

Quantum Computation and Quantum Information

Hsi-Sheng Goan

1 Overview

53 quantum bits (Quantum supremacy)

Task that super computer takes 100000 years (IBM days) only takes 200 sec on Quantum Computer

IBM 53 qubits have not been optimized

2^{100} state seems powerful

2 Speech

RSA cryptography: Factor two prime number Factor 309-digit number: Classical THz computer take 150000 years, and quantum computer take $< 1s$

2.1 Quantum bit

Classical bit: 0 or 1

Quantum bit: QM two-state system $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

Two qubit: We can have four state simultaneously $|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \tau|11\rangle$

So in quantum register, for 3 bit, we can have 8 states simultaneously, unlike classical register only 1 state

2.2 Development

2016 IBM 5-qubit online

2017 IBM 16-qubit online (but 1 or 2 malfunction)

50 qubits need to pay The temperature for Quantum computer is nearly 20mK to superconduct

Noisy Intermediate Scale Quantum (*NISQ*)

In classical computer, we can prevent noise just put on threshold, but quantum error is hard to correct. We may add another error to that

Google v.s. IBM: 53 qubits 200s and 72 petabyte memory few days

2.3 implementation

- 1998 proposal: Silicon-based electron-mediated nuclear spin (2012 implement)
- Electron spins in quantum dots
- 2015 two-qubit logic gate in silicon (Using semiconductor 15nm!!)

2.4 Challenge

- Much larger numbers of qubits e.g. shor's need thousand qubits
- Much greater connectivity with fewer restriction
- Much lower error rate
- True fault tolerance-error correction

- Higher operating temperature

2.5 HQC

Hybrid Quantum-Classical (HQC) Algorithm

Variational quantum circuit algorithm

Data encoding scheme

Variational Quantum Eigensolver (VQE)

2.6 Application

- Artificial intelligence
- Medicine and Materials (Molecule simulation)
- Supply chain
- Cloud Security

3 Quantum Computation & Quantum Information (QC&QI)

It is the study of information processing and computing tasks that can be accomplished using QM system.

Remark *IBM using classical approach to simulate 32 qubits QM system.*

Remark *Quantum system is rare in our daily life. It seems the nature is against it.*

Explore and exploit Quantum effect, based on the principle of QM to compute and process information in ways that are **faster** or **more efficient** than or **even impossible** on conventional computers or information processing devices.

Example

Shor's Quantum factoring algorithms (1994)

Grover's Quantum search algorithms (1996)

Quantum simulation (exponential enhancement in memory size) Feynman 1982

Quantum Teleportation (1993) Bennett et al.

Quantum superdense coding (1992) Bennett and Wiesner

Quantum Cryptography (1984) Bennett and Brassard

Remark *Only Quantum machine can simulate quantum system. Because quantum system grows too fast.*

Remark *Quantum Teleportation: Transfer quantum state from one place to another place*

Quantum superdense coding: Use a few qubit to transfer more bit information

Remark *Shor's: Prime factorization, exponential speed up*

Grover's: Unsorted data, quadratic speed up

What is the killer application ?

4 Quantum Information Sciences (QIS)

To catch all aspects of QC & QI

4.1 Fundamental questions of IS

1. Given a physical resources - energy, time, space, bit, gates
2. Given an information processing task - data compression, information transmission, computing task, factoring
3. Given a criterion for success

We ask the question: How much of 1 do I need to achieve 2 while satisfying 3 ?

Pursuing this question in the quantum case has led to and presumably will continue to lead to interesting new information processing capability.

4.2 Knowing the rules of QM \neq Understanding the QM

What high-level principles are implied by QM?

To discuss these high-level principles, we may need to know the basic rules of QM first.

QM has a fearsome popular image because the mathematics required to apply QM to problems like determining the energy spectra of molecules and calculating scattering cross-section is difficult or intimidating.

By contrast, the mathematics used in application to QIS is "relatively painless". Do not need to read the traditional QM textbooks. Here, I mean the mathematics required to understand those algorithms protocols. However, the math for physical implementation and consideration of real world, noise and decoherence may be a little bit involved.

What is Quantum Mechanics?

Is it a complete physical theory of the world in its own right? No!! misconception!!
It is a framework for the development of physical theory.

QM consists of a set of mathematical postulates:

4 suspensingly simple postulates which lay the ground rules for our description of the world.

Most physicists believe that theory of everything will be a QM theory:

1. Attempts to describe gravitation in the framework of QM has so far not yet been successful.
2. Conceptual issue, so called "measurement problem" remains to be clarified.

4.3 The Structure of QM for QIS

$$\left\{ \begin{array}{l} \text{linear algebra: Matrix, finite-dimension} \\ \text{Dirac notation: } |\psi\rangle, \langle\phi|, \langle A| \\ 4 \text{ postulates of QM} \end{array} \right.$$

1. How to describe Quantum state of a closed system?
State space (Hilbert space), state vector
2. How to describe Quantum dynamics (time evolution)?
Unitary evolution
3. How to describe measurements of a Quantum system?
Projective measurement \rightarrow POVM measurement, Generalized Quantum measurement

4. How to describe Quantum of a composite system?
tensor product

Postulate Associated to any isolated physical system is a complex vector space with inner product (that is Hilbert space) known as the state space of the system. Thy system is completely described by its state vector which is a unit vector in the system's state space.

Remark QM does not tell us, for a given physical system, whate the state space of that system is, nor does it tell us the state vector of the system is.

Remark Finding that out for a specific system is a difficult problem for which physicists have developed many beautiful rules (e.g. QED)

Example Quantum bit (qubit) (Two level system)

"bit" is the fundamental element for information processing concept of classical Computation and Information. It can exist in two distinct states represented by 0 and 1.

It is over \mathbb{C}^2 and quantum state is just a unit vector in that space.

$$\begin{aligned} |\psi\rangle &= \alpha |0\rangle + \beta |1\rangle \\ |\psi\rangle &= \alpha |0\rangle + \beta |1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}_{\text{in } |0\rangle, |1\rangle \text{ basis}} = \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ \langle\psi|\psi\rangle &= (\alpha^* \quad \beta^*) \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = |\alpha|^2 + |\beta|^2 = 1 \end{aligned}$$

Postulate The evolution of a closed Quantum system is described by a unitary transformation

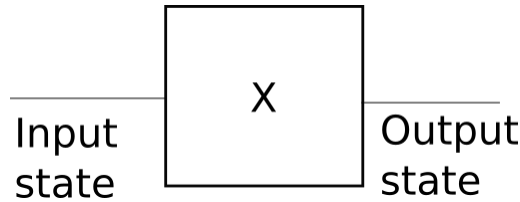
$$|\psi(t_2)\rangle = U(t_1, t_2) |\psi(t_1)\rangle \quad U \text{ is unitary to preserve normalize}$$

Remark QM does not prescribe this unitary evolution for particular system. Physicsts figure it out by a complex interplay between theory and experiement

Remark matrix = transformation = linear operator = map = Quantum gate

Example Pauli gate (Pauli sigma matrices)

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$



Quantum wire: The qubit is carried along by this Quantum wire until it reaches the X gate, not necessarily means that it carries qubit through space, may represnt a stationary qubit which is simply sitting there, passing through time until the X gate is applied.

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

Quantum NOT gate

Postulate *The time evolution of the state of a closed quantum system by Schrödinger equation:*

$$i\hbar \frac{\partial |\psi\rangle}{\partial t} = \mathcal{H} |\psi\rangle$$

if \mathcal{H} is independent of time

$$U(t_1, t_2) = e^{-i\mathcal{H}(t_2-t_1)/\hbar}$$

if \mathcal{H} depends on time, we have to do the integration on Hamiltonian

Postulate (General Measurement) *Quantum measurements are described by a collection $\{M_n\}$ of measurement operators. There are operators acting on the state space of the system being measured. The index m refers to the measurement outcomes that may occur in the experiment. If the state of the quantum system is $|\psi\rangle$ immediately before the measurement then:*

1. *The probability that result m occurs is given by*

$$p(m) = \langle \psi | M_m^\dagger M_m | \psi \rangle$$

2. *And the state of the system after the measurement is*

$$\frac{M_m |\psi\rangle}{\sqrt{\langle \psi | M_m^\dagger M_m | \psi \rangle}}$$

The measurement operators satisfy the completeness equation $\sum_m M_m^\dagger M_m = \mathbb{1}$

Example Measurement of a qubit in the computation basis

$$\begin{aligned} |\psi\rangle &= \alpha |0\rangle + \beta |1\rangle \\ &= \frac{1}{\sqrt{2}} [(\alpha + \beta) |+\rangle + (\alpha - \beta) |-\rangle] \end{aligned}$$

$$M_0 = |0\rangle \langle 0| = M_0^\dagger$$

$$M_1 = |1\rangle \langle 1| = M_1^\dagger$$

- *Probability*

$$p(0) = \langle \psi | M_0^\dagger M_0 | \psi \rangle = \langle \psi | M_0 | \psi \rangle = |\alpha|^2$$

$$p(1) = \langle \psi | M_1^\dagger M_1 | \psi \rangle = \langle \psi | M_1 | \psi \rangle = |\beta|^2$$

- *Post-Measurement*

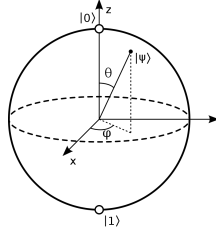
$$\frac{M_m |\psi\rangle}{\sqrt{\langle \psi | M_m^\dagger M_m | \psi \rangle}} = \frac{\alpha}{\sqrt{|\alpha|^2}} |0\rangle = \frac{\alpha}{|\alpha|^2} |0\rangle = e^{i\theta} |0\rangle$$

Remark

$$\mathcal{O} = \begin{pmatrix} \mathcal{O}_{00} & \mathcal{O}_{01} \\ \mathcal{O}_{10} & \mathcal{O}_{11} \end{pmatrix} \text{ and } \mathcal{O} = \sum_{i,j} \mathcal{O}_{ij} |i\rangle \langle j|$$

Remark *Global phase doesn't matter, but relative phase does.*

Bloch Shpere representation



$$\hat{n} = (\sin \theta \cos \phi, \sin \theta \sin \phi, \cos \theta)$$

$$|+\rangle_{\hat{n}} = \cos \frac{\theta}{2} |0\rangle + e^{i\phi} \sin \frac{\theta}{2} |1\rangle$$

$$|-\rangle_{\hat{n}} = -\sin \frac{\theta}{2} |0\rangle + \cos \frac{\theta}{2} e^{i\phi} |1\rangle$$

$|+\rangle_n$ means the eigenstate of Pauli matrix in \hat{n} direction. That is, $\hat{\sigma} \cdot \hat{n}$.

For arbitrary state, the expectation value $\langle X \rangle^2 + \langle Y \rangle^2 + \langle Z \rangle^2 = 1$

Remark In Quantum Mechanics, we can not determined all spin component simultaneously since $[S_i, S_j] = i\hbar \epsilon_{ijk} S_k$. Hence, in quantum case, we can only calculate the expectation value of three obervables S_x, S_y, S_z .

Remark

$$\text{qubit: } |\psi\rangle = \cos \frac{\theta}{2} |0\rangle + \sin \frac{\theta}{2} e^{i\phi} |1\rangle$$

Since θ and ϕ are continuous, it seems that we can carry all information in θ and ϕ . However, if we want to extract the probability of $|0\rangle$, we have to prepare "many" pure state. But the precision of the coefficient is related to how many pure state we observe. If we can do measurement infinitely, then we can get exact qunit.

Distinguishing Quantum States

Distinguishability: a set of states $|\psi_i\rangle$, $1 \leq i \leq n$ known to Alice and Bob. Alice choose a state $|\psi_i\rangle$ and gives it to Bob, whose task is to identify the index j of the state Alice has given him.

1. Suppose $|\psi_i\rangle$ are orthonormal $\langle \psi_i | \psi_j \rangle = \delta_{ij}$. Define $M_j = |\psi_j\rangle \langle \psi_j|$. If the state $|\psi_j\rangle$ is prepared, then $p(j) = \langle \psi_j | M_j^\dagger M_j | \psi_j \rangle = 1$; $p(i) = \langle \psi_i | M_j^\dagger M_j | \psi_i \rangle = 0$.

Remark Since Alice only choose n states, there are some states that are not chosen. Hence, we adjust the complettness relation $\sum_{i=1}^n M_i^\dagger M_i + M_0^\dagger M_0 = \mathbb{1}$. M_0 is the rest of the states.

