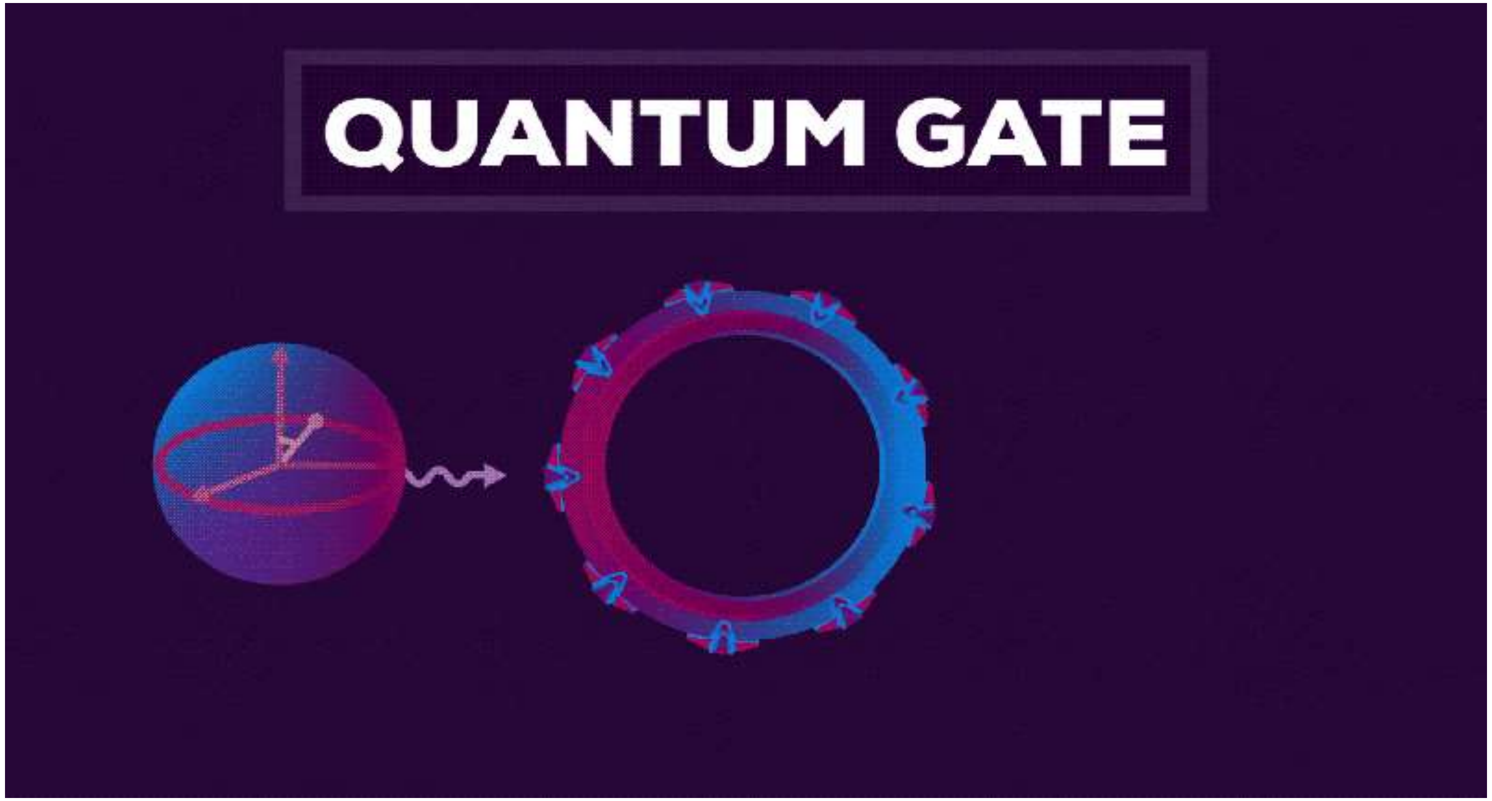
Quantum Information and Quantum Computation

Yuanyuan Chen

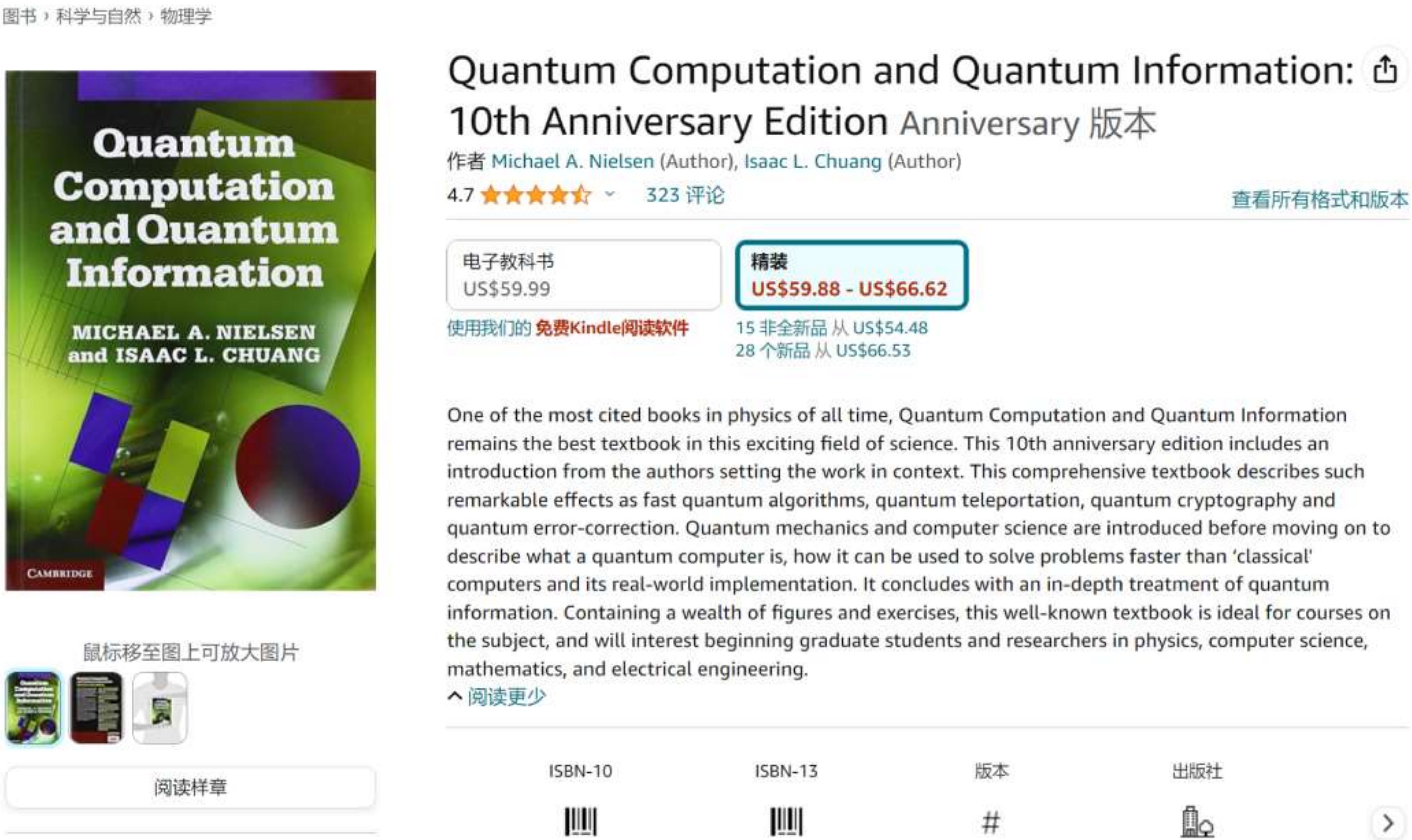
College of Physical Science and Technology
Xiamen University
Email: chenyy@xmu.edu.cn
http://qolab.xmu.edu.cn

Lecture 9

Quantum gates



经典教材推荐



图书 › 科学与自然 › 物理学

Quantum Computation and Quantum Information: 10th Anniversary Edition Anniversary 版本

作者 Michael A. Nielsen (Author), Isaac L. Chuang (Author)

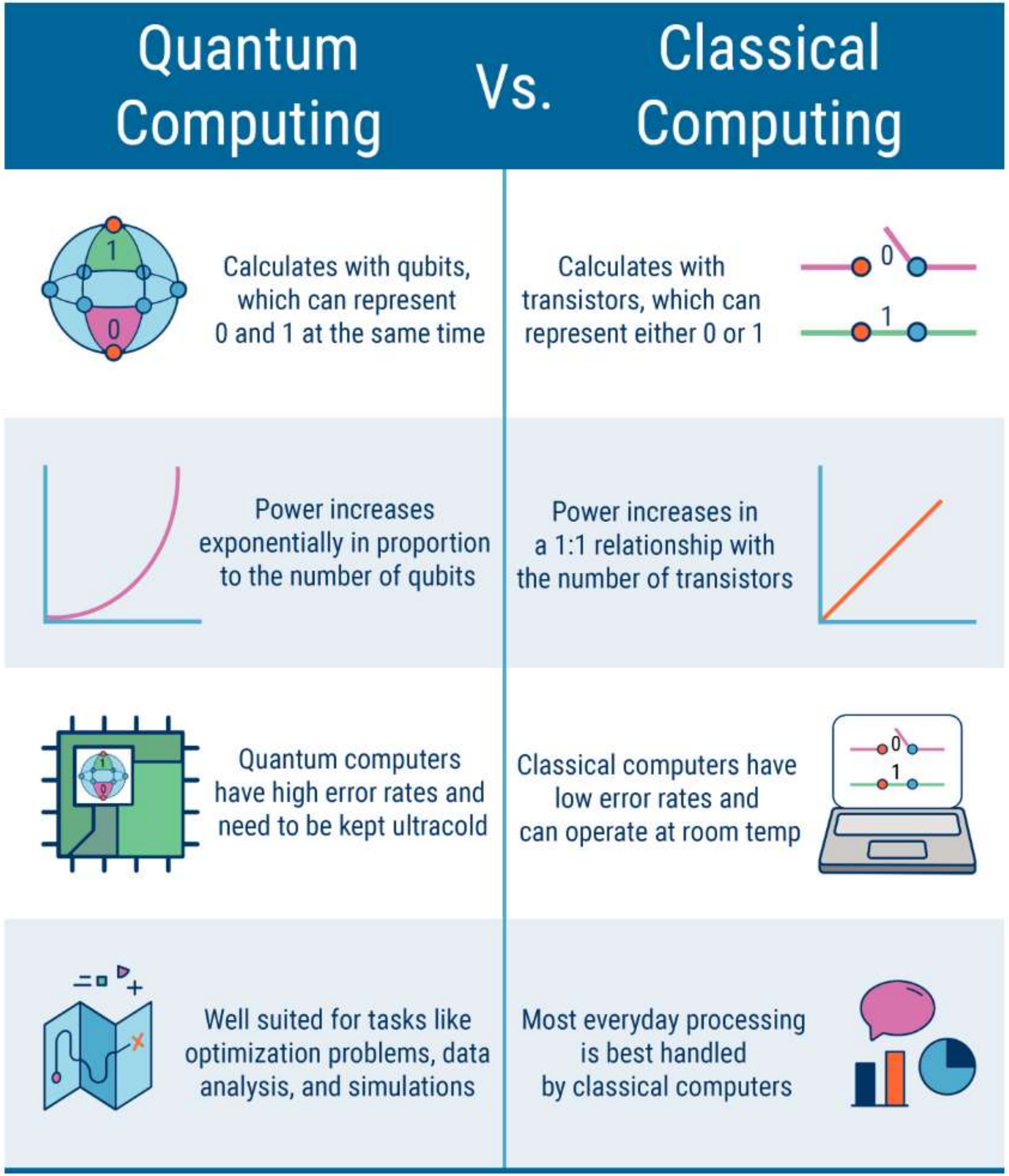
4.7 ★★★★☆ 323 评论

查看所有格式和版本

电子教科书	精装
US$59.99	US$59.88 - US$66.62
使用我们的 免费Kindle阅读软件	15 非全新品 从 US$54.48 28 个新品 从 US$66.53

One of the most cited books in physics of all time, Quantum Computation and Quantum Information remains the best textbook in this exciting field of science. This 10th anniversary edition includes an introduction from the authors setting the work in context. This comprehensive textbook describes such remarkable effects as fast quantum algorithms, quantum teleportation, quantum cryptography and quantum error-correction. Quantum mechanics and computer science are introduced before moving on to describe what a quantum computer is, how it can be used to solve problems faster than 'classical' computers and its real-world implementation. It concludes with an in-depth treatment of quantum information. Containing a wealth of figures and exercises, this well-known textbook is ideal for courses on the subject, and will interest beginning graduate students and researchers in physics, computer science, mathematics, and electrical engineering.

