Quantum Computation and Quantum Information

Hsi-Sheng Goan

1 Overview

53 quantum bits (Quantum supremency)
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 momory few days

2.3 implementation

- 1998 proposol: Sillicon-based electron-immediated nuclear spin (2012 implement)
- Electron spins in quantum dots
- 2015 two-quibt 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 temperture

2.5 HQC

Hybrid Quantum-Classical (HQC) Algorithm
Variational quantum circuit algorithm
Data encoding scheme
Vairational 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) Feynamn 1982
Quantum Teleportation (1993) Bennett et al.
Quantum superdense coding (1992)Bemett 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, qudratic speed up

What is the killer application ?

4 Quantum Information Sciences (QIS)

To catch all aspectes of QC & QI

4.1 Fundamental questions of IS

1. Given a physical resoures - 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 intimidateing.

By contrast, the mathematics used in application to QIS is "relatively painless". Do not need to read the tranditional 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 therory of the world in its own right? No!! msiconception!!
It is a framework for the development of physical theory.

QM consists of a set of mathematical postulates:

4 supensingly simple postulates witch lay the ground rules for our desceiption of the world.

Most physicsts 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

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

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?
   Projectile measurement → POVM measurement, Genernalized 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.

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}_{in\ |0\rangle,|1\rangle\ basis} = \alpha\begin{pmatrix}1\\0\end{pmatrix} + \beta\begin{pmatrix}0\\1\end{pmatrix}$$

$$\langle\psi|\psi\rangle = \begin{pmatrix}\alpha^* & \beta^*\end{pmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = |\alpha|^2 + |\beta|^2 = 1$$

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

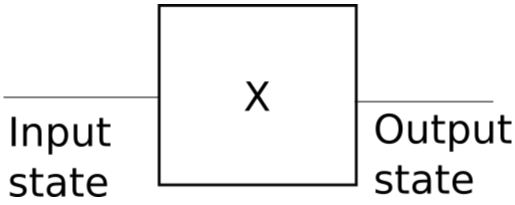
$$|\psi(t_2)\rangle = U(t_1,t_2)|\psi(t_1)\rangle \qquad U \textit{ is unitary to preserve normalize}$$

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)*

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



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.

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

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

Quantum NOT gate

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

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

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 $\left|\psi\right\rangle$ 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*

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

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***

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

$$\begin{aligned}M_0 &= \left|0\right\rangle\left\langle 0\right| = M_0^\dagger \\ M_1 &= \left|1\right\rangle\left\langle 1\right| = M_1^\dagger\end{aligned}$$

- *Probability*

$$\begin{aligned}p(0) &= \langle\psi|M_0^\dagger M_0|\psi\rangle = \langle\psi|M_0|\psi\rangle = |\alpha|^2 \\ p(1) &= \langle\psi|M_1^\dagger M_1|\psi\rangle = \langle\psi|M_1|\psi\rangle = |\beta|^2\end{aligned}$$

- *Post-Measurement*

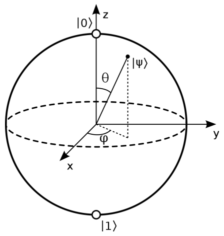
$$\frac{M_m\left|\psi\right\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}} = \frac{\alpha}{\sqrt{|\alpha|^2}}\left|0\right\rangle = \frac{\alpha}{|\alpha|^2}\left|0\right\rangle = e^{i\theta}\left|0\right\rangle$$

Remark

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

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

Bloch Shpere representation



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

$|+\rangle_n$ 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

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

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 $|\psi_i\rangle$, $1 \le i \le n$ 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 completness 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. $\langle\psi_i|\psi_j\rangle \ne 0$ for $i \ne j$

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

$$\mathcal{M} = \sum_m mP_m$$

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 usderstood as a special case of general measurement*

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

From postulate of projective measurement, $M_m^\dagger = M_m (Hermition)$ *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 $x, y \in \mathbb{R}$

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

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

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

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

By the Cauchy-Schwartz inequality:

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

Hence

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

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

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

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

There is an intrinsic limit to the accureacy 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 probabilriy of different outcomes m. The complete set* $\{E_m\}$ *is known as POVM.* E_m *is the POVM element.*

Example

$$|\psi_1\rangle = |0\rangle$$
$$|\psi_2\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

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

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

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.*