量子信息导论
PHYS5251P

中国科学技术大学
物理学院/合肥微尺度物质科学国家研究中心

陈凯

2026.1

第六章 量子计算

1. **经典计算机发展**
2. 量子计算机简介
3. 量子计算实现准则
4. 量子计算的物理实现、商业化进程
5. 量子比特表示、量子线路
6. 量子协议的线路实现
7. 典型量子算法
8. 单向量子计算
9. 量子算法总结

第六章 量子计算

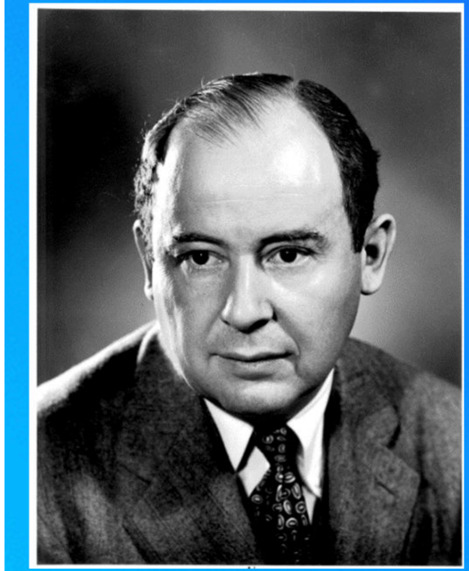
量子计算的基本理论，几个特殊形式的量子算法

Classical Computers

- Alan Turing (1912 – 1954)

- In 1936, Turing published a paper referring to an abstract machine which moved from one state to another using a precise finite set of rules (given by a finite table) depending on a single symbol it read from a tape

经典计算机和信息处理



冯·诺依曼

第一代计算机

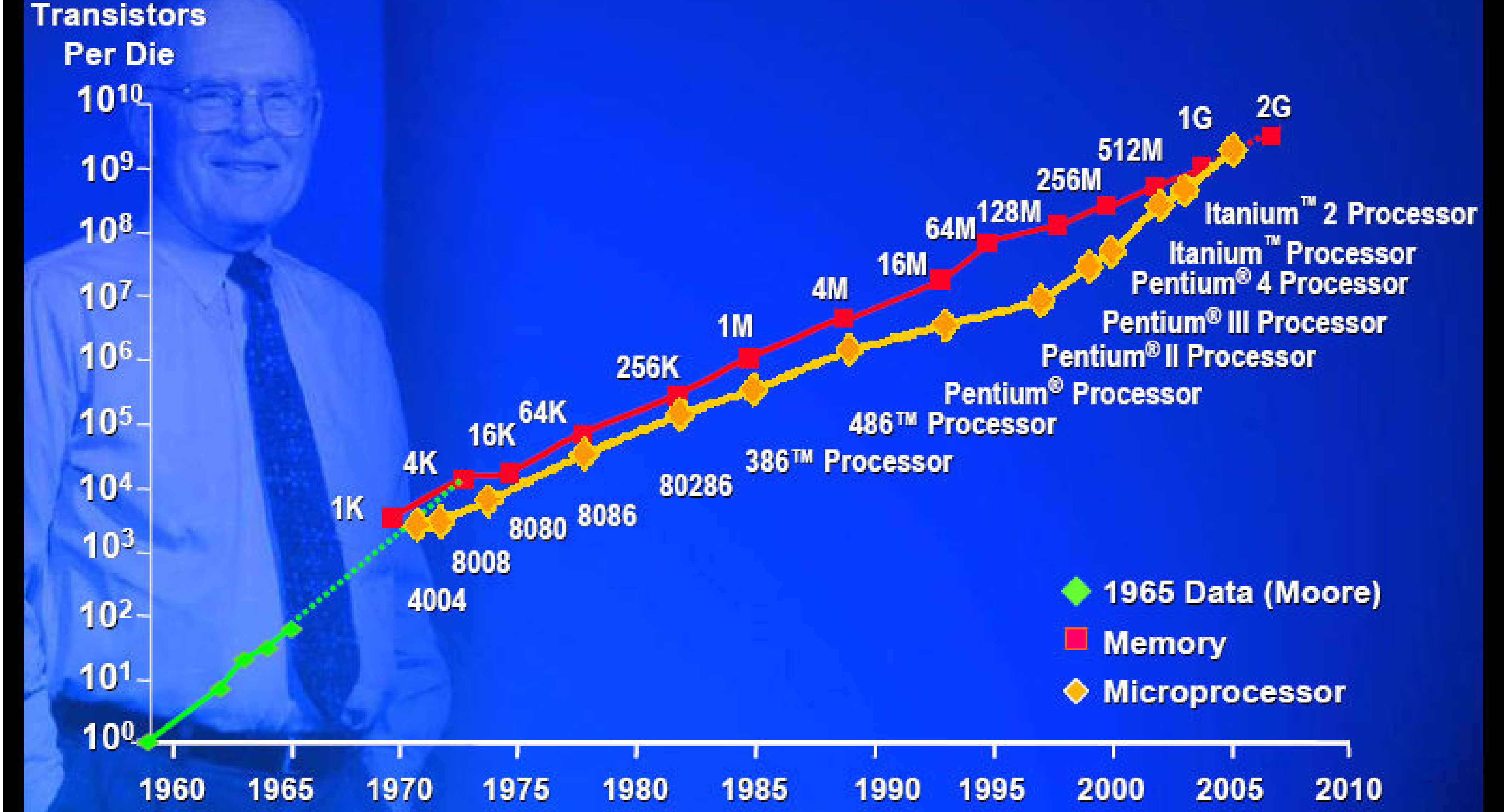
Roadrunner超级计算机

高速互联通信网

最新苹果电脑

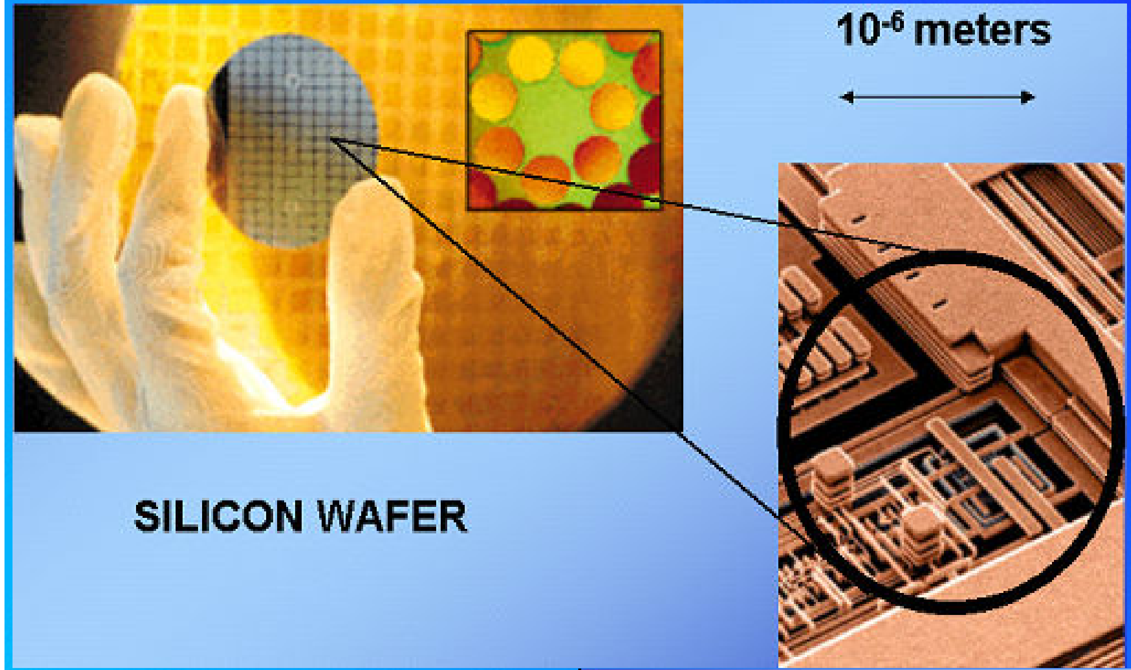
中国科学技术大学 陈凯

Moore's Law - 2005



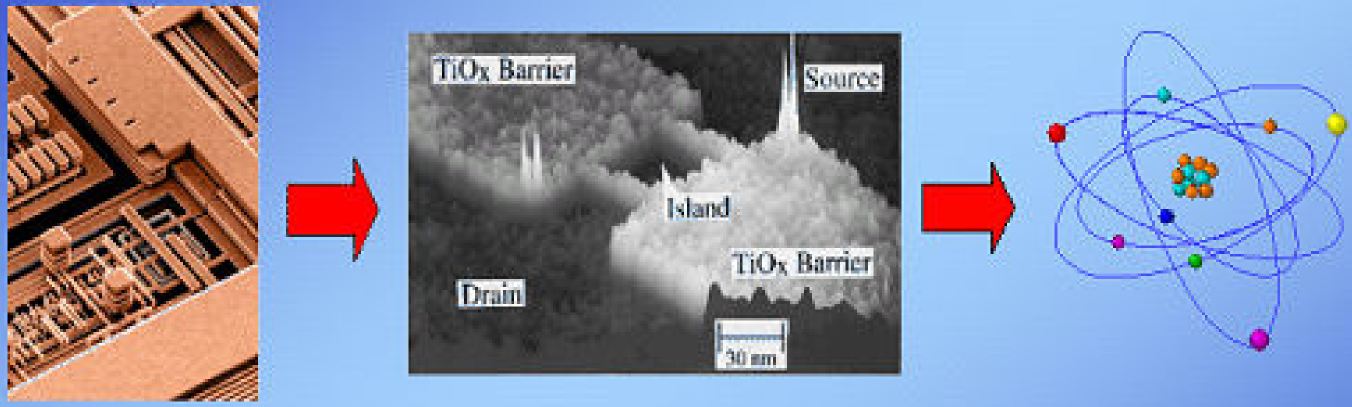
Source: Intel

经典计算机发展状况



10^{-6} meters

SILICON WAFER



10^{-6} meters

10^{-8} meters

10^{-10} meters

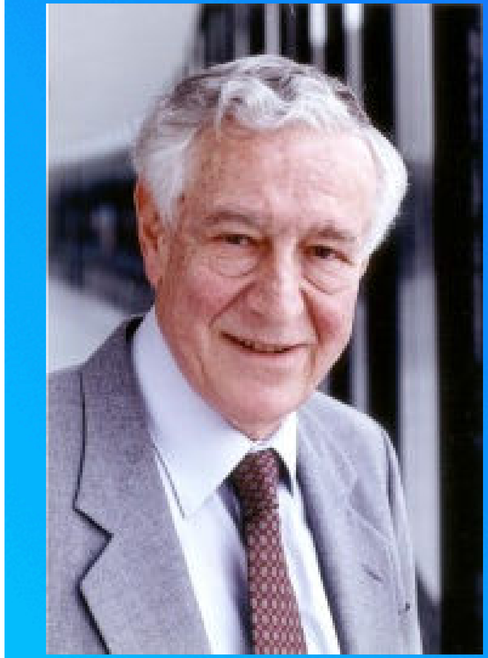
TODAY

TOMORROW

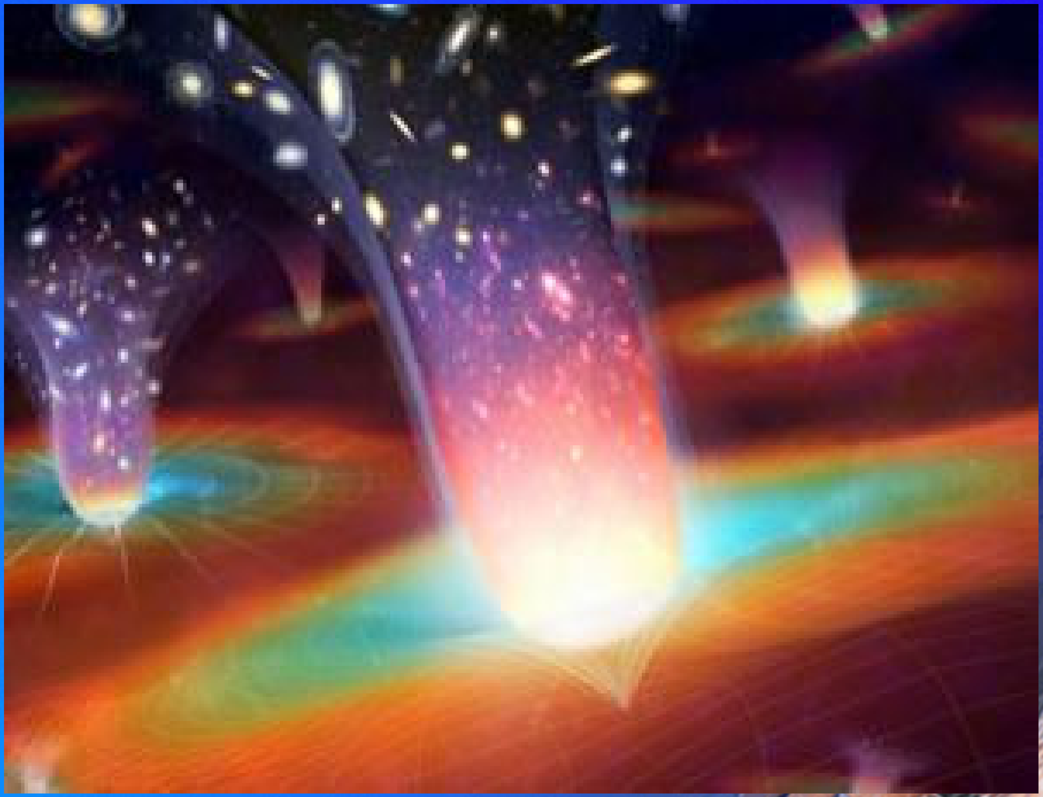
第六章 量子计算

1. 经典计算机发展
2. **量子计算机简介**
3. 量子计算实现准则
4. 量子计算的物理实现、商业化进程
5. 量子比特表示、量子线路
6. 量子协议的线路实现
7. 典型量子算法
8. 单向量子计算
9. 量子算法总结

What is quantum information?



