Bob does not know any information from Alice.

Density Matrix and Mix State

When Bob is observing his state

- Bob does not even know whether Alice has measured her qubit.
- What information does Bob have about his qubit?
- 50% chance: $|0\rangle$. 50% chance: $|1\rangle$.
- We need new method to extend the previous state representation.
- Density matrix:

$$\rho = \sum_k p_k |\varphi_k\rangle\langle\varphi_k|.$$

- The state ρ has probability p_k to be pure state $|\varphi_k\rangle$.
- Bob's state is

$$\rho^B = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|.$$

- Mathematically, ρ is a positive-semidefinite Hermitian.
- Mix state: there are at least two terms with $p_k > 0$.

Partial Trace

- How to mathematically calculate their states?
- Partial trace:

$$A = \mathrm{Tr}_B(C) = \begin{pmatrix} \mathrm{Tr}(B_{0,0}) & \cdots & \mathrm{Tr}(B_{0,m-1}) \\ \vdots & \ddots & \vdots \\ \mathrm{Tr}(B_{n-1,0}) & \cdots & \mathrm{Tr}(B_{n-1,m-1}) \end{pmatrix}.$$

- Here $B_{i,j}$ is the (i,j)-th submatrix when B is divided into $n \times m$ matrices with same size.

Entanglement

- Notice that for Alice and Bob, the information they have in hand is

$$\rho^A = \rho^B = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|.$$

- But $\rho^A \otimes \rho^B \neq \rho^{AB} = |\Phi\rangle$.
- There is information outside of them.
- Entanglement makes their measurement results be the same.
- Separable state ρ^{AB} :

$$\rho^{AB} = \sum_k p_k \rho_k^A \otimes \rho_k^B.$$

- Entangled state: state that is not separable.

Two No-Go Theorems

No cloning theorem and no deleting theorem

- No cloning theorem: it is impossible to clone arbitrary quantum state.
- Mathematically, there is no channel U satisfies:

$$\forall|\varphi\rangle, U(|\varphi\rangle|0\rangle) = |\varphi\rangle|\varphi\rangle.$$

- Reverse it, we also have dual result.
- No deleting theorem: it is impossible to delete arbitrary quantum state.
- Mathematically, there is no channel U satisfies:

$$\forall|\varphi\rangle, U(|\varphi\rangle|\varphi\rangle) = |\varphi\rangle|0\rangle.$$

- Information conservation.

Basic Operators

Pauli operators

- In $\mathcal{H}_2$, there are three special operators:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

- Acting an operator U on pure state $|\varphi\rangle$ results in $U|\varphi\rangle$.
- These operators can be viewed as the 180° rotation along each axis.
- For example:

$$X|0\rangle = |1\rangle, X|1\rangle = |0\rangle, X|i\rangle = |-i\rangle, X|-i\rangle = |i\rangle,$$

$$X|+\rangle = |+\rangle, X|-\rangle = |-\rangle.$$

- In physics, these operators are more likely to be prepared.

Basic Operators

Hadamard gate

- Hadamard gate:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

- Examples:

$$H|0\rangle = |+\rangle,$$
$$H|1\rangle = |-\rangle.$$

- Superposition generating gate.
- This gate is also relatively easy to prepare.

Basic Operators

T gate

- T gate:

$$T = \begin{pmatrix} 1 & \\ & e^{\frac{i\pi}{8}} \end{pmatrix}.$$

- Also called $\frac{\pi}{8}$ phase gate.
- Phase gates are the gates adding a phase to $|1\rangle$, and keeps $|0\rangle$ intact.
- Later on an important theorem will involve this gate.

Basic Operators

Controlled-NOT gate

- CNOT gate:

$$\text{CNOT} = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & & 1 \\ & & 1 & \end{pmatrix}.$$

- This is a two-qubit operator.
- It flips the second qubit when the first qubit is $|1\rangle$.
- Example:

$$\text{CNOT}|+\rangle|0\rangle = \frac{1}{\sqrt{2}}(\text{CNOT}|00\rangle + \text{CNOT}|10\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

General Operators

Unitary transformation

- Unitary operator U satisfies:

$$UU^\dagger = U^\dagger U = I.$$

- Acting U on pure state $|\varphi\rangle$ results in $U|\varphi\rangle$.
- Acting U on density matrix ρ results in $U\rho U^\dagger$.
- Unitary transfomations are rotations in $\mathcal{H}_n$.
- They are linear and reversible.
- The (only) preliminary of quantum computation is linear algebra.

