USC Quantum Computing Workshop, Lecture 1:

Quantum Computing Basics

Meijian Li [meijian.li@usc.es]

Instituto Galego de Física de Altas Enerxías, Universidade de Santiago de Compostela (IGFAE-USC), Spain

@ 15:00-17:00, Feb 28th, Facultad de Física, USC

What we will learn

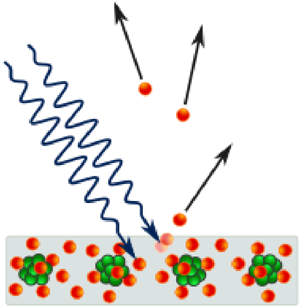
1. A brief history of quantum computing (reading material)
2. ***Quantum Mechanics in a nutshell***
3. ***What is qubit?***
4. ***How do we construct a quantum circuit?***
5. What is density operator? (reading material)

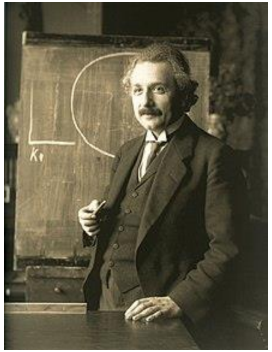
1. How does quantum computing develop?

➢ **Quantum**

- In 1905, Albert Einstein explains the photoelectric effect—shining light on certain materials can function to release electrons from the material—and suggests that light itself consists of individual quantum particles or photons.

- In 1924, the term quantum mechanics is first used in a paper by Max Born.

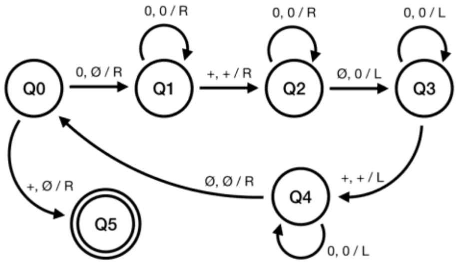


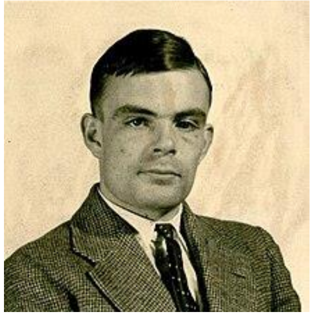


1. How does quantum computing develop?

➢ **Computing**

- David Hilbert's 1928 problem: ``*what can humans know about mathematics, in principle, and what (if any) parts of mathematics are forever unknowable by humans?”*
- To tackle this problem, in 1936, Alan Turing described what we now call a Turing machine: a single, universal programmable computing device that could perform any algorithm whatsoever.



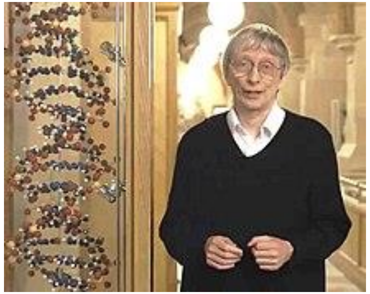


1. How does quantum computing develop?

➢ **Quantum & Computing**

- In 1985, David Deutsch invented a new type of computing system, a quantum computer, with stating `` *'quantum parallelism', a method by which certain probabilistic tasks can be performed faster by a universal quantum computer than by any classical restriction of it."*

- In 1982, Richard Feynman suggested that building computers based on the principles of quantum mechanics would allow us to avoid the essential difficulties in simulating quantum mechanical systems on classical computers.

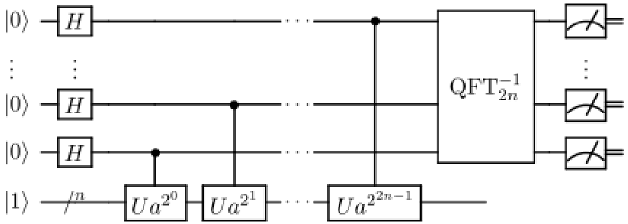


1. How does quantum computing develop?

➢ **Quantum advantage** (over classical computers)

- In <u>1994</u>, Peter Shor demonstrated that the problem of finding the prime factors of an integer, and the '*discrete logarithm*' problem could be solved efficiently on a quantum computer.

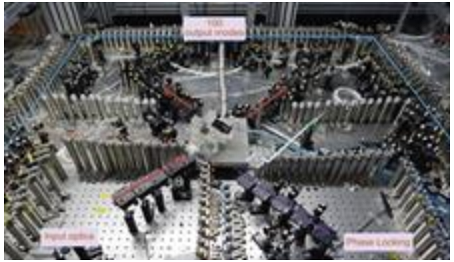
- In <u>1995</u>, Lov Grover invented the quantum *database search algorithm*.



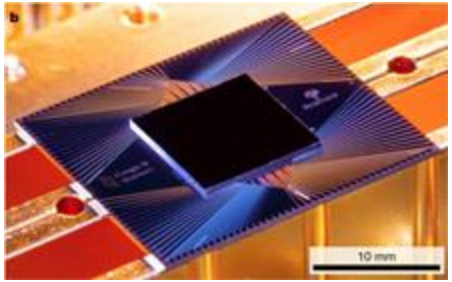
1. How does quantum computing develop?

➢ Quantum supremacy

- In 2004, First five-photon entanglement demonstrated by Jian-Wei Pan's group at the University of Science and Technology in China.
- In 2019, Google claims to have reached quantum supremacy by performing a series of operations in 200 seconds that would take a supercomputer about 10,000 years to complete.
- In 2022, the IBM Quantum Summit announced new breakthrough advancements in quantum hardware and software and outlining its pioneering vision for quantum-centric supercomputing.



UTSC, Jian-Wei Pan’s group, Science 370, 1460 (2020)



Google AI Quantum 1910.11333 (2019)

IBM Quantum at CES 2020

1. How does quantum computing develop?

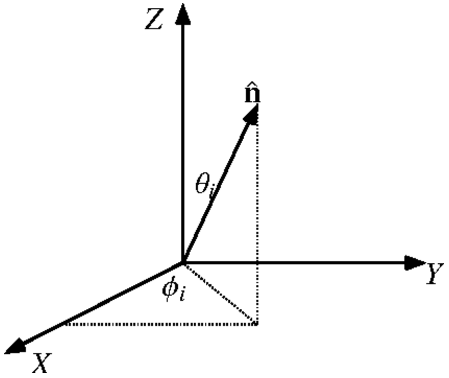
➢ Quantum supremacy

- In 2023, Galicia acquires the most powerful quantum computer in Spain and one of the first in Europe, a 32-qubit computer based on superconducting technology in the Galician Supercomputing Center (CESGA).