“Information is physical.” 1960s *by Rolf Landauer* from IBM Research



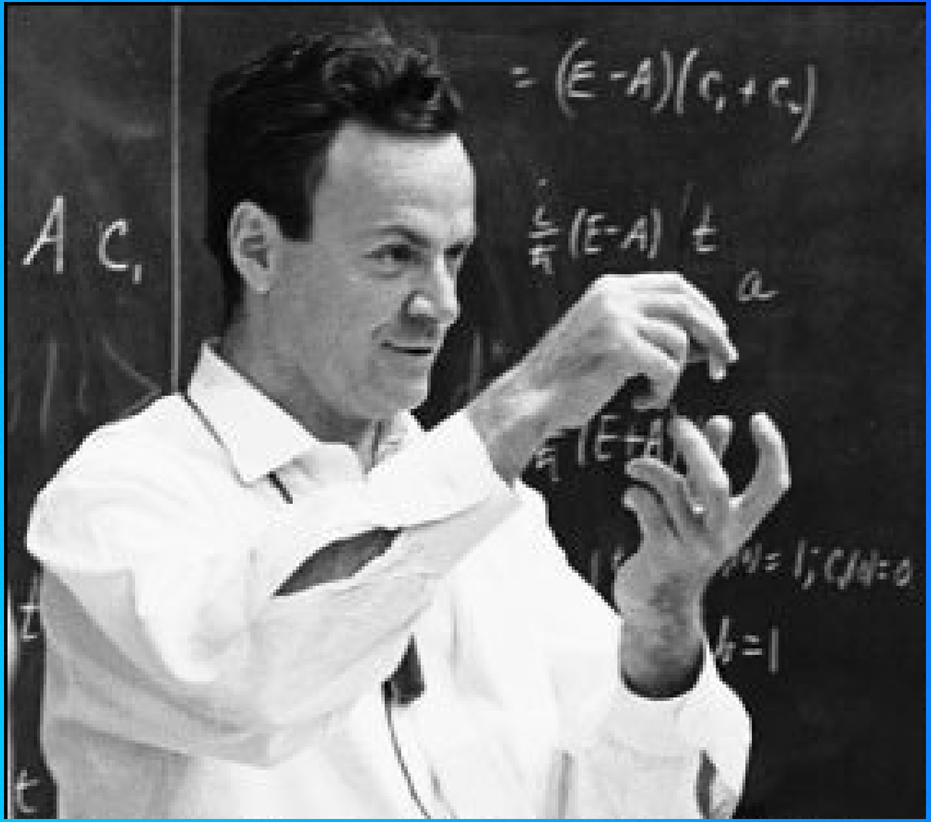
Quantum information is that kind of information which is carried by quantum systems from the preparation device to the measuring apparatus in a quantum mechanical experiment. *by R.F. Werner*

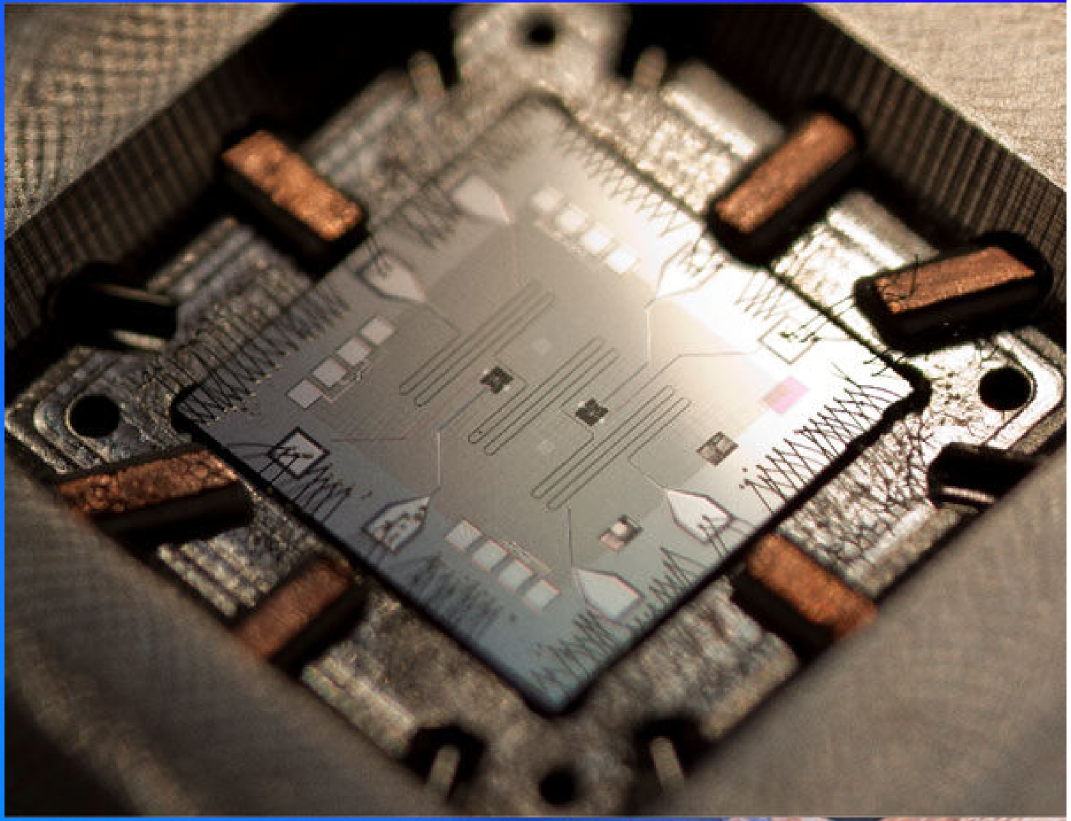
from New Scientist 2011

"There is plenty of room at the bottom." (Dec 29, 1959)

"It seems that the laws of physics present no barrier to reducing the size of computers until bits are the size of atoms, and quantum behavior holds dominant sway."

——Richard P. Feynman (1985)





Nobel prize 1965

from New Scientist 2011

Quantum Algorithms

- Deutsch-Jozsa (D-J)
  - Proc. R. Soc. London A, 439, 553 (1992)
- Grover's search algorithm
  - Phys. Rev. Lett., 79, 325 (1997)
- Shor's algorithm for factoring large numbers
  - SIAM J. Comp., 26, 1484 (1997)

D. Deutsch

R. Jozsa

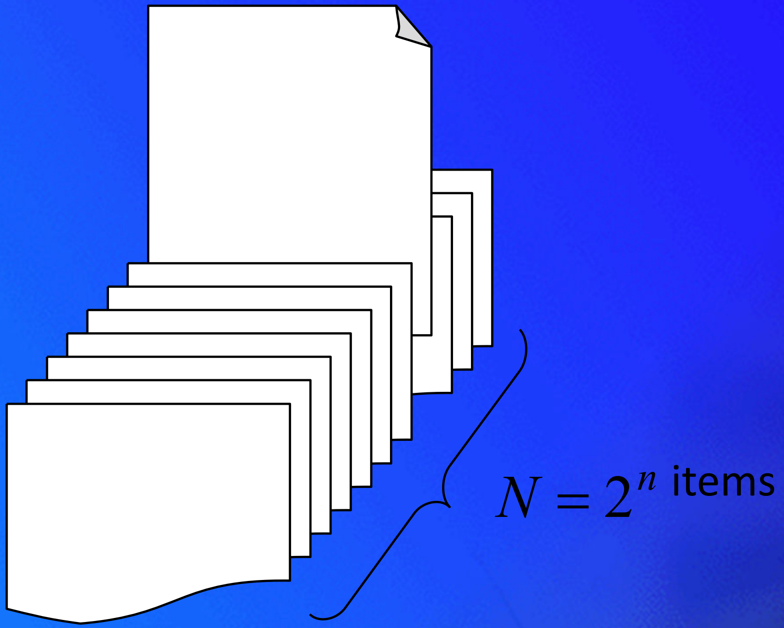
ROTATION IN 2-DIMENSIONAL SPACE !!
LEADS TO ALGORITHM FOR RANDOM SEARCH
L. K. Grover

P. W. Shor

Grover's Search

$N = 2^n$ unordered items, we're looking for one item

Classically, would have to check about N/2 items



Hard task!

By using Grover's algorithm,

$\sqrt{N}$ repetitions are sufficient!

第六章 量子计算

1. 经典计算机发展
2. 量子计算机简介
3. **量子计算实现准则**
4. 量子计算的物理实现、商业化进程
5. 量子比特表示、量子线路
6. 量子协议的线路实现
7. 典型量子算法
8. 单向量子计算
9. 量子算法总结

DiVincenzo’s Criteria

DiVincenzo, Fortschr. Phys. **48**, 771 (2000)

1. ***Scalability:*** A scalable physical system with well characterized parts, usually qubits.

2. ***Initialization:*** The ability to initialize the system in a simple fiducial state.

3. ***Control:*** The ability to control the state of the computer using sequences of elementary universal gates.

4. ***Stability:*** Decoherence times much longer than gate times, together with the ability to suppress decoherence through error correction and fault-tolerant computation.

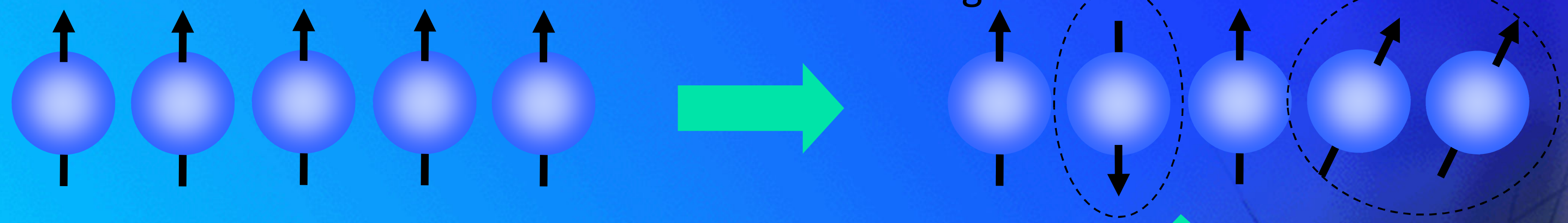
5. ***Measurement:*** The ability to read out the state of the computer in a convenient product basis.