General Operators

Decomposition theorems

- Theorem for single qubit operators:
  Any single qubit operator can be approximated within ε error using $\text{poly}(\log \frac{1}{\varepsilon})$ gates of $\{X, Y, Z, H, T\}$.
- Theorem for unitary transformations:
  Any unitary transformation can be decomposed to two-qubit CNOT gate and single qubit operators.

Measurement

Projection-valued measurement

- Projection-valued measurement $\{M_k\}_{k=1}^m$ satisfies:

$$M_k = M_k^\dagger,$$

$$\sum_{k=1}^{m} M_k^\dagger M_k = I,$$

$$M_p M_q = \delta_{p,q} M_p.$$

- When measuring a pure state $|\varphi\rangle$, we have probability $\langle\varphi|M_k|\varphi\rangle$ to gain $\frac{M_k|\varphi\rangle}{\langle\varphi|M_k|\varphi\rangle}$.
- When measuring a density matrix ρ, we have probability $\mathrm{Tr}[M_k\rho M_k^\dagger]$ to gain $\frac{M_k\rho M_k^\dagger}{\langle\varphi|M_k|\varphi\rangle}$.
- Measurement will change the state.
- General measurement: positive operator-valued measurement.

Measurement

A simple PVM

- Consider a simple PVM, where we measure a sequence of qubits sequentially in basis $\{|0\rangle, |1\rangle\}$.
- Then $M_k = |k\rangle\langle k|$.
- It satisfies all the properties.

Quantum Circuits

- Due to the no cloning theorem and no deleting theorem, each wire is used only once.
- Well-aligned circuit visualization.
- Basic elements:

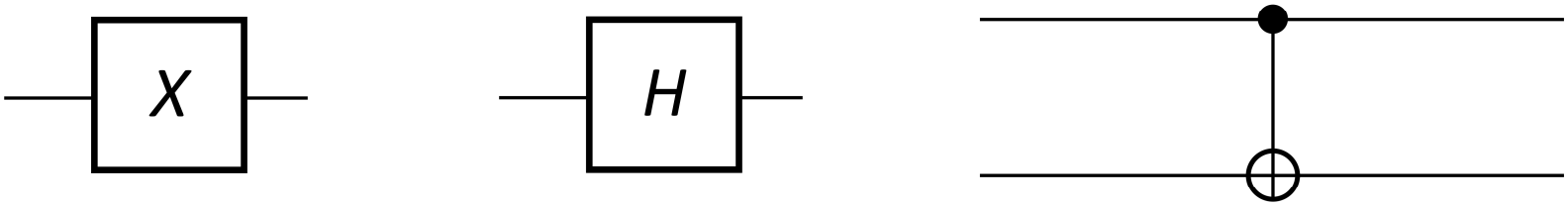

Figure: X gate, H gate, and CNOT gate.

Quantum Circuits

- Example: generating Bell state.

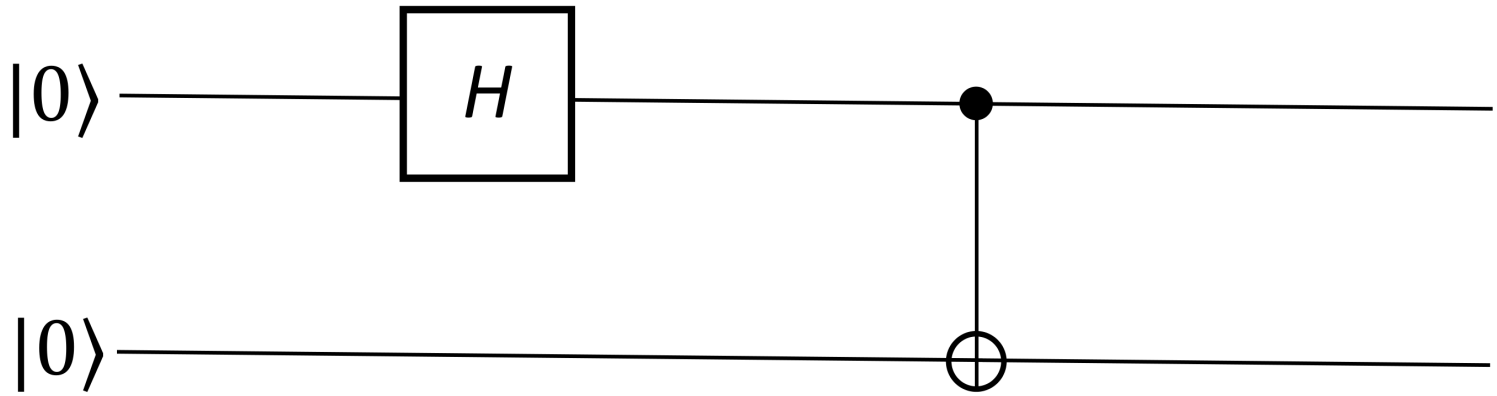

Figure: Circuit generating Bell state.