2. What is quantum mechanics?

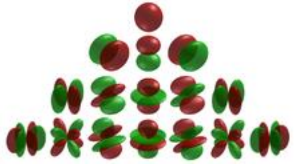
➢ A mathematical framework for the development of physical theories

- **Postulate 1**: Associated to any isolated physical system is a complex vector space with inner product (that is, a Hilbert space) known as the state space of the system. The system is completely described by its state vector, which is a unit vector in the system’s state space.



state space

e.g., HOs



Dirac notation

$$|u\rangle = \begin{pmatrix} u_1 \\ u_2 \\ u_3 \\ \vdots \\ u_n \end{pmatrix}$$

$$\langle u| = (u_1^*, u_2^*, u_3^*, \dots, u_n^*)$$

$$\langle u|v\rangle = \sum_{i=1}^{n} u_i^* v_i$$

2. What is quantum mechanics?

➢ A mathematical framework for the development of physical theories

- **Postulate 2:** The evolution of a closed quantum system is described by a unitary transformation. That is, the state $|\psi\rangle$ of the system at time t_1 is related to the state $|\psi'\rangle$ of the system at time t_1 by a unitary operator U which depends only on the times t_1 and t_2,

$$|\psi(t_2)\rangle = U(t_1; t_2)|\psi(t_1)\rangle$$

the time-dependent Schrödinger equation

$$H|\psi(t)\rangle = \mathrm{i}\hbar\frac{\partial}{\partial t}|\psi(t)\rangle \quad \Longrightarrow \quad U(t_1; t_2) = e^{-iH(t_2-t_1)/\hbar}$$

2. What is quantum mechanics?

➢ A mathematical framework for the development of physical theories

- **Postulate 3**: Quantum measurements are described by a collection $\{M_m\}$ of measurement operators. These 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 the probability that the result m occurs is given by

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

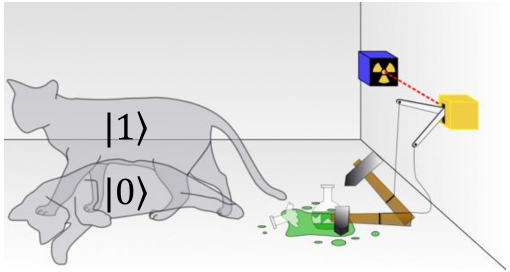
and the state of the system after the measurement is $\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^{\dagger} M_m|\psi\rangle}}$

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

2. What is quantum mechanics?

➢ A mathematical framework for the development of physical theories

- **Postulate 3**: Quantum measurements example



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

$$M_0|\psi\rangle = |0\rangle\langle 0|\psi\rangle = \alpha|0\rangle$$

$$M_1|\psi\rangle = |1\rangle\langle 1|\psi\rangle = \beta|1\rangle$$

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

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

2. What is quantum mechanics?

- A mathematical framework for the development of physical theories

- **Postulate 4**: The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. Moreover, if we have systems numbered 1 through n, and system number i is prepared in the state $|\psi_i\rangle$, then the joint state of the total system is

$$|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$$

$$|u\rangle \otimes |v\rangle = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix} \otimes \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} u_1 v_1 \\ u_1 v_2 \\ \vdots \\ u_1 v_n \\ \vdots \\ \vdots \\ u_n v_1 \\ u_n v_2 \\ \vdots \\ u_n v_n \end{pmatrix}$$

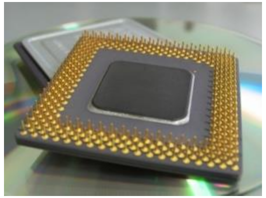
3. What is qubit? [Notebook] Sec.1.1

- A **(classical) bit** is a state of 0 or 1, a mathematical concept in classical computing.

○ **1**

○ **0**

- Bits are stored as tiny electric charges on nanometer-scale capacitors.



3. What is qubit?

- A **quantum bit**, i.e., qubit, is a mathematical concept in quantum computing. It is a state of 2-dimensional unit vector,

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

α and β are complex values, satisfying $|\alpha|^2 + |\beta|^2 = 1$.

➢ *What is the degree of freedom, number of independent real variables, in one qubit?*

3. What is qubit?

- A **quantum bit**, i.e., qubit, is a mathematical concept in quantum computing. It is a state of 2-dimensional unit vector,

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

α and β are complex values, satisfying $|\alpha|^2 + |\beta|^2 = 1$.

➢ *What is the degree of freedom, number of independent real variables, in one qubit?*

$$2(\text{variables}) \times 2(\text{complex}) - 1(\text{normalization constraint}) = \mathbf{3}$$

3. What is qubit?

- A **qubit state:**

$$\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \alpha \underbrace{\begin{pmatrix}1\\ 0\end{pmatrix}}_{|0\rangle \,\Downarrow\, 0} + \beta \underbrace{\begin{pmatrix}0\\ 1\end{pmatrix}}_{|1\rangle \,\Downarrow\, 1}$$

computational basis states

classical bits

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

superposition / linear combination

3. What is qubit?

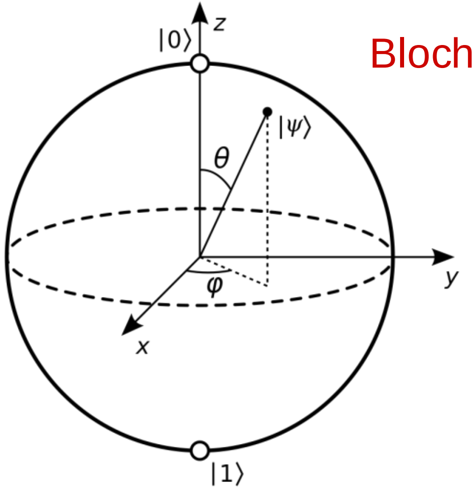
- A **qubit state:**

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

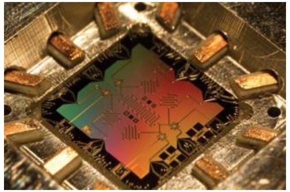
$$= e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle\right)$$