DiVincenzo’s Criteria

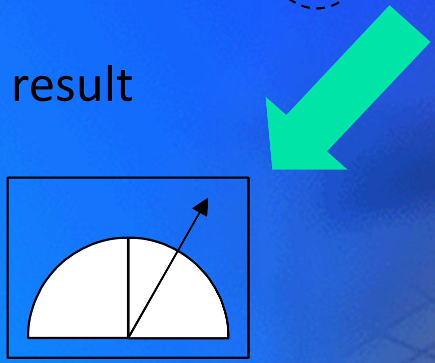
1. Well defined extensible qubit array
2. Preparable in the “000…” state
3. Long decoherence time
4. Universal set of gate operations
5. Single quantum measurements

Qubit initialization

Execution of an algorithm



Read the result



Must be done within decoherence time!

中国科学技术大学 陈凯

第六章 量子计算

1. 经典计算机发展
2. 量子计算机简介
3. 量子计算实现准则
4. **量子计算的物理实现、商业化进程**
5. 量子比特表示、量子线路
6. 量子协议的线路实现
7. 典型量子算法
8. 单向量子计算
9. 量子算法总结

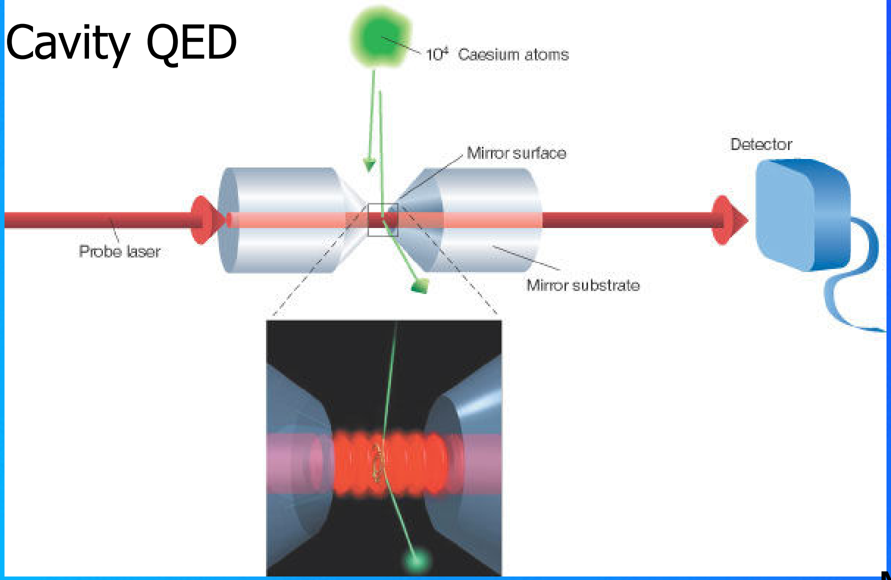
Qubit Representations

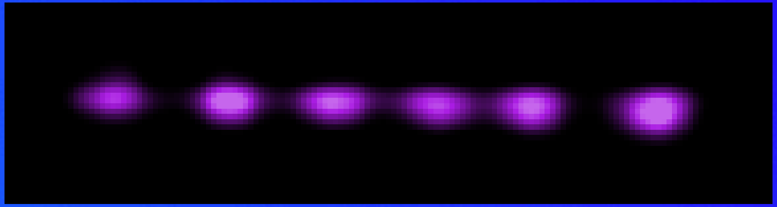
- Electron: number, spin, energy level
- Nucleus: spin
- Photon: number, polarization, time, angular momentum, momentum (energy)
- Flux (current)
- Anything that can be quantized and follows Schrödinger's equation

A Few Physical Experiments

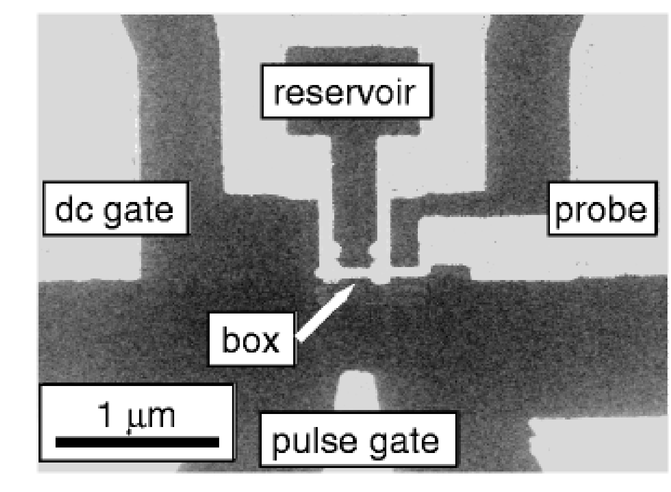
- IBM, Stanford, Berkeley, MIT, USTC (solution NMR)
- NEC (Josephson junction charge)
- Delft (JJ flux)
- NTT (JJ, quantum dot)
- Tokyo U., USTC (quantum dot, optical lattice, ...)
- Keio U. (silicon NMR, quantum dot)
- Caltech, Berkeley, Stanford (quantum dot)
- Austria, USTC (linear optics)
- Australia, NIST (ion trap)
- Many others (cavity QED, Kane NMR, ...)

Physical Realization

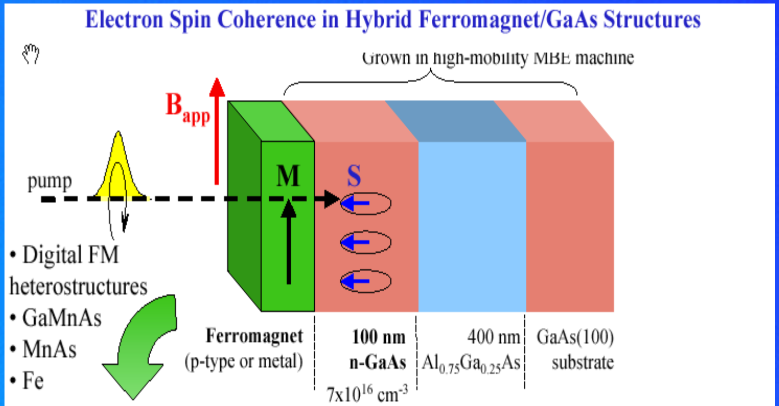

Cavity QED


Ion trap

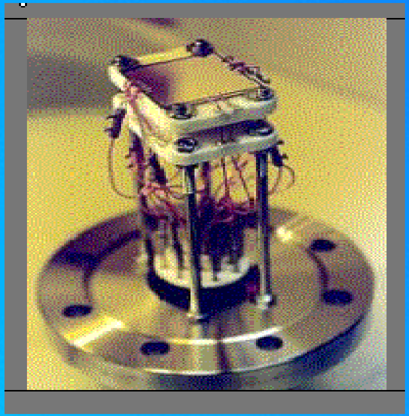
Magnetic resonance



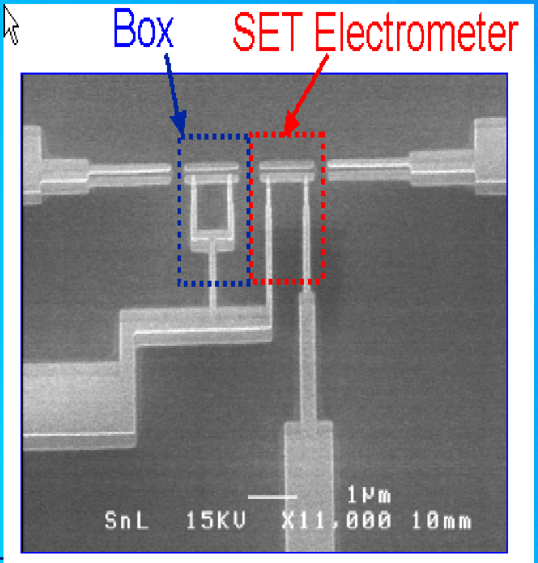
Superconductor


Electron Spin Coherence in Hybrid Ferromagnet/GaAs Structures
Grown in high-mobility MBE machine
B_{app}
pump
M
S
• Digital FM heterostructures
• GaMnAs
• MnAs
• Fe
Ferromagnet (p-type or metal)
100 nm n-GaAs
7×10^{16} cm^{-3}
400 nm $Al_{0.75}Ga_{0.25}As$
GaAs(100) substrate

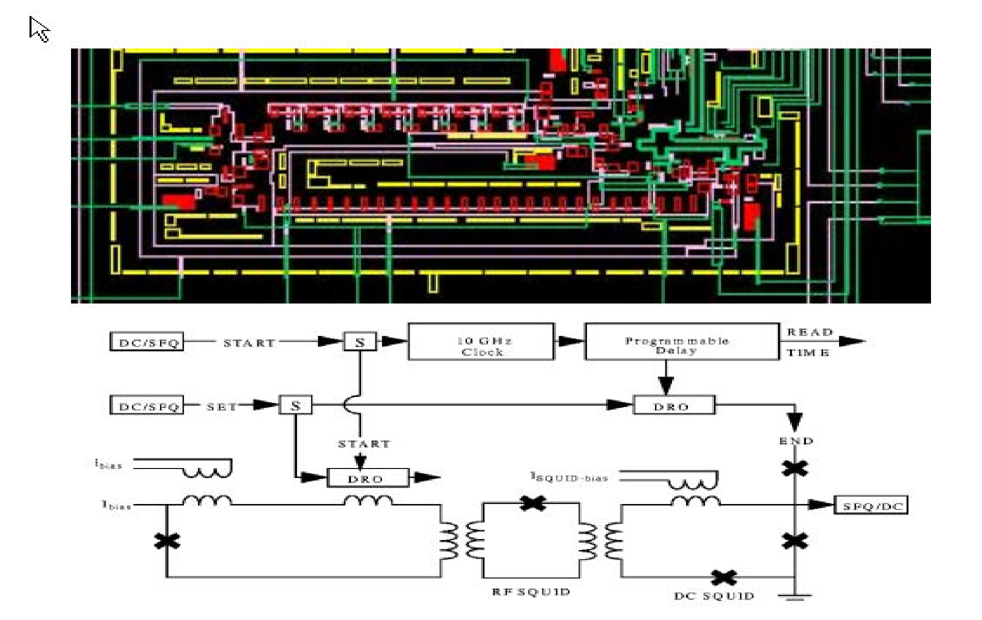
Spintronics



Atom Chip



Cooper Pair Box

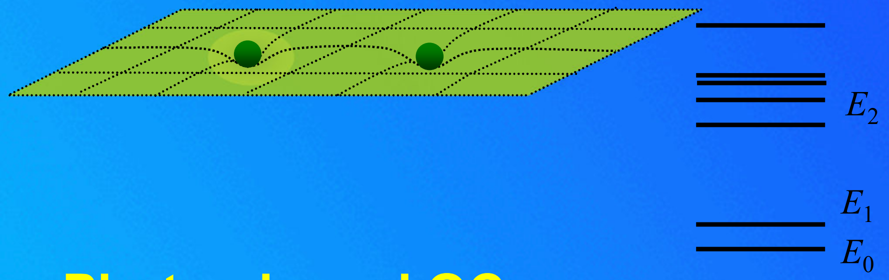


RF-SQUID

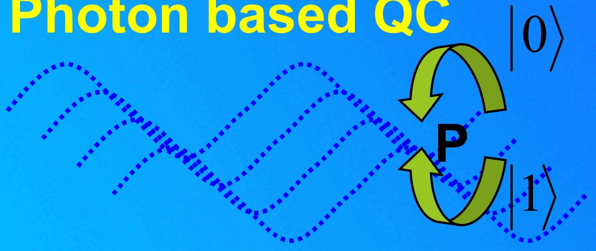
Quantum computation

Physical realization of a qubit

- Ion traps and neutral atoms

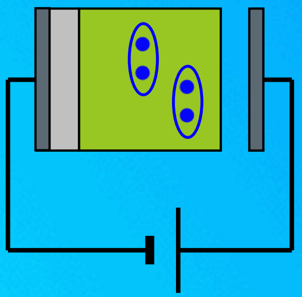


- Photon based QC

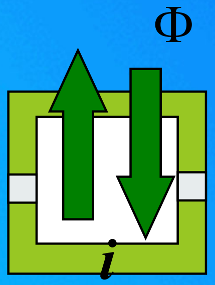


- Superconducting qubit

Cooper pair box



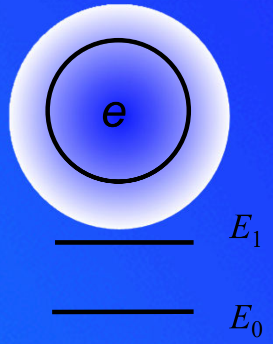
SQUID



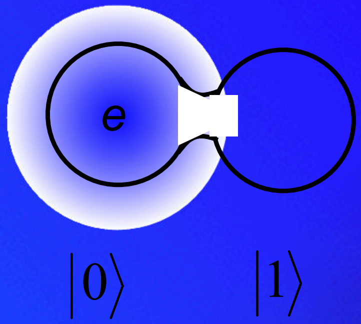
N pairs - $|0\rangle$ N+1 pairs - $|1\rangle$