- How to calculate?

$$\begin{aligned} \text{Init} &\to |00\rangle \\ H &\to |+0\rangle = \tfrac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \\ \text{CNOT} &\to \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \end{aligned}$$

Quantum Teleportation

Scenario

- How can we transmit a state from Alice to distant Bob?
- In physics, a quantum state is hard to store and transmit.
- Can we do this in quantum way?
- Assume that Alice and Bob shares a pair of Bell state. Alice has Φ_0, and Bob has Φ_1.
- Alice want to teleport state $|\varphi\rangle = a|0\rangle + b|1\rangle$.
- In fact, the protocol for mix states is the same.

Quantum Teleportation

Protocol

- Alice executes circuit:

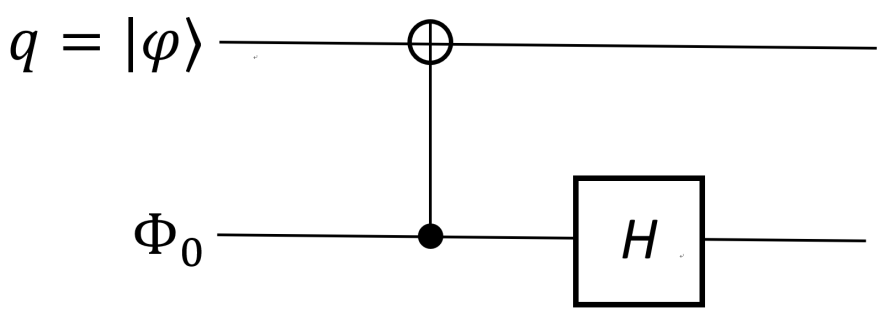

Figure: Alice's circuit for quantum teleportation.

- Then Alice measures the two qubits q and Φ_0, into two classical bits b_0 and b_1, and send the results to Bob.
- Bob acts X on Φ_1 if $b_1 = 1$.
- Bob acts Z on Φ_1 if $b_0 = 1$.

Quantum Teleportation

How does this work?

- Why do we consider only pure states? Linearity.
- Consider the state evolution in this protocol:

$$\begin{aligned}
\text{Init} &\to |\varphi\rangle|\Phi\rangle \\
&= \tfrac{1}{\sqrt{2}}(a|000\rangle + b|100\rangle + a|011\rangle + b|111\rangle) \\
\text{CNOT} &\to \tfrac{1}{\sqrt{2}}(a|000\rangle + b|100\rangle + a|111\rangle + b|011\rangle) \\
H &\to \tfrac{1}{2}(|00\rangle(a|0\rangle + b|1\rangle) + |01\rangle(a|0\rangle - b|1\rangle) \\
&\quad + |10\rangle(b|0\rangle + a|1\rangle) + |11\rangle(b|0\rangle - a|1\rangle)).
\end{aligned}$$

- When Alice measures q and Φ_0, Bob could correspondingly recover $|\varphi\rangle$.

Quantum Oracles

- To consider classical problems in quantum computing, we need to depict functions.
- For $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$, we provide an oracle U_f, such that:

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

- We define $N = 2^n$.

Deutsh-Jozsa Algorithm

Problem

- You are given a function f (and also the oracle U_f), and you need to distinguish the following two cases:
  -Balanced: $f(x) = 1$ for exact half of the inputs.
  -Constant: $f \equiv 1$ or $f \equiv 0$.
- You can hardly find an efficient classical algorithm ($o(N)$) with 0 error probability to solve it.
- You have to observe exactly $\frac{N}{2} + 1$ cells to determine it.