Quantum Computation and Quantum Information
MICHAEL A. NIELSEN and ISAAC L. CHUANG
CAMBRIDGE
鼠标移至图上可放大图片
阅读样章
阅读更少
ISBN-10
ISBN-13
版本
出版社



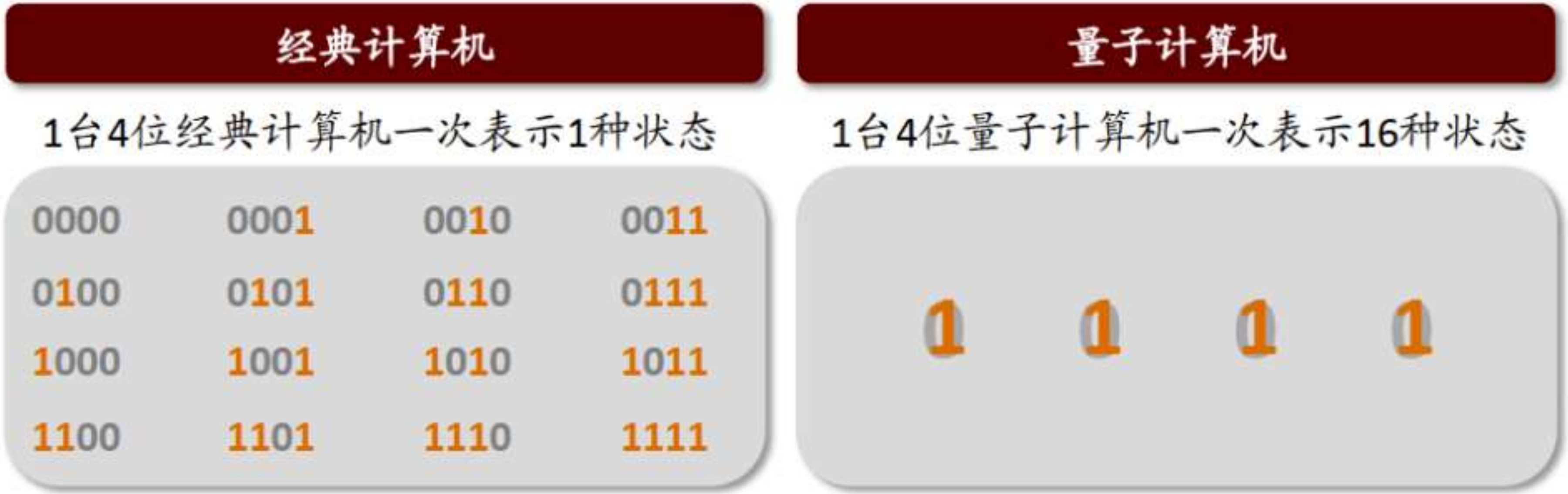
Quantum Computing	Vs.	Classical Computing
Calculates with qubits, which can represent 0 and 1 at the same time		Calculates with transistors, which can represent either 0 or 1
Power increases exponentially in proportion to the number of qubits		Power increases in a 1:1 relationship with the number of transistors
Quantum computers have high error rates and need to be kept ultracold		Classical computers have low error rates and can operate at room temp
Well suited for tasks like optimization problems, data analysis, and simulations		Most everyday processing is best handled by classical computers

1. 量子计算的supremacy

2. 实现量子计算的困难

3. 通用量子计算的设计

1. 量子计算的supremacy



经典计算机

1台4位经典计算机一次表示1种状态

0000	0001	0010	0011
0100	0101	0110	0111
1000	1001	1010	1011
1100	1101	1110	1111

量子计算机

1台4位量子计算机一次表示16种状态

1台n位经典计算机一次表示1种状态，1台n位量子计算机一次表示2^n种状态。

理论上，1台n位的量子计算机算力=2^n台n位的经典计算机算力。

2. 实现量子计算的困难

- ❖ 量子通信信道容量
- ❖ 量子计算速度
- ❖ 量子精密测量精确度
- ❖ ……

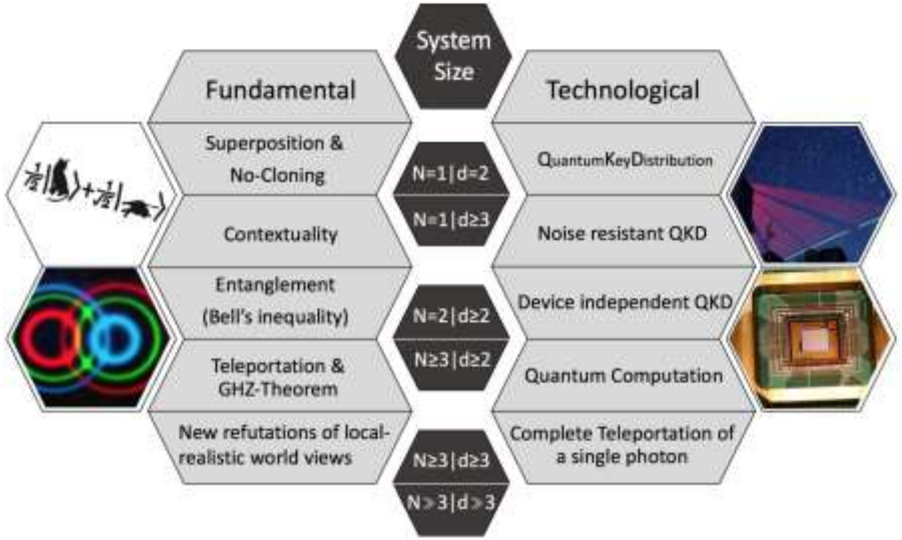
量子系统的规模化拓展

更多光子数量

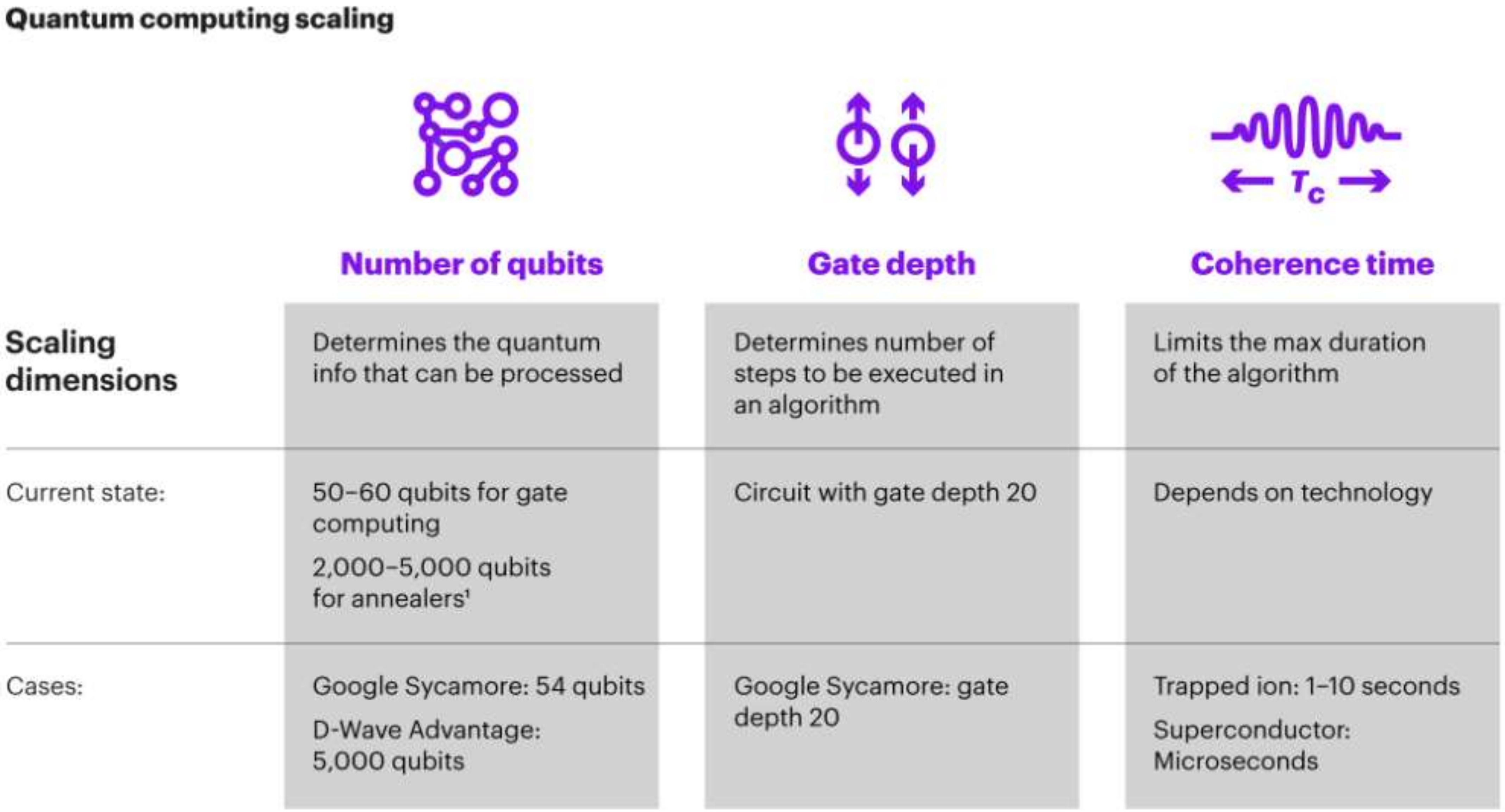
更高光子维度

九章三号量子计算原型机首次突破了255个光子的操纵技术

比上一代九章二号提升一百万倍


System Size
Fundamental
Technological
Superposition & No-Cloning
Contextuality
Entanglement (Bell's inequality)
Teleportation & GHZ-Theorem
New refutations of local-realistic world views
N=1|d=2
N=1|d≥3
N=2|d≥2
N≥3|d≥2
N≥3|d≥3
N>3|d>3
QuantumKeyDistribution
Noise resistant QKD
Device independent QKD
Quantum Computation
Complete Teleportation of a single photon