- Semiconductor charge qubit

Single QD

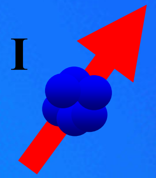


Double QD

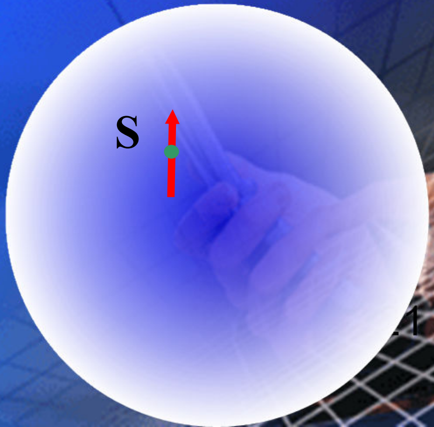


- Spin qubit

Nuclear spin
(liquid state NMR,
solid state NMR)



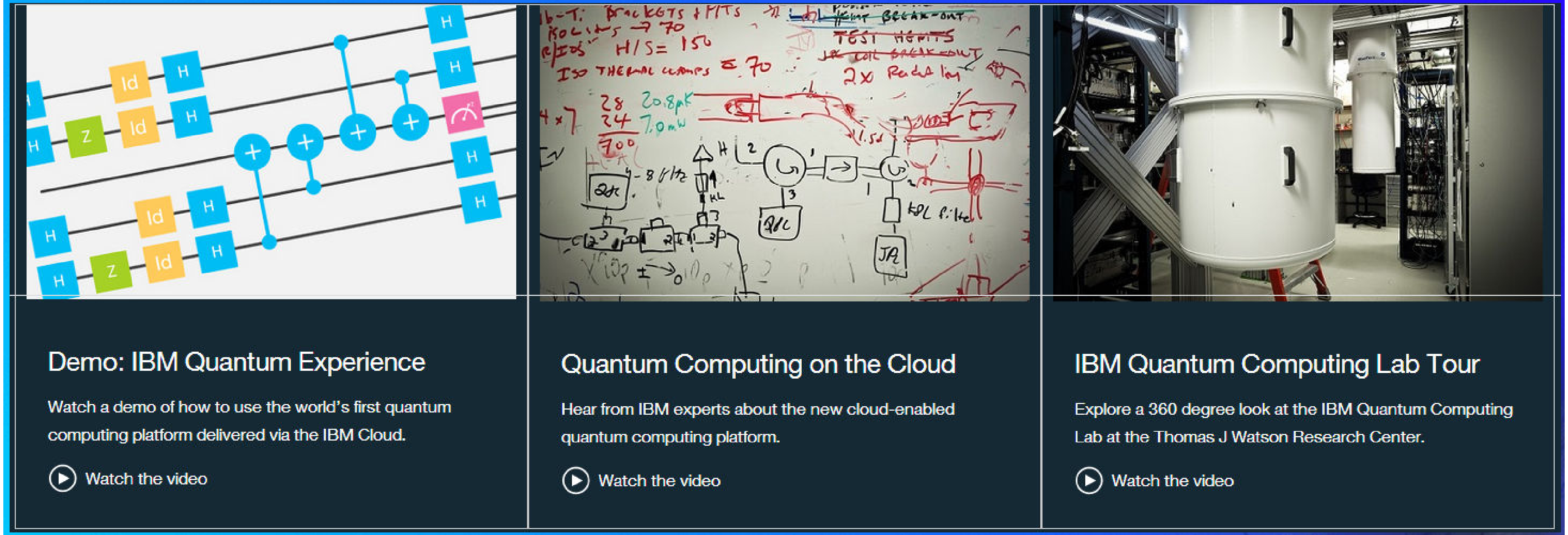
Electron spin



量子信息，谁在做？

- Aarhus
- Berkeley
- Caltech
- Cambridge
- College Park
- Delft
- DERA (U.K.)
- École normale supérieure
- Geneva
- HP Labs (Palo Alto and Bristol)
- Hitachi
- id Quantique
- IBM Research (Yorktown Heights and Palo Alto)
- Innsbruck
- Los Alamos National Labs
- McMaster
- MagiQ
- Max Planck Institute-Munich
- Melbourne
- MIT
- NEC
- New South Wales
- NIST
- NRC
- Orsay
- Oxford
- Paris
- Queensland
- Santa Barbara
- Stanford
- Toronto
- USTC
- Vienna
- Waterloo
- Yale
- many others…

量子计算



Demo: IBM Quantum Experience

Watch a demo of how to use the world's first quantum computing platform delivered via the IBM Cloud.

Watch the video

Quantum Computing on the Cloud

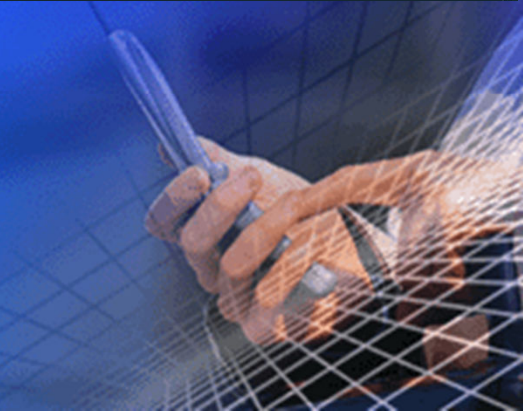
Hear from IBM experts about the new cloud-enabled quantum computing platform.

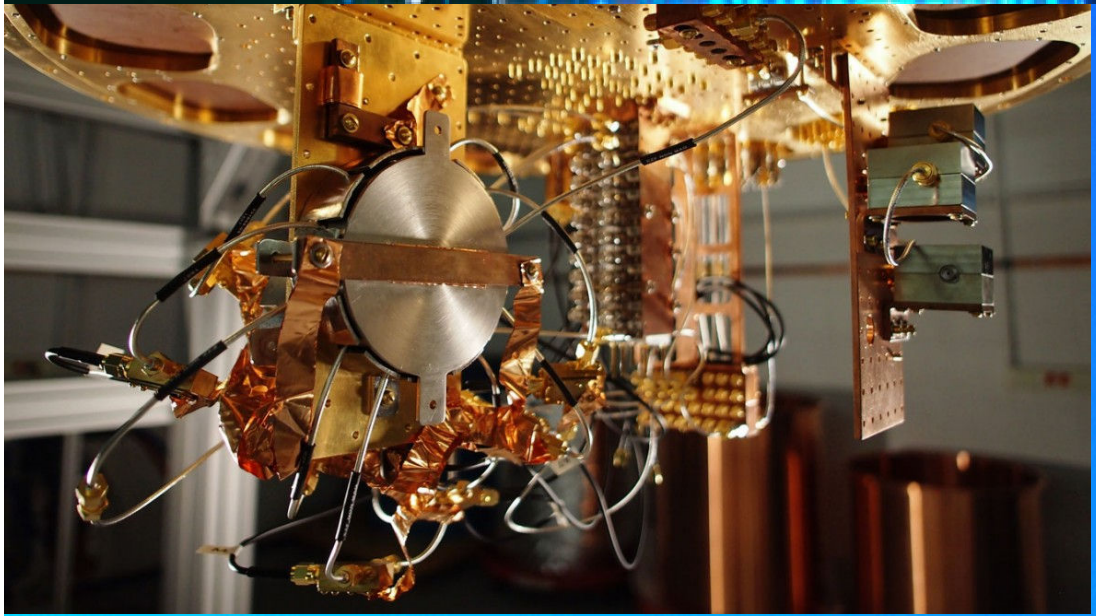
Watch the video

IBM Quantum Computing Lab Tour

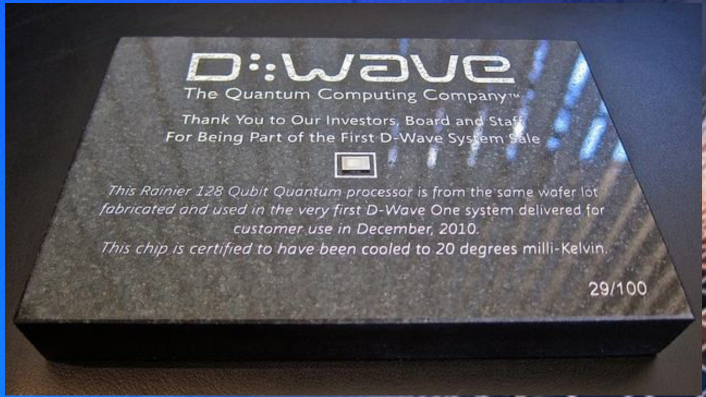
Explore a 360 degree look at the IBM Quantum Computing Lab at the Thomas J Watson Research Center.

Watch the video





量子计算？ *有争议！*



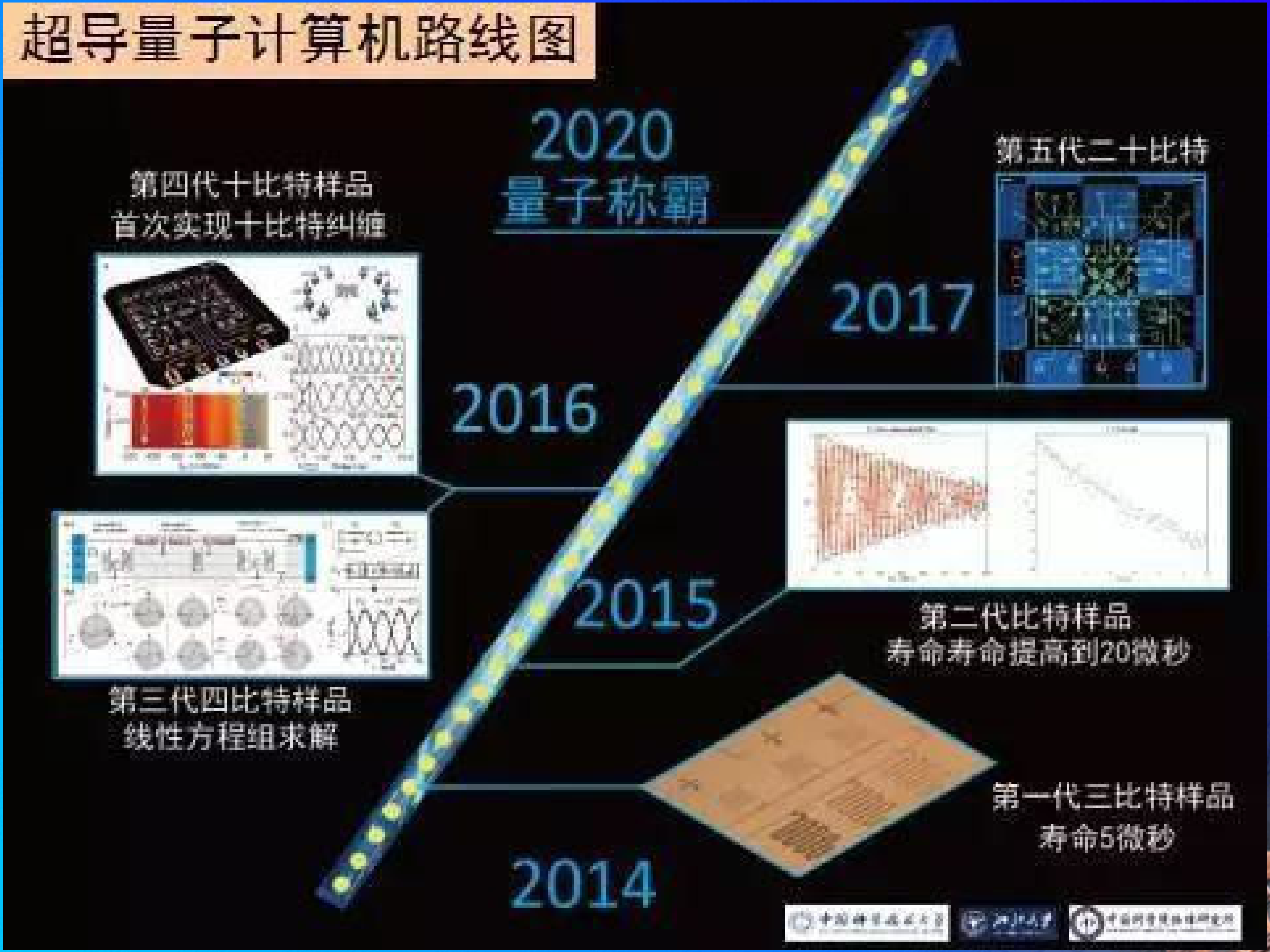
D:wave

The Quantum Computing Company™

Thank You to Our Investors, Board and Staff
For Being Part of the First D-Wave System Sale

This Rainier 128 Qubit Quantum processor is from the same wafer lot fabricated and used in the very first D-Wave One system delivered for customer use in December, 2010.
This chip is certified to have been cooled to 20 degrees milli-Kelvin.