overall phase — *polar angle* — *azimuthal angle*

3 real variables



Bloch sphere



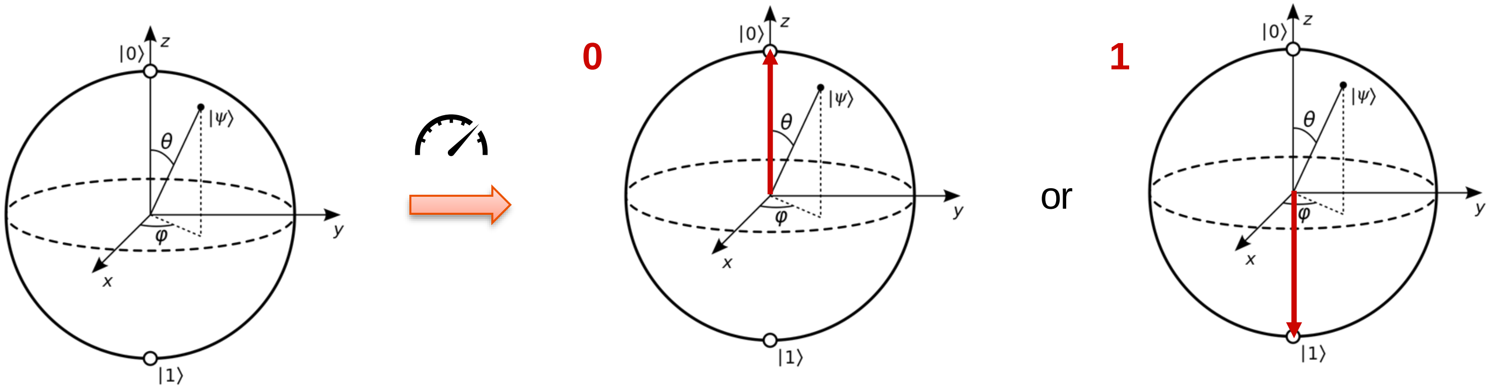
- The state of the qubit can be stored on an electron, photon, or an atom.

3. What is qubit?

- A **qubit state:** $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

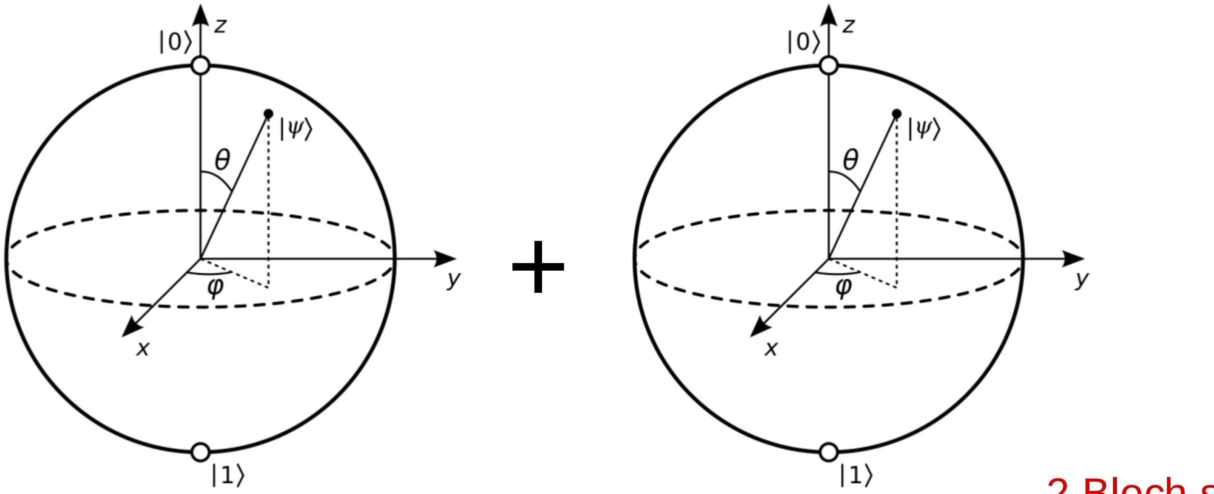
➢ What is the physical meaning of the amplitudes α and β?

Recall what happens after a measurement in QM



3. What is qubit?

- A **2-qubit state**



?

2 Bloch spheres

3. What is qubit?

- A **2-qubit state**

$$|\psi\rangle = c_{00}|00\rangle + c_{01}|01\rangle + c_{10}\,|10\rangle + c_{11}|11\rangle$$
$$\neq (\alpha|0\rangle + \beta|1\rangle)(\alpha'|0\rangle + \beta'|1\rangle)$$

Recall in QM, building the state space of a composite system is through tensor product

➢ *What is the degree of freedom, number of independent real variables, in a two-qubit state?*

3. What is qubit?

- A **2-qubit state**

$$|\psi\rangle = c_{00}|00\rangle + c_{01}|01\rangle + c_{10}\,|10\rangle + c_{11}|11\rangle$$

$$\neq (\alpha|0\rangle + \beta|1\rangle)(\alpha'|0\rangle + \beta'|1\rangle)$$

Recall in QM, building the state space of a composite system is through tensor product

➢ *What is the degree of freedom, number of independent real variables, in a two-qubit state?*

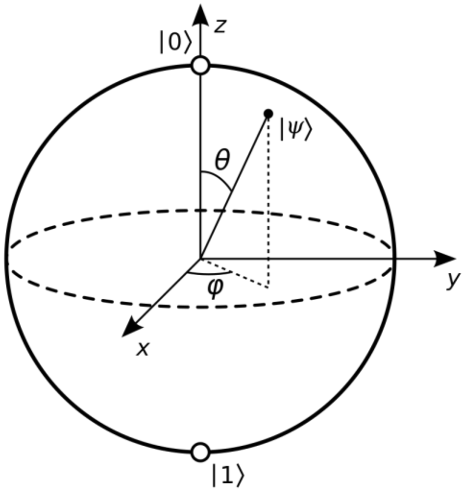
$$4(\text{variables}) \times 2(\text{complex}) - 1(\text{normalization constraint}) = \mathbf{7}$$

$$\neq 2(\text{qubits}) \times 3$$

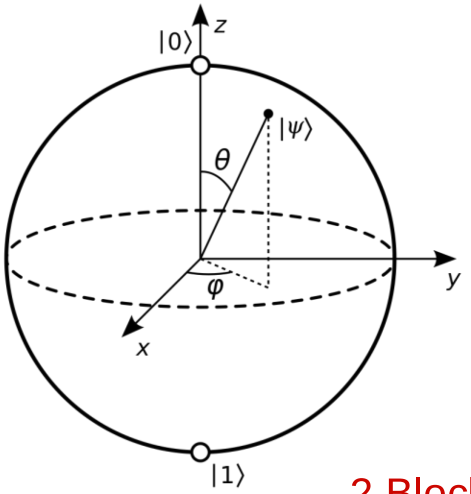
3. What is qubit?