2. If the state $|\psi_i\rangle$ are not orthonormal then there is no Quantum measurement capable of distinguishing these state. $\langle \psi_i | \psi_j \rangle \neq 0$ for $i \neq j$

Postulate (Projective measurement) A projective measurement is described by an observable, a Hermitian operator \mathcal{M} with spectral decomposition

$$\mathcal{M} = \sum_m m P_m$$

where $P_m = |m\rangle \langle m|$ is the projector onto the eigenspace of \mathcal{M} with eigenvalue m .

The possible outcomes of the measurement correspond to the eigenvalues m and the outcome m occurs with probability

$$p(m) = \langle \psi | P_m | \psi \rangle$$

The corresponding post-measurement is

$$\frac{P_m |\psi\rangle}{\sqrt{\langle\psi|P_m|\psi\rangle}}$$

Example

$$S_z = \frac{\hbar}{2} |+\rangle \langle +| - \frac{\hbar}{2} |-\rangle \langle -|$$

Remark Projective measurement can be understood as a special case of general measurement

$$\sum_m M_m^\dagger M_m = \mathbb{1}$$

From postulate of projective measurement, $M_m^\dagger = M_m$ (Hermitian) and $M_m M_{m'} = M_m \delta_{mm'}$ (Orthogonal Projector)
 $p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle = \langle\psi|M_m|\psi\rangle$ and $\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}} = \frac{M_m|\psi\rangle}{\sqrt{p(m)}} = \frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m|\psi\rangle}}$

The Heisenberg uncertainty principle

Suppose A and B are two Hermitian operators $A^\dagger = A, B^\dagger = B$. Suppose $\langle\psi|AB|\psi\rangle = x + iy$ where $x, y \in \mathbb{R}$

$$\langle\psi|BA|\psi\rangle = \langle\psi|B^\dagger A|\psi\rangle = \langle\psi|A^\dagger B|\psi\rangle^* = \langle\psi|AB|\psi\rangle^*$$

$$\langle\psi|[A, B]|\psi\rangle = \langle\psi|AB - BA|\psi\rangle = 2iy$$

$$\langle\psi|\{A, B\}|\psi\rangle = \langle\psi|AB + BA|\psi\rangle = 2x$$

$$|\langle\psi|[A, B]|\psi\rangle|^2 + |\langle\psi|\{A, B\}|\psi\rangle|^2 = 4|\langle\psi|AB|\psi\rangle|^2$$

By the Cauchy-Schwartz inequality:

$$|\langle\psi|AB|\psi\rangle|^2 \leq \langle\psi|A^2|\psi\rangle \langle\psi|B^2|\psi\rangle$$

Hence

$$|\langle\psi|[A, B]|\psi\rangle|^2 \leq 4|\langle\psi|AB|\psi\rangle|^2 \leq 4\langle\psi|A^2|\psi\rangle \langle\psi|B^2|\psi\rangle$$

Suppose C and D are two observables and $A = C - \langle C \rangle, B = D - \langle D \rangle \Rightarrow [A, B] = [C, D]$

$$|\langle\psi|[C, D]|\psi\rangle|^2 \leq 4(\Delta C)^2 (\Delta D)^2$$

$$\frac{1}{2} |\langle\psi|[C, D]|\psi\rangle| \leq (\Delta C)(\Delta D)$$

There is an intrinsic limit to the accuracy of the simultaneous measurement of both C and D if $[C, D] \neq 0$. The measurement of one observable necessarily disturbs the other if $[C, D] \neq 0$

Positive Operator-valued Measure (POVM) measurement

Positive operator: A special subclass of Hermitian operators defined as for any vector $|v\rangle, \langle v|A|v\rangle$ is a real, non-negative numbers.

Positive definite: If $\langle v|A|v\rangle$ is strictly greater than zero for all $|v\rangle \neq 0$

POVM: A set of $\{E_m\}, \sum_m E_m = \mathbb{1}, p(m) = \langle\psi|E_m|\psi\rangle$

Remark POVM is a simple consequence of the general measurement. The set of E_m is sufficient to determine probability of different outcomes m . The complete set $\{E_m\}$ is known as POVM. E_m is the POVM element.

Example

$$\begin{aligned} |\psi_1\rangle &= |0\rangle \\ |\psi_2\rangle &= \frac{|0\rangle + |1\rangle}{\sqrt{2}} \end{aligned}$$

It is impossible for Bob to perform a measurement which distinguishes the states.
Consider POVM containing

$$\begin{aligned} E_1 &= \frac{\sqrt{2}}{1 + \sqrt{2}} |1\rangle \langle 1| \\ E_2 &= \frac{\sqrt{2}}{1 + \sqrt{2}} \frac{(|0\rangle - |1\rangle)(\langle 0| - \langle 1|)}{2} \\ E_3 &= \mathbb{1} - E_1 - E_2 \end{aligned}$$

If the outcome is m_1 , the state will not be $|\psi_1\rangle$ since $\langle \psi_1 | E_1 | \psi_1 \rangle = 0$. The state must be $|\psi_2\rangle$.
If the outcome is m_2 , the state will not be $|\psi_2\rangle$ since $\langle \psi_2 | E_2 | \psi_2 \rangle = 0$. The state must be $|\psi_1\rangle$.
If the outcome is m_3 , however, we do not sure whether we get $|\psi_1\rangle$ or $|\psi_2\rangle$. We get no information.

Postulate The state space of a composite physical system is the tensor product of the state space of the compoment physical system. Moreover, if we have system numbered 1 through n , and the system number i is prepared in the state $|\psi_i\rangle$, then the joint state of the total system is

$$|\psi_i\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$$

Example Two qubit system

Two-qubit state space is $\mathbb{C}^2 \otimes \mathbb{C}^2 = \mathbb{C}^4$

$$\begin{array}{c} |0\rangle \\ |1\rangle \end{array} \otimes \begin{array}{c} |0\rangle \\ |1\rangle \end{array} \Rightarrow \begin{cases} |0\rangle \otimes |0\rangle = |0,0\rangle = |0\rangle |0\rangle \\ |0\rangle \otimes |1\rangle \\ |1\rangle \otimes |0\rangle \\ |1\rangle \otimes |1\rangle \end{cases}$$

100 qubits $2^{100} \approx 10^{30}$ memory!! Hilbert space is indeed a big place!

Example

$$\begin{aligned} &(\mathbb{1} \otimes X) \sqrt{0.1} |00\rangle + \sqrt{0.2} |01\rangle + \sqrt{0.3} |10\rangle + \sqrt{0.4} |11\rangle \\ &= \sqrt{0.1} |01\rangle + \sqrt{0.2} |00\rangle + \sqrt{0.3} |11\rangle + \sqrt{0.4} |10\rangle \end{aligned}$$

The first operator $\mathbb{1}$ acts on the first qubit space and the second one X acts on the second qubit space.

Remark Through we can compute parallely, we have to do many measurements to get the information of the amplitute. Thus, we often use interference to left the amplitute of interese and measure it.

Basic properties of tensor product under $\mathbb{V} \otimes \mathbb{W}$

1. $z(|v\rangle \otimes |w\rangle) = z|v\rangle \otimes |w\rangle = |v\rangle \otimes (z|w\rangle) \quad \forall z \in \mathbb{C}$
2. $|v_1\rangle$ and $|v_2\rangle \in \mathbb{V}$ and $|w\rangle \in \mathbb{W}$, $(|v_1\rangle + |v_2\rangle) \otimes |w\rangle = |v_1\rangle \otimes |w\rangle + |v_2\rangle \otimes |w\rangle$
3. $|v\rangle \otimes (|w_1\rangle + |w_2\rangle) = |v\rangle \otimes |w_1\rangle + |v\rangle \otimes |w_2\rangle$

Suppose A and B are linear operators on \mathbb{V} and \mathbb{W} respectively.

4. $(A \otimes B)(|v\rangle \otimes |w\rangle) = A|v\rangle \otimes B|w\rangle$
5. $(A \otimes B)(\sum_i a_i |v_i\rangle \otimes |w_i\rangle) = \sum_i a_i (A|v_i\rangle \otimes B|w_i\rangle)$

6.

$$A_{m \times n} \otimes B_{p \times q} = \begin{pmatrix} A_{11}B & A_{12}B & \cdots & A_{1n}B \\ A_{21}B & A_{22}B & \cdots & A_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ A_{m1}B & A_{m2}B & \cdots & A_{mn}B \end{pmatrix}_{mp \times nq}$$

Partial measurement

If the state of a two-qubit system is

$$|\psi\rangle = \alpha_0 |00\rangle + \alpha_1 |01\rangle + \alpha_2 |10\rangle + \alpha_3 |11\rangle$$

Measure qubit 1 in its computational basis.

$$P_0 \otimes \mathbb{1} = |0\rangle \langle 0| \otimes \mathbb{1}$$

$$P_1 \otimes \mathbb{1} = |1\rangle \langle 1| \otimes \mathbb{1}$$

$$\begin{aligned} P(m=0) &= \langle \psi | M_0^\dagger M_0 | \psi \rangle = \langle \psi | M_0 | \psi \rangle = \langle \psi | P_0 \otimes \mathbb{1} | \psi \rangle \\ &= (\langle 00 | \alpha_0^* + \langle 01 | \alpha_1^* + \langle 10 | \alpha_2^* + \langle 11 | \alpha_3^*) (\alpha_0 | 00\rangle + \alpha_1 | 01\rangle) \\ &= |\alpha_0|^2 + |\alpha_1|^2 \\ P(m=1) &= |\alpha_2|^2 + |\alpha_3|^2 \end{aligned}$$

Post-measurement state

$$\frac{P_0 \otimes \mathbb{1} |\psi\rangle}{\sqrt{P(m=0)}} = \frac{\alpha_0 |00\rangle + \alpha_1 |01\rangle}{\sqrt{|\alpha_1|^2 + |\alpha_0|^2}} = |0\rangle \otimes \frac{\alpha_0 |0\rangle + \alpha_1 |1\rangle}{\sqrt{|\alpha_1|^2 + |\alpha_0|^2}}$$

Example

$$\psi = \frac{2}{3} |01\rangle + \frac{2}{3}i |10\rangle + \frac{1}{3} |00\rangle$$

Measure 1st qubit $m_1 = 0$

$$\frac{\frac{2}{3} |01\rangle + \frac{1}{3} |00\rangle}{\sqrt{\frac{2}{3}^2 + \frac{1}{3}^2}} = \frac{2}{\sqrt{5}} |01\rangle + \frac{1}{\sqrt{5}} |00\rangle = |0\rangle \otimes \frac{2|1\rangle + |0\rangle}{\sqrt{5}}$$

Measure 2nd qubit $m_2 = 0$

$$\frac{\frac{2}{3}i |10\rangle + \frac{1}{3} |00\rangle}{\sqrt{\frac{2i}{3}^2 + \frac{1}{3}^2}} = \frac{2i |1\rangle + |0\rangle}{\sqrt{5}} \otimes |0\rangle$$

Measure 2nd qubit $m_2 = 1$

$$\frac{\frac{2}{3} |01\rangle}{\sqrt{\frac{2}{3}^2}} = |01\rangle = |0\rangle \otimes |1\rangle$$

Quantum entanglement

$$\text{Bell state : } |\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

$$|\psi\rangle \neq |a\rangle |b\rangle \text{ non-separable}$$

If the state is separable:

$$|\psi\rangle = (\alpha |0\rangle + \beta |1\rangle) \otimes (\gamma |0\rangle + \delta |1\rangle) = \alpha\gamma |00\rangle + \beta\gamma |10\rangle + \alpha\delta |01\rangle + \beta\delta |11\rangle$$

$$\gamma\beta = 0 \text{ or } \alpha\delta = 0 \Leftrightarrow \alpha\gamma = 1 \text{ and } \beta\delta = 1$$

We describe such state being "entangled state" since they can not be understood in terms of Alice's and Bob's individual system, but rather embody some joint property of the system.

Schrödinger(1935): I would not call entangled one but rather the characteristic trait of quantum mechanics the one that enforces its entire departure from classical lines of thought.