29/100



超导量子计算机路线图

2020
量子称霸

第五代二十比特

2017

第四代十比特样品
首次实现十比特纠缠

2016

2015

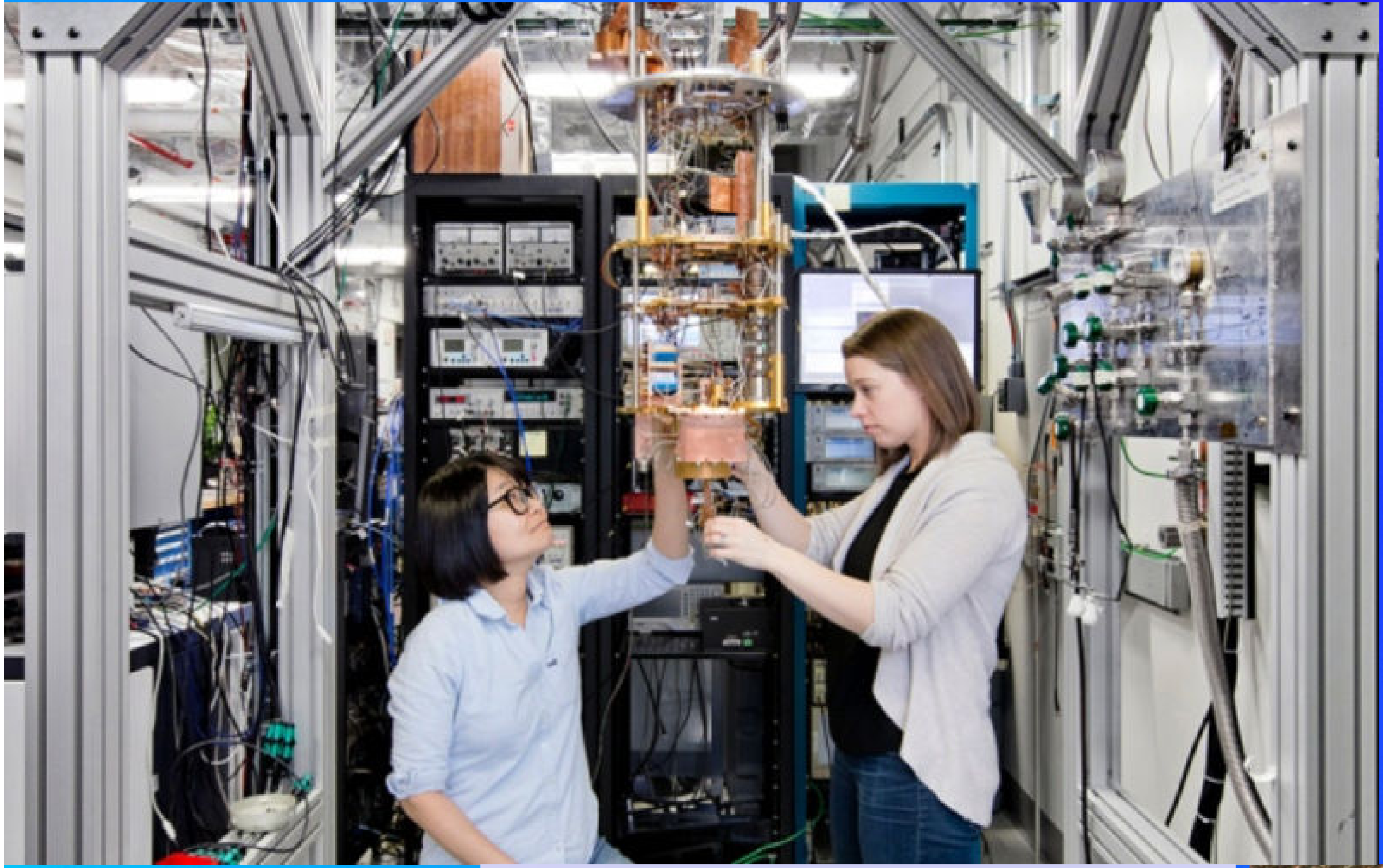
第二代比特样品
寿命寿命提高到20微秒

第三代四比特样品
线性方程组求解

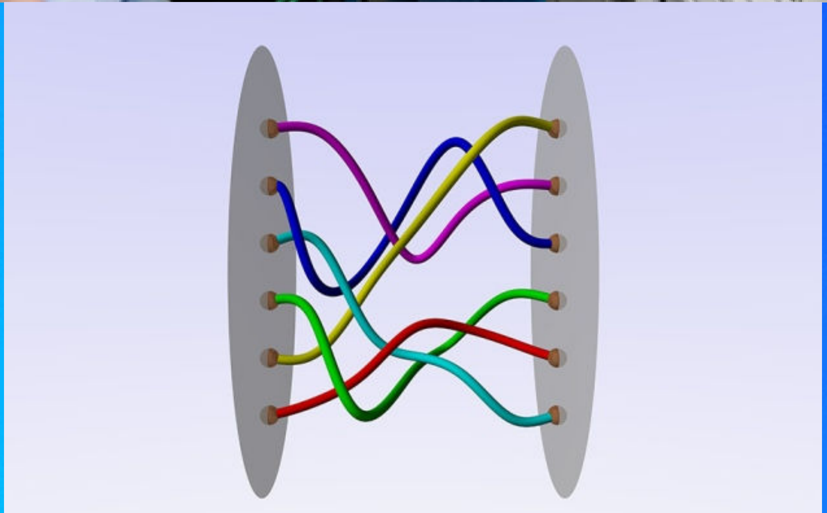
第一代三比特样品
寿命5微秒

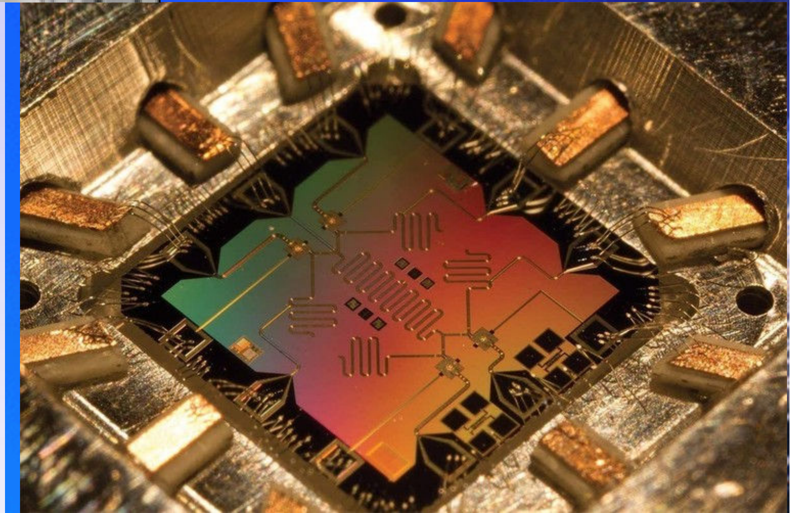
2014

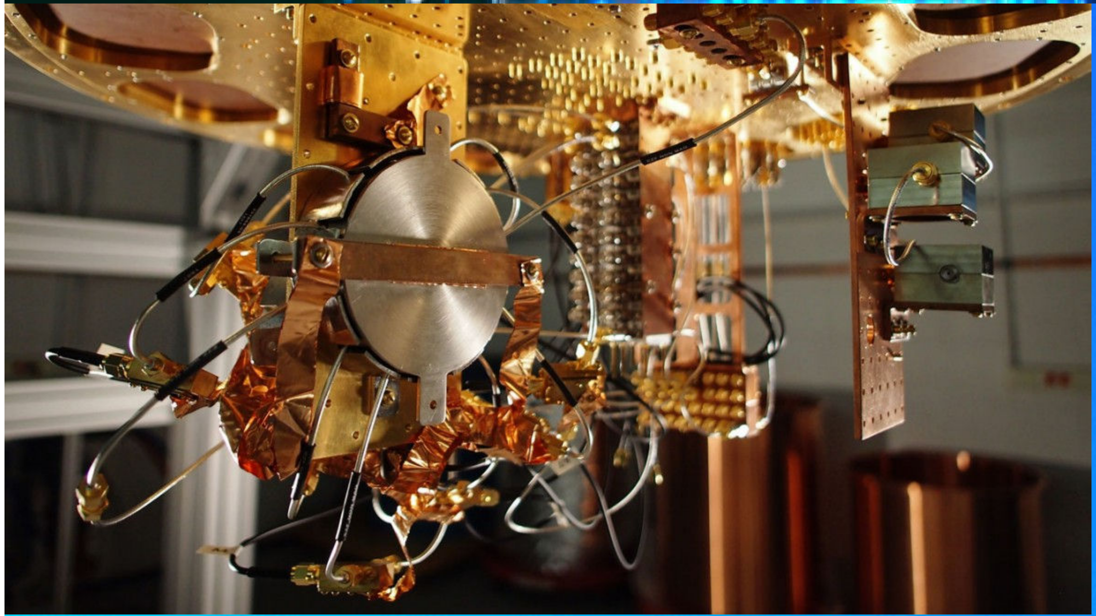
量子计算机竞赛



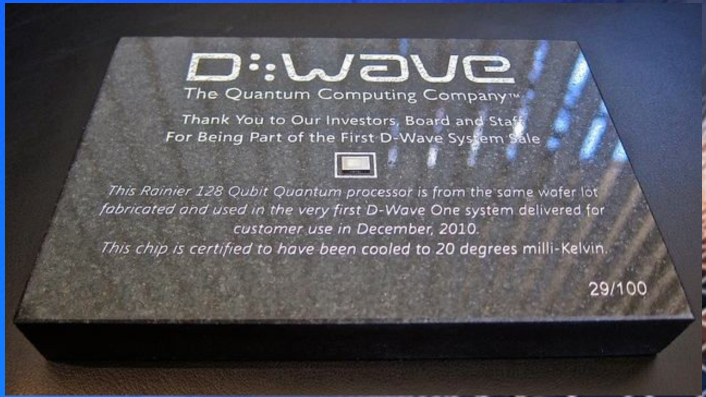
IBM，微软，Google等







量子计算？ *有争议！*



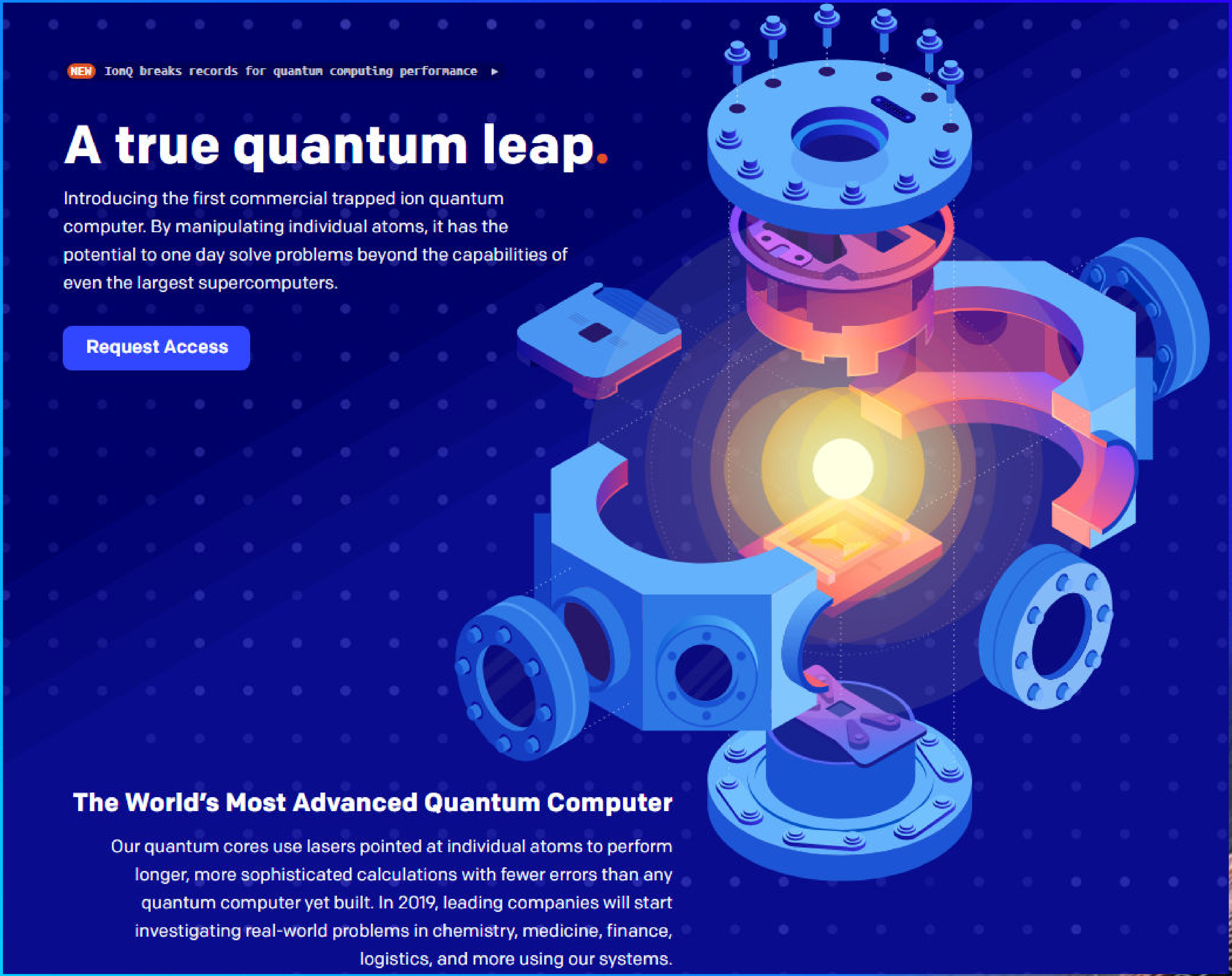
D:wave

The Quantum Computing Company™

Thank You to Our Investors, Board and Staff
For Being Part of the First D-Wave System Sale

This Rainier 128 Qubit Quantum processor is from the same wafer lot fabricated and used in the very first D-Wave One system delivered for customer use in December, 2010.
This chip is certified to have been cooled to 20 degrees milli-Kelvin.

29/100



NEW IonQ breaks records for quantum computing performance ▸

A true quantum leap.

Introducing the first commercial trapped ion quantum computer. By manipulating individual atoms, it has the potential to one day solve problems beyond the capabilities of even the largest supercomputers.

The World's Most Advanced Quantum Computer

Our quantum cores use lasers pointed at individual atoms to perform longer, more sophisticated calculations with fewer errors than any quantum computer yet built. In 2019, leading companies will start investigating real-world problems in chemistry, medicine, finance, logistics, and more using our systems.

Preliminary benchmark test results on IonQ hardware as of December 10, 2018.

Qubits

Qubits are the basic unit of information storage on a quantum computer. After they're initialized, logical operations—called gates—are performed on them.

Maximum loaded 160 qubits

Single-qubit gates performed on up to 79 qubits

Two-qubit gates performed on all pairs of up to 11 qubits

Error Rate

Gate fidelity is a measure of the accuracy of a single gate. Gates that manipulate one qubit at a time are less complex and less error-prone than gates that operate on two qubits. The following benchmarks were captured on a fully-connected 11-qubit configuration.

Average fidelities

Single-qubit gates >99%

Two-qubit gates >98%*

Best fidelities

Single-qubit gates 99.97%

Two-qubit gates 99.3%*

Minimum fidelities

