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 $\rightarrow$ 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*

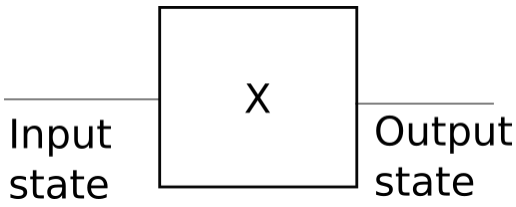
$$|\psi(t_2)\rangle = U(t_1,t_2)\,|\psi(t_1)\rangle \qquad U \text{ is unitary to preserve normalize}$$

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)*

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



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:*

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

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***

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

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

- *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*

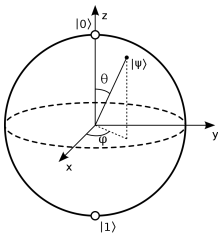
$$\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}} = \frac{\alpha}{\sqrt{|\alpha|^2}}|0\rangle = \frac{\alpha}{|\alpha|^2}|0\rangle = e^{i\theta}|0\rangle$$

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



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

$|+\rangle_n$ 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

Distinguishibility: 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. $\langle\psi_i|\psi_j\rangle \neq 0$ for $i \neq j$

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

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

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* $M_m M_{m'} = M_m \delta_{mm'}(OrthogonalProjector)$ $p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle = \langle\psi|M_m|\psi\rangle$ *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 $x, y \in \mathbb{R}$

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

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

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

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

By the Cauchy-Schwartz inequality:

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

Hence

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

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

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

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

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

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

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.

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*

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

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

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

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

Example

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

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 parallelly, we have to do many measurements to get the information of the amplitute. Thus, we often use interference to left the amplitute of interest 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 tis 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 1^{st} *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 2^{nd} *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 2^{nd} *qubit* $m_2=1$

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

Quantum entanglement

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

$$|\psi\rangle\neq|a\rangle|b\rangle\ \ non-sepearable$$

If the state is separable:

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

$$\gamma\beta=0\ or\ \alpha\delta=0\leftrightarrow\alpha\gamma=1\ and\ \beta\delta=1$$

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

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

Suppose the initial system state vector is $|\psi(t)\rangle$, and say, there s a second Quantum system called ancilla system (or the meter) in an initial state $|\phi(t)\rangle$. So the intitial 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 fo a time T_1

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

$$|\Psi(t+T_1)\rangle = U(T_1)\,|\psi(t)\rangle\,|\phi(t)\rangle$$

$$= \sum_m \beta_m(t)\,|\psi_m(t)\rangle\,|\phi_m\rangle$$

$$|\phi_m\rangle \ \textit{is the orthonomal basis, but} \ |\psi_m(t)\rangle \ \textit{may not orthogonal.}$$

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

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

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

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

The completeness condition:

$$\sum_m M_m^\dagger M_m = \sum_m \langle\phi(t)|U^\dagger(T_1)|\phi_m\rangle\,\langle\phi_m|U(T_1)|\phi(t)\rangle$$

$$= \langle\phi(t)|U^\dagger(T_1)U(T_1)|\phi(t)\rangle = \mathbb{1}$$

EPR paradox and Bell's inequality

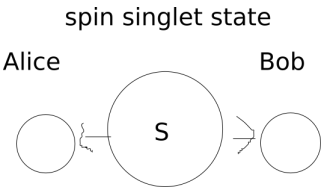
- Perhaps, the most spectacular and counter-intuitive manifestation of quantum mechanics is the phenonmenon of entanglement observed in composite quantum system.
- According to quantum mechanics, and unobserved particle do not posses physical properties thate exist independent of observation (reality 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. thennis ball, moon, color of a chalk
  (2) Locality principle: If two system are causally disconnected, the result of any measurement performed one a system cannot influence the result of a measurement performed 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 fasten 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 tha 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)

$$\begin{array}{cc} \textit{Alice} & \textit{Bob} \\ \downarrow & \downarrow \\ \textit{white} & \textit{black} \\ (L) & (R) \end{array}$$

Locality and Reality

The result 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 $\sigma_b^B : +1$

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

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

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 unpon the nature of the observable measured on the other particle.

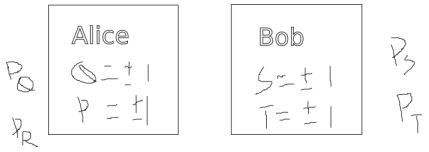
$$|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = \frac{1}{\sqrt{2}}(|+\rangle\,|-\rangle - |-\rangle\,|+\rangle) = \frac{1}{\sqrt{2}}(|+\rangle_n\,|-\rangle_n - |-\rangle_n\,|+\rangle_n)$$

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 $\langle\psi|P_m|\psi\rangle =_a \langle -|+\rangle_b\, {}_b\langle +|-\rangle_a = \sin^2\frac{\theta_{ab}}{2} \;\Rightarrow\; P(a_+, b_+) = \frac{1}{2}\sin^2\frac{\theta_{ab}}{2}$

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

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 $\theta = 60^o \Rightarrow \left(\frac{\sqrt{3}}{2}\right)^2 \leq 2\left(\frac{1}{2}\right)^2 \Rightarrow \frac{3}{4} \leq \frac{2}{4}$!!!! **The Quantum Mechanics will violate Bell's inequatlity.**

- 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).