- A **2-qubit state**

$\neq$



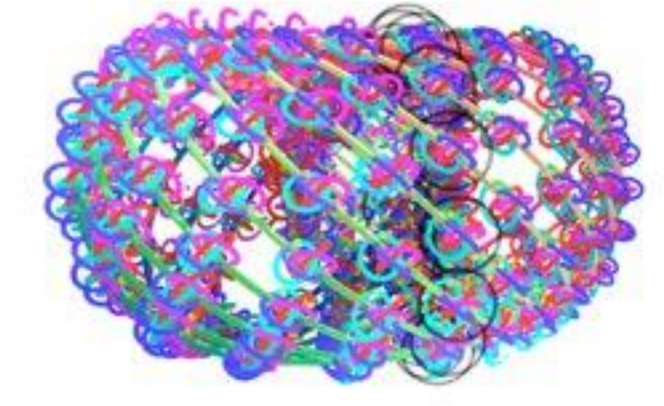
+



2 Bloch spheres

3. What is qubit?

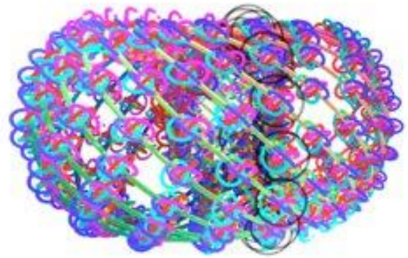
- A **2-qubit state**



hypersphere in 7 dimension

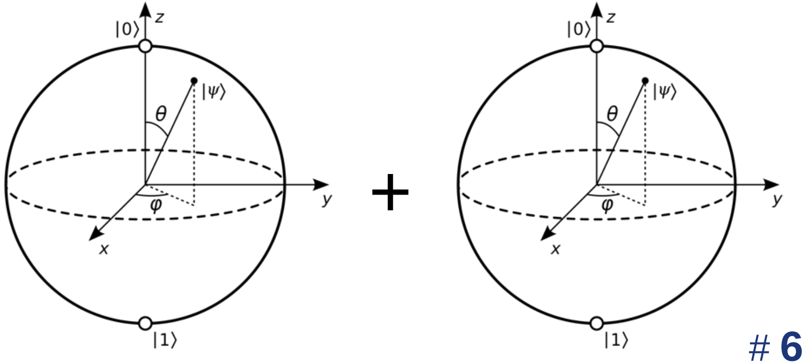
3. What is qubit?

- A **2-qubit state**



7

$\neq$

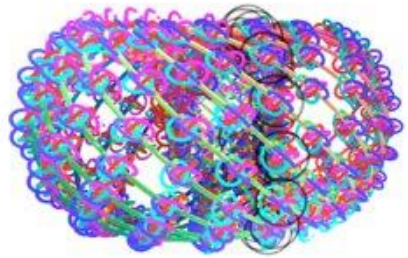


6

➢ *What is missing on the right-hand side?*

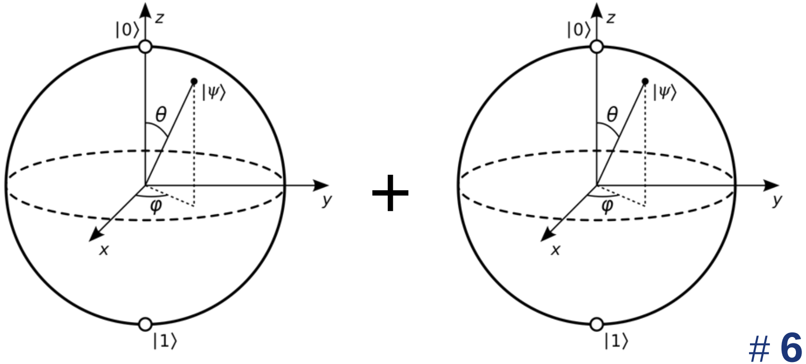
3. What is qubit?

- A **2-qubit state**



7

≠



6

➢ *What is missing on the right-hand side?*

Correlation between the two qubits.

3. What is qubit?

- A **n-qubit state**

$$
\begin{aligned}
|\psi\rangle \quad &= c_{00\ldots0}|00\ldots0\rangle + c_{00\ldots1}|00\ldots1\rangle + \cdots + c_{11\ldots1}|11\ldots1\rangle \\
&\neq \left(\alpha_1|0\rangle + \beta_1|1\rangle\right)\left(\alpha_2|0\rangle + \beta_2|1\rangle\right) \ldots \left(\alpha_n|0\rangle + \beta_n|1\rangle\right)
\end{aligned}
$$

➢ *What is the degree of freedom, number of independent real variables, in a n-qubit state?*

3. What is qubit?

- A **n-qubit state**

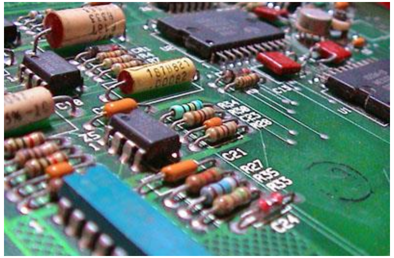
$$
\begin{aligned}
|\psi\rangle \quad &= c_{00\ldots0}|00\ldots0\rangle + c_{00\ldots1}|00\ldots1\rangle + \cdots + c_{11\ldots1}|11\ldots1\rangle \\
&\neq (\alpha_1|0\rangle + \beta_1|1\rangle)(\alpha_2|0\rangle + \beta_2|1\rangle)\ldots(\alpha_n|0\rangle + \beta_n|1\rangle)
\end{aligned}
$$

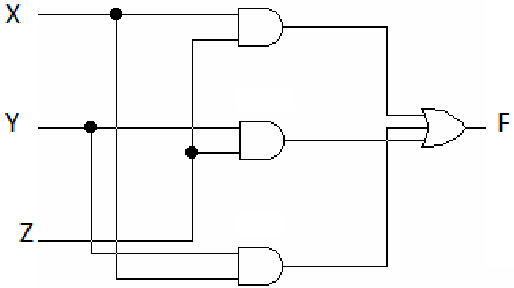
➢ *What is the degree of freedom, number of independent real variables, in a n-qubit state?*

2^n(variables) $\times$ 2(complex) $-$ 1(normalization constraint) = $\mathbf{2^{n+1}}$**-1** $\gg$ 2n

4. How do we construct a quantum circuit?

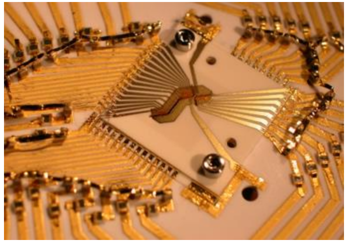
- A **classical computer** is built from an electrical circuit containing wires and logic gates.