Single-qubit gates >99%

Two-qubit gates >96%*

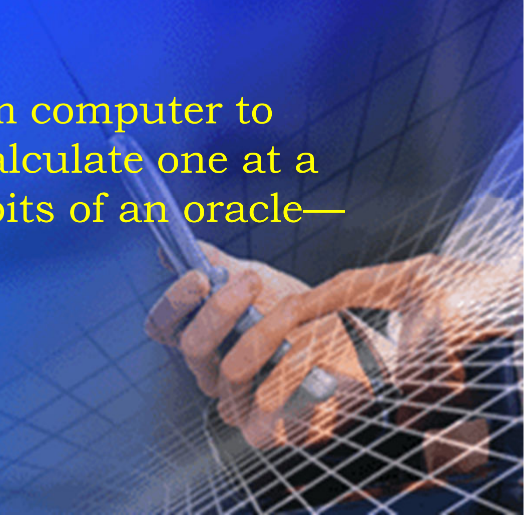
* not corrected for state preparation and measurement errors.

Benchmark: Bernstein-Vazirani Algorithm

The Bernstein-Vazirani Algorithm is a basic test of the ability of a quantum computer to simultaneously evaluate possibilities that conventional computers must calculate one at a time. The complexity of the test is determined by the maximum length in bits of an oracle—an arbitrary number the computer must determine.

10-qubit oracle success rate 73.0%

Classical computer success rate ~0.2%



Technologies for QC

- Liquid NMR
- Solid-state NMR
- Quantum dots
- Superconducting Josephson junctions
- Ion trap
- Optical lattice
- All-optical

第六章 量子计算

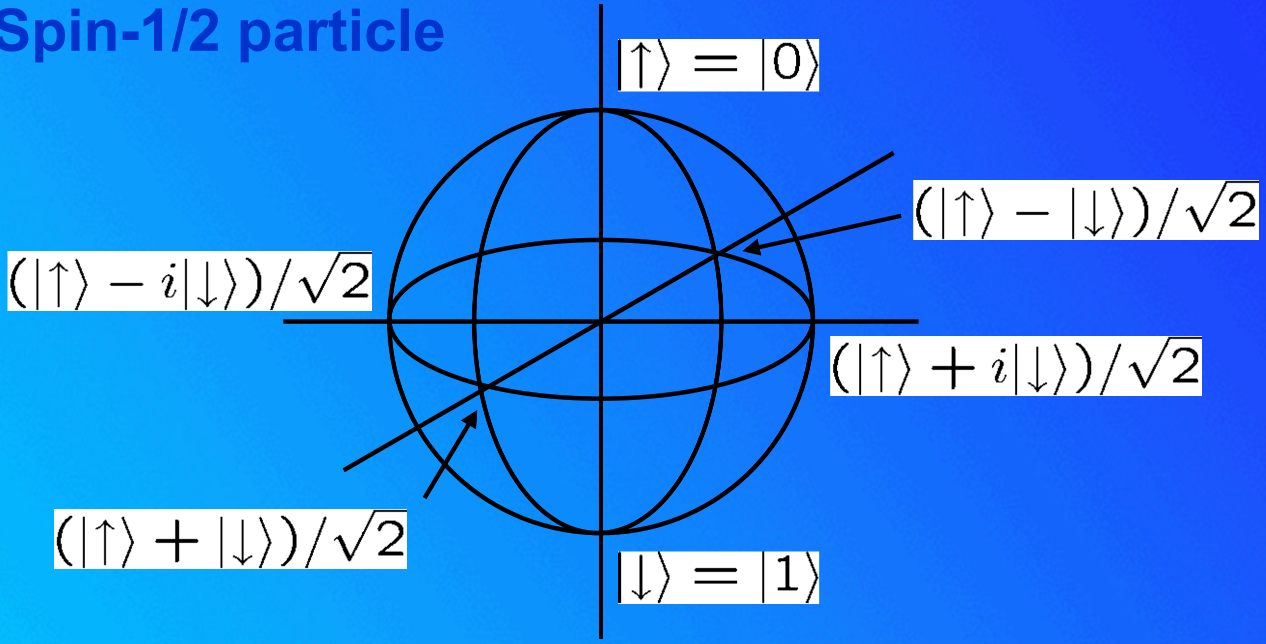
1. 经典计算机发展
2. 量子计算机简介
3. 量子计算实现准则
4. 量子计算的物理实现、商业化进程
5. **量子比特表示、量子线路**
6. 量子协议的线路实现
7. 典型量子算法
8. 单向量子计算
9. 量子算法总结

Qubitology. States

$$|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\phi}\sin(\theta/2)|1\rangle = |\mathbf{n}\rangle$$

Direction of spin

Spin-1/2 particle


$|\uparrow\rangle = |0\rangle$
$(|\uparrow\rangle - |\downarrow\rangle)/\sqrt{2}$
$(|\uparrow\rangle - i|\downarrow\rangle)/\sqrt{2}$
$(|\uparrow\rangle + i|\downarrow\rangle)/\sqrt{2}$
$(|\uparrow\rangle + |\downarrow\rangle)/\sqrt{2}$
$|\downarrow\rangle = |1\rangle$

Bloch sphere

From Caves

$$\begin{aligned}|\mathbf{n}\rangle\langle\mathbf{n}| &= \frac{1}{2}(I + \sigma_x n_x + \sigma_y n_y + \sigma_z n_z) \\ &= \frac{1}{2}(I + \mathbf{n}\cdot\sigma)\end{aligned}$$

Pauli representation

$$\begin{aligned}\sigma_x &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = X \\ \sigma_y &= \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = Y \\ \sigma_z &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = Z\end{aligned}$$

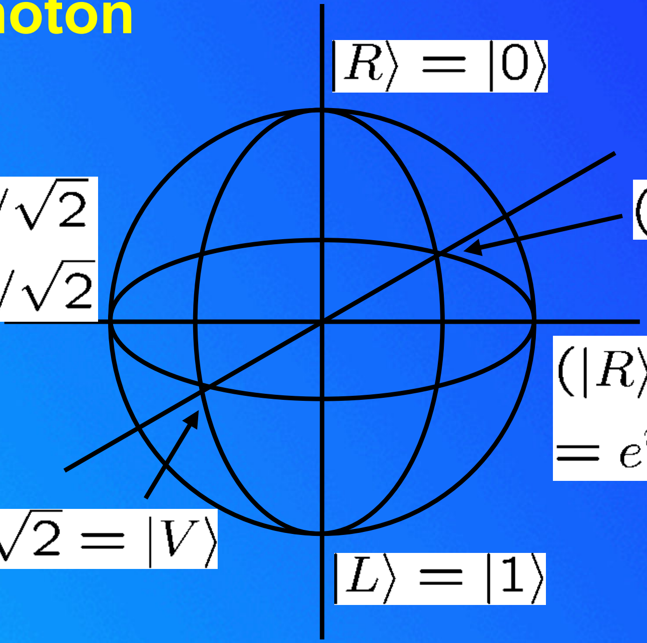
中国科学技术大学 陈凯

Qubitology. States

$$|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\phi}\sin(\theta/2)|1\rangle = |\mathbf{n}\rangle$$

Abstract "direction"

Polarization of a photon



$|R\rangle = |0\rangle$

$(|R\rangle - i|L\rangle)/\sqrt{2}$
$= e^{-i\pi/4}(|V\rangle - |H\rangle)/\sqrt{2}$

$(|R\rangle - |L\rangle)/\sqrt{2} = i|H\rangle$

$(|R\rangle + i|L\rangle)/\sqrt{2}$
$= e^{i\pi/4}(|V\rangle + |H\rangle)/\sqrt{2}$