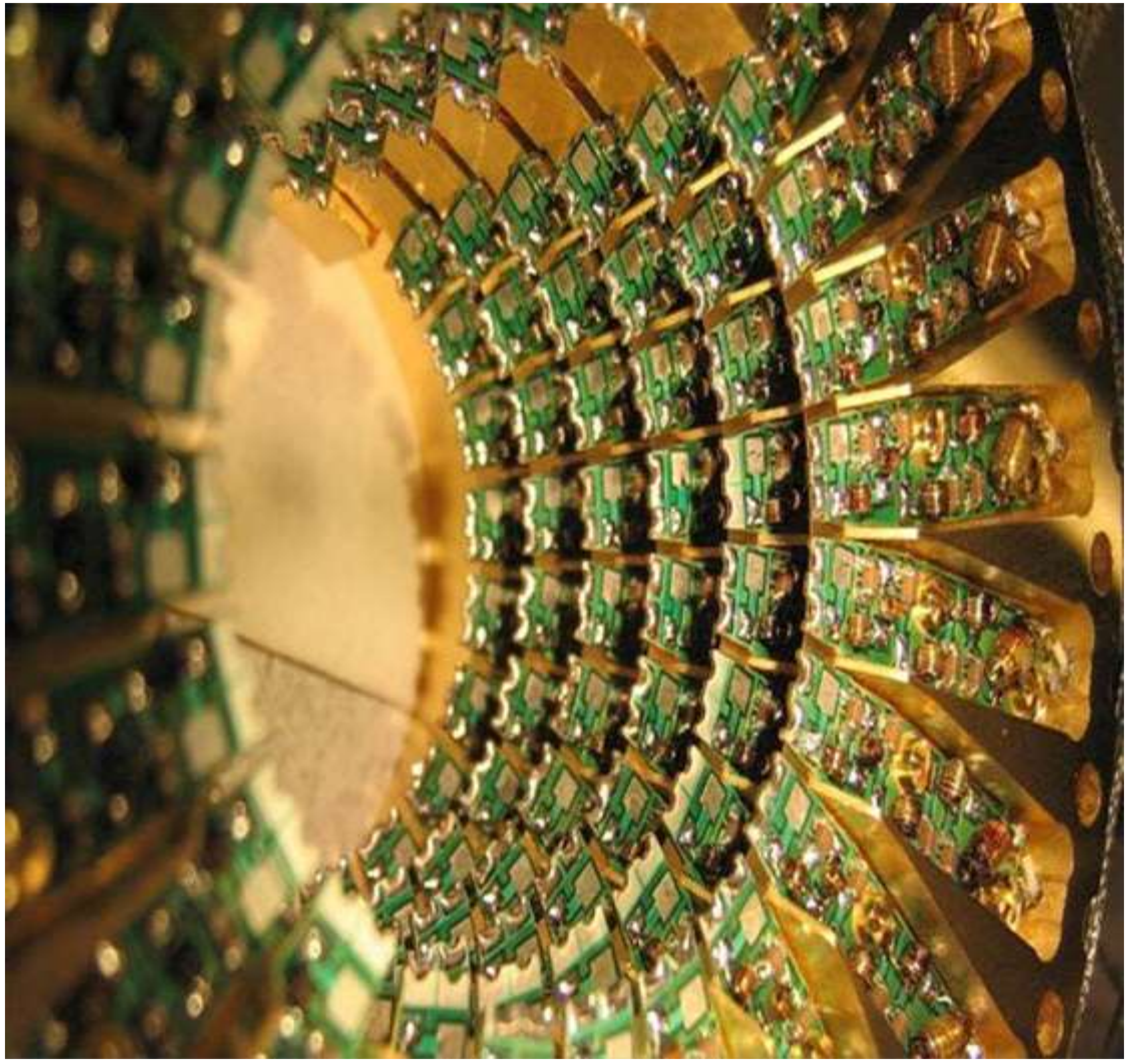
2. 实现量子计算的困难



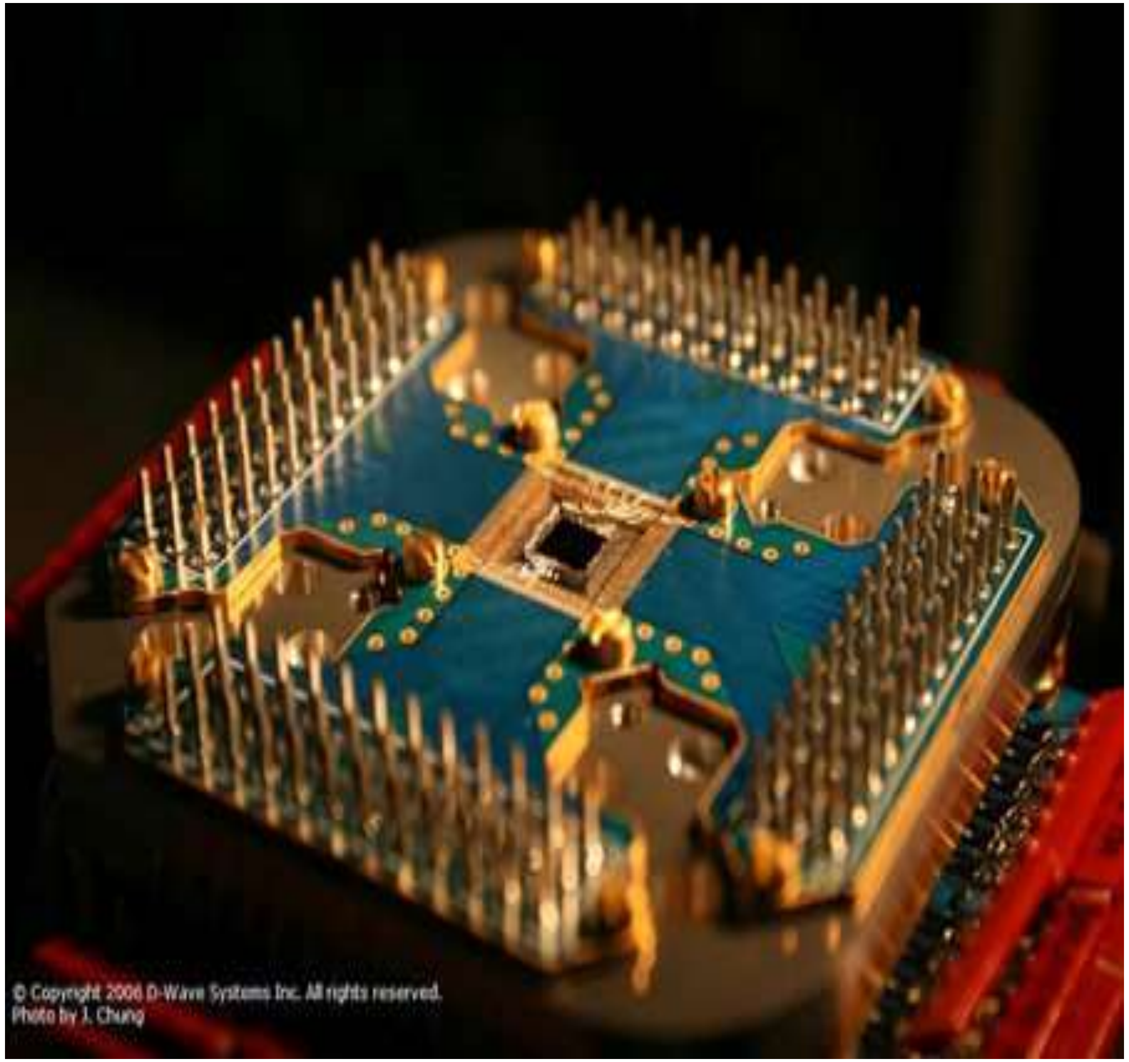
Quantum computing scaling

	Number of qubits	Gate depth	Coherence time
Scaling dimensions	Determines the quantum info that can be processed	Determines number of steps to be executed in an algorithm	Limits the max duration of the algorithm
Current state:	50–60 qubits for gate computing 2,000–5,000 qubits for annealers[1]	Circuit with gate depth 20	Depends on technology
Cases:	Google Sycamore: 54 qubits D-Wave Advantage: 5,000 qubits	Google Sycamore: gate depth 20	Trapped ion: 1–10 seconds Superconductor: Microseconds

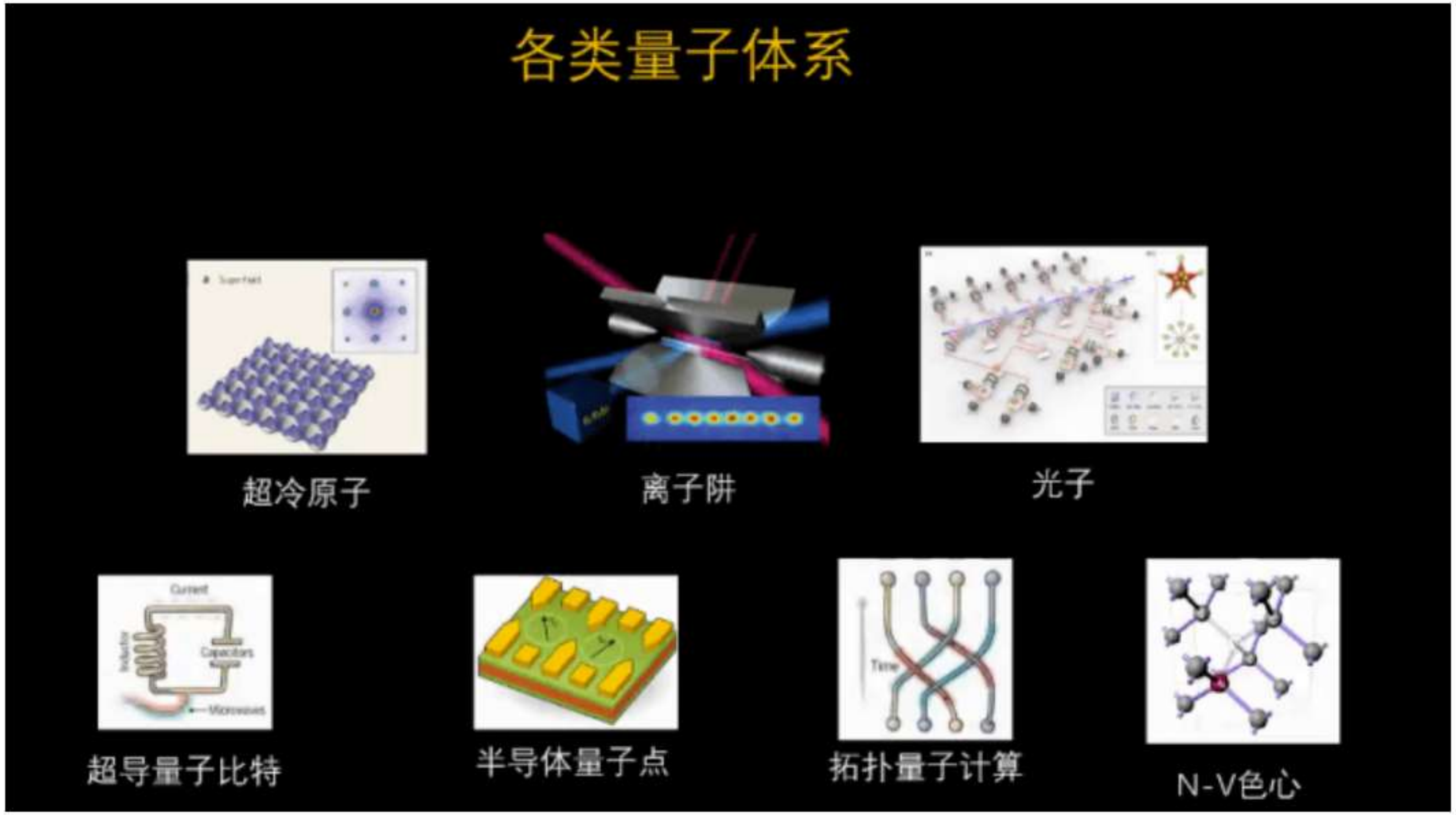
Quantum computer



Silicon chip (16 qubits)



3. 通用量子计算的设计



各类量子体系

超冷原子

离子阱

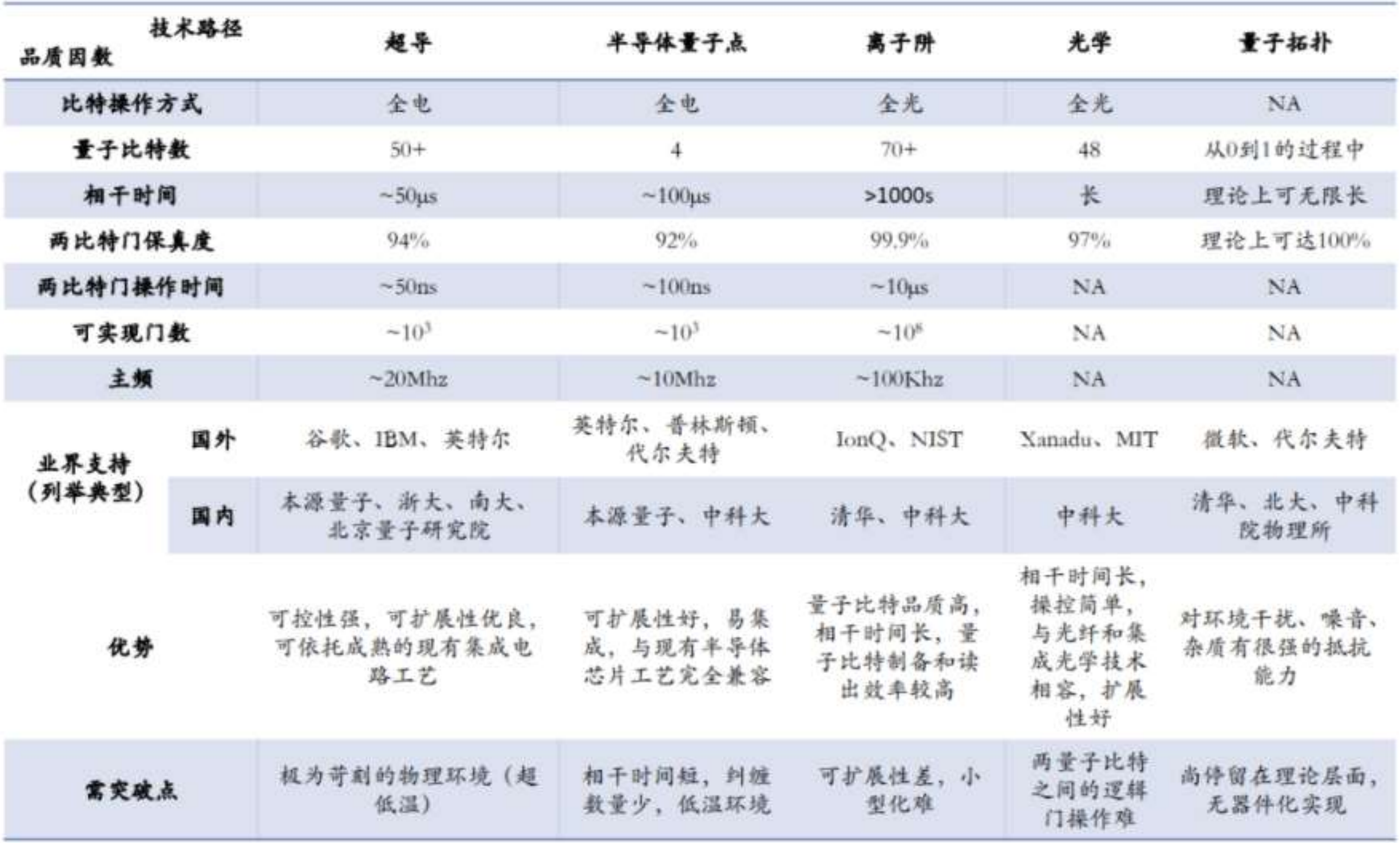
光子

超导量子比特

半导体量子点

拓扑量子计算

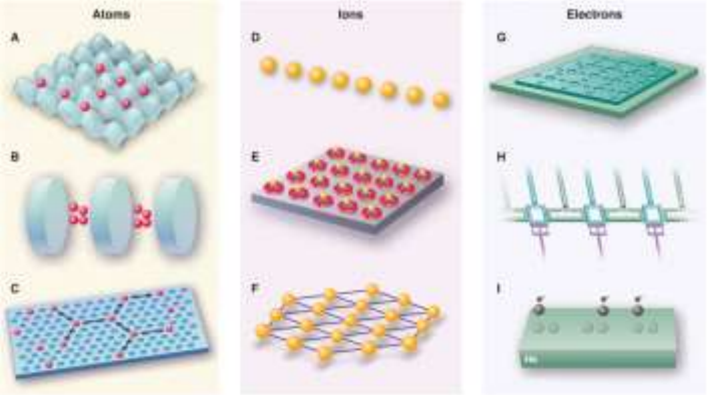
N-V色心



技术路径 品质因数		超导	半导体量子点	离子阱	光学	量子拓扑
比特操作方式		全电	全电	全光	全光	NA
量子比特数		50+	4	70+	48	从0到1的过程中
相干时间		~50μs	~100μs	>1000s	长	理论上可无限长
两比特门保真度		94%	92%	99.9%	97%	理论上可达100%
两比特门操作时间		~50ns	~100ns	~10μs	NA	NA
可实现门数		~10^3	~10^3	~10^8	NA	NA
主频		~20Mhz	~10Mhz	~100Khz	NA	NA
业界支持（列举典型）	国外	谷歌、IBM、英特尔	英特尔、普林斯顿、代尔夫特	IonQ、NIST	Xanadu、MIT	微软、代尔夫特
	国内	本源量子、浙大、南大、北京量子研究院	本源量子、中科大	清华、中科大	中科大	清华、北大、中科院物理所
优势		可控性强，可扩展性优良，可依托成熟的现有集成电路工艺	可扩展性好，易集成，与现有半导体芯片工艺完全兼容	量子比特品质高，相干时间长，量子比特制备和读出效率较高	相干时间长，操控简单，与光纤和集成光学技术相容，扩展性好	对环境干扰、噪音、杂质有很强的抵抗能力
需突破点		极为苛刻的物理环境（超低温）	相干时间短，纠缠数量少，低温环境	可扩展性差，小型化难	两量子比特之间的逻辑门操作难	尚停留在理论层面，无器件化实现

Applications of Quantum Computing

1. Cryptography: Quantum computers could break many of the current cryptographic algorithms, but they could also be used to create new, more secure ones.



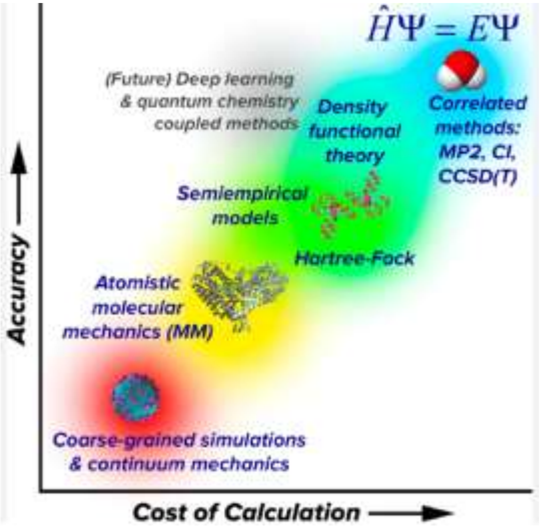
2. Simulation: Quantum computers could be used to simulate complex systems such as chemical reactions, which would be very difficult for classical computers to do.

3. Optimization: Quantum computers could be used to solve optimization problems, which are important in fields such as logistics, finance, and transportation.