Suppose the initial system state vector is $|\psi(t)\rangle$, and say, there is a second Quantum system called ancilla system (or the meter) in an initial state $|\phi(t)\rangle$. So the initial states of the combined system is :

$$|\Psi(t)\rangle = |\psi(t)\rangle \otimes |\phi(t)\rangle = |\psi(t)\rangle |\phi(t)\rangle$$

Let the two system be coupled together for a time T_1

$$U(T_1) = e^{-i\mathcal{H}T_1/\hbar} \quad \mathcal{H} : \text{total Hamiltonian}$$

$$\begin{aligned} |\Psi(t + T_1)\rangle &= U(T_1) |\psi(t)\rangle |\phi(t)\rangle \\ &= \sum_m \beta_m(t) |\psi_m(t)\rangle |\phi_m\rangle \end{aligned}$$

$|\phi_m\rangle$ is the orthonormal basis, but $|\psi_m(t)\rangle$ may not be orthogonal.

Now let the meter be measured projectively over a small time interval T_2 and the outcome is m , the post measurement state is

$$|\Psi_m(t + T_1 + T_2)\rangle = \frac{[\mathbb{1} \otimes |\phi_m\rangle \langle \phi_m|] U(T_1) |\psi(t)\rangle |\phi(t)\rangle}{\sqrt{P_m(T_2)}} = \frac{M_m}{\sqrt{P_m}} |\phi_m\rangle |\psi(t)\rangle$$

$$\begin{aligned} P_m(T_2) &= \langle \Psi(t + T_1) | P_m | \Psi(t + T_1) \rangle \\ &= \langle \phi(t) | \langle \psi(t) | U^\dagger(T_1) [\mathbb{1} \otimes |\phi_m\rangle \langle \phi_m|] U(T_1) |\psi(t)\rangle |\phi(t)\rangle \\ &= \langle \psi(t) | M_m^\dagger M_m | \psi(t) \rangle \end{aligned}$$

$\forall M_m = \langle \phi_m | U(T_1) | \phi(t) \rangle$ acting on the system Hilbert space only

The completeness condition:

$$\begin{aligned} \sum_m M_m^\dagger M_m &= \sum_m \langle \phi(t) | U^\dagger(T_1) | \phi_m \rangle \langle \phi_m | U(T_1) | \phi(t) \rangle \\ &= \langle \phi(t) | U^\dagger(T_1) U(T_1) | \phi(t) \rangle = \mathbb{1} \end{aligned}$$

EPR paradox and Bell's inequality

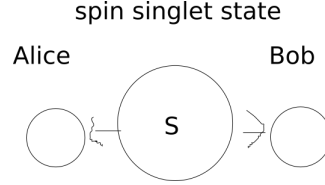
- Perhaps, the most spectacular and counter-intuitive manifestation of quantum mechanics is the phenomenon of entanglement observed in composite quantum system.
- According to quantum mechanics, and unobserved particle do not possess physical properties that exist independent of observation (reality assumption). Rather, such physical arise as a consequence of measurement performed upon the system.
- In early days of the development of quantum mechanics, many physicists rejected this view of Nature. The most prominent objector was Albert Einstein.
- 1935, Albert Einstein, Nathan Rosen, Boris Podolsky proposed a thought experiment which they believed demonstrated that QM is not a complete theory of Nature \Rightarrow QM leads to a contradiction, provided that we accept the following two seemingly natural assumptions (that Nature ought to obey)
 - (1) **Reality principle:** If we can predict with certainty the value of a physical quantity, then this value has physical reality, independent of observations. e.g. tennis ball, moon, color of a chalk
 - (2) **Locality principle:** If two system are causally disconnected, the result of any measurement performed on one system cannot influence the result of a measurement performed on the second system.

Theory of relativity: two events taking place at space-time coordinates $(x_1, t_1), (x_2, t_2)$ respectively. The two events are disconnected if $(\Delta x)^2 > (c\Delta t)^2$ (Space-like events). That is, physical influence cannot propagate faster than light.

- 1964, John Bell formulated inequality assuming the principle of realism and locality. Since it is possible to **devise situations** in which QM predicts a violation of these inequalities, any experimental observation of such a violation excludes the possibility of a local and realistic description of natural phenomena.

Remark *It turns out that Nature experimentally invalidates EPR's points of view, while agreeing with QM. To device Bell's inequality, we should forget about QM for a moment, and use the classical common sense notion of how the world works, the sort of notion EPR thought Nature ought to obey.*

- The thought experiment:



1. A source that is capable of repeating the experimental procedure to prepare two particle.
2. Once the particles are prepared, one particle is sent to A(lice) and the other to B(ob).
3. The timing of the experiment is arranged so that Alice and Bob do their measurements at the same time (or in a causally disconnected manner).
4. Alice and Bob can measure the polarization along 3 different axes a,b,c.

According to the reality principle, we may assign well defined values to the spin components along the three axes. That is, we assume that these values have physical reality independent of our observation. The result of the measurement of Alice and Bob are perfectly anti-correlated.

Classical intuitive example: two balls (one black, one white), a pair of gloves (one left-handed, one right-handed)

<i>Alice</i>	<i>Bob</i>
↓	↓
<i>white</i>	<i>black</i>
<i>(L)</i>	<i>(R)</i>

Locality and Reality

The results are mutually exclusive groups:

Population	Alice's particle	Bob's particle
N_1	(a_+, b_+, c_+)	(a_-, b_-, c_-)
N_2	(a_+, b_+, c_-)	(a_-, b_-, c_+)
N_3	(a_+, b_-, c_+)	(a_-, b_+, c_-)
N_4	(a_+, b_-, c_-)	(a_-, b_+, c_+)
N_5	(a_-, b_+, c_+)	(a_+, b_-, c_-)
N_6	(a_-, b_+, c_-)	(a_+, b_-, c_+)
N_7	(a_-, b_-, c_+)	(a_+, b_+, c_-)
N_8	(a_-, b_-, c_-)	(a_+, b_+, c_+)

Let $P(a_+, b_+)$ denote the probability that Alice obtains $\sigma_a^A : +1$ and Bob obtains $\sigma_b^B : +1$

$$P(a_+, b_+) = \frac{N_3 + N_4}{N} \quad P(a_+, c_+) = \frac{N_2 + N_3}{N} \quad P(c_+, b_+) = \frac{N_3 + N_7}{N}$$

$$N_3 + N_4 \leq (N_2 + N_4) + (N_3 + N_7) \\ \Rightarrow P(a_+, b_+) \leq P(a_+, c_+) + P(c_+, b_+) \quad (\text{Bell's inequality})$$

Reality: We can establish the above table.

Locality: If a pair belongs to group 1, and Alice's choose to measure σ_a^A , then she will certainly obtain outcome +1, i.e. a_+ , independently of the fact that Bob may choose to perform a measurement along the axes a,b or c.

Quantum Theory

The state of one particle depends upon the nature of the observable measured on the other particle.

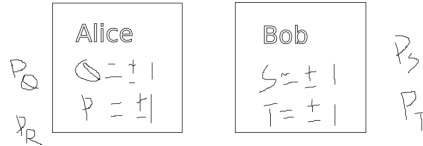
$$|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = \frac{1}{\sqrt{2}}(|+\rangle|-\rangle - |-\rangle|+\rangle) = \frac{1}{\sqrt{2}}(|+\rangle_n|-\rangle_n - |-\rangle_n|+\rangle_n)$$

If Alice finds $\sigma_a^A : +1$, then the state of Bob's particle collapses to the eigenstate of $|-\rangle_a \Rightarrow \sigma_b^B$ with probability $\langle\psi|P_m|\psi\rangle = {}_a\langle-|+\rangle_b {}_b\langle+|-\rangle_a = \sin^2 \frac{\theta_{ab}}{2} \Rightarrow P(a_+, b_+) = \frac{1}{2} \sin^2 \frac{\theta_{ab}}{2}$

$$\sin^2 \frac{\theta_{ab}}{2} \leq \sin^2 \frac{\theta_{ac}}{2} + \sin^2 \frac{\theta_{cb}}{2} \quad (\text{Substitute in Bell's inequality})$$

If we choose $\theta_{ab} = 2\theta, \theta_{ac} = \theta_{cb} = \theta$, then the inequality becomes $\sin^2 \theta \leq 2 \sin^2 \frac{\theta}{2}$. If $\theta = 60^\circ \Rightarrow \left(\frac{\sqrt{3}}{2}\right)^2 \leq 2 \left(\frac{1}{2}\right)^2 \Rightarrow \frac{3}{4} \leq \frac{2}{4}$!!!! **The Quantum Mechanics will violate Bell's inequality.**

- 1968, **CHSH(Clauser, Horne, Shimony and Holt) inequality.** (Example of a larger set of Bell's inequalities)



They do not decide which property she or he will measure.

Reality and Locality

Reality: physical properties of P_Q, P_R, P_S, P_T have definite values Q,R,S,T which exist independent of observation.

Locality: Timing of measurement \Rightarrow Causally disconnected! The measurement which Alice performed cannot disturb the result of Bob's measurement (or vice versa).

$$QS + RS + RT - QT = (Q + R)S + (R - Q)T = \pm 2 \\ (\text{Suppose } R, Q = \pm 1. \text{ Thus, } (R + Q)S = 0 \text{ or } (R - Q)T = 0)$$

Ensemble average: (The curly words mean operator)

$$E(QS + RS + RT - QT) = \sum p(Q, R, S, T)(QS + RS + RT - QT) \leq \sum p(Q, R, S, T) \cdot 2 = 2$$

Quantum Theory

$$E(QS + RS + RT - QT) = \langle \psi | QS + RS + RT - QT | \psi \rangle = \langle QS \rangle + \langle RS \rangle + \langle RT \rangle - \langle QT \rangle$$

Example

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

$$Q = Z_1 \quad R = X_1 \quad S = \frac{-Z_2 - X_2}{\sqrt{2}} \quad T = \frac{Z_2 - X_2}{\sqrt{2}}$$

$$\langle QS \rangle + \langle RS \rangle + \langle RT \rangle - \langle QT \rangle = 2\sqrt{2} > 2!! \quad \text{\textit{The Quantum Theory violates Bell's inequality.}}$$

- 1981. *Violation of CHSH inequality and an excellent agreement with QM*

- Photon detection efficiency $\eta \approx 0.05$ 0.33
- Separation between trapped ions $d \approx 1m$

A loophole-free experiment will require.

- Spacelike separation between Alice's and Bob's measurements (locality loophole)
- Sufficient large number of detections of the prepared particles (detection loophole)

1. B.Hensen et al., Nature 528, 682 (2015)
2. M.Giustina et al. Physical Review Letters 115, 250401 (2015)
3. L.K.Shalin et al. Physical Review Letters 115, 250402 (2015)

- 1969, The CHSH Game

The game itself does not involve quantum mechanics, but quantum mechanics can help us win it. Alice and Bob are placed in separate rooms and are each given a challenge bit (x and y, respectively). The challenge bits are chosen uniformly at random, and independently of each other. Then Alice sends an answer bit a back to the referee, and Bob sends back an answer bit b . Alice and Bob win the game iff

$$a + b = xy \pmod{2}$$

So if either x or y is 0: a and b should be equal. But if x=y=1: a and b should be different.

Alice and Bob are allowed to agree on a strategy in advance and to share random bits.

Classical Strategy

The classical strategy to maximize winning probability is simply that Alice and Bob always send the referee $a=b=0$ regardless of what x and y are. In this case, Alice and Bob win 75% of the time, losing only if x and y are both 1. The Bell's inequality, in this framework, is just the slightly-boring statement that the maximum classical win probability in the CHSH game is 75%.

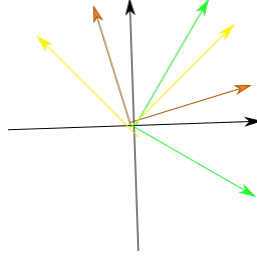
Quantum Strategy

If Alice and Bob had pre-shared Bell pair $\frac{|00\rangle + |11\rangle}{\sqrt{2}} = \frac{|++\rangle + |--\rangle}{\sqrt{2}}$, then there is a better strategy

$$|\frac{\pi}{8}\rangle = \cos(\frac{\pi}{8})|0\rangle + \sin(\frac{\pi}{8})|1\rangle$$

$$|+\rangle = \cos(\frac{\pi}{4})|0\rangle + \sin(\frac{\pi}{4})|1\rangle$$

$$|-\frac{\pi}{8}\rangle = \cos(-\frac{\pi}{8})|0\rangle + \sin(-\frac{\pi}{8})|1\rangle$$



The strategy:

If $x = 0$, Alice measure in $\{|0\rangle, |1\rangle\}$ and if $x = 1$, Alice measure in $\{|+\rangle, |-\rangle\}$. She sets a to 0 if she measures $|0\rangle$ and $|+\rangle$ and 1 if she measures $|1\rangle$ or $|-\rangle$

If $y = 0$, Bob measure in $\{|\frac{\pi}{8}\rangle, |\frac{\pi}{8} + \frac{\pi}{2}\rangle\}$ and if $y = 1$, Bob measure in $\{|-\frac{\pi}{8}\rangle, |-\frac{\pi}{8} + \frac{\pi}{2}\rangle\}$. He sets b to 0 if he measures $|\frac{\pi}{8}\rangle$ or $|-\frac{\pi}{8}\rangle$ and 1 if otherwise.