$(|R\rangle + |L\rangle)/\sqrt{2} = |V\rangle$

$|L\rangle = |1\rangle$

Poincare sphere

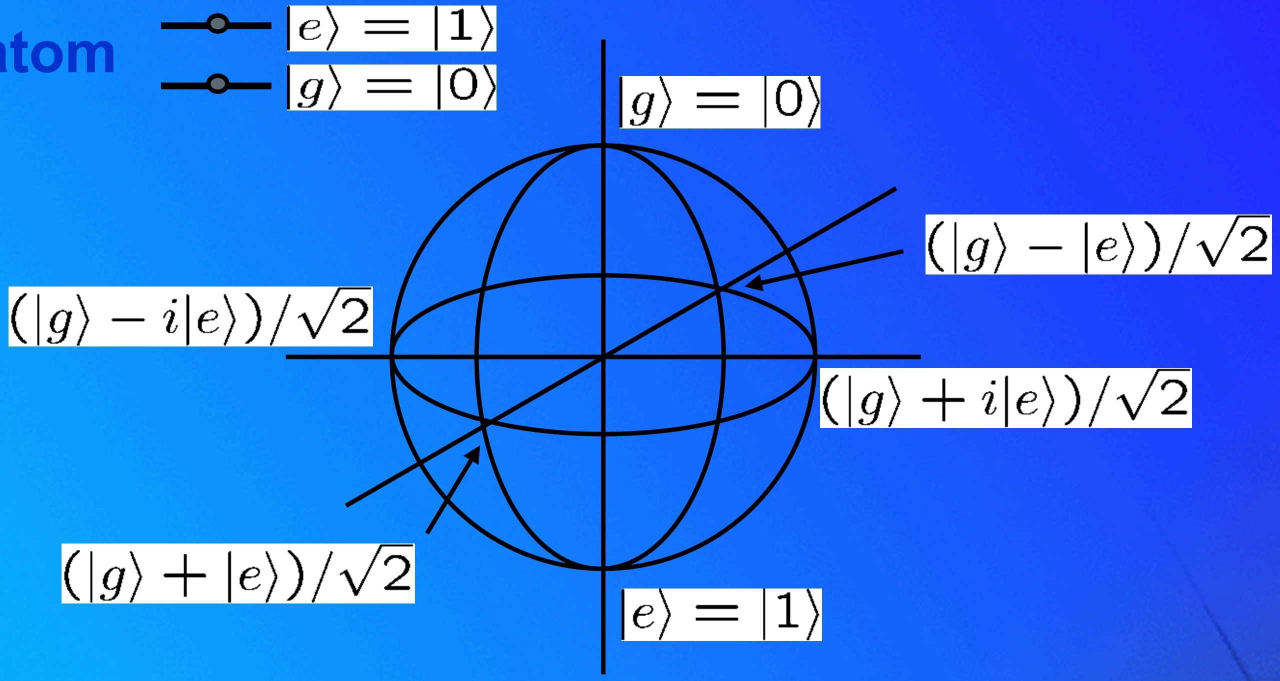
From Caves

Qubitology. States

$$|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\phi}\sin(\theta/2)|1\rangle = |\mathbf{n}\rangle$$

Abstract "direction"

Two-level atom


$|e\rangle = |1\rangle$
$|g\rangle = |0\rangle$
$|g\rangle = |0\rangle$
$(|g\rangle - |e\rangle)/\sqrt{2}$
$(|g\rangle - i|e\rangle)/\sqrt{2}$
$(|g\rangle + i|e\rangle)/\sqrt{2}$
$(|g\rangle + |e\rangle)/\sqrt{2}$
$|e\rangle = |1\rangle$

Bloch sphere

From Caves

Qubitology

Single-qubit **states** are points on the Bloch sphere.

Single-qubit **operations (unitary operators)** are rotations of the Bloch sphere.

Single-qubit **measurements** are rotations followed by a measurement in the computational basis (measurement of *z* spin component).

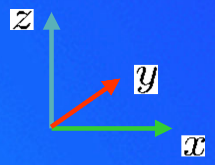
$$
\begin{aligned}
p_0 &= |\langle 0|\mathbf{n}\rangle|^2 = \frac{1}{2}(1+n_z) \\
p_1 &= |\langle 1|\mathbf{n}\rangle|^2 = \frac{1}{2}(1-n_z)
\end{aligned}
$$

Platform-independent description:
Hallmark of an information theory

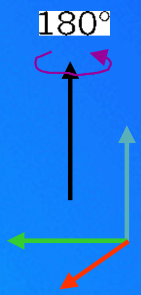
From Caves

Qubitology. Gates and quantum circuits

Single-qubit gates



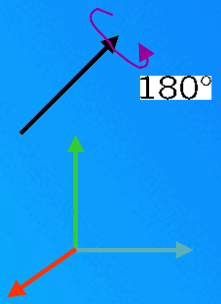
$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = S^2$$



Phase flip

$$|a\rangle \;—\boxed{Z}—\; (-1)^a|a\rangle$$

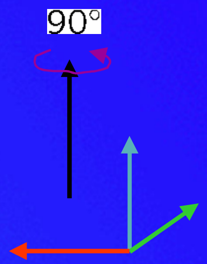
$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$



Hadamard

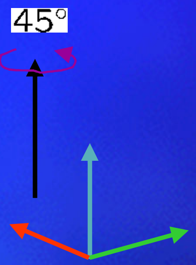
$$|a\rangle \;—\boxed{H}—\; (|0\rangle + (-1)^a|1\rangle)/\sqrt{2}$$

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} = T^2$$



$$|a\rangle \;—\boxed{S}—\; i^a|a\rangle$$

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



$$|a\rangle \;—\boxed{T}—\; e^{ia\pi/4}|a\rangle$$

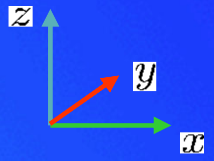
$$Z^2 = H^2 = I$$

From Caves

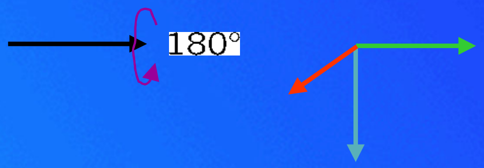
中国科学技术大学 陈凯

Qubitology. Gates and quantum circuits

More single-qubit gates



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

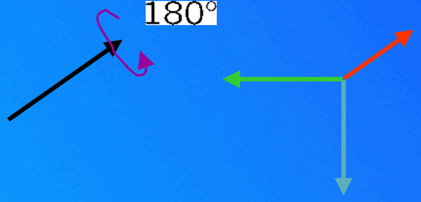


Bit flip

$$|a\rangle \;-\!\!\boxed{X}\!\!-\; |a\oplus 1\rangle \;=\; -\!\!\boxed{H}\!\!-\!\!\boxed{Z}\!\!-\!\!\boxed{H}\!\!-$$

$$X^2=Y^2=I$$

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



Phase-bit flip

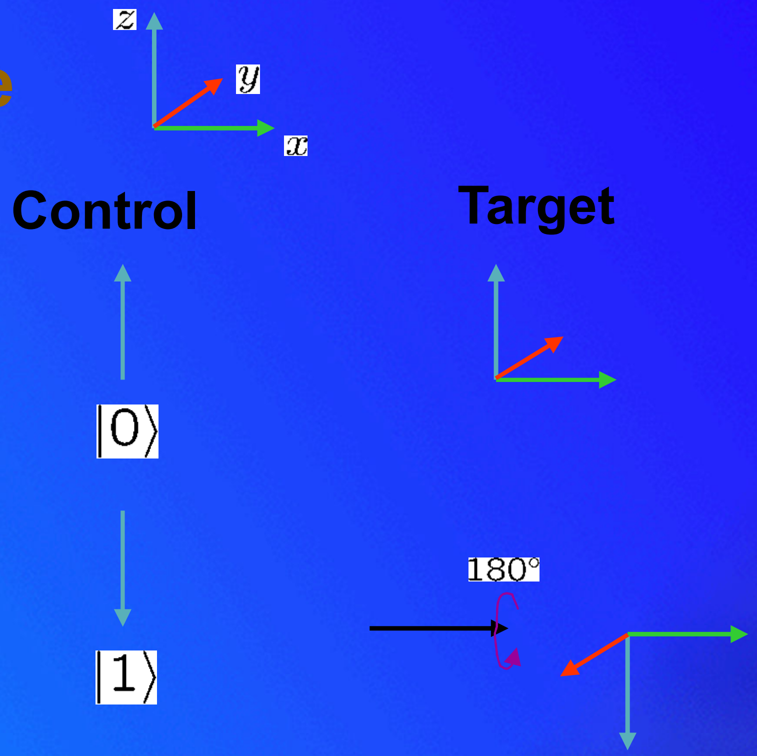
$$|a\rangle \;-\!\!\boxed{iY}\!\!-\; (-1)^{a+1}|a\oplus 1\rangle$$

$$= -\!\!\boxed{X}\!\!-\!\!\boxed{Z}\!\!- \;=\; -\!\!\boxed{H}\!\!-\!\!\boxed{Z}\!\!-\!\!\boxed{H}\!\!-\!\!\boxed{Z}\!\!-$$

From Caves

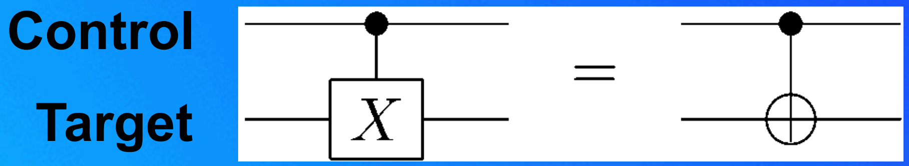
Qubitology. Gates and quantum circuits

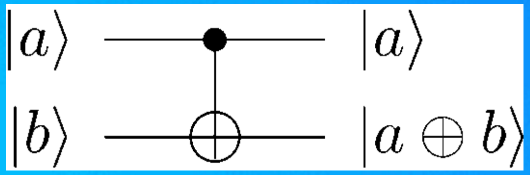
Control-target two-qubit gate



$$\text{C-NOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$= |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$$