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

Emsemble average: (The curly words mean operator)

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

Quantum Theory

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

Example

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

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

$\langle\mathcal{QS}\rangle+\langle\mathcal{RS}\rangle+\langle\mathcal{RT}\rangle-\langle\mathcal{QT}\rangle=2\sqrt{2}>2$!! ***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
  - Seperation 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 involved 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 indpendently of each other. Then Alice sends an answer bit a back to the refree, and Bob sends back an answer bit b. Alice and Bob win the game iff

  $$a+b=xy \mod 2$$

  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 simply that Alice and Bob always send the refree 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%.

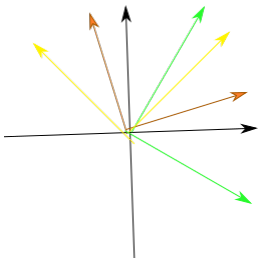
Quantum Strategy

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

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

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

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



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.

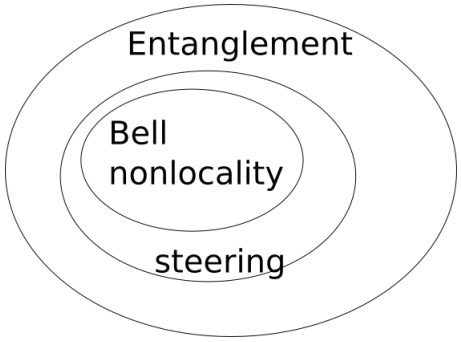
Let's consider the case where Alice gets x=0 and measure $|0\rangle$.

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 probabiltiy 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 probabiltiy 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-seperable 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* $|s\rangle$

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

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 —[X]— $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ —[Y]— $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ —[Z]— $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

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

Phase gate —[S]— $S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$ $\frac{\pi}{8}$ *gate* —[T]— $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}$

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

Rotation operator

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

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

—[U]— $U = e^{i\delta}R_z(\alpha)R_y(\gamma)R_z(\beta) = \begin{pmatrix} e^{i(\delta-\frac{\alpha}{2}-\frac{\beta}{2})}\cos(\frac{\gamma}{2}) & -e^{i(\delta-\frac{\alpha}{2}+\frac{\beta}{2})}\sin(\frac{\gamma}{2}) \\ e^{i(\delta+\frac{\alpha}{2}-\frac{\beta}{2})}\sin(\frac{\gamma}{2}) & e^{i(\delta+\frac{\alpha}{2}+\frac{\beta}{2})}\cos(\frac{\gamma}{2}) \end{pmatrix}$

Transformation of gate

—[H]—[X]—[H]— $HXH = \frac{1}{\sqrt{2}}(X+Z)X\frac{1}{\sqrt{2}}(X+Z) = \frac{1}{2}(X+Z+Z+ZXZ) = Z$

—[H]—[Y]—[H]— $HYH = \frac{1}{\sqrt{2}}(X+Z)Y\frac{1}{\sqrt{2}}(X+Z) = \frac{1}{2}(XYX+ZYX+XYZ+ZYZ) = -Y$

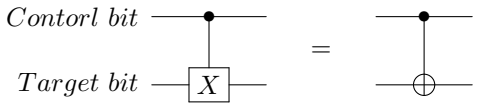
—[H]—[Z]—[H]— $HZH = \frac{1}{\sqrt{2}}(X+Z)Z\frac{1}{\sqrt{2}}(X+Z) = \frac{1}{2}(XZX+X+Z+X) = X$

It can be verfied from commuation and anti-commutaion relation

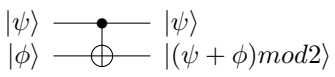
$$\{\sigma_i, \sigma_j\} = 2\delta_{ij} I \quad [\sigma_i, \sigma_j] = 2i\epsilon_{ijk}\sigma_k$$

Two qubit gates

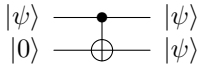
CNOT gate (controlled-not)



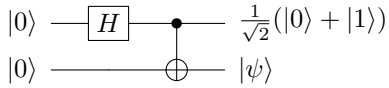
$$\begin{aligned} |00\rangle &\to |00\rangle \\ |01\rangle &\to |01\rangle \\ |10\rangle &\to |11\rangle \\ |11\rangle &\to |10\rangle \end{aligned} \qquad CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$