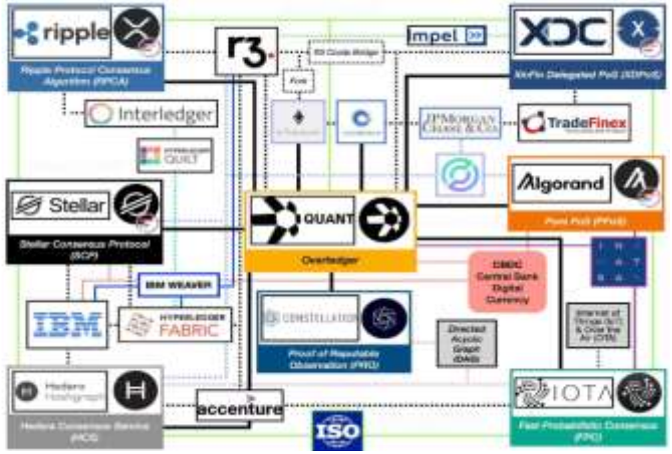
4. Machine learning: Quantum computers could be used to improve machine learning algorithms, allowing for faster and more accurate predictions.

Applications of Quantum Computing

5. Quantum chemistry: Quantum computers could be used to study and design new materials and drugs, potentially leading to breakthroughs in fields such as medicine and energy.

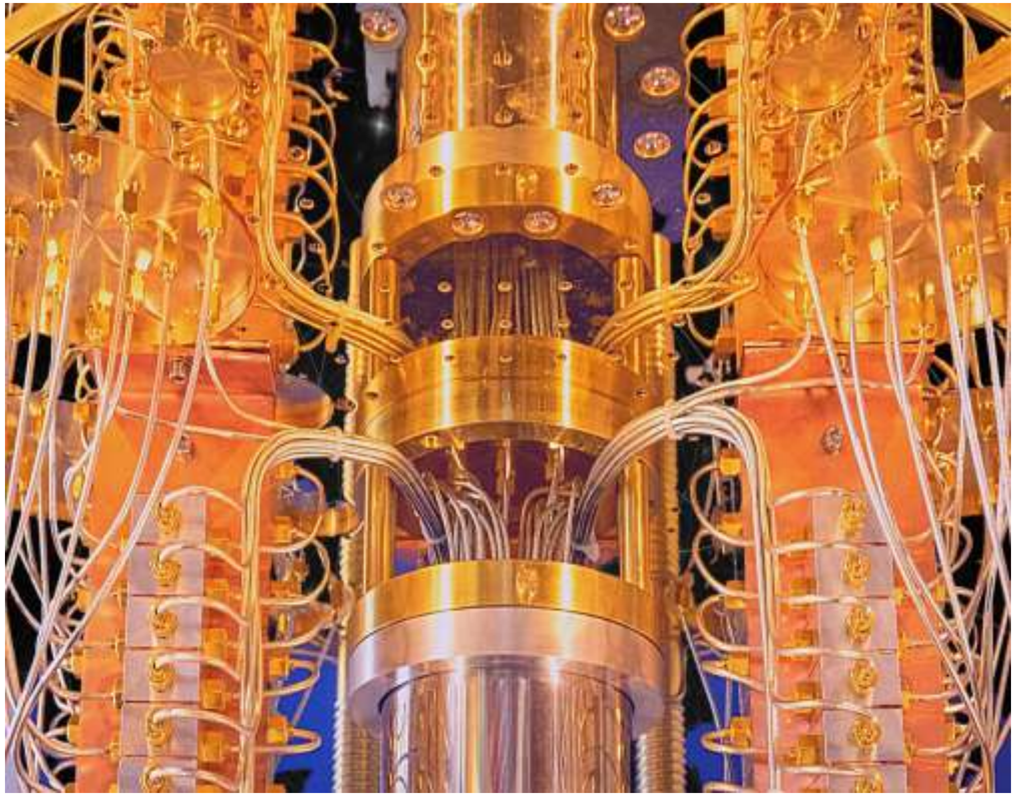


6. Financial modeling: Quantum computers could be used to simulate financial markets and optimize investment portfolios.

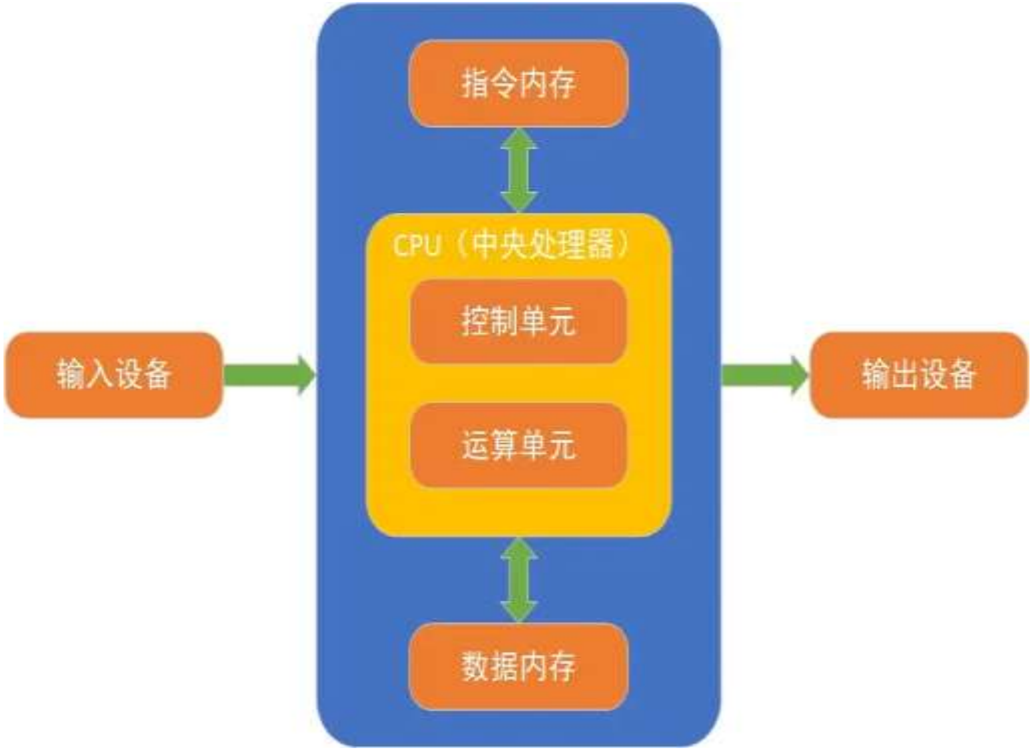

ripple
Ripple Protocol Consensus Algorithm (RPCA)
r3
R3 Corda Bridge
Fork
Impel
XDC
XinFin Delegated PoS (XDPoS)
Interledger
Hyperledger Quilt
JPMorgan Chase & Co.
TradeFinex
Stellar
Stellar Consensus Protocol (SCP)
QUANT
Overledger
Algorand
Pure PoS (PPoS)
IBM Weaver
IBM
Hyperledger Fabric
Constellation
Proof of Reputable Observation (PRO)
CBDC Central Bank Digital Currency
Directed Acyclic Graph (DAG)
Internet of Things (IoT) & Over the Air (OTA)
Hedera Hashgraph
Hedera Consensus Service (HCS)
accenture
ISO
IOTA
Fast Probabilistic Consensus (FPC)

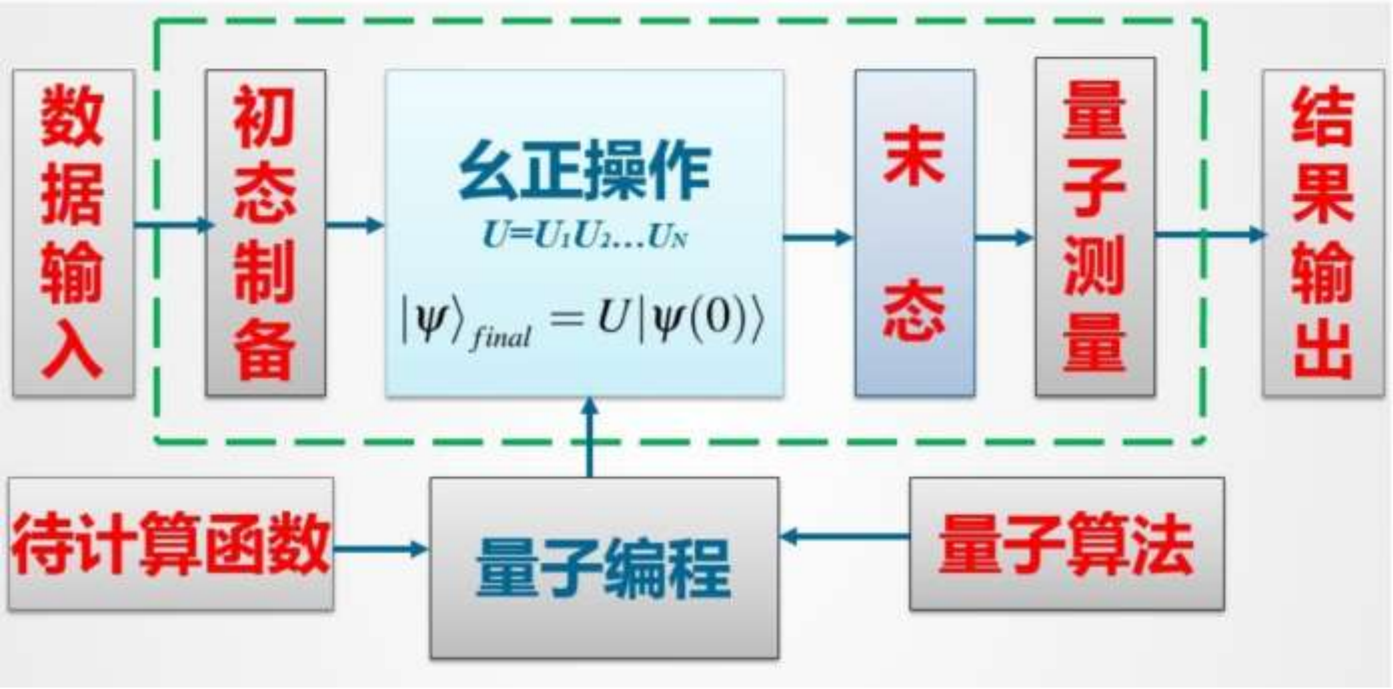
7. Weather forecasting: Quantum computers could be used to improve weather forecasting models, leading to more accurate predictions and better disaster preparedness.

Quantum computer



Quantum circuits

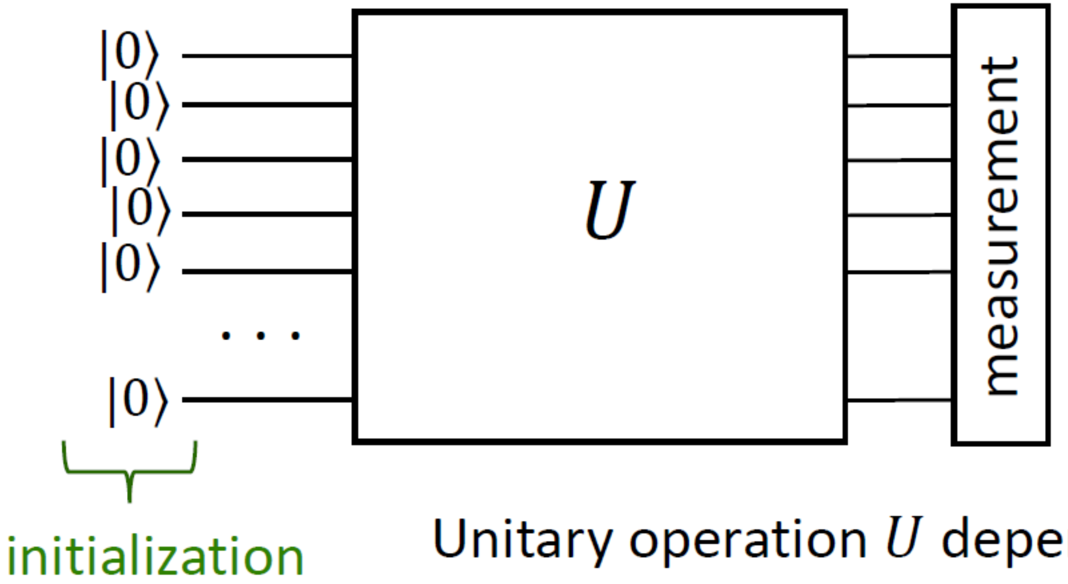




经典计算机架构

量子计算机架构

Simple structure of a quantum computer (without error correction)



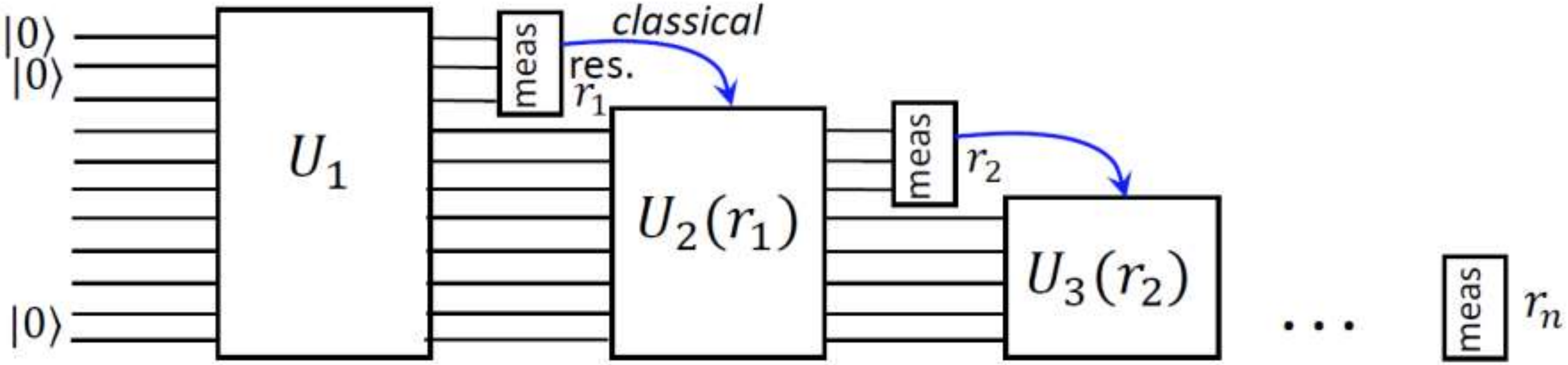
(quantum circuit diagram,
read left-to-right)