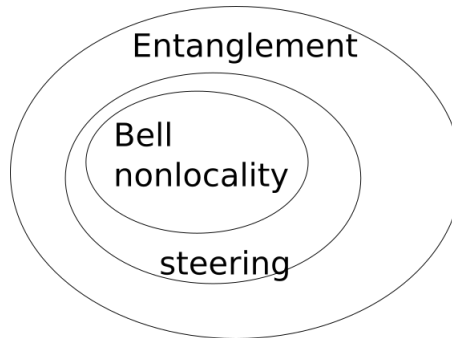
Let's consider the case where Alice gets $x=0$ and measure $|0\rangle$.

She will output $a = 0$, and she and Bob will win iff Bob outputs $b = 0$. Given that Alice measured her qubit already, Bob's qubit collapsed to the $|0\rangle$ state. First suppose $y = 0$, Then Bob measures the state $|0\rangle$ in the $|\frac{\pi}{8}\rangle$ basis. He outputs $b = 0$ if he measure $|\frac{\pi}{8}\rangle$. Thus, the probability that Bob output 0 in this case is $|\langle \frac{\pi}{8} | 0 \rangle|^2 = \cos^2 \frac{\pi}{8} \approx 85\%$. For $y = 1$, Bob measure in $|0\rangle$ in $|-\frac{\pi}{8}\rangle$ basis. The probability that Bob output 0 in this case $\approx 85\%$

Consider the case where Alice gets $x=1$ and Bob gets $y=1$. Alice measure $|-\rangle$

She will output $a = 1$, and she and Bob will win iff Bob outputs $b = 0$. Given that Alice measured her qubit already, Bob's qubit collapsed to the $|-\rangle$ state. Bob measure in $|-\rangle$ in $|-\frac{\pi}{8}\rangle$ basis. The probability that Bob output 0 in this case is still $|\langle - | -\frac{\pi}{8} \rangle|^2 \approx 85\%$

- **Entanglement EPR steering and Bell's nonlocality**



- Entanglement: non-separable to product state
- Bell's nonlocality: violation of Bell's inequality
- Steering: Manipulate the other state.

- **1982, No-cloning theorem**

- Quantum mechanics does not allow the copying of arbitrary quantum state or no arbitrary copying by unitary transformation.

- It is not possible to make a copy of an arbitrary unknown quantum state.

Proof. Suppose we have a quantum machine *data slot* $|\psi\rangle$ and *target slot* $|s\rangle$

$$|\psi\rangle \otimes |s\rangle \rightarrow U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle$$

Proof 1

$$U(|\psi_1\rangle \otimes |\psi_1\rangle) = |\psi_1\rangle \otimes |\psi_1\rangle$$

$$U(|\psi_2\rangle \otimes |\psi_1\rangle) = |\psi_2\rangle \otimes |\psi_2\rangle$$

$$U((|\psi_2\rangle + |\psi_1\rangle) \otimes |\psi_1\rangle) = (|\psi_2\rangle + |\psi_1\rangle) \otimes (|\psi_2\rangle + |\psi_1\rangle)$$

But

$$U((|\psi_2\rangle + |\psi_1\rangle) \otimes |\psi_1\rangle) = U(|\psi_1\rangle \otimes |\psi_1\rangle) + U(|\psi_2\rangle \otimes |\psi_1\rangle) = |\psi_1\rangle \otimes |\psi_1\rangle + |\psi_2\rangle \otimes |\psi_2\rangle \Leftrightarrow$$

Proof 2

$$U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle$$

$$U(|\phi\rangle \otimes |s\rangle) = |\phi\rangle \otimes |\phi\rangle$$

Take the inner product

$$\langle\psi|\phi\rangle \langle\psi|\phi\rangle = \langle\psi| \otimes \langle s| U^\dagger U |\phi\rangle \otimes |s\rangle = \langle\psi|\phi\rangle \langle s|s\rangle = \langle\psi|\phi\rangle$$

So a cloning device can only clone states which are orthogonal to one another and therefore a general quantum cloning device is not possible. Hence, a potential quantum machine cannot clone both $|\psi\rangle = |0\rangle$ and $|\phi\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$ since these states are not orthogonal.

Quantum Circuit Model

Pauli gate $\text{---}\boxed{X}\text{---}$ $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ $\text{---}\boxed{Y}\text{---}$ $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ $\text{---}\boxed{Z}\text{---}$ $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

Hadamard gate $\text{---}\boxed{H}\text{---}$ $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}}(Z + X)$ $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ $H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Phase gate $\text{---}\boxed{S}\text{---}$ $S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$ $\frac{\pi}{8}$ *gate* $\text{---}\boxed{T}\text{---}$ $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}$

$$X^2 = Y^2 = Z^2 = H^2 = I \quad S^2 = Z \quad T^2 = S$$

Rotation operator

$$R_{\hat{n}}(\theta) = e^{-i\frac{\theta}{2}(\hat{n} \cdot \sigma)} = \cos\left(\frac{\theta}{2}\right)I + \sin\left(\frac{\theta}{2}\right)(\hat{n} \cdot \sigma)$$

Unitary single-qubit gate (Rotate qubit on Bloch's sphere)

$$\text{---}\boxed{U}\text{---} \quad U = e^{i\delta}R_z(\alpha)R_y(\gamma)R_z(\beta) = \begin{pmatrix} e^{i(\delta - \frac{\alpha}{2} - \frac{\beta}{2})} \cos\left(\frac{\gamma}{2}\right) & -e^{i(\delta - \frac{\alpha}{2} + \frac{\beta}{2})} \sin\left(\frac{\gamma}{2}\right) \\ e^{i(\delta + \frac{\alpha}{2} - \frac{\beta}{2})} \sin\left(\frac{\gamma}{2}\right) & e^{i(\delta + \frac{\alpha}{2} + \frac{\beta}{2})} \cos\left(\frac{\gamma}{2}\right) \end{pmatrix}$$

Transformation of gate

$$\text{---}\boxed{H}\text{---}\boxed{X}\text{---}\boxed{H}\text{---} \quad HXH = \frac{1}{\sqrt{2}}(X + Z)X\frac{1}{\sqrt{2}}(X + Z) = \frac{1}{2}(X + Z + Z + ZXZ) = Z$$

$$\text{---}\boxed{H}\text{---}\boxed{Y}\text{---}\boxed{H}\text{---} \quad HYH = \frac{1}{\sqrt{2}}(X + Z)Y\frac{1}{\sqrt{2}}(X + Z) = \frac{1}{2}(XYX + ZYX + XYZ + ZYZ) = -Y$$

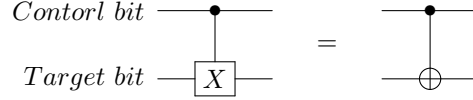
$$\text{---}\boxed{H}\text{---}\boxed{Z}\text{---}\boxed{H}\text{---} \quad HZH = \frac{1}{\sqrt{2}}(X + Z)Z\frac{1}{\sqrt{2}}(X + Z) = \frac{1}{2}(XZX + X + Z + X) = X$$

It can be verified from commutation and anti-commutation relation

$$\{\sigma_i, \sigma_j\} = 2\delta_{ij}I \quad [\sigma_i, \sigma_j] = 2i\epsilon_{ijk}\sigma_k$$

Two qubit gates

CNOT gate (controlled-not)



$$\begin{aligned} |00\rangle &\rightarrow |00\rangle \\ |01\rangle &\rightarrow |01\rangle \\ |10\rangle &\rightarrow |11\rangle \\ |11\rangle &\rightarrow |10\rangle \end{aligned} \quad CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$\begin{aligned} |\psi\rangle &\text{---} \bullet \text{---} |\psi\rangle \\ |\phi\rangle &\text{---} \oplus \text{---} |(\psi + \phi) \bmod 2\rangle \end{aligned}$$

Thus, CNOT gate can reproduce $|0\rangle$ and $|1\rangle$

$$\begin{aligned} |\psi\rangle &\text{---} \bullet \text{---} |\psi\rangle \\ |0\rangle &\text{---} \oplus \text{---} |\psi\rangle \end{aligned}$$

CNOT gate combined with Hadamard gate can transform basis state into Bell state

$$\begin{aligned} |0\rangle &\text{---} \boxed{H} \text{---} \bullet \text{---} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |0\rangle &\text{---} \oplus \text{---} |\psi\rangle \end{aligned}$$

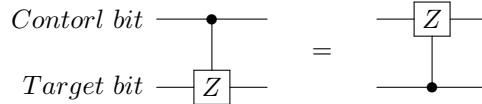
Thus, we can not determine $|\psi\rangle$. $|\psi\rangle$ is entangled with control bit now

$$|Control\rangle \otimes |Target\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

In general, if one of input state is superposed, the output will entangle. It can be computed by matrix.

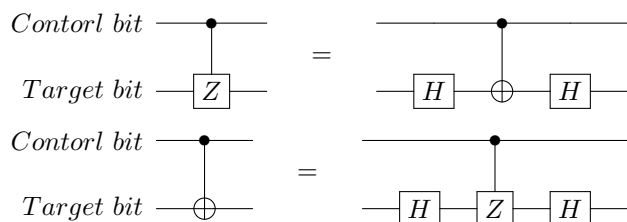
$$\begin{aligned} \alpha|0\rangle + \beta|1\rangle &\text{---} \bullet \text{---} ? \\ \gamma|0\rangle + r|1\rangle &\text{---} \oplus \text{---} ? \end{aligned}$$

CZ gate (controlled-Z)



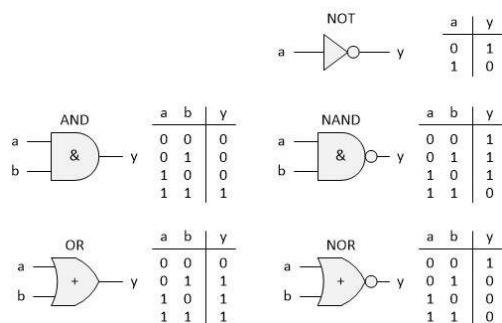
$$\begin{aligned} |00\rangle &\rightarrow |00\rangle \\ |01\rangle &\rightarrow |01\rangle \\ |10\rangle &\rightarrow |10\rangle \\ |11\rangle &\rightarrow -|11\rangle \end{aligned} \quad CZ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

Relation between CNOT and CZ gate

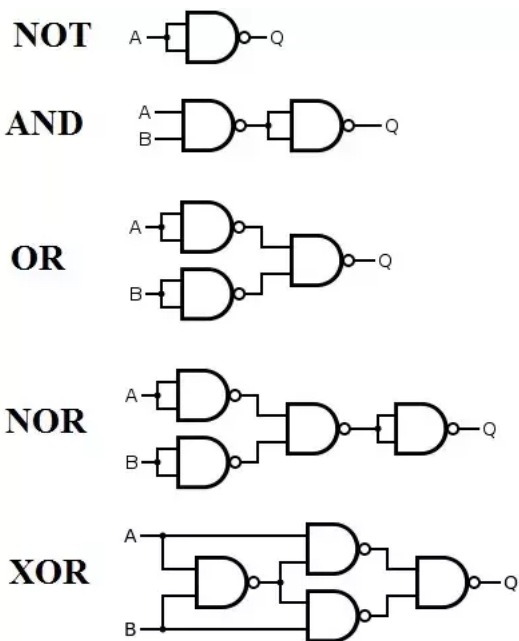


Classical computation

AND, OR, NAND, XOR, NOT



Universal gate: NAND gate can be used to simulate the AND, OR, XOR and NOT gate, provided wires ancilla bits and Fanout are available.



1961, Rolf Landauer: Only process in a computation which are irreversible are those which erase information. Any irreversible operation in a computation is necessarily accompanied by heat dissipation into the environment.