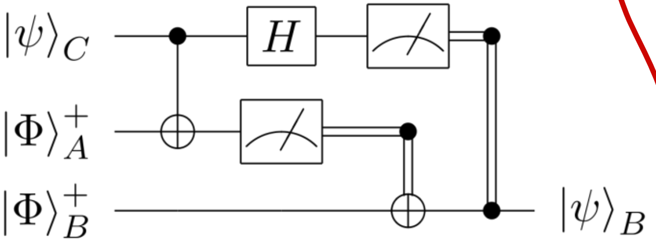




4. How do we construct a quantum circuit?

- A **quantum computer** is built from a quantum circuit containing wires and elementary quantum gates to carry around and manipulate quantum information (qubits).





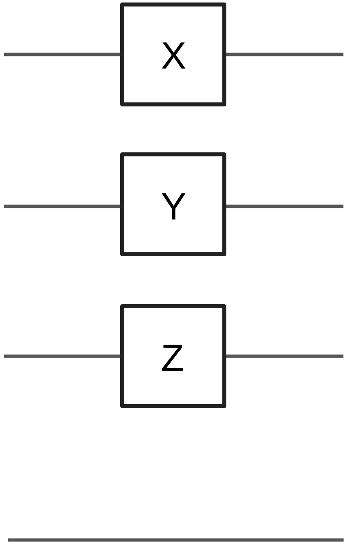
4.1 Quantum wire

- The simplest quantum circuit is a **quantum wire**, which does nothing.

➢ *However, it is also the hardest to implement in practice. The reason is that quantum states are often incredibly fragile, as stored in a single photon or a single atom.*

4.2 Single qubit operations [Notebook] Sec.1.2

- **Single qubit operations** are described by 2×2 unitary matrices. For example, Pauli matrices, X, Y and Z,



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

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

4.2 Single qubit operations

- **Single qubit operations** are described by 2×2 unitary matrices, say U, and the state after the operation reads

$$|\psi'\rangle = U|\psi\rangle$$

  - *Why does the operation have to be unitary?*

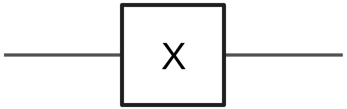
    Unitary matrices preserve the length of their inputs.

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

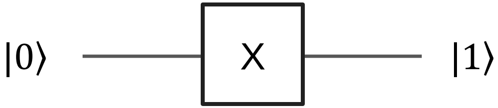
$$\langle\psi'|\psi'\rangle = \langle\psi|U^\dagger U|\psi\rangle = \langle\psi|\psi\rangle = 1$$

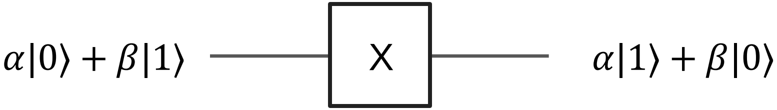
4.2 Single qubit operations

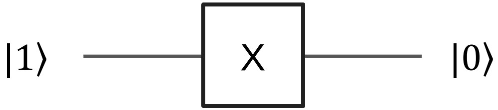
- The **Quantum NOT gate/ X gate**



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

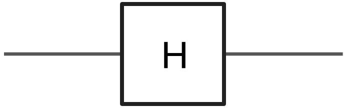






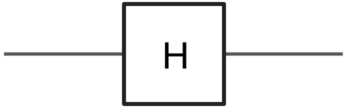
4.2 Single qubit operations

- The **Hadamard gate/ H gate**



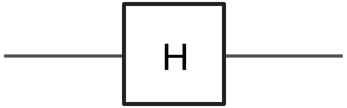
$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$|0\rangle$



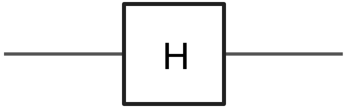
$$\frac{|0\rangle + |1\rangle}{\sqrt{2}} \equiv |+\rangle$$

$|1\rangle$



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

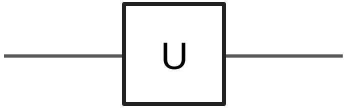
$\alpha|0\rangle + \beta|1\rangle$



$\alpha|+\rangle + \beta|-\rangle$

4.2 Single qubit operations

- An arbitrary single qubit gate



$$U = e^{i\alpha}\begin{pmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{pmatrix}\begin{pmatrix} \cos(\gamma/2) & -\sin(\gamma/2) \\ \sin(\gamma/2) & \cos(\gamma/2) \end{pmatrix}\begin{pmatrix} e^{-i\delta/2} & 0 \\ 0 & e^{i\delta/2} \end{pmatrix}$$

α, β, γ, and δ are real variables

➢ *Unitarity constraint is the only constraint on quantum gates.*

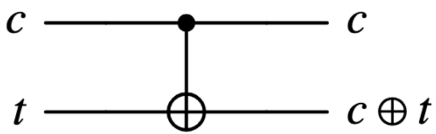
4.2 Multiple qubit gates

[Notebook] Sec.1.3

- The **C**(ontrolled-)**NOT gate**

control qubit

target qubit



addition modulo 2

$0 \oplus 0 = 0$

$0 \oplus 1 = 1$

$1 \oplus 0 = 1$

$1 \oplus 1 = 0$

➢ *What is the matrix representation of the CNOT gate?*

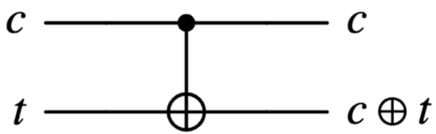
$$\text{CNOT}=\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