Unitary operation U depends on what we need
(e.g., a number to factor)

Idea: at the measurement stage some states are preferable (amplitudes of other states are ≈ 0), the result tells us what we need

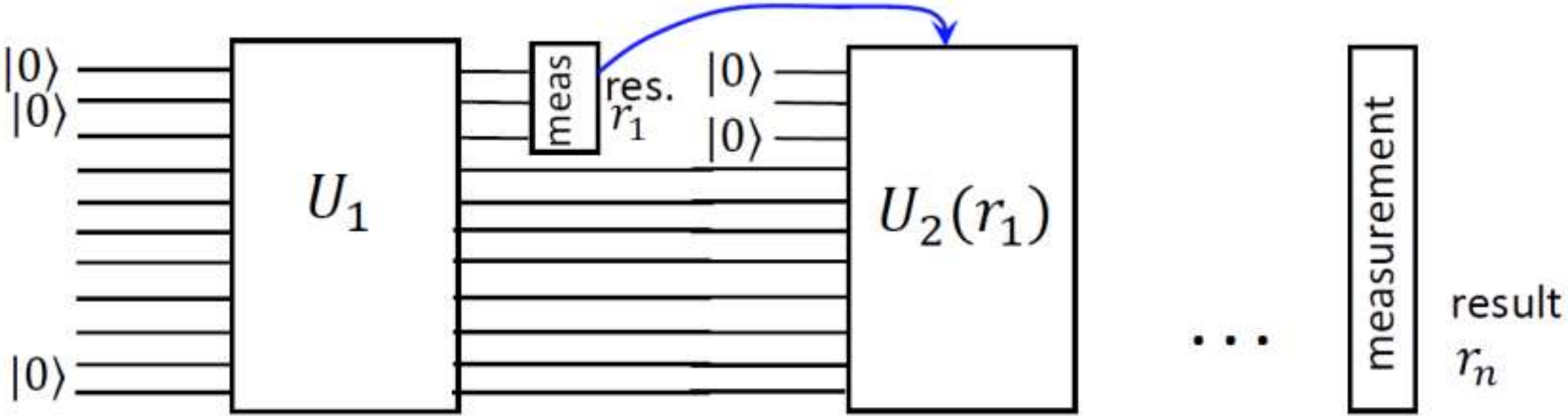
- We may need to measure only some qubits
- Still some randomness of the result (so mostly "hard to solve, easy to check" problems)

QC structure with error correction



Unitary operations U_i do not necessarily involve all qubits

Technical issue: physical qubits can be reused

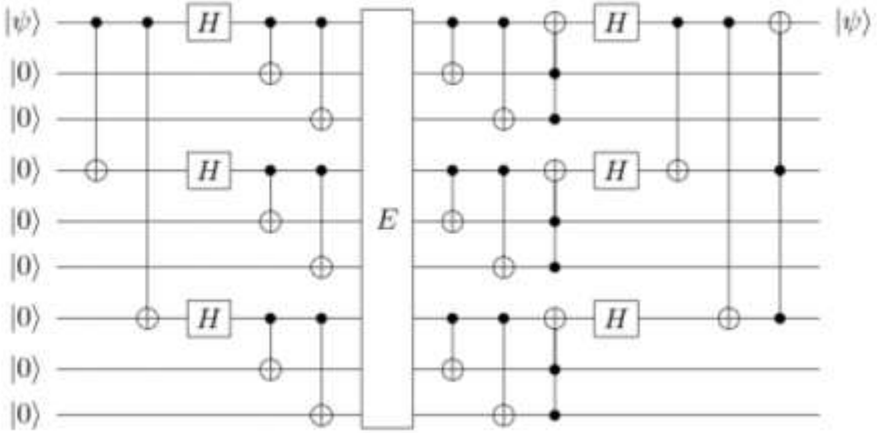


Unitary operations U_i can be decomposed into simpler gates (usually 1-qubit or 2-qubit, sometimes 3-qubit gates).

Unitary operations are reversible, so QC is related to reversible computing (classically permutations, often permutations in QC as well); measurement is irreversible.

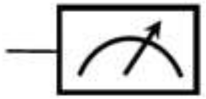
Language of quantum circuit diagrams

(more notations later when we need them)



qubit idling: thin line (“wire”) ———

several idling qubits —/— (Nielsen-Chuang’s book) ━━━ (Mermin’s book)

measurement  (N-C book) $\overset{\boxed{x}}{-\boxed{\mathrm{M}}}$ ← result (Mermin) $-\boxed{\text{meas.}}$

Read quantum circuit diagrams from left to right (⟶)

$$|\psi\rangle \;—\boxed{U}—\; U|\psi\rangle$$

$$|\psi\rangle \;—\boxed{U}—\boxed{V}—\; VU|\psi\rangle$$

So $-\boxed{U}-\boxed{V}- \;=\; -\boxed{VU}-$

One-qubit logic gates

“gate” = “operation” = “function” = “map” = “transformation”

Classically, 4 one-bit functions: $$\underbrace{\begin{matrix}0\to0\\1\to1\end{matrix}}_{\mathbb{I}} \quad \underbrace{\begin{matrix}0\to1\\1\to0\end{matrix}}_{\text{NOT}} \quad \underbrace{\underbrace{\begin{matrix}0\to0\\1\to0\end{matrix}}_{\text{erase}} \quad \underbrace{\begin{matrix}0\to1\\1\to1\end{matrix}}_{\text{erase}'}}_{\text{not reversible}}$$

So, only 2 reversible 1-bit operations: NOT ($0 \leftrightarrow 1$) and unity operation

Quantum 1-qubit gate: any **unitary** 2×2 matrix

“Unitary” means $UU^\dagger = UU^\dagger = \mathbb{I}\ (= \hat{1})$

Actually, not U(2) group, but SU(2); “special” means $\det(U) = 1$

overall phase is not important for a 1-qubit gate
(though will be important for control-gates)

A unitary matrix has $8 - 4 = 4$ degrees of freedom

$\nwarrow UU^\dagger = \mathbb{I}$

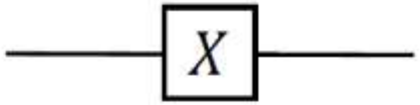
A matrix from SU(2) has 3 degrees of freedom, SU(2)↔SO(3) (3D rotation group)

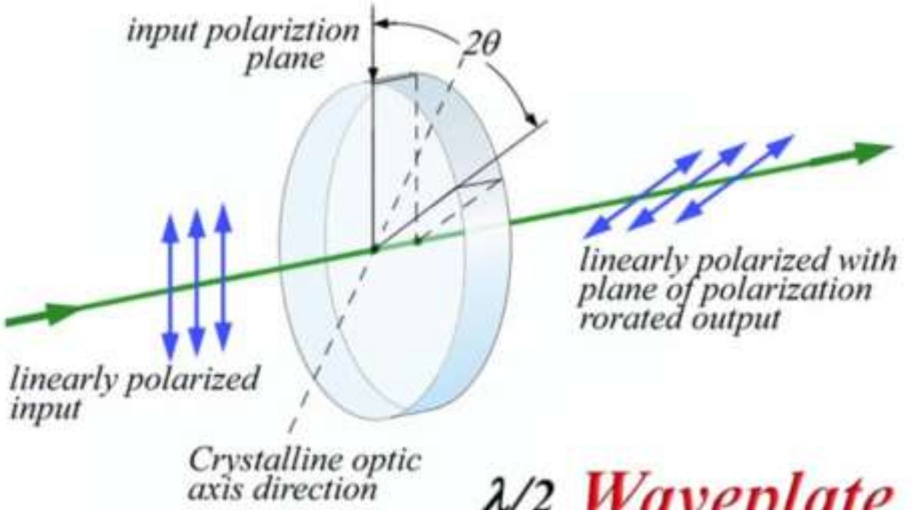
A qubit state: direction of spin, a rotation is characterized by 3 Euler angles

Most important 1-qubit gates

1. Bit flip (NOT, X-gate, Pauli-X)

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = X = \sigma_X = NOT$$




input polariztion plane
2θ
linearly polarized with plane of polarization rorated output
linearly polarized input
Crystalline optic axis direction

λ/2 **Waveplate**

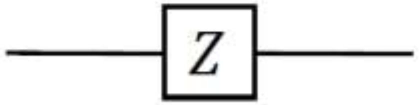
$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix} \quad \text{so} \quad \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \rightarrow \begin{pmatrix} \beta \\ \alpha \end{pmatrix} \begin{array}{l} \longleftarrow |0\rangle \\ \longleftarrow |1\rangle \end{array}$$

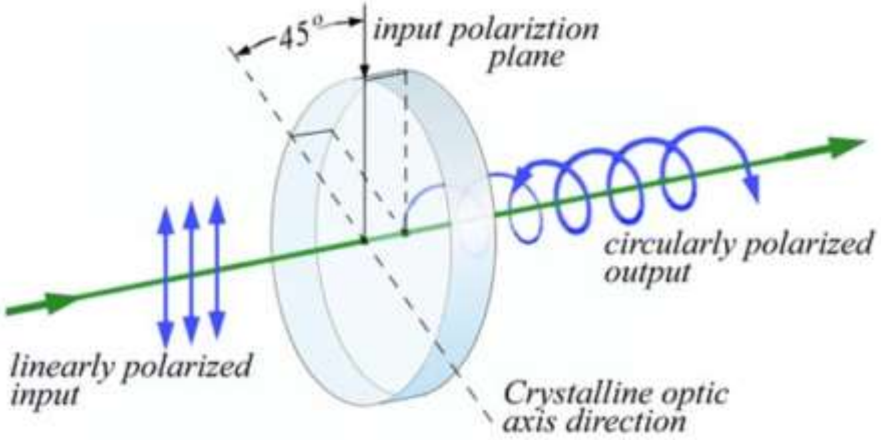
$$\alpha|0\rangle + \beta|1\rangle \rightarrow \beta|0\rangle + \alpha|1\rangle$$

$$X|0\rangle = |1\rangle$$
$$X|1\rangle = |0\rangle$$

2. Phase flip (Z-gate)

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





λ/4 **Waveplate**

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

$$Z[\alpha|0\rangle + \beta|1\rangle] = \alpha|0\rangle - \beta|1\rangle$$

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

$$Z|0\rangle = |0\rangle$$
$$Z|1\rangle = -|1\rangle$$

Most important 1-qubit gates (cont.)

3. Phase & bit flip (Y-gate)

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

$$Y[\alpha|0\rangle + \beta|1\rangle] = -i\beta|0\rangle + i\alpha|1\rangle$$

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \rightarrow \begin{pmatrix} -i\beta \\ i\alpha \end{pmatrix}$$

$$Y|0\rangle = i|1\rangle$$
$$Y|1\rangle = -i|0\rangle$$

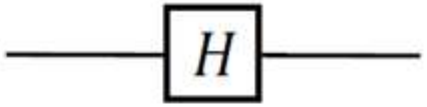
$$Y = iXZ = -iZX$$

Very often defined differently: $Y = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ or $Y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ Mermin-web (Eqs. 1.48, 1.49)

In Mermin-book the usual definition (Eq. 1.51), except in Ch. 5 (error correction)

4. Hadamard

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



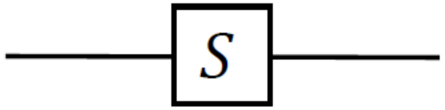
$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \rightarrow \begin{pmatrix} \dfrac{\alpha + \beta}{\sqrt{2}} \\ \dfrac{\alpha - \beta}{\sqrt{2}} \end{pmatrix}$$

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \qquad H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Most important 1-qubit gates (cont.)

5. Phase gate

$$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/2} \end{pmatrix} = S$$



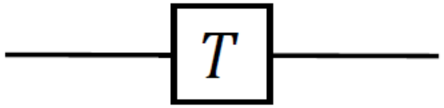
Notation from N-C book

$$S = \sqrt{Z} \quad \text{since} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi} \end{pmatrix}$$

Do not confuse with Mermin's notation S_{ij} for SWAP

6. "$\pi/8$"-gate or T-gate

$$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} = T$$



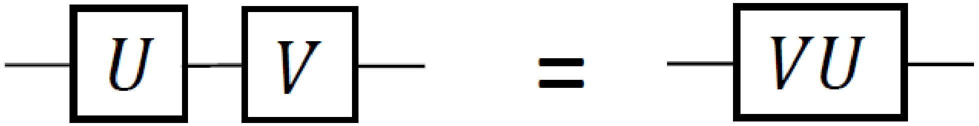
Notation from N-C book

$$T = \sqrt{S}$$

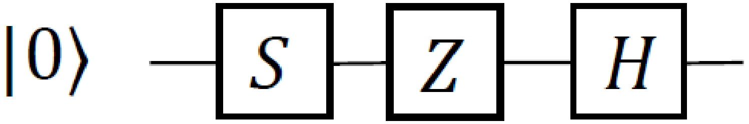
Called $\pi/8$ because equivalent to $\exp(-i\frac{\pi}{8}Z)$

Sequential gates

Possible confusion: left-to-right in quantum circuit diagrams,
right-to-left in matrix notations



Example



means

$$H\,Z\,S\,|0\rangle = \underset{H}{\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}} \underset{Z}{\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}} \underset{S}{\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}} \underset{|0\rangle}{\begin{pmatrix} 1 \\ 0 \end{pmatrix}}$$

Some useful relations

$$\boxed{X^2 = Y^2 = Z^2 = \mathbb{I}} \qquad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$\boxed{H^2 = \mathbb{I}} \qquad H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$XY = -YX = iZ$$

$$YZ = -ZY = iX$$

$$ZX = -XZ = iY$$

The factor i is not important (overall phase), therefore sufficient to consider X and Z.