Deutsh-Jozsa Algorithm

Solve it in quantum way

- The circuit is:

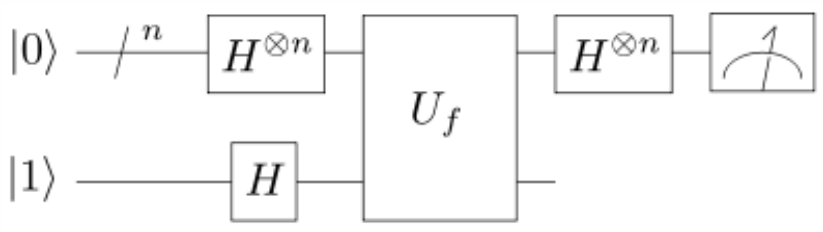

Figure: Circuit of Deutsh-Jozsa algorithm.

- First we consider $H^{\otimes n}$ acting on $|0\rangle^n$.
- It turns to

$$\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right)^n = \frac{1}{\sqrt{N}} \sum_{x=0}^{2^n-1} |x\rangle$$

Deutsh-Jozsa Algorithm

Solve it in quantum way

- Acting the oracle U_f on it joint with $|-\rangle$.
- For given $|x\rangle$, this leads to

$$\begin{aligned} \text{Init} \quad & \to |x\rangle|-\rangle \\ & = |x\rangle(|0\rangle - |1\rangle) \\ U_f \quad & \to |x\rangle(|f(x)\rangle - |f(x) \oplus 1\rangle) \\ & = (-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle) \\ & = (-1)^{f(x)}|x\rangle|-\rangle. \end{aligned}$$

- If f is constant, the phase turns to a global phase and is absorbed. The result of this circuit is 0^n.
- If f is balanced, the probability of resulting in all zeros is $|\frac{1}{2^n}\sum_{x=0}^{2^n-1}(-1)^{f(x)}|^2 = 0$.

Simon's Algorithm

Problem

- You are given a function f (and also the oracle U_f), satisfying:

$$f(x) = f(y) \quad \text{iff} \quad x \oplus y \in \{0, a\}.$$

- You need to find a.
- This is hard in classical computation given we accept solution with small error probability.

Simon's Algorithm

Solve it in quantum way

- The circuit is:

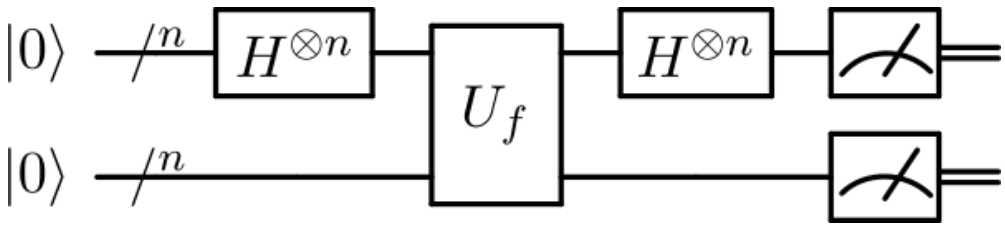

Figure: Circuit of Simon's algorithm.

- Which is almost the same as the Deutsch-Jozsa algorithm.

Simon's Algorithm

Solve it in quantum way

- The first step is also generating the superposition.
- For given $|x\rangle$, acting the oracle on it gives

$$|x\rangle|0\rangle \to |x\rangle|f(x)\rangle.$$

- Acting another $H^{\otimes n}$ gives

$$\to (\frac{1}{\sqrt{N}} \sum_{y=0}^{2^n-1} (-1)^{x\cdot y}|y\rangle) \otimes |f(x)\rangle.$$

- Rewrite the enumeration, the final state is

$$\frac{1}{N} \sum_{y=0}^{2^n-1} \left(|y\rangle \otimes \left(\sum_{x=0}^{2^n-1} ((-1)^{x\cdot y}|f(x)\rangle) \right) \right).$$

Simon's Algorithm

Solve it in quantum way

- Combining the same $f(x)$, it results to

$$\frac{1}{N}\sum_{y=0}^{2^n-1}\left(|y\rangle\otimes\left(\sum_{z\in\mathrm{Img(f)}}\left((-1)^{f_1^{-1}(z)\cdot y}(1+(-1)^{a\cdot y})|z\rangle\right)\right)\right).$$

- Hence, when $y\cdot a=1$, the corresponding terms vanish.
- Measuring the first register will always result in $y\cdot a=0$. We can also see that for different y satisfying this condition, the probability is the same.
- We repeat this procedure for $O(n)$ time, and when we gain n linearly independent y, the answer can be solved.