4.2 Multiple qubit gates

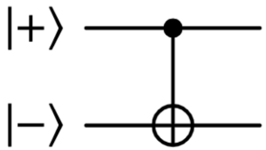
- The **C**(ontrolled-)**NOT gate**

control qubit

target qubit

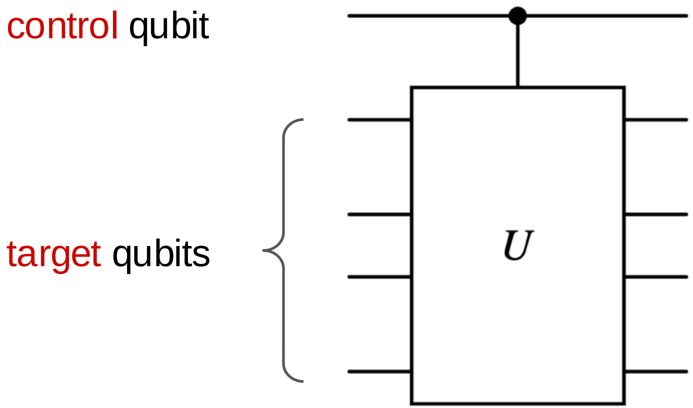


> *Is the control qubit always unchanged after the CNOT gate?*



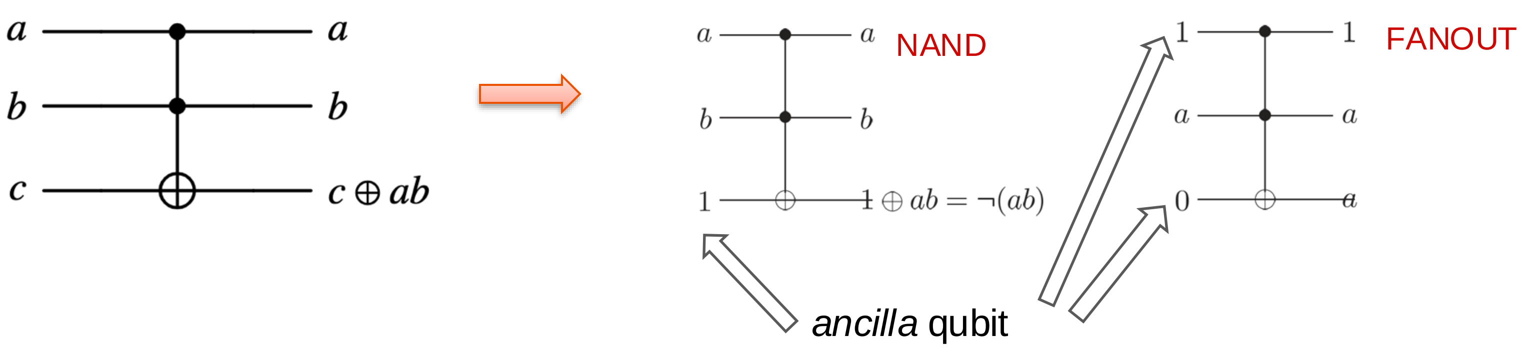
4.2 Multiple qubit gates

- The **Controlled-U gate**



4.2 Multiple qubit gates

- The **Toffoli gate/ CCNOT gate**



➢ *Toffoli gate is universal, in the sense that any classical reversible circuit can be constructed from it.*

4.3 Measurement [Notebook] Sec.2

- The circuit representation of the measurement is

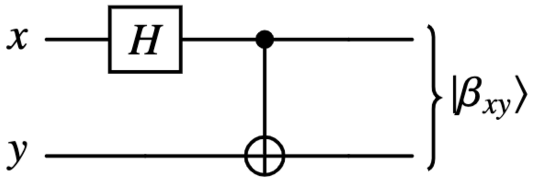
The double line coming out of the measurement carry classical bit.

> ➢ *Could we get the values of α and β of $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ through measurement?*

4.4 Quantum circuit I: the Bell state [Notebook] Sec.3.1

- The **Bell states / EPR** (Einstein, Podolsky, and Rosen) **pairs** represent the simplest examples of quantum entanglementment.

$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}},$$
$$|\beta_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}},$$
$$|\beta_{10}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}},$$
$$|\beta_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}},$$



4.4 Quantum circuit II: quantum addition [Notebook] Sec.3.2

- How to compute a+b on a quantum circuit?
  - Classical Addition

$\vert q_0 = a\rangle$	———	$\vert a\rangle$
$\vert q_1 = b\rangle$	———	$\vert a+b\rangle$

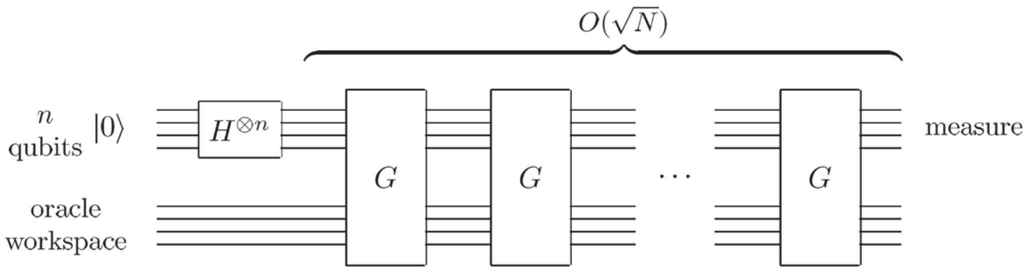
  - Quantum Addition

	Phase Encoding		Phase Addition		Phase Decoding	
$\vert q_0 = a\rangle$	———	$\vert a\rangle$	———	$\vert a\rangle$	———	$\vert a\rangle$
$\vert q_1 = b\rangle$	———	$\vert \phi(b)\rangle$	———	$\vert \phi(a+b)\rangle$	———	$\vert a+b\rangle$

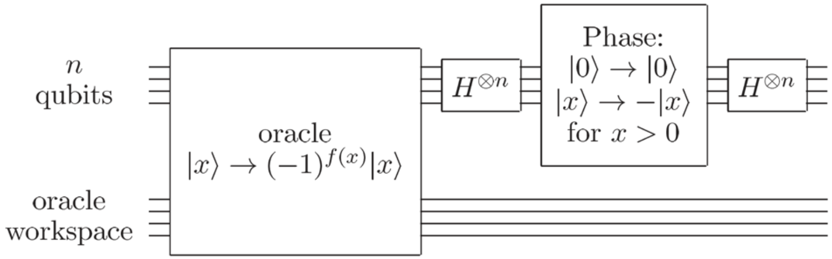
4.4 Quantum circuit III: quantum search algorithm

[Notebook] Sec.3.3.2

- How to find the correct answer faster than classical algorithm?