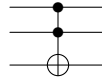
Erasing one bit \Rightarrow reducing the number of state by a factor of 2 \Rightarrow reduce the entropy of the computer by $k_B \ln 2 \Rightarrow$ the entropy of the entire universe cannot decrease $\Delta S_{computer} = -k_B \ln 2 \Rightarrow \Delta S_{rest} \geq k_B \ln 2$

$$\Delta Q_{rest} = T \Delta S_{rest} = k_B T \ln 2$$

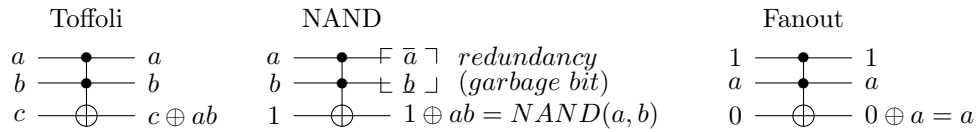
1973, Chales Bennett, main trick to computer using only reversible circuit elements by embedding the gate in a larger reversible gate, possibly making use of some extra ancilla bits.

1982, Ed Fredkin & Tom Toffoli showed independently the way to bulid reversible computation. By avoiding to erase information, one creates and also must carry along a signigicant amount of redundancy.

Toffoli gate



The information processing by any classical NAND logical gate can be replaced by a Toffoli gate and the ability to prepared and ancilla bit. **Toffoli gate is universal for classical computation.**

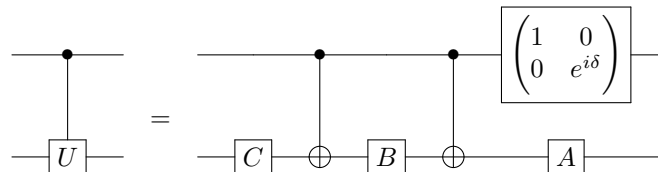


Universal quantum gates

1. Single-qubit gates (arbitrary rotations two orthogonal axes) and CNOT gates (arbitrary entangling gate)
2. A discrete set of universal operation Hadomard gate, $\frac{\pi}{8}$ gate and CNOT gate. H & $\frac{\pi}{8}$ gates can be used to approximate any single qubit unitary operation to arbitrary accuracy. (+ phase gate S: Fault-tolerant gate set. Quantum state is much more fragile than classical memory)

Fault-tolerant QC: In principle, an arbitrarily long QC can be performed reliably provided that the average probability of error per gate is less than a certain critical value (the accuracy/error threshold, which depending on the choice of error correction code (ECC))

Two qubit gate decomposition



$$\forall \quad ABC = I \text{ and } U = e^{i\delta} AXBX C$$

For single qubit state

$$U = e^{i\delta} R_z(\alpha) R_y(\gamma) R_z(\beta)$$

Let

$$A = R_z(\alpha)R_y(\frac{\gamma}{2}) \quad B = R_y(-\frac{\gamma}{2})R_z(-\frac{\alpha+\beta}{2}) \quad C = R_z(\frac{\beta-\alpha}{2})$$

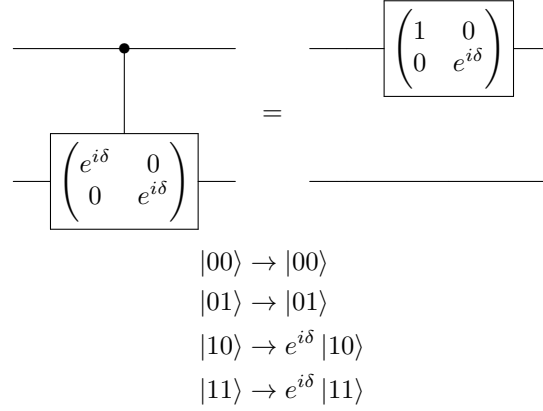
From $XYX = -Y \Rightarrow XR_y(\theta)X = R_y(-\theta)$, thus,

$$XBX = XR_y(-\frac{\gamma}{2})XXR_z(-\frac{\alpha+\beta}{2})X = R_y(\frac{\gamma}{2})R_z(\frac{\alpha+\beta}{2})$$

Thus,

$$AXBXC = R_z(\alpha)R_y(\gamma)R_z(\beta)$$

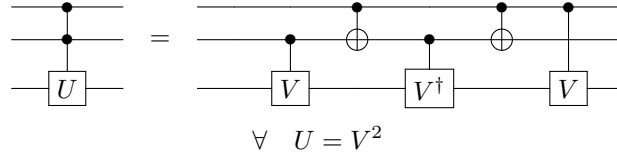
The phase operation



If control qubit $|0\rangle$: Nothing happen(LHS), $ABC = I$ (RHS)

If control qubit $|1\rangle$: U (LHS) , $e^{i\delta}AXBXC$ (RHS)

Three qubit gate decomposition

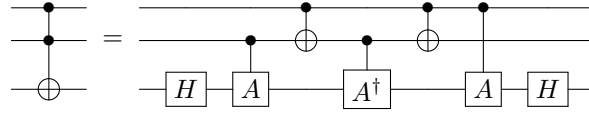


Show

$$\begin{aligned}
 |00i_3\rangle &\rightarrow |00i_3\rangle \\
 |01i_3\rangle &\rightarrow |01i_3\rangle \\
 |10i_3\rangle &\rightarrow |10i_3\rangle \\
 |11i_3\rangle &\rightarrow |11\rangle U |i_3\rangle
 \end{aligned}$$

RHS

$$\begin{aligned}
 |00i_3\rangle &\rightarrow |00i_3\rangle \rightarrow |00i_3\rangle \rightarrow |00i_3\rangle \\
 |01i_3\rangle &\rightarrow |01\rangle V |i_3\rangle \rightarrow |01\rangle V |i_3\rangle \rightarrow |01\rangle V^\dagger V |i_3\rangle \rightarrow |01i_3\rangle \\
 |10i_3\rangle &\rightarrow |10i_3\rangle \rightarrow |11i_3\rangle \rightarrow |11\rangle V^\dagger \rightarrow |10\rangle V^\dagger |i_3\rangle \rightarrow |10\rangle V V^\dagger |i_3\rangle \\
 |11i_3\rangle &\rightarrow |11\rangle V |i_3\rangle \rightarrow |10\rangle V |i_3\rangle \rightarrow |10\rangle V |i_3\rangle \rightarrow |11\rangle V |i_3\rangle \rightarrow |11\rangle V^2 |i_3\rangle
 \end{aligned}$$

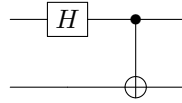


$$\forall \quad A = \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix} \quad V = HAH \quad U = V^2 = HA^2H = HZH = X$$

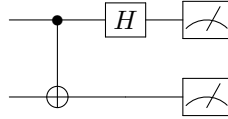
GHZ(Greenberg, Horne, Zeilinger) state

$$\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

Transform the computational basis state to the Bell states

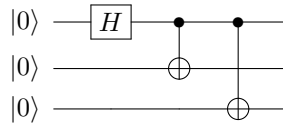


Transform the Bell states to the computational basis state



$$\begin{aligned} |00\rangle &\rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \rightarrow \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\phi^+\rangle \\ |01\rangle &\rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|1\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |11\rangle) \rightarrow \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = |\psi^+\rangle \\ |10\rangle &\rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)|0\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |10\rangle) \rightarrow \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = |\phi^-\rangle \\ |11\rangle &\rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)|1\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |11\rangle) \rightarrow \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = |\psi^-\rangle \end{aligned}$$

Transform computational basis state to the GHZ state



$$|000\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|00\rangle \rightarrow \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)|0\rangle \rightarrow \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

Key elements of quantum circuit model

1. Classical resources
2. A suitable state space
3. Ability to prepare states in the computational basis
4. Ability to perform quantum gates
5. Ability to perform measurements in the computational basis

Application

Superdense coding

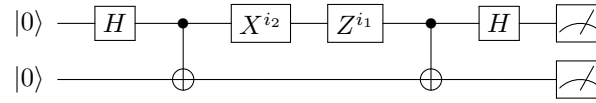
Q: Can Alice transmit 2 classical bits of information to Bob by sending him only one qubit?

Case I

If the qubit has never been contacted with the rest of the world, i.e. isolated qubit, then the answer to this question is "No!" $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ could be tempted to say that single qubit could store infinite amount of information α, β . But there is a catch to extract information we must perform measurement. Infinitely many measurements on identically prepared single-qubit states are required to obtain α and β . Not possible to transmit more than one classical bit of information per qubit.

Case II

Superdense coding protocol enables something similar to be done. (**Key: quantum entanglement**)



- A source generate an EPR(Bell) state pair shared by Alice and Bob.
- Alice applies a local operation (determined by the two classical bits of information $i_1 i_2$) to her single qubit which changes the joint state of the pair.
- Alice then sends her qubit to Bob, who is now able to perform a measurement on the pair, which reveals the values of $i_1 i_2$

$$\begin{aligned}
 i_1 i_2 = 00 & \quad |\phi^+\rangle \rightarrow |\phi^+\rangle \rightarrow 00 \\
 i_1 i_2 = 01 & \quad |\phi^+\rangle \rightarrow |\psi^+\rangle \rightarrow 01 \\
 i_1 i_2 = 10 & \quad |\phi^+\rangle \rightarrow |\phi^-\rangle \rightarrow 01 \\
 i_1 i_2 = 11 & \quad |\phi^+\rangle \rightarrow |\psi^-\rangle \rightarrow 11
 \end{aligned}$$

Summary

Superdense coding is a remarkable procedure because Alice only even comes in contact with one qubit, yet still manage to convey two bits of classical information.

Remark *It is very good example of quantum information process in action (entanglement as a resource)*

Remark *Superdense coding can be viewed as a statement about the interchangibility of physical resources.*

$$1 \text{ entangle bit} + 1 \text{ qubit of communication} \geq 2 \text{ bits of classical information}$$

B P William et al, Phys po Lett 118,050501 (2017) "Superdense coding over optical fibers line with complete Bell-State measurement" ≈ 1.665 classical bits

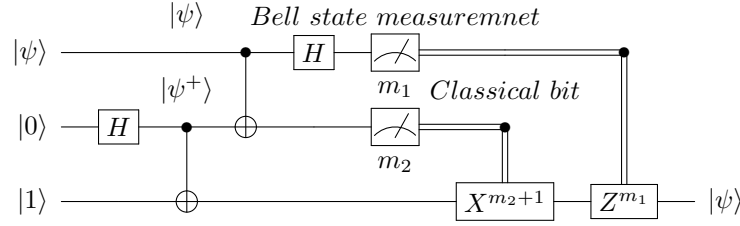
Quantum Teleportation

Q: Can Alice transmit any arbitrary qubit quantum state to Bob using only 2 classical bits of information?

Why doesn't Alice just tell Bob?

1. To specify two complete numbers of a qubit state to arbitrary precisions requires infinite amount of information
2. Alice may not know what her qubit state is

By using quantum entanglement, it becomes possible!



$$\begin{aligned}
|\psi\rangle \otimes |\psi^+\rangle &= (\alpha|0\rangle + \beta|1\rangle) \otimes \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\
&= \frac{\alpha}{\sqrt{2}}(|001\rangle + |010\rangle) + \frac{\beta}{\sqrt{2}}(|101\rangle + |110\rangle) \\
&= \frac{\alpha}{\sqrt{2}}\left(\frac{|\phi^+\rangle + |\phi^-\rangle}{\sqrt{2}}\right)|1\rangle + \frac{\alpha}{\sqrt{2}}\left(\frac{|\psi^+\rangle + |\psi^-\rangle}{\sqrt{2}}\right)|0\rangle + \frac{\beta}{\sqrt{2}}\left(\frac{|\psi^+\rangle - |\psi^-\rangle}{\sqrt{2}}\right)|1\rangle + \frac{\beta}{\sqrt{2}}\left(\frac{|\phi^+\rangle - |\phi^-\rangle}{\sqrt{2}}\right)|0\rangle \\
&= \frac{1}{2}|\psi^+\rangle(\alpha|0\rangle + \beta|1\rangle) + \frac{1}{2}|\psi^-\rangle(\alpha|0\rangle - \beta|1\rangle) + \frac{1}{2}|\phi^+\rangle(\alpha|1\rangle + \beta|0\rangle) + \frac{1}{2}|\phi^-\rangle(\alpha|1\rangle - \beta|0\rangle)
\end{aligned}$$

Alice performs a Bell basis measurement with equal probability $p = \frac{1}{4}$

$$\begin{aligned}
|\psi^+\rangle &\rightarrow |01\rangle \quad \text{Bob } I \\
|\psi^-\rangle &\rightarrow |11\rangle \quad \text{Bob } Z \\
|\phi^+\rangle &\rightarrow |00\rangle \quad \text{Bob } X \\
|\phi^-\rangle &\rightarrow |10\rangle \quad \text{Bob } ZX
\end{aligned}$$

1. "Infinite information" with only two classical bits

It only involves two bits of classical communication. This is rather remarkable when you consider that giving a classical description of Alice's quantum state would require infinite amount of classical information.