$$\boxed{HXH = Z, \ \ HZH = X}$$

Check

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

exchange rows

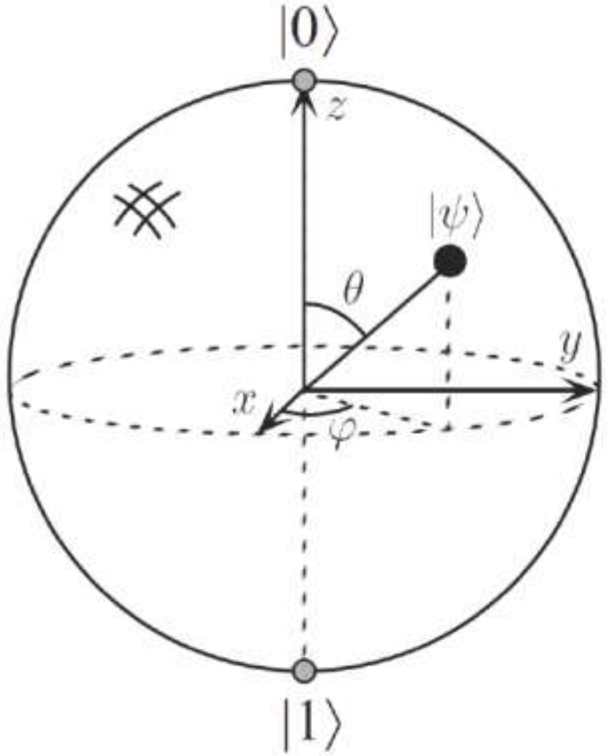
$$XA = A_{\text{EXCHANGED ROWS}} \qquad AX = A_{\text{EXCHANGED COLUMNS}}$$

The second equation $HXH = Z \Rightarrow HH\underbrace{X}HH = HZH$

Bloch sphere (some physical meaning)

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

irrelevant



θ: zenith (polar) angle, $0 \le \theta \le \pi$

φ: azimuth angle, $\mod 2\pi$

(often $|0\rangle$ at the bottom, $|1\rangle$ at the top)

Corresponds to direction of a spin in real space

Z axis → $|0\rangle$

$-Z$ axis → $|1\rangle$

X axis → $\dfrac{|0\rangle + |1\rangle}{\sqrt{2}}$

$-X$ axis → $\dfrac{|0\rangle - |1\rangle}{\sqrt{2}}$

Y axis → $\dfrac{|0\rangle + i|1\rangle}{\sqrt{2}}$

$-Y$ axis → $\dfrac{|0\rangle - i|1\rangle}{\sqrt{2}}$

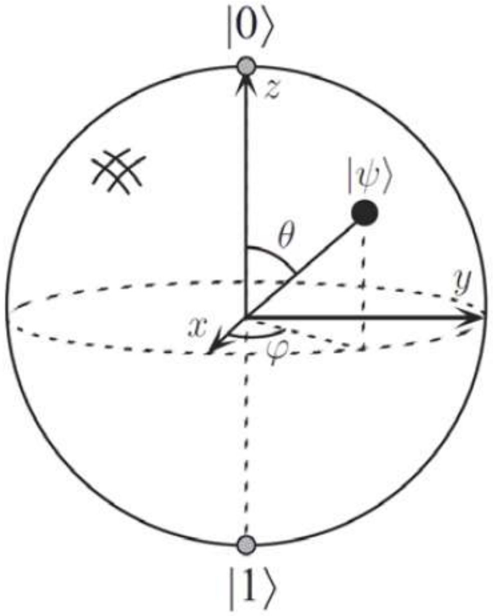
equator → $\dfrac{|0\rangle + e^{i\varphi}|1\rangle}{\sqrt{2}}$

XZ plane → $\cos\frac{\theta}{2}|0\rangle \pm \sin\frac{\theta}{2}|1\rangle$

YZ plane → $\cos\frac{\theta}{2}|0\rangle \pm i\sin\frac{\theta}{2}|1\rangle$

Orthogonal vectors in Hilbert space correspond to opposite directions on Bloch sphere

Main 1-qubit operations on the Bloch sphere (cont.)



$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ Rotation about Z-axis by π (180°)

$Y = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}$ Rotation about Y-axis by π (180°)

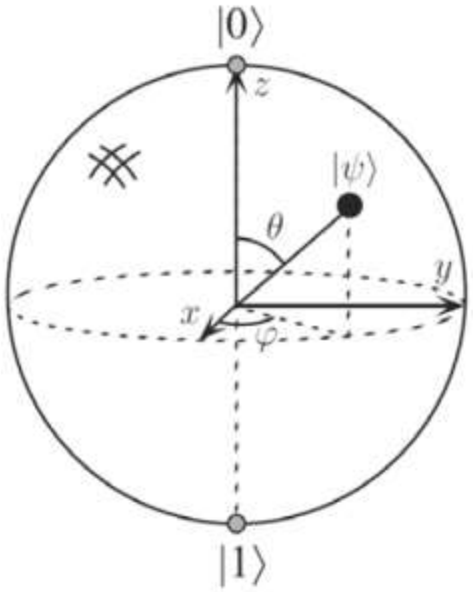
$H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ Rotation by π about axis in XZ plane, which is at angle $\pi/4$ from Z and X

Now it is obvious why $X^2 = Y^2 = Z^2 = H^2 = \hat{1}$, just a rotation by 2π

$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$ Rotation about Z-axis by $\pi/2$ (90°)

$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$ Rotation about Z-axis by $\pi/4$ (45°)

Main 1-qubit operations on the Bloch sphere (cont.)



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

Rotation by π about axis in XZ plane, which is at angle $\pi/4$ from Z and X

Another rotation realization for Hadamard

$$H = R_Y(\pi/2)\, R_Z(\pi)$$

(rotation about Z by π and rotation about Y by $\pi/2$)

Check:

$$\underbrace{\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$\left.\begin{aligned} |0\rangle &\to \frac{|0\rangle + |1\rangle}{\sqrt{2}} \\ |1\rangle &\to \frac{-|0\rangle + |1\rangle}{\sqrt{2}} \end{aligned}\right\}$$

Counterclockwise rotation about Y by $\pi/2$

Bell states

Entanglement-based protocols generally rely on using the following four states of a two-qubit system, known as the Bell states:

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \qquad |\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$
$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \qquad |\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

They form an orthonormal basis for $\mathbb{C}^4$, known as the Bell basis.
An orthogonal measurement in this basis is called Bell measurement.

These states can be written concisely as follows ($\bar{x} \equiv x \oplus 1$):

$$|\beta_{zx}\rangle = \frac{1}{\sqrt{2}}(|0, x\rangle + (-1)^z|1, \bar{x}\rangle)$$

Note that, in each of the states, measuring either qubit in the computational basis yields $|0\rangle$ or $|1\rangle$ with equal probability, and after the measurement, the other bit is uniquely determined.

Super-Dense Coding with Entangled Photons

- Alice and Bob Share a Singlet State of Two Photons:

$$|\psi^-\rangle_{AB} = \frac{|H\rangle_A|V\rangle_B - |V\rangle_A|H\rangle_B}{\sqrt{2}}$$

- Alice Uses Two Classical Bits to Modulate Her Photon:

$$\begin{aligned}
\alpha|H\rangle_A + \beta|V\rangle_A &\longrightarrow \alpha|H\rangle_A + \beta|V\rangle_A, \quad \text{if } m = 00 \\
\alpha|H\rangle_A + \beta|V\rangle_A &\longrightarrow \alpha|H\rangle_A - \beta|V\rangle_A, \quad \text{if } m = 01 \\
\alpha|H\rangle_A + \beta|V\rangle_A &\longrightarrow \alpha|V\rangle_A + \beta|H\rangle_A, \quad \text{if } m = 10 \\
\alpha|H\rangle_A + \beta|V\rangle_A &\longrightarrow \alpha|V\rangle_A - \beta|H\rangle_A, \quad \text{if } m = 11
\end{aligned}$$

Two-qubit states and 2-qubit gates

Two-qubit states

$$|\psi\rangle = \underset{\substack{\parallel \\ \alpha_1}}{\alpha_{00}}|00\rangle + \underset{\substack{\parallel \\ \alpha_2}}{\alpha_{01}}|01\rangle + \underset{\substack{\parallel \\ \alpha_3}}{\alpha_{10}}|10\rangle + \underset{\substack{\parallel \\ \alpha_4}}{\alpha_{11}}|11\rangle = \begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{pmatrix}$$

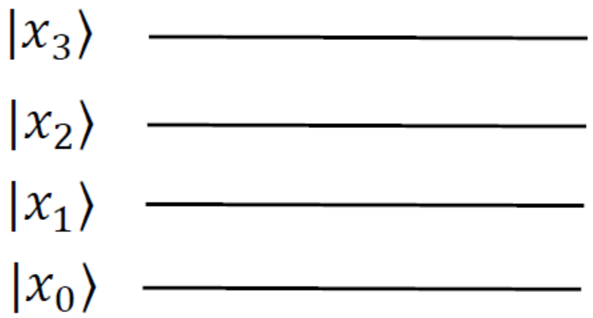
$$\begin{cases} |\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1 \\ \text{Overall phase is not important} \Rightarrow \text{can choose } \alpha_0 \text{ real} \end{cases}$$

$8 - 2 = 6$ degrees of freedom $(2 \cdot 2^k - 2$ degrees of freedom for k qubits$)$

Notations for multi-qubit computational-basis states

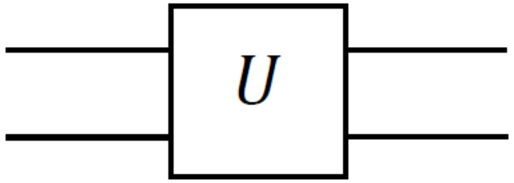
$$|x_3\, x_2\, x_1\, x_0\rangle \equiv |x_3\rangle|x_2\rangle|x_1\rangle|x_0\rangle \equiv |x_3\rangle \otimes |x_2\rangle \otimes |x_1\rangle \otimes |x_0\rangle$$

Computational-basis state, represents classical state $\sum x_n 2^n$



(most significant bit at the top)

Two-qubit gates



Any unitary 4×4 matrix
(overall phase is not important)

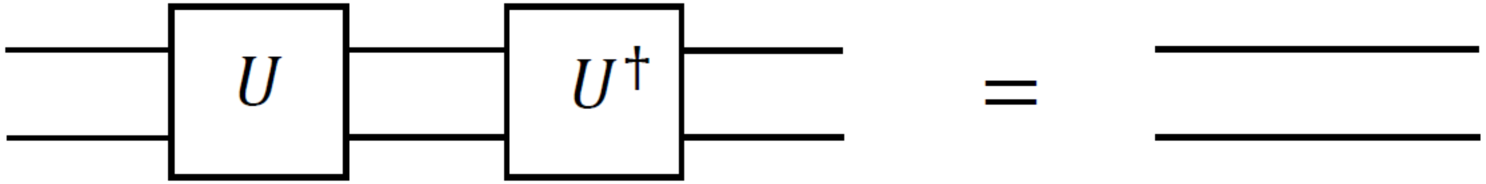
Can be defined by transformation of the basis vectors:

$|00\rangle \to$ … (4 complex numbers)
$|01\rangle \to$ … (4)
$|10\rangle \to$ … (4)
$|11\rangle \to$ … (4)

Then linearity

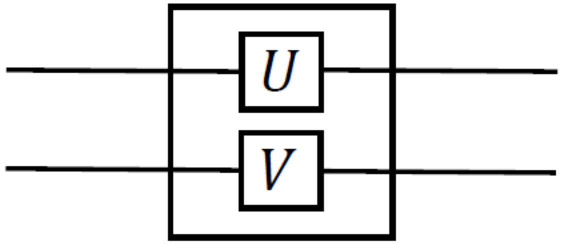
Degrees of freedom: $32 - \underset{\text{unitary}}{16} - \underset{\text{overall phase}}{1} = 15$ (for k qubits $4^k - 1$)

Reversible:



Examples of two-qubit gates

1. Trivial: tensor-product gates

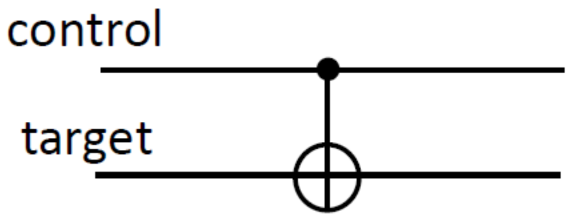


Math structure: tensor-product of matrices

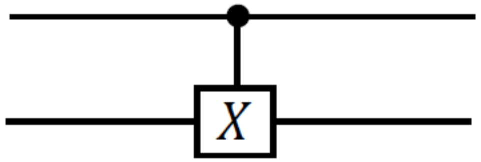
$$U \otimes V = \begin{pmatrix} U_{00}\begin{pmatrix} V_{00} & V_{01} \\ V_{10} & V_{11} \end{pmatrix} & U_{01}\begin{pmatrix} V_{00} & V_{01} \\ V_{10} & V_{11} \end{pmatrix} \\ U_{10}\begin{pmatrix} V_{00} & V_{01} \\ V_{10} & V_{11} \end{pmatrix} & U_{11}\begin{pmatrix} V_{00} & V_{01} \\ V_{10} & V_{11} \end{pmatrix} \end{pmatrix}$$

2– 5. Many gates are of controlled type: one qubit controls the other one (consider next)

2. Controlled-NOT (CNOT)



or



(Mermin's book)

Generalizes classical CNOT: target bit is flipped if control bit is 1

control target

$$|00\rangle \to |00\rangle$$
$$|01\rangle \to |01\rangle$$
$$|10\rangle \to |11\rangle$$
$$|11\rangle \to |10\rangle$$

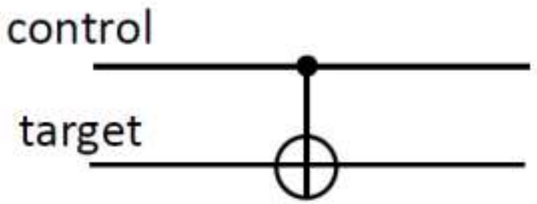
Matrix

$$\begin{array}{cc} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} & \begin{array}{l} \longleftarrow 00 \\ \longleftarrow 01 \\ \longleftarrow 10 \\ \longleftarrow 11 \end{array} \end{array}$$

Unitary matrix; can be checked, but actually trivial, because a permutation of computational basis

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

CNOT (cont.)