G=



5. What is density operator?

- Suppose a quantum system is in one of a number of states $|\psi_i\rangle$ with respective probabilities p_i, where i is an index. We call $\{p_i, |\psi_i\rangle\}$ an ensemble of *pure* states. The **density operator/matrix** is defined as

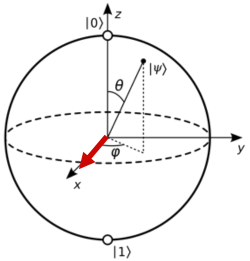
$$\rho \equiv \sum_i p_i |\psi_i\rangle \langle\psi_i|$$

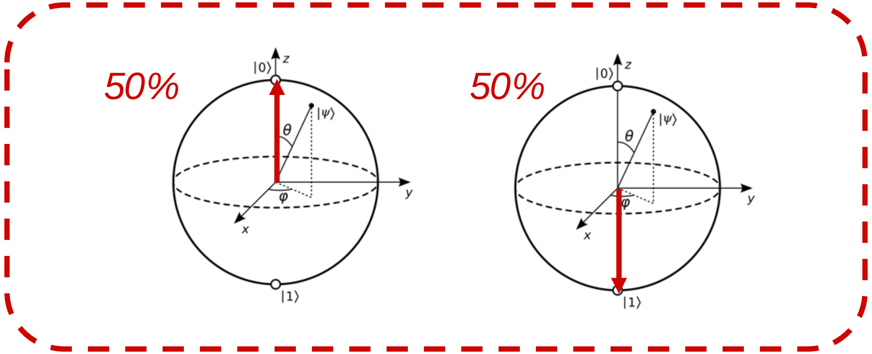
5.1 Pure & mixed states

- If the state of the system is known exactly, i.e., an ensemble of $\{1, |\psi\rangle\}$, we say the system is in a *pure state*, and

$$\rho = |\psi\rangle \langle\psi|$$

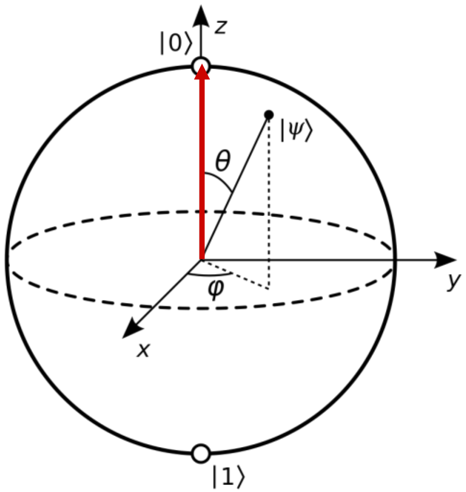
- Otherwise, the system is a mixture of different pure states $|\psi_i\rangle$, and we say it is in a *mixed state*.





5.1 Pure & mixed states

➢ Pure or mixed? $|\psi\rangle = |0\rangle$



Pure

$$\rho = |0\rangle\langle 0| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} (1\ 0)$$

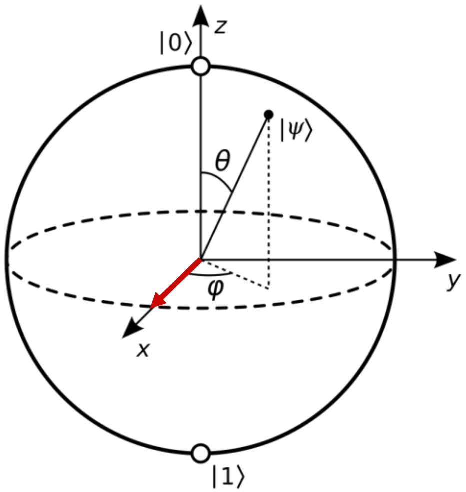
$$= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$\mathrm{Tr}\,\rho = 1$

$\mathrm{Tr}\,\rho^2 = 1$

5.1 Pure & mixed states

- Pure or mixed? $|\psi\rangle = |+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$



Pure

$$\rho = |+\rangle\langle+| = \frac{1}{2}\begin{pmatrix}1\\1\end{pmatrix}(1\ 1)$$

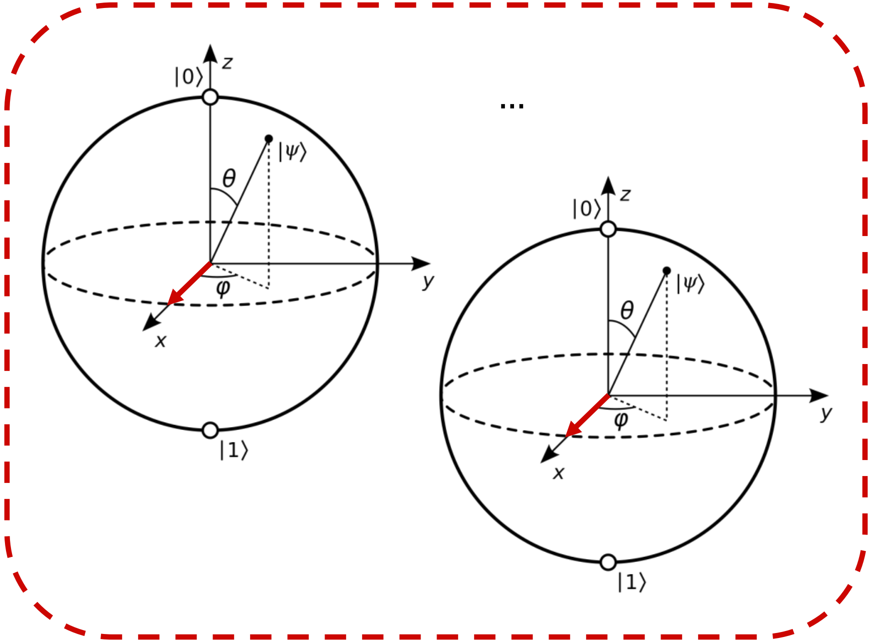
$$= \frac{1}{2}\begin{pmatrix}1 & 1\\1 & 1\end{pmatrix}$$

$\mathrm{Tr}\,\rho = 1$

$\mathrm{Tr}\,\rho^2 = 1$

5.1 Pure & mixed states

➢ Pure or mixed? $\{1, |+\rangle\}$



Pure

$$\rho = |+\rangle\langle +| = \frac{1}{2}\begin{pmatrix}1\\1\end{pmatrix}(1\ 1)$$