Comparison to UTR#3: Quantum Break

- It provides you with a lot of arrays a with a length of 2^n.
- For each a, there are only two non-zero entry x, y. (with the same value)
- We know that $x \oplus y$ is a constant. The task is to find it out.
- Each time the worker works on one particular array.
- Several interactive functions:
- 1. query(): Randomly return a label v with probability $\frac{a[v]^2}{\sum_i a[i]^2}$. Then this array is disposed, and the worker turns to another array.
- 2. manipulate(A, i): For each k such that the i-th bit is 0, act a linear mapping A to $a[k], a[k+2^i]$.
- (The problem is slightly modified.)

Grover's Algorithm

Problem

- You are given a database, and are required to find out a particular item. The item is marked with a function f. $f(x) = 1$ if and only if $x = a$.
- The oracle here is a phase oracle, where

$$U_a|x\rangle = (-1)^{[x \neq a]}|x\rangle.$$

- This can be write as $U_a = 2|a\rangle\langle a| - I$.
- We can also construct $U_{\Phi_n} = 2|\Phi_n\rangle\langle\Phi_n| - I$.
- These are reflections in $\mathcal{H}_N$.
- The algorithm is simply acting $U_\Phi U_a$ for $\sqrt{N}$ times on uniform superposition.
- Measure the result will give a in high probability.

Grover's Algorithm

Reflection

- The reflection is about the particular state.

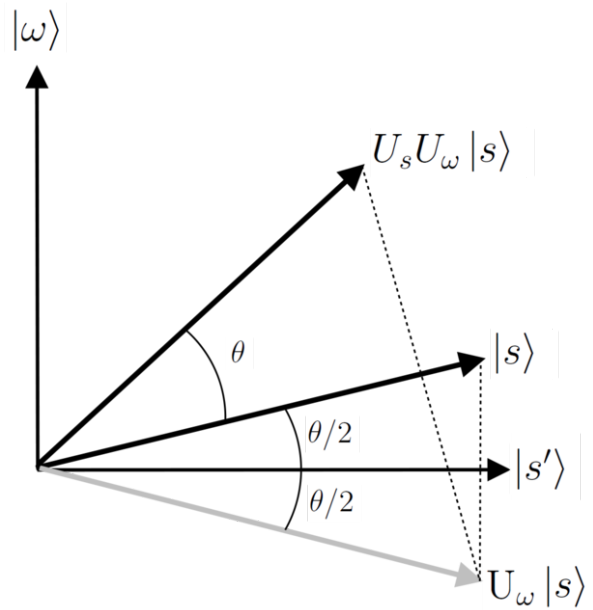

Figure: The core part of Grover's algorithm.

- In this picture, $\omega = a$, $s = \Phi$, $|s'\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq a} |x\rangle$.

Quantum Fourier Transform

- To present the Shor's algorithm, we introduce quantum Fourier transform (QFT) first.
- Let $\omega_k = e^{\frac{2\pi i}{k}}$.
- Discrete Fourier transform:

$$x = (x_0, x_1, \ldots, x_{N-1}) \to y = \left(y_j = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega_N^{j \cdot k} x_k \right)_{j=0}^{N-1}.$$

- Quantum Fourier transform:

$$|x\rangle \to |y\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega_N^{x \cdot k} |k\rangle$$

Quantum Fourier Transform

Implementation

- Let:

$$R_k = \begin{pmatrix} 1 & \\ & \omega_{2^k} \end{pmatrix}.$$

$$[0.a_1\, a_2 \ldots a_l] = \sum_{j=1}^{l} 2^{-j} a_j.$$

- The algorithm is:

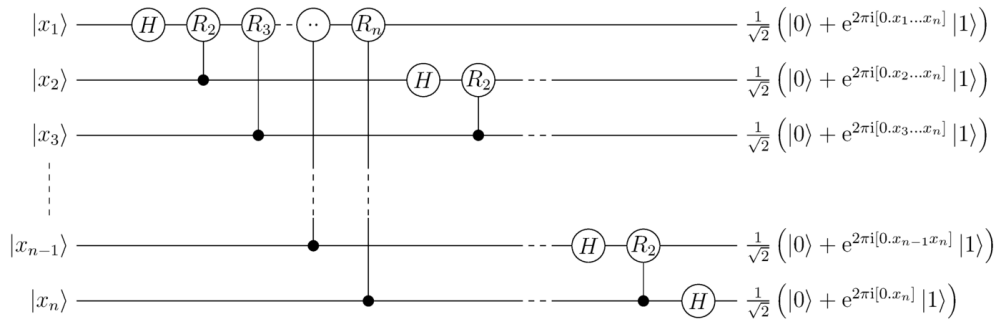

Figure: The QFT algorithm.