2. Blind nature of the protocol

Even more remarkable when you consider that Alice did not even need to know what her quantum state was to perform that protocol. The rules of quantum mechanics prevent her from even determining the state of her system. Yet she and Bob still succeeded in retransmitting that state using just two bits of classical information and a pre-shared Bell state.

3. Violation of light-speed limit

Does quantum teleportation violate the rule saying that information cannot be retransmitted faster than light? After all, doesn't Alice's measurement cause Bob to obtain Alice's state $|\psi\rangle$ or at least something related to it? It turns out that in fact it is not possible for Alice and Bob to use this effect to communicate faster than light. Indeed, Alice must send two bits of classical information to allow Bob to reconstruct the state $|\psi\rangle$. This information is transmitted by classical means at a speed not greater than that of light.

4. Transmission of information not physical system itself

It is the information about the quantum state of the qubit that passed from A to B and not the physical system itself. The physical systems implementing the qubit can be very different in Alice and Bob's location.

5. No information about the state is carried by the two classical bits

The probabilities of the measurement outcomes do not depend on the state being teleported. The classical message from Alice to Bob contains in some sense, no information about the identity of the state being teleported.

6. Consistent with no-cloning theory (No arbitray copying)

$$\text{Alice} : |\psi\rangle \rightarrow |0\rangle \text{ or } |1\rangle \quad \text{Bob} : \text{Bell's state} \rightarrow |\psi\rangle$$

So the unknown quantum state $|\psi\rangle$ vanishes in one place and reappears in another.

7. Close connnection between SC and QT

8. QT and SC can be viewed as a statement about interchangibility of physical resources

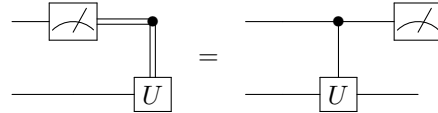
QT: 1 entangle bit + 2 classical bits of communication \geq 1 qubit of communication

SC: 1 entangle bit + 2 qubit of communication \geq 2 bits of classical communication

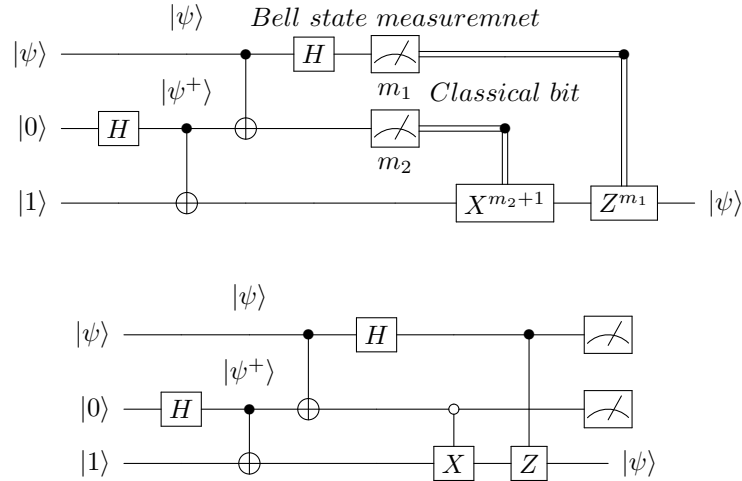
1 qubit communication = 2 classical bits of communication

Principle of defferd measurement

Measurements can be moved from an intermediate state of a quantum circuit to the end of the circuit. If the measurement results are used at any state of circuit to conditionally control subsequent quantum gate, then the classically controlled operation can be replaced by conditional quantum operation.



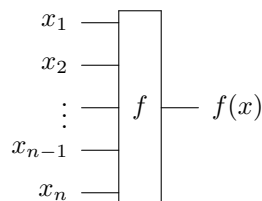
Remark Measurement commutes with quantum gates when the qubit being measured is a control qubit.



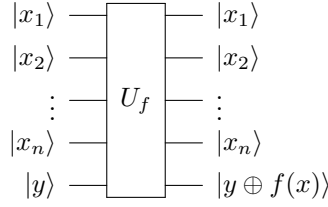
Remark No communication but only teleportation

Function evalution

Classical computer $f : \{0, 1\}^n \rightarrow \{0, 1\}$ n-inputs to 1-output e.g. NAND



In general, can make it reversible if we add own ancillary and quantum mechanically



$$U_f |x_1, x_2 \cdots x_n\rangle |y\rangle = |x_1, x_2 \cdots x_n\rangle |y \oplus f(x_1, x_2 \cdots x_n)\rangle$$

One can show that U_f is also unitary

$$U_f^2 |x\rangle |y\rangle = U_f |x\rangle |y \oplus f(x)\rangle = |x\rangle |(y \oplus f(x)) \oplus f(x)\rangle = |x\rangle |y\rangle$$

Thus, $U_f^2 = I \Rightarrow U_f^{-1} = U_f$. Let's show U_f is Hamiltonian matrix element in computational basis

$$U(x, y; x', y') = \langle x | \langle y | U_f | x' \rangle | y' \rangle = \langle x | x' \rangle \langle y | y' \oplus f(x) \rangle = \delta_{xx'} \delta_{y, y' \oplus f(x)}$$

$$U^\dagger(x, y; x', y') = U_f(x', y'; x, y) = \delta_{x'x} \delta_{y', y \oplus f(x')}$$

They yield the same result. Thus $U_f^\dagger = U_f = U_f^{-1}$ is unitary.

Quantum parallelism

n = 1

$$\begin{aligned} U_f\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |0\rangle\right) &= \frac{1}{\sqrt{2}}(U_f |0\rangle |0\rangle + U_f |1\rangle |0\rangle) \\ &= \frac{1}{\sqrt{2}}(|0\rangle |0 \oplus f(0)\rangle + |1\rangle |0 \oplus f(1)\rangle) \\ &= \frac{1}{\sqrt{2}}(|0\rangle |f(0)\rangle + |1\rangle |f(1)\rangle) \end{aligned}$$

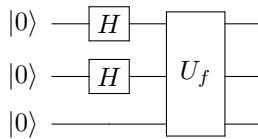
Although U_f is applied once, the output state contains informations about both $f(0)$ and $f(1)$; it is almost as if we have evaluated $f(x)$ for the two values of x simultaneously, a feature known as quantum parallelism

n = 2

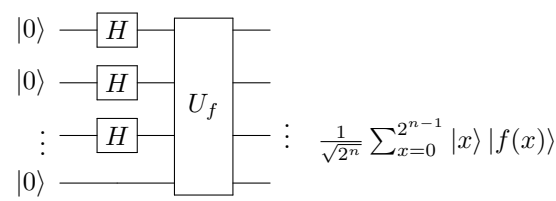
$$U_f\left(\frac{1}{\sqrt{2^2}}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) |0\rangle\right) = \frac{1}{\sqrt{2^2}}(|00\rangle |f(00)\rangle + |01\rangle |f(01)\rangle + |10\rangle |f(10)\rangle + |11\rangle |f(11)\rangle)$$

Remark We can do the 2^2 calculation simultaneously!!!

The Hardmard gate is useful to generate superposition gate



Thus, for n-qubit

$$H^{\otimes n} |0\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle \quad \forall x \text{ is all possible value}$$


$$U_f(H^{\otimes n} |0\rangle \otimes |0\rangle) = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle |f(x)\rangle$$

In some sense, this massive quantum parallelism enables all possible values of the function f to be evaluated simultaneously, even though we apparently only evaluate U_f once. However, this quantum parallelism is not immediately useful! (\because Measurement of the state $\sum_x |x, f(x)\rangle$ would give only $f(x)$ for a single value of $x = x^{(i)}$. Of course, a classical computer can do this easily!) Quantum computer requires something more than just quantum parallelism to be useful; It requires the ability to extract useful information efficiently, e.g. extract information about more than one value of $f(x)$ from superposition state like $\sum_x |x, f(x)\rangle$

Quantum algorithm

Deutsch's algorithm

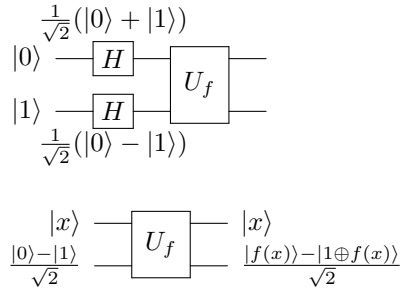
Deutsch's problem: Given a "black box" computing a function $f : \{0,1\} \rightarrow \{0,1\}$. Our task is to determine whether f is a constant or balanced.

Classically: we need to evaluate both $f(0)$ and $f(1)$

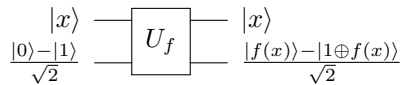
Quantumly: we need only to use the black box for $f(x)$ once!

Deutsch's algorithm: Combine quantum parallelism with quantum interference to solve the problem by using the black box function f only once.

Idea: To put information about the function f in the phase of the quantum state.

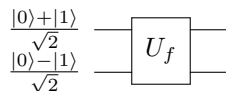


$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

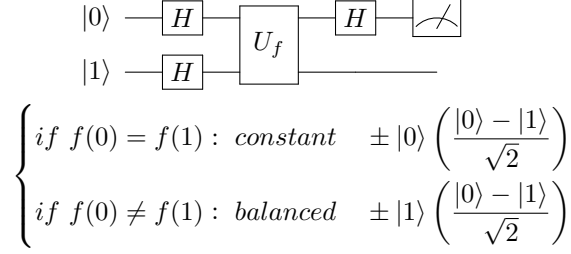
$$\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$


$$\frac{|0\rangle - |1\rangle}{\sqrt{2}} \xrightarrow{U_f} \frac{|f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}}$$

$$\begin{aligned} \text{If } f(x) = 0 &\Rightarrow |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \Rightarrow |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \rightarrow (-1)^{f(x)} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \\ \text{If } f(x) = 1 &\Rightarrow |x\rangle \left(\frac{|1\rangle - |0\rangle}{\sqrt{2}} \right) \Rightarrow |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \rightarrow (-1)^{f(x)} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \end{aligned}$$

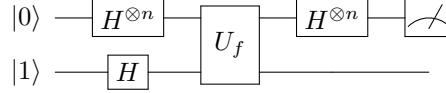


$$\begin{bmatrix} (-1)^{f(0)} \frac{|0\rangle}{\sqrt{2}} + (-1)^{f(1)} \frac{|1\rangle}{\sqrt{2}} \end{bmatrix} \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) = \begin{cases} \text{if } f(0) = f(1) : \text{constant} & \pm \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \\ \text{if } f(0) \neq f(1) : \text{balanced} & \pm \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \end{cases}$$



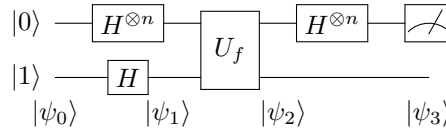
So by measuring 1st qubit, we may determine a global property $f(0) \oplus f(1)$ using one evaluation of $f(x)$

For n-qubit case



Classically: The best deterministic classical algorithm requires $\left(\frac{2^n}{2} + 1\right)$

Quantumly: Could solve the problem with only one query.



$$\begin{aligned} |\psi_0\rangle &= |0\rangle^{\otimes n} |1\rangle \\ |\psi_1\rangle &= \sum_{x \in \{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}} \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \\ |\psi_2\rangle &= \sum_x \frac{(-1)^{f(x)} |x\rangle}{\sqrt{2^n}} \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \\ |\psi_3\rangle &= \sum_z \sum_x \frac{(-1)^{x \cdot z + f(x)}}{2^n} |z\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \end{aligned}$$

Remark $H|x\rangle = \sum_{z=0,1} \frac{(-1)^{xz}}{\sqrt{2}} |z\rangle$; $H^{\otimes n} |x_1 \dots x_n\rangle = \frac{\sum_{z_1 \dots z_n} (-1)^{x_1 z_1 + \dots + x_n z_n} |z_1 \dots z_n\rangle}{\sqrt{2^n}}$; $H^{\otimes n} |x\rangle = \frac{\sum_z (-1)^{x \cdot z}}{\sqrt{2^n}} |z\rangle$

For $|z\rangle = |0\rangle^{\otimes n}$ state, the amplitude is $\sum_x \frac{(-1)^{f(x)}}{2^n}$

1. If f is constant, $\sum_x \frac{(-1)^{f(x)}}{2^n} = \pm 1 \sum_x \frac{1}{2^n} = \pm 1 \therefore |\psi_3\rangle$ is of unit length \Rightarrow all other amplitudes must be zero.
2. If f is balanced. $\sum_x \frac{(-1)^{f(x)}}{2^n} = 0$ (positive and negative contributions cancel) \Rightarrow A measurement must yield a result other than zero on at least one qubit in the data register qubits.