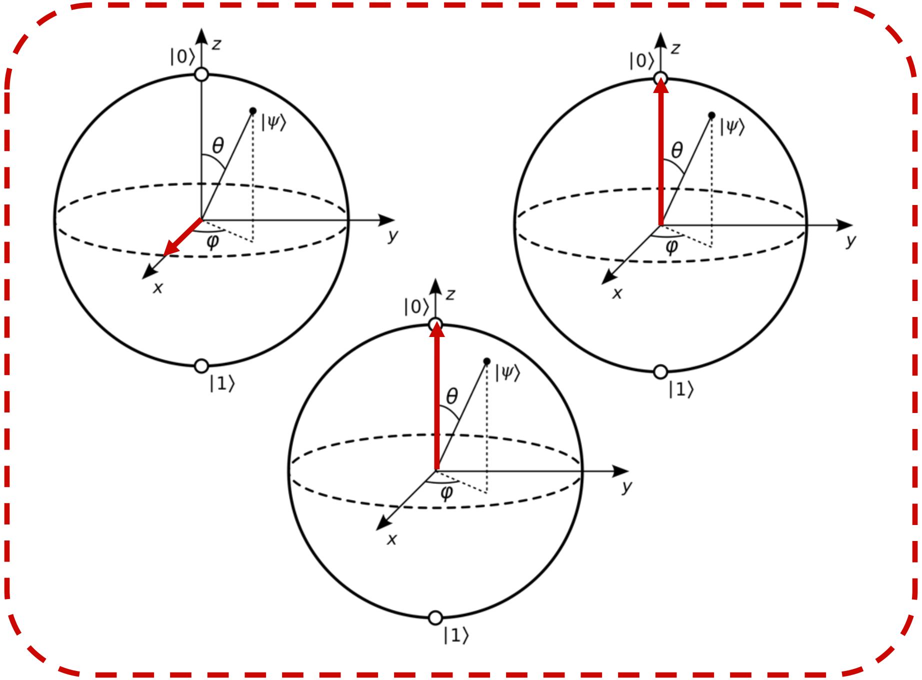
$$= \frac{1}{2}\begin{pmatrix}1 & 1\\1 & 1\end{pmatrix}$$

$\mathrm{Tr}\,\rho = 1$

$\mathrm{Tr}\,\rho^2 = 1$

5.1 Pure & mixed states

- Pure or mixed? $\{\frac{1}{3}, |+\rangle; \frac{2}{3}, |0>\}$



Mixed

$$\rho = \frac{1}{3}|+\rangle\langle+| + \frac{2}{3}|0\rangle\langle 0|$$

$$= \frac{1}{3}\frac{1}{2}\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix} + \frac{2}{3}\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}$$

$$= \frac{1}{6}\begin{pmatrix}5 & 1\\ 1 & 1\end{pmatrix}$$

$$\mathrm{Tr}\,\rho = 1$$

$$\mathrm{Tr}\,\rho^2 = \frac{7}{9}$$ *purity*

5.2 Properties of the density matrix

1) **Trace condition**

$$\operatorname{Tr}\rho = 1$$

$$\operatorname{tr}(\rho) = \sum_i p_i \operatorname{tr}(|\psi_i\rangle\langle\psi_i|) = \sum_i p_i = 1,$$

2) **Positivity condition**

$$\langle\phi|\rho|\phi\rangle \geq 0$$

$$\begin{aligned}\langle\varphi|\rho|\varphi\rangle &= \sum_i p_i \langle\varphi|\psi_i\rangle\langle\psi_i|\varphi\rangle \\ &= \sum_i p_i |\langle\varphi|\psi_i\rangle|^2\end{aligned}$$

$\Updownarrow$

ρ is the density operator

5.3 Operations with the density matrix

- If the evolution of the system is given by the unitary operator U,

$$|\psi_i\rangle \xrightarrow{U} U|\psi_i\rangle$$

that of the density operator follows as

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| \xrightarrow{U} \sum_i p_i U|\psi_i\rangle\langle\psi_i| U^\dagger = \boxed{U\rho U^\dagger}$$

5.3 Operations with the density matrix

- For a measurement with operators M_m, the probability of getting result m given the initial state $|\psi_i\rangle$ is,

$$p(m|i) = \langle\psi_i| M_m^\dagger M_m |\psi_i\rangle = \mathrm{Tr}(M_m^\dagger M_m |\psi_i\rangle\langle\psi_i|)$$

then the total probability of getting m is,

$$p(m) = \sum_i p_i p(m|i) = \sum_i p_i \, \mathrm{Tr}(M_m^\dagger M_m |\psi_i\rangle\langle\psi_i|) = \mathrm{Tr}(M_m^\dagger M_m \rho)$$

5.3 Operations with the density matrix

- After the measurement, state with outcome m becomes

$$|\psi_i\rangle \rightarrow \quad |\psi_i^m\rangle = \frac{M_m |\psi_i\rangle}{\sqrt{\langle\psi_i| M_m^\dagger M_m |\psi_i\rangle}}$$

the subsystem with m is an ensemble of $\{p(i|m), |\psi_i^m\rangle\}$,

$$\rho_m = \sum_i p(i|m) |\psi_i^m\rangle \langle\psi_i^m| \quad = \sum_i \frac{p(m|i)p_i}{p(m)} \frac{M_m |\psi_i\rangle \langle\psi_i| M_m^\dagger}{\langle\psi_i| M_m^\dagger M_m |\psi_i\rangle} \quad = \sum_i p_i \frac{M_m |\psi_i\rangle \langle\psi_i| M_m^\dagger}{\mathrm{Tr}(M_m^\dagger M_m \rho)}$$

$$= \frac{M_m \rho M_m^\dagger}{\mathrm{Tr}(M_m^\dagger M_m \rho)} \; .$$

5.3 Operations with the density matrix

- Therefore, after the measurement, the density matrix becomes

$$\rho = \sum_m p(m)\rho_m = \boxed{\sum_m M_m \rho M_m}$$

➢ *The density matrix, ρ, provides an alternative language, as compared to state vectors, $|\psi\rangle$, of Quantum Mechanics, for pure and mixed states.*

5.4 QM in terms of the density matrix

- **Postulate 1**: Associated to any isolated physical system is a complex vector space with inner product (that is, a Hilbert space) known as the state space of the system. The system is completely described by its density operator ρ.

- **Postulate 2:** The evolution of a closed quantum system is described by a unitary transformation.

$$\rho \rightarrow U \rho U^{\dagger}$$

5.4 QM in terms of the density matrix

- **Postulate 3**: Quantum measurements are described by a collection $\{M_m\}$ of measurement operators. If the state of the quantum system is ρ immediately before the measurement, then the probability that result m occurs is given by

$$p(m) = \mathrm{Tr}(M_m^\dagger M_m \rho)$$

  and the state of the system after the measurement is $\frac{M_m \rho M_m^\dagger}{\sqrt{M_m^\dagger M_m \rho}}$

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

- **Postulate 4**: The state space of a composite physical system is the tensor product of the state spaces of the component physical systems, $\rho_1 \otimes \rho_2 \otimes \cdots \otimes \rho_n$

What we have learned

1. A brief history of quantum computing (reading material)
2. ***Quantum Mechanics in a nutshell***
3. ***What is qubit?***
4. ***How do we construct a quantum circuit?***
5. What is density operator? (reading material)