Quantum Phase Estimation

Problem

- Given an unitary transformation U and the eigenvalue $|\psi\rangle$, estimate θ such that:

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

- This is the core solution of hidden subgroup problems.

Quantum Phase Estimation

Implementation

- We assume $\tau = [0.\theta_1\theta_2\cdots\theta_n]$.
- The algorithm is:

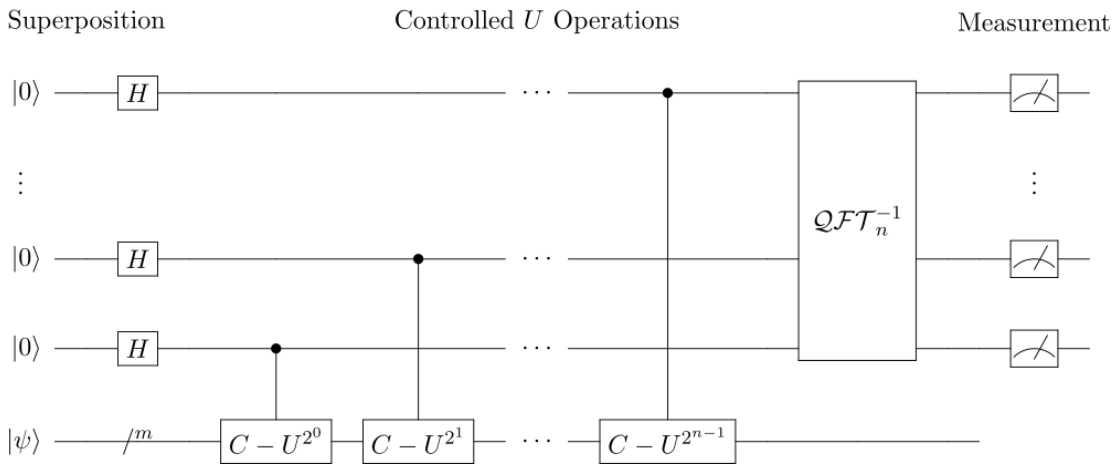

Figure: The phase estimation algorithm.

- For the j-th wire, we see that it transfromed from $|+\rangle$ to

$$\rightarrow \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i 2^{j-1}\theta}|1\rangle).$$

Quantum Phase Estimation

Implementation

- If $\tau = \theta$, this is exactly the QFT's result.
- Otherwise, the measurement result is close to θ.

Comparison to Training Team Problemset: Unnamable

- You need to find out a complex number x whose norm is 1.
- You are provided with an array with a length of 2^n. Initially, the only non-zero term is a_0.
- Several interactive functions:
- 1. CU(d, k): For each i such that the d-th bit is 1, multiply a phase x^k to $a[i]$.
- 2. CR(d_1, d_2, A): For each i such that the d_1-th bit and d_2-th bit is 1, act a linear mapping A to $a[i-2^{d_2}]$, $a[i]$.
- 3. QR(): Randomly return a label v with probability $\frac{|a[v]|^2}{\sum_i |a[i]|^2}$.
- (The problem is slightly modified.)

Shor's Algorithm

Quantum period-finding algorithm

- The key component of Shor's factorization is the quantum period-finding algorithm.
- For $a < C$, define the period r be the smallest positive integer such that $a^r \equiv 1 \pmod{C}$.
- Shor provided an algorithm to find r given $gcd(a, C) = 1$, using $O(\log^3 C)$ quantum gates.

Shor's Algorithm

Method

- Let
$$U_{a^{2^w}}|x\rangle = |x \times a^{2^w}\rangle.$$
- The period finding algorithm estimate the phases of this unitary transformation, and provides information about the period.
- The measurement result needs a continued fraction expansion to reveal the period of a.
- The classical part is illustrated in lecture notes.
- This method could also solve the discrete logarithm problem.

Acknowledgement

- Thanks to Fangjun Hu for discussion on this introduction.
- Thanks to CCF for providing the platform.
- Thanks to OIers who introduce interesting materials to us.

References

1 Michael Nielson and Issac Chuang, Quantum Computation and Quantum Information, Tsinghua University Press, 2015.

2 Xiongfeng Ma, Quantum Information Lecture Notes, 2016.

3 Wikipedia.org.

Q&A&Q