Notation: CNOT_{ij} or C_{ij} (Mermin’s book)

control target

$$\mathrm{CNOT}_{10}|x\rangle|y\rangle = |x\rangle\,|y \oplus x\rangle$$

for computational basis

qubit 1 qubit 0 addition modulo 2

(again, transformation for other states defined by linearity)

$$\mathrm{CNOT}_{01}|x\rangle|y\rangle = |x \oplus y\rangle\,|y\rangle$$

Actually, not possible to say that nothing happens to the control qubit; this is true only if it is $|0\rangle$ or $|1\rangle$. If control qubit is in a superposition state, it gets entangled with the target qubit. Then it will not have a state by itself, and it may depend on what happens next with the target qubit.

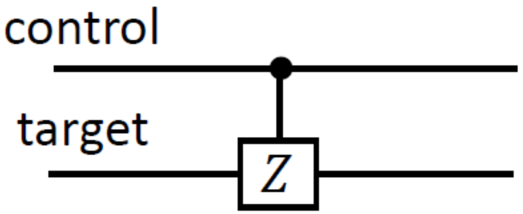
Example

$$\frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}} = \frac{|00\rangle-|01\rangle+|10\rangle-|11\rangle}{2} \longrightarrow$$

Control changes, while target the same!

$$\longrightarrow \frac{|00\rangle-|01\rangle+|11\rangle-|10\rangle}{2} = \frac{|0\rangle-|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

3. Controlled-Z (CZ)



Phase-flip of target if control is $|1\rangle$

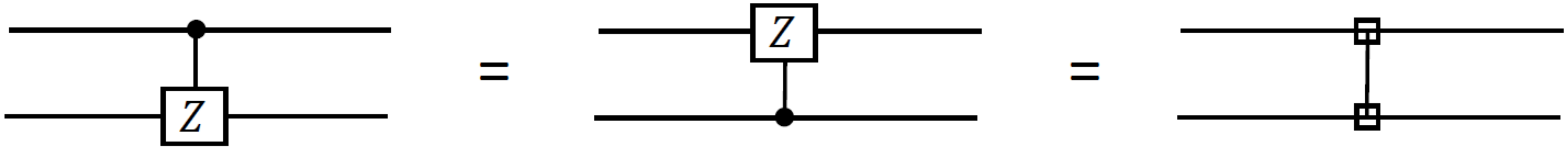
control target

$$|00\rangle \rightarrow |00\rangle$$
$$|01\rangle \rightarrow |01\rangle$$
$$|10\rangle \rightarrow |10\rangle$$
$$|11\rangle \rightarrow -|11\rangle$$

Matrix

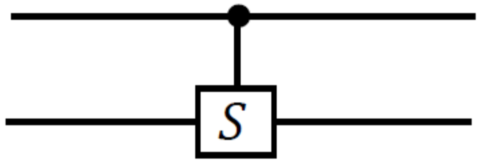
$$\begin{array}{cl} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} & \begin{array}{l} \leftarrow 00 \\ \leftarrow 01 \\ \leftarrow 10 \\ \leftarrow 11 \end{array} \end{array}$$

Somewhat surprisingly, symmetric



(Nielsen-Chuang)

4. Controlled-phase (C-phase)



Phase-S gate if control is $|1\rangle$

control target

$$|00\rangle \rightarrow |00\rangle$$
$$|01\rangle \rightarrow |01\rangle$$
$$|10\rangle \rightarrow |10\rangle$$
$$|11\rangle \rightarrow i|11\rangle$$

Matrix

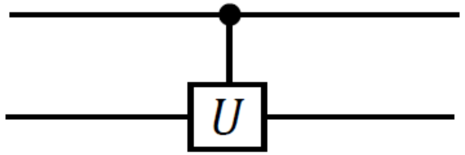
$$\begin{array}{cc} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \end{pmatrix} & \begin{array}{l} \leftarrow 00 \\ \leftarrow 01 \\ \leftarrow 10 \\ \leftarrow 11 \end{array} \end{array}$$

Also symmetric

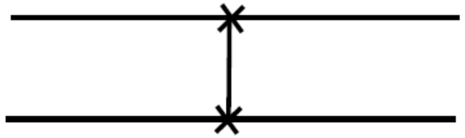
Note that often controlled-phase means $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\varphi} \end{pmatrix}$

Examples of two-qubit gates (cont.)

5. Any controlled-U



5. SWAP



(Nielsen-Chuang)

$|00\rangle \rightarrow |00\rangle$

$|01\rangle \rightarrow |10\rangle$

$|10\rangle \rightarrow |01\rangle$

$|11\rangle \rightarrow |11\rangle$

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

Symmetric

Notation SWAP_{ij}

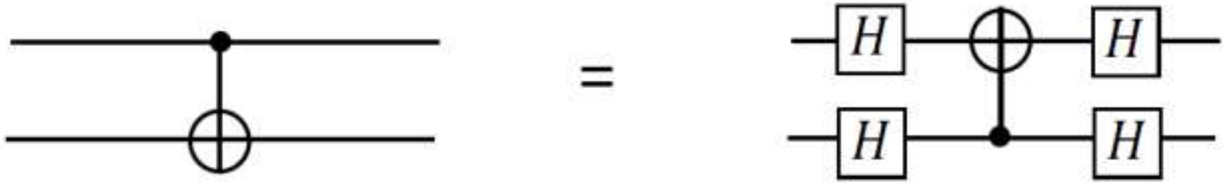
S_{ij} (Mermin)

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

Useful relations between two-qubit gates

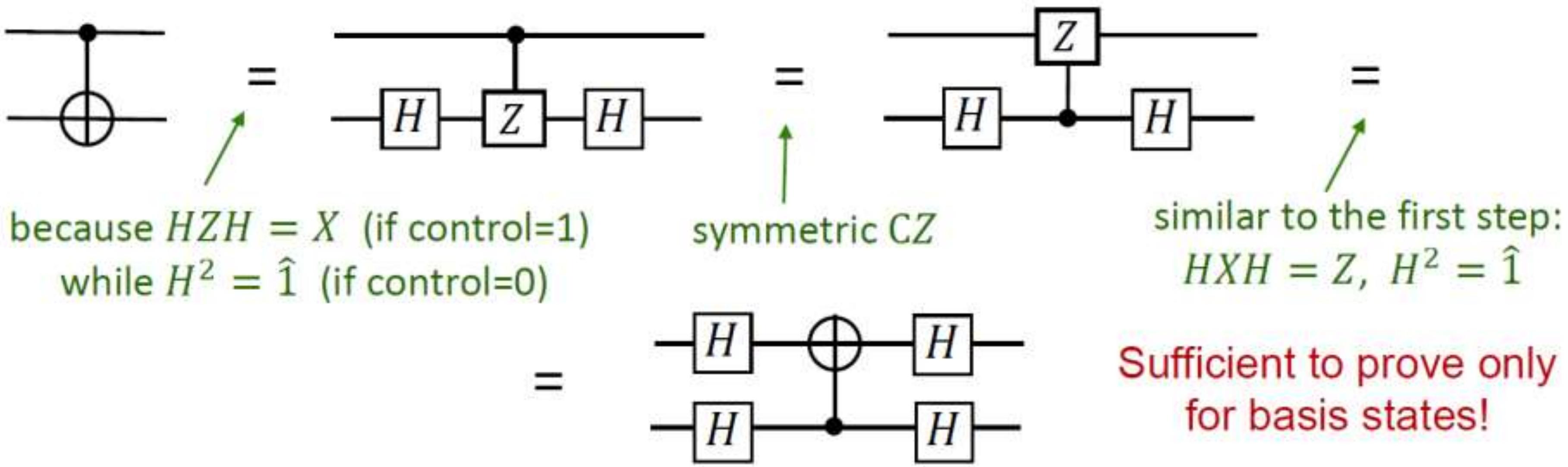
1. $$\left(\mathrm{CNOT}_{ij}\right)^2 = \left(\mathrm{CZ}_{ij}\right)^2 = \left(\mathrm{SWAP}_{ij}\right)^2 = \hat{1}$$

2. $$\mathrm{CNOT}_{ij} = \left(H_i H_j\right) \mathrm{CNOT}_{ji} \left(H_i H_j\right)$$



So, who controls whom is a matter of preference!

Proof



because $HZH = X$ (if control=1)
while $H^2 = \hat{1}$ (if control=0)

symmetric CZ

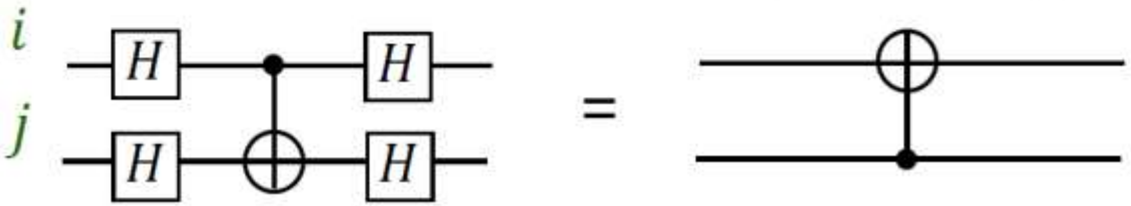
similar to the first step:
$HXH = Z,\ H^2 = \hat{1}$

Sufficient to prove only for basis states!

$\mathrm{CNOT}_{ij} = \left(H_iH_j\right)\mathrm{CNOT}_{ji}\left(H_iH_j\right)$ (cont.)

One more (direct) proof

Let us prove the opposite (equivalent) relation



$$|00\rangle \xrightarrow{H_iH_j} \frac{|0\rangle+|1\rangle}{\sqrt{2}}\,\frac{|0\rangle+|1\rangle}{\sqrt{2}} = \frac{1}{2}\left(|00\rangle+|01\rangle+|10\rangle+|11\rangle\right) \longrightarrow$$

$$\xrightarrow{\mathrm{CNOT}_{ij}} \frac{1}{2}\left(|00\rangle+|01\rangle+|11\rangle+|10\rangle\right) \xrightarrow{H_iH_j} |00\rangle$$

(as should be)

(the same)

$$|01\rangle \xrightarrow{H_iH_j} \frac{|0\rangle+|1\rangle}{\sqrt{2}}\,\frac{|0\rangle-|1\rangle}{\sqrt{2}} = \frac{1}{2}\left(|00\rangle-|01\rangle+|10\rangle-|11\rangle\right) \longrightarrow$$

$$\xrightarrow{\mathrm{CNOT}_{ij}} \frac{1}{2}\left(|00\rangle-|01\rangle+|11\rangle-|10\rangle\right) = \frac{\left(|0\rangle-|1\rangle\right)|0\rangle-\left(|0\rangle-|1\rangle\right)|1\rangle}{2} =$$

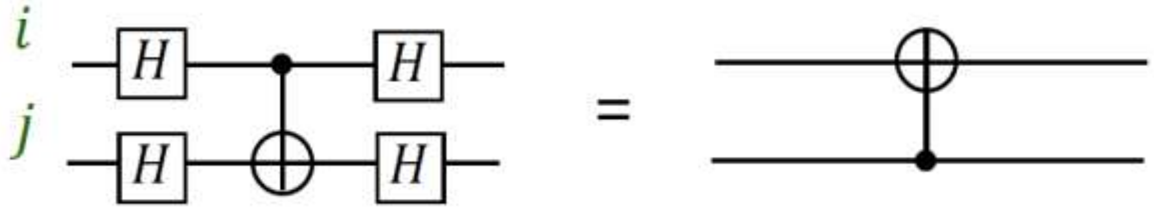
$$= \frac{|0\rangle-|1\rangle}{\sqrt{2}}\,\frac{|0\rangle-|1\rangle}{\sqrt{2}} \xrightarrow{H_iH_j} |11\rangle$$

(as should be)

since $H^2 = \hat{1}$

Two more initial states

$\mathrm{CNOT}_{ij} = \left(H_i H_j\right) \mathrm{CNOT}_{ji} \left(H_i H_j\right)$ (cont.)



(equivalent relation, $i \leftrightarrow j$)

Already showed: $|00\rangle \longrightarrow |00\rangle$, $|01\rangle \longrightarrow |11\rangle$

$$|10\rangle \xrightarrow{H_i H_j} \frac{0-1}{\sqrt{2}} \frac{0+1}{\sqrt{2}} \xrightarrow{\mathrm{CNOT}_{ij}} \frac{0\,(0+1) - 1\,(1+0)}{2} = \frac{0-1}{\sqrt{2}} \frac{0+1}{\sqrt{2}} \xrightarrow{H_i H_j} |10\rangle$$

(for brevity do not write ket-notation)

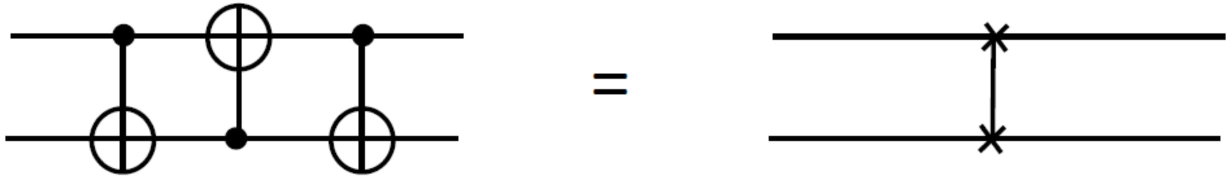
$$|11\rangle \xrightarrow{H_i H_j} \frac{0-1}{\sqrt{2}} \frac{0-1}{\sqrt{2}} \xrightarrow{\mathrm{CNOT}_{ij}} \frac{0\,(0-1) - 1\,(1-0)}{2} = \frac{0+1}{\sqrt{2}} \frac{0-1}{\sqrt{2}} \xrightarrow{H_i H_j} |01\rangle$$

We proved the relation for 4 initial basis states $\Rightarrow$ should hold for <u>any</u> initial state

Important example, it shows that CNOT is not a one-way action,
this is an interaction (has "quantum back-action")

Useful relations between two-qubit gates (cont.)