\therefore If one measures all 0's, $|0\rangle^{\otimes n}$, then the function is constant otherwise the function is balanced.

Shor's factoring algorithm

$$\text{Quantum phase estimation algorithm} \begin{cases} \text{Quantum Fourier transformation} \\ H \text{ gates} \\ \text{Controlled} - U \text{ gates} \end{cases}$$

Equivalence of factoring and order finding

Solving order finding using quantum phase estimation algorithm

Quantum Fourier transform (QFT)

- One of the most useful ways of solving a problem in mathematics and computer science is to transform it into some other problem for which a solution is known.
- One such transformation is the discrete Fourier transform DFT. Take as input a vector of N complex numbers $x_0, x_1 \dots x_{N-1}$ and then outputs the sequence $y_0, y_1 \dots y_{N-1}$ defined by

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi i j k / N} = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \omega^{jk}, \quad \forall \omega = e^{2\pi i / N}$$

The inverse DFT

$$x_j = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} y_k e^{-2\pi i j k / N} = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} y_k \omega^{-jk}, \quad \forall \omega = e^{2\pi i / N}$$

If we let x and y be N -by-1 vectors, then $y = Dx$ $\forall D_{kj} = \frac{1}{\sqrt{N}} \omega^{jk}$ and $x = D^{-1}y$ $\forall D_{kj}^{-1} = \frac{1}{\sqrt{N}} \omega^{-jk}$

$$D = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & 1 & \dots & \dots \\ 1 & \omega & \omega^2 & \omega^3 & \dots & \dots \\ 1 & \omega^2 & \omega^4 & \omega^6 & \dots & \dots \\ 1 & \omega^3 & \omega^6 & \omega^9 & \dots & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots & \ddots \end{pmatrix}$$

- QFT: is a DFT of the amplitude of a quantum state. Suppose we have the state

$$|\psi\rangle = x_0 |0\rangle + x_1 |1\rangle + x_2 |2\rangle \dots + x_{N-1} |N-1\rangle$$

The QFT produces the state

$$|\phi\rangle = y_0 |0\rangle + y_1 |1\rangle + y_2 |2\rangle \dots + y_{N-1} |N-1\rangle$$

QFT is defined to be a linear operator with the following action on the basis state

$$QFT(|j\rangle) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i j k / N} |k\rangle$$

Thus

$$QFT\left(\sum_{j=0}^{N-1} x_j |j\rangle\right) = \sum_{j=0}^{N-1} x_j QFT(|j\rangle) = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \sum_{k=0}^{N-1} x_j e^{2\pi i j k / N} |k\rangle = \sum_{k=0}^{N-1} y_k |k\rangle$$

Example

$$|\psi\rangle = \frac{2}{\sqrt{5}} |0\rangle + \frac{1}{\sqrt{5}} |1\rangle ; D = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & e^{2\pi i / 2} \end{pmatrix} ; |\psi'\rangle = QFT(|\psi\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} \frac{2}{\sqrt{5}} \\ \frac{1}{\sqrt{5}} \end{pmatrix} = \begin{pmatrix} \frac{3}{\sqrt{10}} \\ \frac{1}{\sqrt{10}} \end{pmatrix}$$

- Quantum circuit for QFT

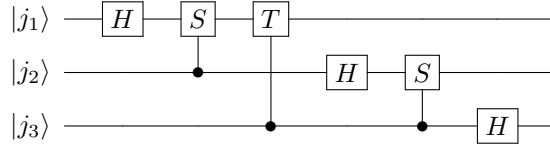
Take $N = 2^n$, n is some integer, and the basis states $|0\rangle, |1\rangle \dots |2^n - 1\rangle$ is the computational basis for an n -qubit QC. Notation: $j = j_1 j_2 \dots j_n = j_1 2^{n-1} + j_2 2^{n-2} + \dots + j_n 2^0 = \sum_{m=1}^n j_m 2^{n-m}$. Binary

fraction: $0.j_l j_{l+1} \dots j_m = \frac{j_l}{2} + \frac{j_{l+1}}{2^2} \dots + \frac{j_m}{2^{m-l+1}}$

$$\begin{aligned}
QFT(|j\rangle) &= \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i j k / 2^n} |k\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i j \sum_{l=1}^n k_l 2^{n-l} / 2^n} |k\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{k_1=0}^1 \sum_{k_2=0}^1 \dots \sum_{k_n=0}^1 e^{2\pi i j \sum_{l=1}^n k_l 2^{-l}} |k_1, k_2, \dots, k_n\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{k_1=0}^1 \sum_{k_2=0}^1 \dots \sum_{k_n=0}^1 \otimes_{l=1}^n e^{2\pi i j k_l 2^{-l}} |k_l\rangle \\
&= \frac{1}{\sqrt{2^n}} \otimes_{l=1}^n \left[\sum_{k_l=0}^1 e^{2\pi i j k_l 2^{-l}} |k_l\rangle \right] \\
&= \frac{1}{\sqrt{2^n}} \otimes_{l=1}^n [|0\rangle + e^{2\pi i j 2^{-l}} |1\rangle] \\
&= \frac{1}{\sqrt{2^n}} \left[(|0\rangle + e^{2\pi i 0 \cdot j_n} |1\rangle) \otimes (|0\rangle + e^{2\pi i 0 \cdot j_{n-1} j_n} |1\rangle) \dots \otimes (|0\rangle + e^{2\pi i 0 \cdot j_1 j_2 \dots j_n} |1\rangle) \right]
\end{aligned}$$

Remark The trick about the Fast Fourier Transform (FFT) is that it only uses the terms of $e^{2\pi i xy / 2^n}$ that correspond to the first circle, i.e. the terms for which $\frac{xy}{2^n} < 1$

Example Three qubit QFT



$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i / 2^2} \end{pmatrix} \quad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i / 2^3} \end{pmatrix} \quad \forall j_1 = 0 \text{ or } 1$$

$$\begin{aligned}
|j_1\rangle &\rightarrow \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i 0 \cdot j_1 j_2 j_3} |1\rangle) \\
|j_2\rangle &\rightarrow \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i 0 \cdot j_2 j_3} |1\rangle) \\
|j_3\rangle &\rightarrow \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i 0 \cdot j_3} |1\rangle)
\end{aligned}$$

Thus, if we can construct $R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i / 2^k} \end{pmatrix}$

- Need swap gates at the end which reverse the order of qubits. This is the desired output from QFT
- This construction also proves that QFT is unitary since each gate in the circuit is unitary.
- The best classical algorithm (FFT), which computes the FT using $\mathcal{O}(n2^n)$ gates.
- How many gates does this QFT circuit use ?
 $(1H + (n-1) \text{ conditional rotation gates}) + (1H + (n-2)) + \dots + (1H) + \frac{n}{2} \text{ swap gate} \approx \mathcal{O}(n^2)$

Exponential speed up !!!

- Can we use QFT to speed up the computation of FT?
Unfortunately, the answer is not positive \because there is no known efficient way to do the following

1. Amplitudes in quantum state cannot be directly accessed by quantum measurement.
 2. In general, no known way to efficiently prepare a generic initial state to be Fourier transformed
 $|\psi\rangle = \sum_j x_j |j\rangle$
- Thus finding use for QFT is more subtle than we might have hope.
 - Quantum algorithms find a way to use QFT and extract efficiently useful information from the quantum state.

Quantum phase estimation (QPE)

QFT is the key to a general procedure known as QPE, and QPE is the key to many quantum algorithms (e.g. Quantum factoring, discrete logarithm, hidden subgroup problems)

Question: Suppose U is a unitary operator with eigenvector $|u\rangle$ and corresponding eigenvalue $e^{2\pi i \phi_u}$

$$U |u\rangle = e^{2\pi i \phi_u} |u\rangle$$

The goal of QPE is to obtain a good estimate of ϕ_u

Assume we have available black boxes (sometimes know as Oracle) capable of

1. Preparing the state $|u\rangle$
2. Performing the controlled- U^{2^j} operations for suitable non-negative integers j .

This seems like a bit of a cheat: after all, in practice aren't we going to need to know how to do these things. The answer to this question is yes, and in specific examples, such as factoring, we will discuss how these black box operations are to be performed.

GRAPHHHHHHHHHHHH!!

QPE uses two registers

- The 1^{st} register: t -qubits, which will be measured to obtain our estimate about ϕ
- The 2^{nd} register: to which U can be applied $U |u\rangle = e^{2\pi i \phi_u} |u\rangle$ contains as many qubits as is necessary to store $|u\rangle$.

How can we choose t depends on

1. The number of digits of accuracy we wish to have in our estimate for ϕ
2. With what probability we wish the QPE to be successful.

$$\left(C - U^{2^j} \right) \left[\frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \right] |u\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle |u\rangle + |1\rangle U^{2^j} |u\rangle \right) = \frac{1}{\sqrt{2}} \left(|0\rangle + |1\rangle e^{2\pi i 2^j \phi} \right) |u\rangle$$

Thus, the output state after acting on t -qubit is

$$\begin{aligned} & \frac{1}{\sqrt{2^t}} (|0\rangle + e^{2\pi i 2^{t-1} \phi} |1\rangle) (|0\rangle + e^{2\pi i 2^{t-2} \phi} |1\rangle) \cdots (|0\rangle + e^{2\pi i 2^0 \phi} |1\rangle) = \frac{1}{\sqrt{2^t}} \sum_{k=0}^{2^t-1} e^{2\pi i \phi k} |k\rangle \\ & \rightarrow \frac{1}{\sqrt{2^t}} (|0\rangle + e^{2\pi i 0 \cdot \phi_t} |1\rangle) (|0\rangle + e^{2\pi i 0 \cdot \phi_{t-1} \phi_t} |1\rangle) \cdots (|0\rangle + e^{2\pi i 0 \cdot \phi_1 \cdots \phi_{t-1} \phi_t} |1\rangle) \end{aligned}$$

Comparing this equation with the product form for QFT. We see that the output state after the inverse QFT is the product state $|\phi_1 \phi_2 \cdots \phi_t\rangle$

The second stage: Apply the inverse QFT on the 1^{st} register

The third stage: Read out the state of the 1^{st} register by doing a measurement in the computational basis.

Suppose $\phi = 0.\phi_1 \phi_2 \cdots \phi_t$ can be expressed exactly in t qubits. A measurement in the computational basis therefore gives us ϕ exactly.

Performance and requirement (not ideal case)

Above analysis applies to the idea case where ϕ can be written exactly with a t -bit binary expression. What happens when this is not the case? \Rightarrow Still produces a pretty good approximation to ϕ with high probability. Let b be the integer in the range 0 to $2^t - 1$ such that

$$\frac{b}{2^t} = 0.b_1b_2 \dots b_t \text{ is the best } t\text{-bit approximation to } \phi \text{ which is less than } \phi$$

Suppose the outcome of the final measurement is m . We aim to bound the probability of obtaining $|m - b| > e$, where e is positive integer characterizing our desired tolerance to error

$$P(|m - b| > e) \leq \frac{1}{2(e - 1)}$$

Suppose we wish to approximate ϕ to an accuracy 2^{-n} , that is we choose

$$e = 2^{t-n} - 1 = 2^p - 1 \quad t = n + p \text{ qubits}$$

Thus,

$$P(|m - b| > e) \leq \frac{1}{2[(2^p - 1) - 1]}$$

Then, the probability of obtaining an approximation correct to this accuracy is at least

$$1 - P(|m - b| > e) = 1 - \frac{1}{2[(2^p - 1) - 1]} = 1 - \epsilon$$

To successfully obtain ϕ accurate to n bits with probability of success at least $1 - \epsilon$, we choose

$$\epsilon = \frac{1}{2(2^p - 2)} \Rightarrow 2^p = 2 + \frac{1}{2\epsilon} \Rightarrow p = \log \left(2 + \frac{1}{2\epsilon} \right)$$

Thus,

$$t = n + \log \left(2 + \frac{1}{2\epsilon} \right)$$

What if we do not know how to prepare the eigenstate $|u\rangle$ of U ?