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



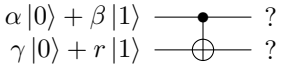
CNOT gate combined with Hadamard gate can transform basis state into Bell state



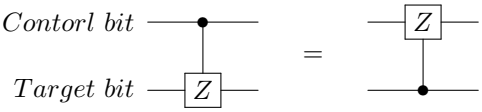
Thus, we can not determined $|\psi\rangle$. $|\psi\rangle$ is entangled with control bit now

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

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

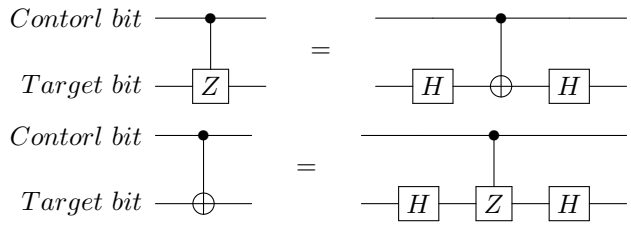


CZ gate (controlled-Z)



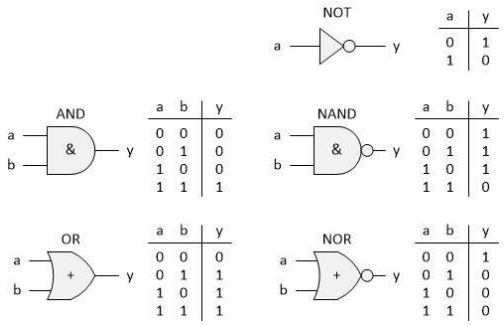
$$\begin{aligned} |00\rangle &\to |00\rangle \\ |01\rangle &\to |01\rangle \\ |10\rangle &\to |10\rangle \\ |11\rangle &\to -|11\rangle \end{aligned} \qquad CZ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

Relation between CNOT and CZ gate

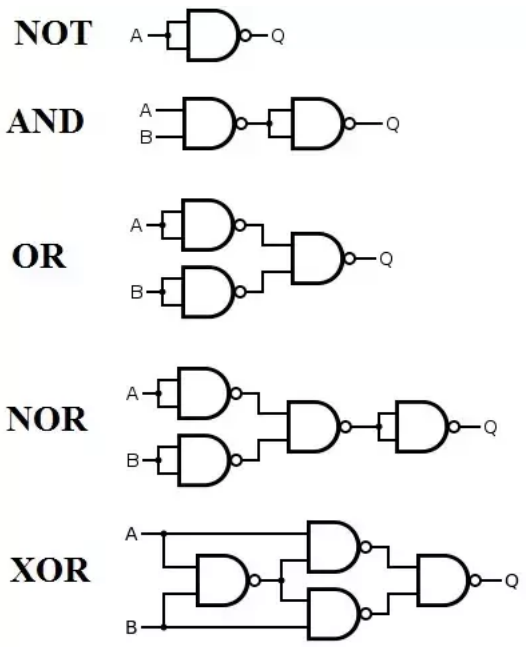


Classical computation

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.

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
where $ABC = I$ and $U = e^{i\delta} AXBXC$.
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,

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

$$|00\rangle \rightarrow |00\rangle$$
$$|01\rangle \rightarrow |01\rangle$$
$$|10\rangle \rightarrow e^{i\delta}|10\rangle$$
$$|11\rangle \rightarrow e^{i\delta}|11\rangle$$

If control qubit $|0\rangle$: Nothing happan(LHS), ABC = I (RHS)
If control qubit $|1\rangle$: U(LHS) , $e^{i\delta} AXBXC$(RHS)

Three qubit gate decomposition

$$U = V^2$$

Show

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

RHS

$$\begin{array}{lll}
|00i_3\rangle \to |00i_3\rangle \to & |00i_3\rangle \to |00i_3\rangle \to & |00i_3\rangle \to |00i_3\rangle \\
|01i_3\rangle \to |01\rangle V |i_3\rangle \to & |01\rangle V |i_3\rangle \to |01\rangle V^\dagger V |i_3\rangle \to & |01i_3\rangle \to |01i_3\rangle \\
|10i_3\rangle \to |10i_3\rangle \to & |11i_3\rangle \to |11\rangle V^\dagger \to & |10\rangle V^\dagger |i_3\rangle \to |10\rangle V V^\dagger |i_3\rangle \\
|11i_3\rangle \to |11\rangle V |i_3\rangle \to & |10\rangle V |i_3\rangle \to |10\rangle V |i_3\rangle \to & |11\rangle V |i_3\rangle \to |11\rangle V^2 |i_3\rangle
\end{array}$$

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

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

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 qubitcould 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 o Bob, who is now able to perform a measurement on the pair, which reveals the values of $i_1 i_2$