3. $$\mathrm{SWAP}_{ij} = \mathrm{CNOT}_{ij}\ \mathrm{CNOT}_{ji}\ \mathrm{CNOT}_{ij}$$



Proof

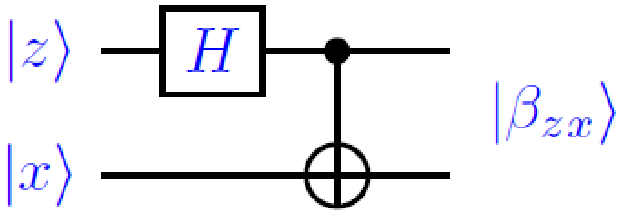
Again, consider only (computational) basis states for initial state

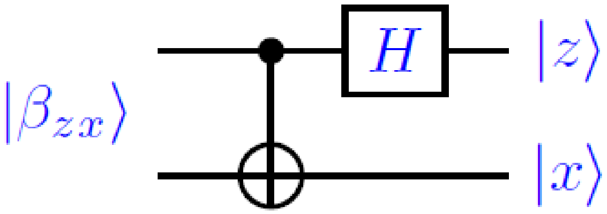
$$|x\rangle_i\,|y\rangle_j \xrightarrow{\mathrm{CNOT}_{ij}} |x\rangle_i\,|x\oplus y\rangle_j \xrightarrow{\mathrm{CNOT}_{ji}} |x\oplus x\oplus y\rangle_i\,|x\oplus y\rangle_j = |y\rangle_i\,|x\oplus y\rangle_j \longrightarrow$$

$$\xrightarrow{\mathrm{CNOT}_{ij}} |y\rangle_i\,|x\oplus y\oplus y\rangle_j = |y\rangle_i\,|x\rangle_j$$

Properties of Bell states

Preparation / unpreparation: A global unitary can generate the Bell states from the computational basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ and vice versa:





$$|\beta_{zx}\rangle = \text{CNOT} \cdot (H \otimes I) \cdot |z, x\rangle \qquad |z, x\rangle = (H \otimes I) \cdot \text{CNOT} \cdot |\beta_{zx}\rangle$$

Local conversion: Any Bell state can be converted into any other by either of the two parties using only local (Pauli) unitaries:

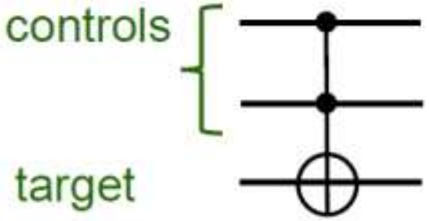
$$|\beta_{zx}\rangle = (Z^z X^x \otimes I) \cdot |\beta_{00}\rangle = (I \otimes X^x Z^z) \cdot |\beta_{00}\rangle$$

The state $|\beta_{00}\rangle$ is often called EPR pair (for Einstein–Podolsky–Rosen).

Toffoli gate

Toffoli gate: controlled-controlled-NOT

Flip target if both controls are 1



$$\begin{pmatrix} 1 & & & & & & & \\ & 1 & & & & \mathbf{0} & & \\ & & 1 & & & & & \\ & & & 1 & & & & \\ & & & & 1 & & & \\ & \mathbf{0} & & & & 1 & & \\ & & & & & & 0 & {\color{red}1} \\ & & & & & & {\color{red}1} & 0 \end{pmatrix}$$

$|110\rangle \leftrightarrow |111\rangle$

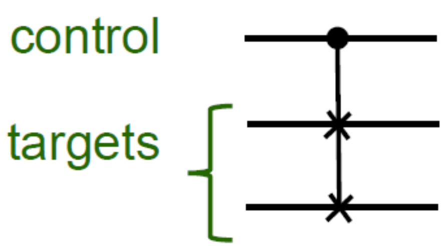
other basis states do not change

Can be constructed with CNOTs and 1-qubit gates (6 CNOTs needed)

Classical Toffoli gate is sufficient for classical reversible computation (to beat informational limit for energy dissipation in computation). Cannot be decomposed into 2-bit gates (in contrast to the quantum case), minimal gate for reversible computation.

Fredkin gate

Fredkin gate: controlled-SWAP



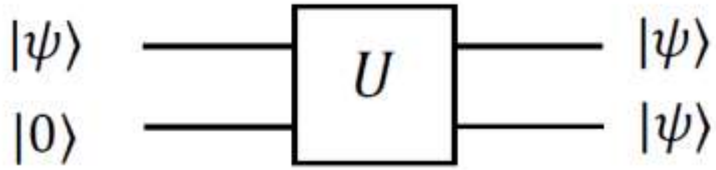
$$\begin{pmatrix} 1 & & & & & & & \\ & 1 & & & & & & \\ & & 1 & & & \mathbf{0} & & \\ & & & 1 & & & & \\ & & & & 1 & & & \\ & \mathbf{0} & & & & 0 & 1 & \\ & & & & & 1 & 0 & \\ & & & & & & & 1 \end{pmatrix}$$

$|101\rangle \leftrightarrow |110\rangle$

other basis states do not change

No fan-out gate (no-cloning theorem)

Theorem: impossible to realize fan-out gate



Proof Assume $U\,|0\rangle|0\rangle = |0\rangle|0\rangle$

$U\,|1\rangle|0\rangle = |1\rangle|1\rangle$

Then $U\,(\alpha|0\rangle + \beta|1\rangle)|0\rangle = \alpha\,|0\rangle|0\rangle + \beta|1\rangle|1\rangle$, while for desired cloning

$$(\alpha|0\rangle + \beta|1\rangle)|0\rangle \longrightarrow (\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle) =$$
$$= \alpha^2\,|0\rangle|0\rangle + \beta^2|1\rangle|1\rangle + \alpha\beta\,|0\rangle|1\rangle + \alpha\beta\,|1\rangle|0\rangle$$

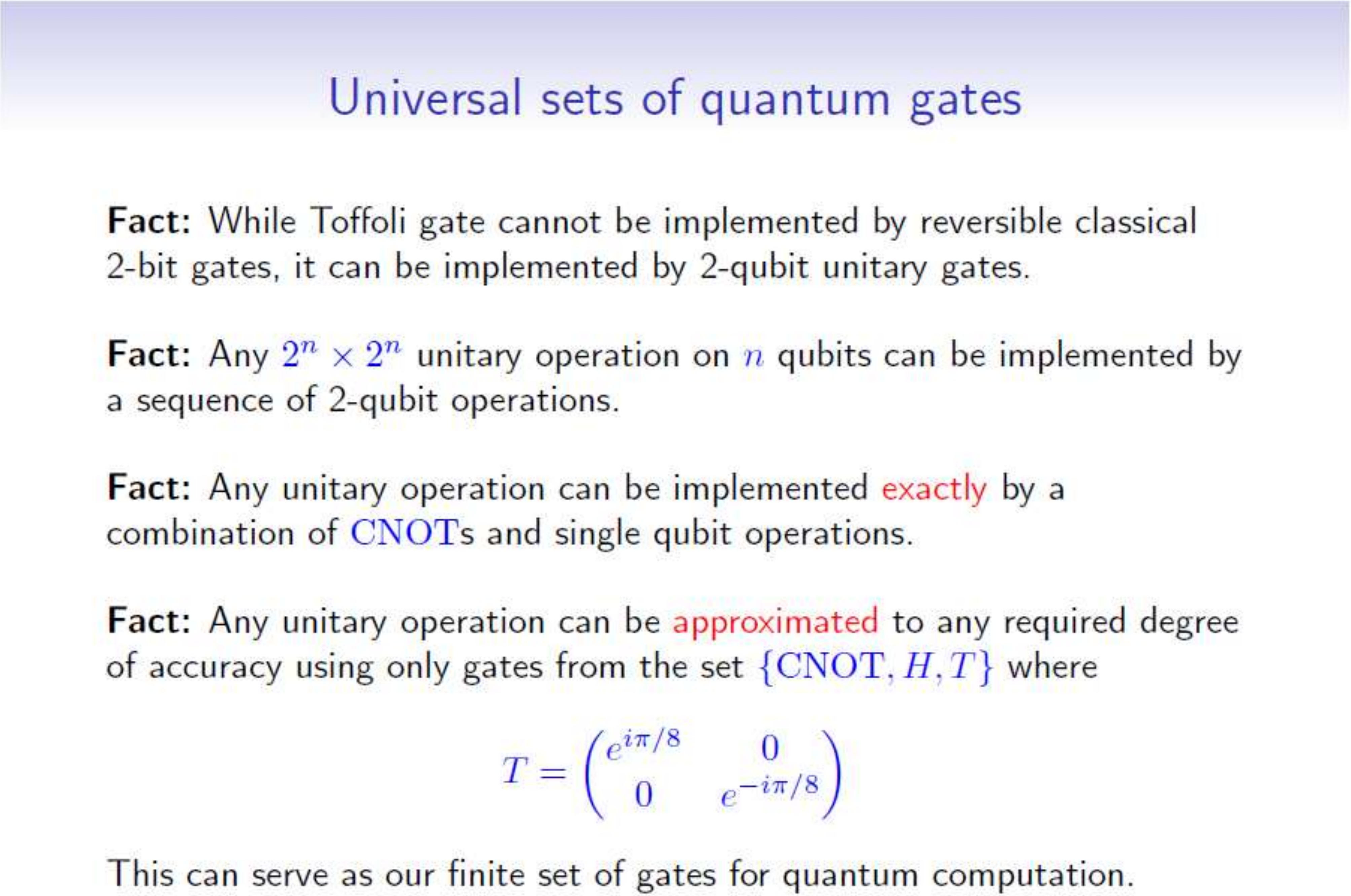
(a different state!)

More general proof Assume $U\,|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle$

$U\,|\phi\rangle|0\rangle = |\phi\rangle|\phi\rangle$

Unitary operation preserves inner product, therefore $\langle\phi|\psi\rangle = (\langle\phi|\psi\rangle)^2$.

This is possible only when $\langle\phi|\psi\rangle = 0$ or 1 (i.e., can clone only orthogonal states)



Universal sets of quantum gates

Fact: While Toffoli gate cannot be implemented by reversible classical 2-bit gates, it can be implemented by 2-qubit unitary gates.

Fact: Any $2^n \times 2^n$ unitary operation on n qubits can be implemented by a sequence of 2-qubit operations.

Fact: Any unitary operation can be implemented exactly by a combination of CNOTs and single qubit operations.

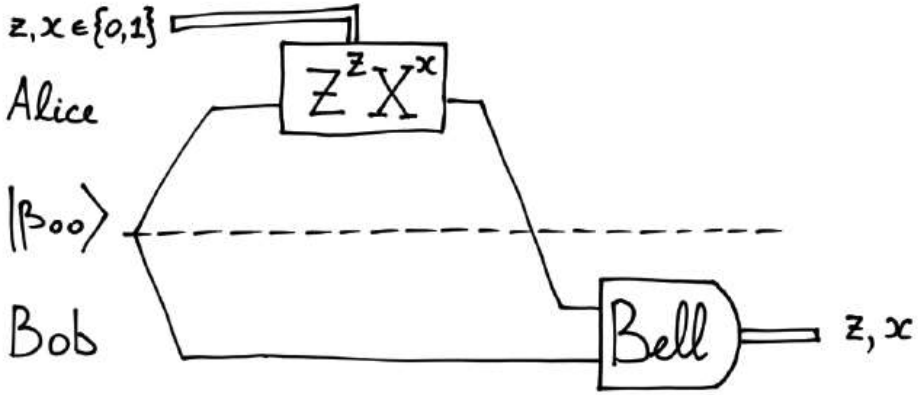
Fact: Any unitary operation can be approximated to any required degree of accuracy using only gates from the set $\{\mathrm{CNOT}, H, T\}$ where

$$T = \begin{pmatrix} e^{i\pi/8} & 0 \\ 0 & e^{-i\pi/8} \end{pmatrix}$$

This can serve as our finite set of gates for quantum computation.

Superdense coding

If *Alice* shares an EPR state $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ with *Bob*, she can locally transform it to any other EPR state $|\beta_{zx}\rangle$ by applying $Z^z X^x$ on her qubit. In this way she can encode two bits $z, x \in \{0, 1\}$ in one of the four orthogonal Bell states $|\beta_{zx}\rangle$. If *Alice* sends her qubit to *Bob*, he can perfectly discriminate the four cases by measuring in the Bell basis:

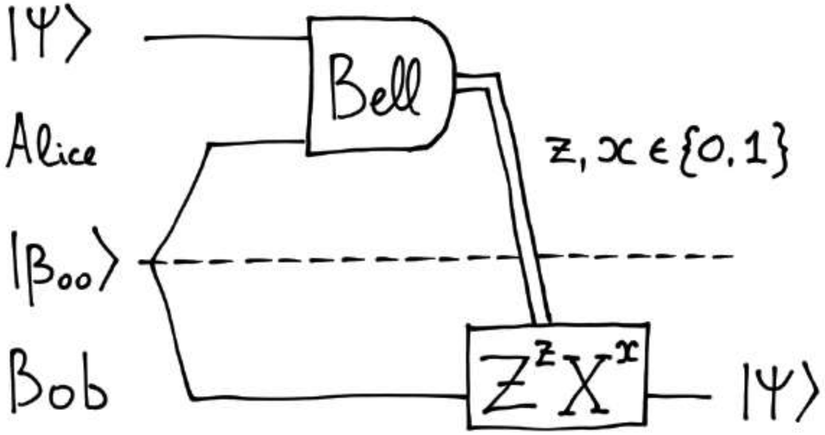


$$(H \otimes I) \cdot \text{CNOT} \cdot (Z^z X^x \otimes I) \cdot |\beta_{00}\rangle = |z, x\rangle$$

Resource trade-off: 1 shared EPR state + 1 qubit of quantum communication = 2 bits of classical communication

Quantum teleportation

Alice has a state $|\psi\rangle$ that she wishes to transmit to *Bob* with whom she shares an EPR state $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. *Alice* measures her qubits in the Bell basis and sends the classical outcomes $z, x \in \{0, 1\}$ to *Bob* who applies the Pauli correction operation $Z^z X^x$ on his qubit:



$$|\psi\rangle \otimes |\beta_{00}\rangle = \frac{1}{2} \sum_{z,x\in\{0,1\}} |\beta_{zx}\rangle \otimes X^x Z^z |\psi\rangle$$

Resource trade-off: 1 shared EPR state + 2 bits of classical communication = 1 qubit of quantum communication