Suppose we prepare a state $|\psi\rangle = \sum_u c_u |u\rangle$, $U|u\rangle = e^{2\pi i \phi_u} |u\rangle \therefore$ Performing the QPE procedure will give an output state close to $\sum_u c_u |\tilde{\phi}_u\rangle |u\rangle$, where $\tilde{\phi}_u$ is a pretty good approximation of ϕ_u . Reading out the 1^{st} register will give us $\tilde{\phi}$, where u is chosen at random with probability $|c_u|^2$. This procedure allows us to avoid preparing a (possibly unknown) eigenstate out the cost of introducing some additional randomness into the algorithm.

Summary

Input:

1. A black box which performs a controlled- U^j operation for integer j
2. An eigenstate $|u\rangle$ of U with eigenstate $e^{2\pi i \phi_u}$
3. 1^{st} register of $t = n + \log \left(2 + \frac{1}{2\epsilon} \right)$ qubits initialized to $|0\rangle$

Output: An n -bit approximation $\tilde{\phi}_u$ to ϕ_u

Runtime: $\mathcal{O}(t^2)$ operations and one call to $C - U^j$ black box succeed with.

Procedure:

1. $|0\rangle^{\otimes t} |u\rangle$ Initial state
2. $\frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle |u\rangle$ Create superposition
3. $\frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} e^{2\pi i j \phi_u} |j\rangle |u\rangle$ Apply black box
4. $|\tilde{\phi}\rangle |u\rangle$ Apply inverse QFT
5. $\tilde{\phi}_u$ Measure the 1^{st} register

RSA cryptosystem protocol (Asymmetric, public cryptography)

Public-key cryptosystem: Alice wishes to create a public key to enable people to send her message and a matching private key with which she can read the message.

1. She chooses two very large enough prime number p and q and compute the product $N=pq$.
2. She also picks at a random number $e < \Phi(N) = (p-1)(q-1)$, which is co-prime to $\Phi(N)$, i.e. $\gcd(e, \Phi(N)) = 1$
3. She computes d such that $ed = 1 \pmod{\Phi(n)}$
4. She publishes the pair (N, e) as her public key, so any body has access to it and use it to send her message.
5. The pair (N, d) is kept to herself as her private key, so only Alice can decrypt the messages that were encrypted by means of the public key.
6. Suppose Bob wants to send a string of bits to Alice
 - (a) Breaks the message up into blocks of length $\log N$ bits each.
 - (b) Regards each single block of bits as encoding a number $x_i, 0 < x_i < N \Rightarrow$ Use the public key (N, e) to encode x_i by $x_i^e \pmod N$
7. To decode the encrypted block, Alice raise the message to the d^{th} power, obtaining

$$(x_i^e)^d \pmod N = x_i \pmod N$$

Shor's Algorithm

Best current method to factor a large semi-prime number on a classical computer requires

$$\exp\left(\mathcal{O}(n^{\frac{1}{3}} \log^{\frac{2}{3}} n)\right)$$

Shor's algorithm

$$\mathcal{O}(n^2 \log n \log \log n)$$

Equivalence of factoring and order finding

Shor's algorithm hinges on a result from number theory. The function $F(a) = x^a \pmod N$ is a periodic function, where x is an integer co-prime to N .

Suppose r is the period of $F(a)$, we know $x^0 \pmod N = 1$, $x^r \pmod N = 1$ and $x^{2r} \pmod N = 1$

$$(x^r - 1) \pmod N = 0 \Rightarrow (x^{r/2} + 1)(x^{r/2} - 1) = kN = km_1m_2 \Rightarrow \begin{cases} \gcd(x^{r/2} - 1, N) = m_1 \\ \gcd(x^{r/2} + 1, N) = m_2 \end{cases}$$

Thus, it is equivalent to factoring N .

Order finding: For positive integers x and N , $x < N$, with no common factors, then order $x \bmod N$ is defined to be the least positive integer r such that $x^r = 1 \bmod N$

- The order finding problem is to determine the order for some specified x and N
- The order finding problem is believed to be a hard problem in a classical computer.
- Calculating x^a for an exponential number of a 's would take exponential time on a classical computer.
- Shor's algorithm utilize quantum parallelism to perform the exponential number of operations in one step!!

Solving order-finding using QPE

$$x^r = 1 \bmod N$$

Consider the operator

$$U|y\rangle = |xy \bmod N\rangle \quad \forall y \in \{0, 1\}^L, L \approx \log_2 N \text{ number of bits needed to specify } N$$

As x and N are co-prime, this operator U is unitary.

$$x \cdot x^{r-1} = 1 \bmod N \Rightarrow x^{r-1} \text{ is an inverse for } x \bmod N$$

$$U^r|y\rangle = U^{r-1}|xy \bmod N\rangle = |x^r y \bmod N\rangle = |y \bmod N\rangle = |y\rangle$$

Thus, $U^r = I$. U 's eigenvalues have the form $e^{2\pi i s/r}$ for some integer s . \therefore If we can apply QPE to find $\frac{s}{r}$, we will have obtained a considerable amount of information to help us determine r .

What are the eigenvalues and eigenvectors of U ?

One set is

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi i s k/r} |x^k \bmod N\rangle \quad \forall 0 \leq s \leq r-1$$

$$U|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi i s k/r} |x^{k+1} \bmod N\rangle = e^{2\pi i s/r} |u_s\rangle$$

Two important requirements to be able to use QPE procedure

1. Must have efficient procedure to implement a $C - U^2$ operation.

Using a procedure known as modular exponentiation with which we can implement the entire sequence of $C - U^2$ operations applied by the QPE procedure using $\mathcal{O}(L^3)$ gates.

Modular exponentiation:

In order finding algorithm, we wish to compute

$$\begin{aligned} |z\rangle|y\rangle &\rightarrow |z\rangle U^{z_t 2^{t-1}} \dots U^{z_2 2^1} U^{z_1 2^0} |y\rangle = |z\rangle |x^{z_t 2^{t-1}} \dots x^{z_2 2^1} x^{z_1 2^0} y \bmod N\rangle \\ &= |z\rangle |x^z y \bmod N\rangle = |z\rangle |x^z \bmod N\rangle |y \bmod N\rangle \end{aligned}$$

Classical computation:

- (a) By square and multiply, a total of $(t-1)$ squaring operations at a cost of $\mathcal{O}(L^2)$ each. The total cost of $\mathcal{O}(L^3)$ for the 1^{st} stage.
- (b) $x^z \bmod N = (x^{z_t 2^{t-1}} \bmod N)(x^{z_{t-1} 2^{t-2}} \bmod N) \dots (x^{z_1 2^0} \bmod N)$ performing $t-1$ modular multiplications with a cost of $\mathcal{O}(L^2)$ for each multiplication. The total cost of $\mathcal{O}(L^3)$ for the second stage.

$$\begin{array}{c}
|y\rangle \text{ --- } \diagup \text{---} \boxed{U_f} \text{---} \diagdown \text{---} |y\rangle \\
|z\rangle \text{ --- } \diagup \text{---} \boxed{U_f} \text{---} \diagdown \text{---} |z \oplus f(y)\rangle
\end{array}$$

$$|y, 0\rangle \rightarrow |y, 0 \oplus x^{2^j} y \bmod N\rangle \rightarrow |y \oplus x^{-2^j} (x^{2^j} y \bmod N), x^{2^j} y \bmod N\rangle = |y \oplus y, x^{2^j} y \bmod N\rangle = |0, x^{2^j} y \bmod N\rangle$$

In performing the QPE procedure, if we use $t = n + \log 2 + \frac{1}{2\epsilon}$ qubits in the 1^{st} register (e.g. $n=2L+1$) and prepare the second register in the state $|1\rangle$, it follows that for each s chosen uniformly at random from the range $0 \leq s \leq r-1$, we will obtain an estimate of the phase $\phi \approx \frac{s}{r}$ accurate to $n=2L+1$ bits, with prob at least $\frac{1}{r}(1-\epsilon)$

The continued fraction expansion: How to obtain the desire answer, r , from the result of the QPE, $\phi \approx \frac{s}{r}$? Given that we only know ϕ to $n=2L+1$ bits, but we also know that it is a rational number. If we could compute the nearest such fraction to ϕ , we might obtain r .

Theorem Suppose $\frac{s}{r}$ is a rational number such that

$$|\frac{s}{r} - \phi| \leq \frac{1}{2r^2}$$

Then $\frac{s}{r}$ is a convergent of continued fraction for ϕ and thus can be computed in $\mathcal{O}(L^3)$ operations using the CF algorithm.

To summerize, given ϕ the CF algorithm efficiently produces number s' and r' with no common factor such that $\frac{s'}{r'} = \frac{s}{r}$. The number r' is our candidate for the order. We can check to see whether it is the order by calculating $x^{r'} \bmod N$ and seeing if the result is 1, i.e. $x^{r'} \bmod N = 1$. If so, then r' is the order of $x \bmod N$, and we are done.

Definition A finite simple CF is defined by

$$[a_0, a_1, a_2, \dots, a_M] = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\ddots + \frac{1}{a_M}}}}$$

We define the n^{th} convergent ($0 \leq n \leq M$) to this CF to be $[a_0, a_1, \dots, a_n]$

Theorem Let a_0, a_1, \dots, a_M be a sequence of positive numbers, then

$$[a_0, a_1, \dots, a_n] = \frac{p_n}{q_n}$$

where p_n and q_n are real numbers defined inductively by

$$p_0 = a_0 \quad q_0 = 1; \quad p_1 = 1 + a_0 a_1 \quad q_1 = a_1; \quad p_n = a_n p_{n-1} + p_{n-2} \quad q_n = a_n q_{n-1} + q_{n-2}$$

Performance of order-finding algorithm

How can order-finding algorithm fail?

- The QPE might produce a bad estimate to $\frac{s}{r}$. This occurs with probability at most ϵ , and can be made small with negligible increase in the size of t .
- $\frac{s}{r}$ might have a common factor, then the number r' returned by the CF algorithm could be a factor of r and not r itself.

One way around the problem is the following. The idea is to repeat the QPE-CF procedure twice obtaining $\frac{s'_1}{r'_1}$ and $\frac{s'_2}{r'_2}$, provided that s'_1 and s'_2 have no common factors, r may be extracted by taking the least common multiple of r_1 and r_2 .

2. Must be able to efficiently prepare an eigenstate $|u_s\rangle$ with a non-trivial eigenvalue or at least a superposition of such eigenstate.

Preparing $|u_s\rangle$ directly requires that we know r , so it is impossible. Fortunately, there is a clever observation which allows us to circumvent this problem. The observation is

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = |1\rangle \left(\because \sum_{s=0}^{r-1} e^{-2\pi i s k / r} = r \delta_{k0} \right)$$

Summary: Quantum order-finding algorithm

Input:

1. A black box U_{xN} which perform the transformation $|j\rangle |k\rangle \rightarrow |j\rangle |x^j k \bmod N\rangle$ for x co-prime to the L bit N .
2. $t = (2L + 1) + \log 2 + \frac{1}{2\epsilon}$ qubits initialized to $|0\rangle$
3. L qubits initialized to $|1\rangle$

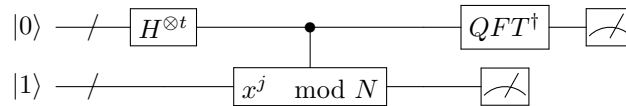
Output: The least integer $r > 0$ such that $x^r = 1 \bmod N$

Runtime: $\mathcal{O}(L^3)$ operations. Succeeds with prob $\mathcal{O}(1 - \epsilon) \approx \mathcal{O}(1)$

Procedure

1. $|0\rangle |1\rangle$ initial state
2. $\rightarrow \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle |1\rangle$ create superposition on the 1^{st} register.
3. $\rightarrow \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle |x^j \bmod N\rangle = \frac{1}{\sqrt{2^t}} \frac{1}{\sqrt{r}} \sum_{s=0}^r \sum_{j=0}^{2^t} e^{2\pi i s j / r} |j\rangle |u_s\rangle$ apply $U_{x,N}$
4. $\rightarrow \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |\frac{s}{r}\rangle |u_s\rangle$ apply QFT^\dagger to the 1^{st} register.
5. $\rightarrow \frac{s_m}{r} |u_s\rangle$ measure the 1^{st} register.
6. $\rightarrow r$ apply CF algorithm

Let us consider



Performing a measurement in the computational basis to determine the bit values in the 2^{nd} register. Suppose the result is m where $m = x^a \bmod N$