$$(\text{C-NOT})^2 = I$$

From Caves

Qubitology. Gates and quantum circuits

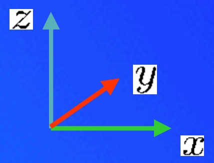
Universal set of quantum gates

- *T* (45-degree rotation about *z*)
- *H* (Hadamard)
- C-NOT

From Caves

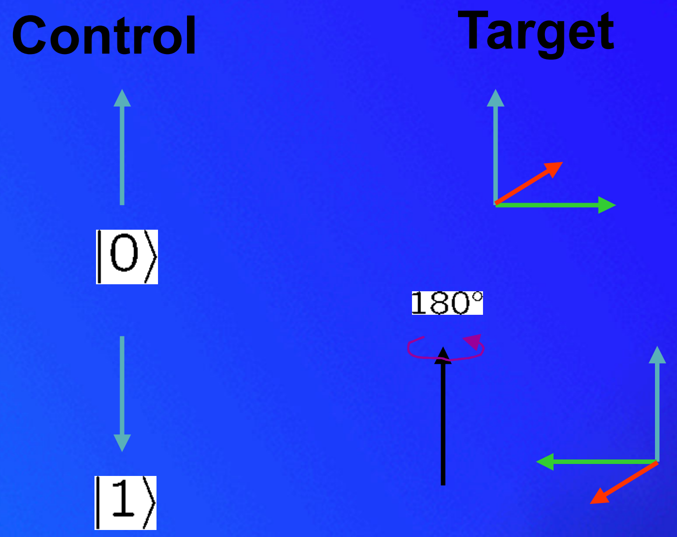
Qubitology. Gates and quantum circuits

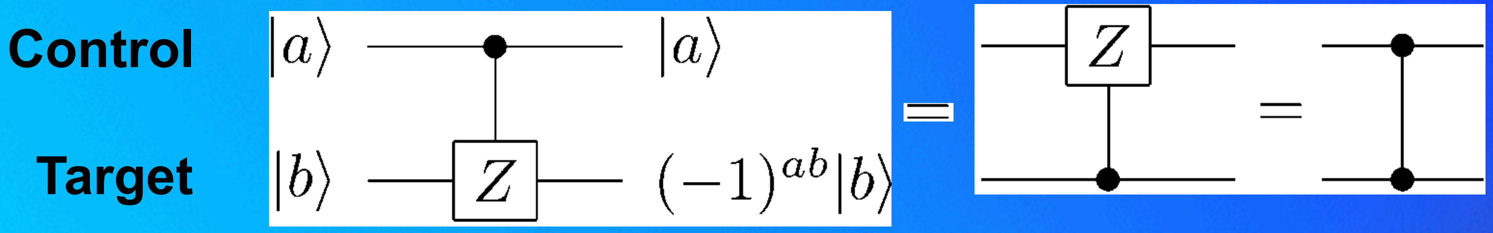
Another two-qubit gate

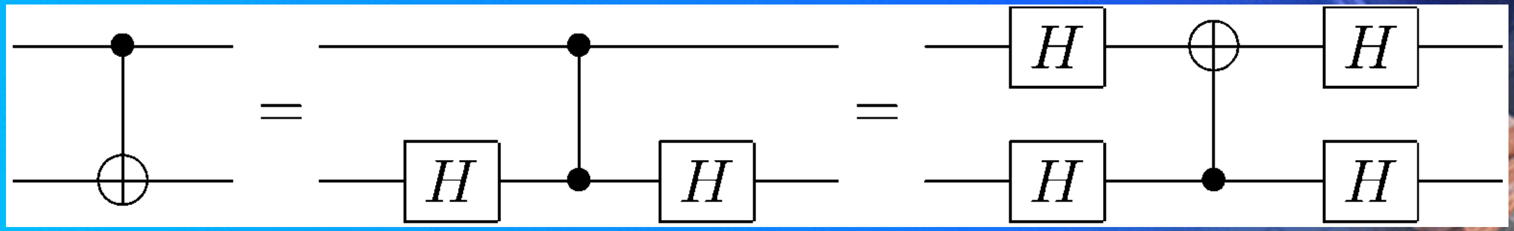


$$\text{C-PHASE} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

$$= |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Z$$



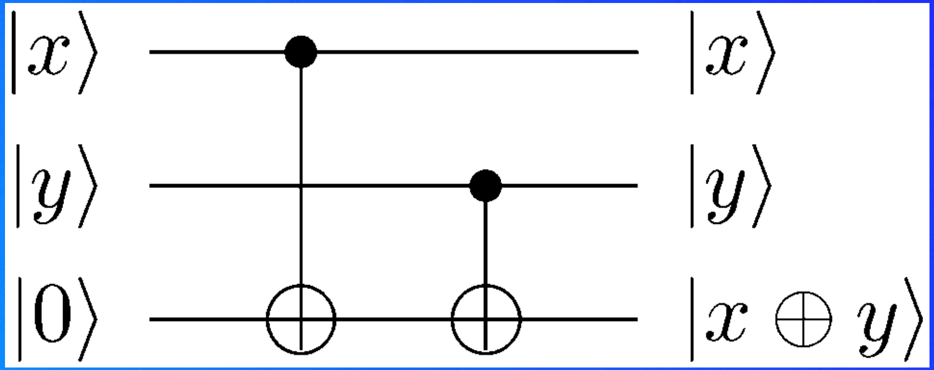




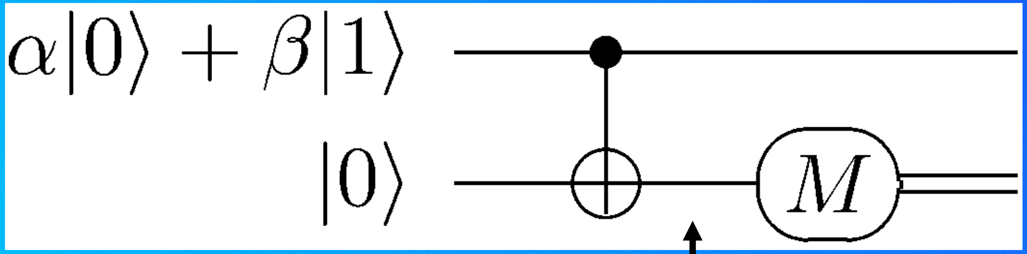
From Caves

Qubitology. Gates and quantum circuits

C-NOT as parity check



C-NOT as measurement gate



$$\begin{cases} |0\rangle \\ |1\rangle \end{cases}$$

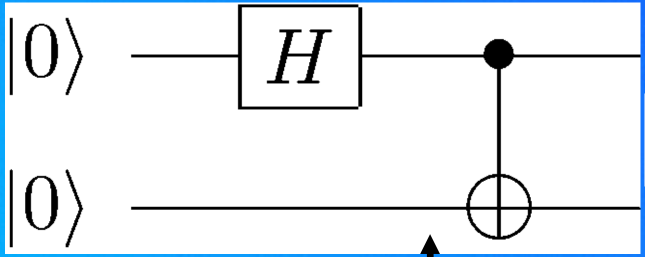
$$\begin{cases} 0, & p_0 = |\alpha|^2 \\ 1, & p_1 = |\beta|^2 \end{cases}$$

$$\alpha|00\rangle + \beta|11\rangle$$

From Caves

Qubitology. Gates and quantum circuits

Making Bell states using C-NOT

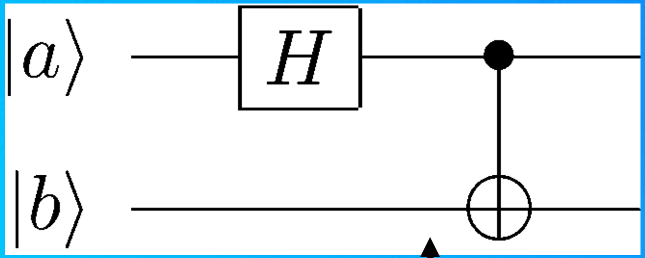


$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

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

Bell states

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



$\frac{1}{\sqrt{2}}(|0b\rangle + (-1)^a|1, b \oplus 1\rangle) \equiv |\beta_{ab}\rangle$

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

phase bit

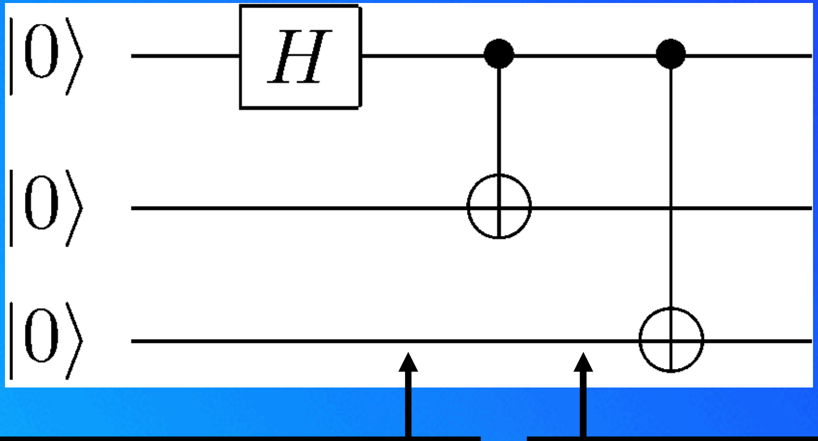
parity bit

From Caves

中国科学技术大学 陈凯

Qubitology. Gates and quantum circuits

Making cat states using C-NOT



$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|00\rangle$

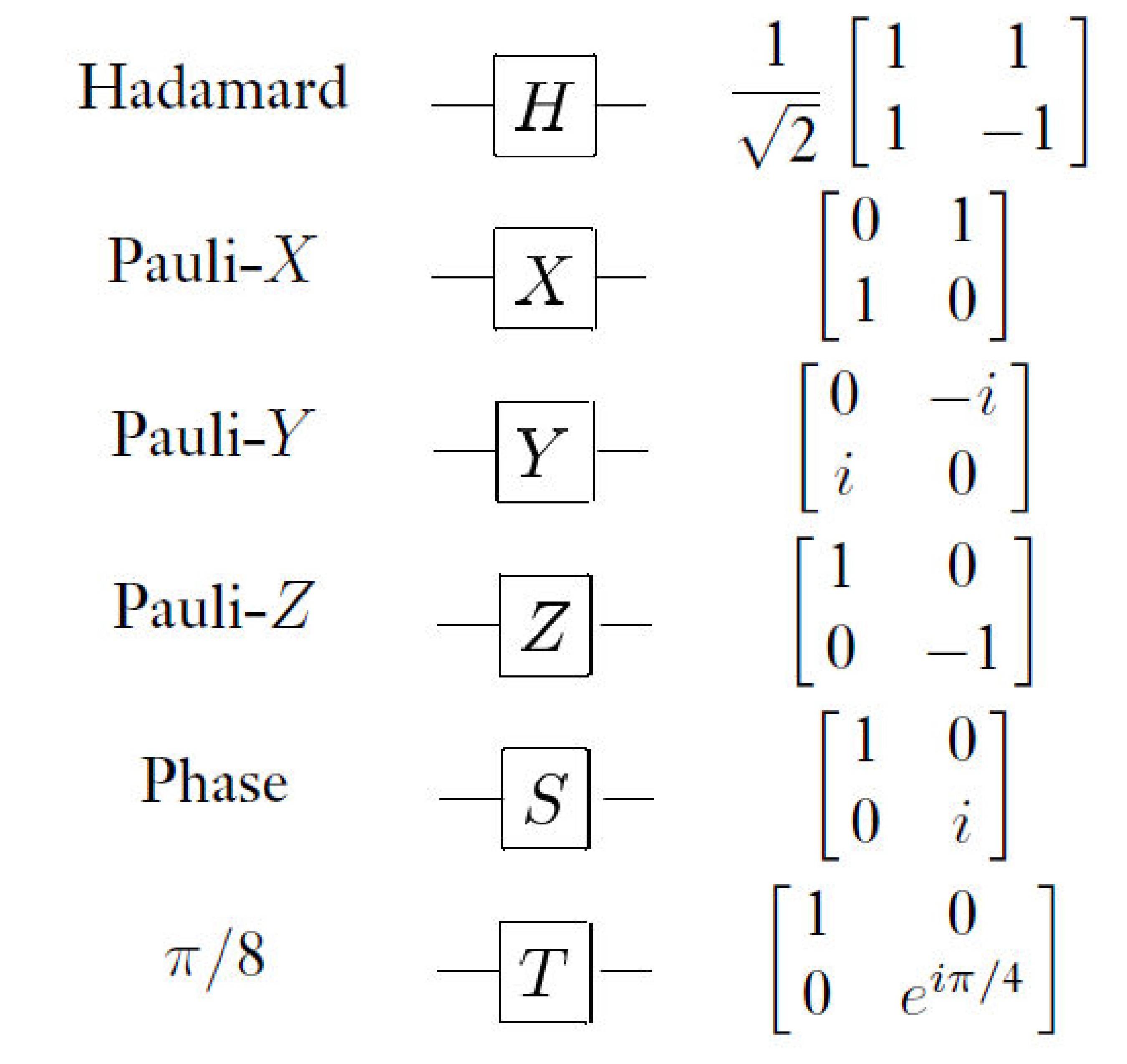
$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)|0\rangle$

GHZ (cat) state

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

From Caves

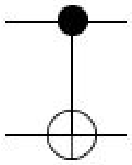
典型的单比特量子门



Hadamard	$-\boxed{H}-$	$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$
Pauli-X	$-\boxed{X}-$	$\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$
Pauli-Y	$-\boxed{Y}-$	$\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix}$
Pauli-Z	$-\boxed{Z}-$	$\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$
Phase	$-\boxed{S}-$	$\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}$
$\pi/8$	$-\boxed{T}-$	$\begin{bmatrix}1 & 0\\ 0 & e^{i\pi/4}\end{bmatrix}$

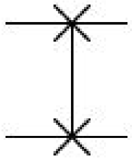
典型的多比特量子门

controlled-NOT



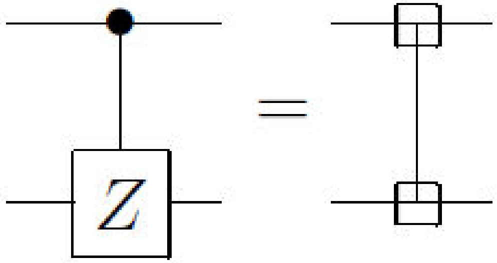
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

swap



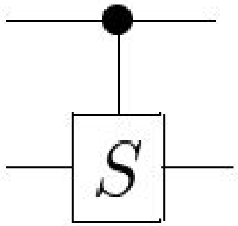
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

controlled-Z



$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

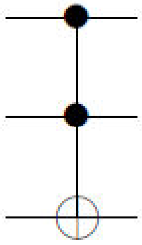
controlled-phase



$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \end{bmatrix}$$

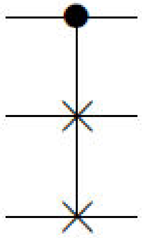
典型的多比特量子门

Toffoli



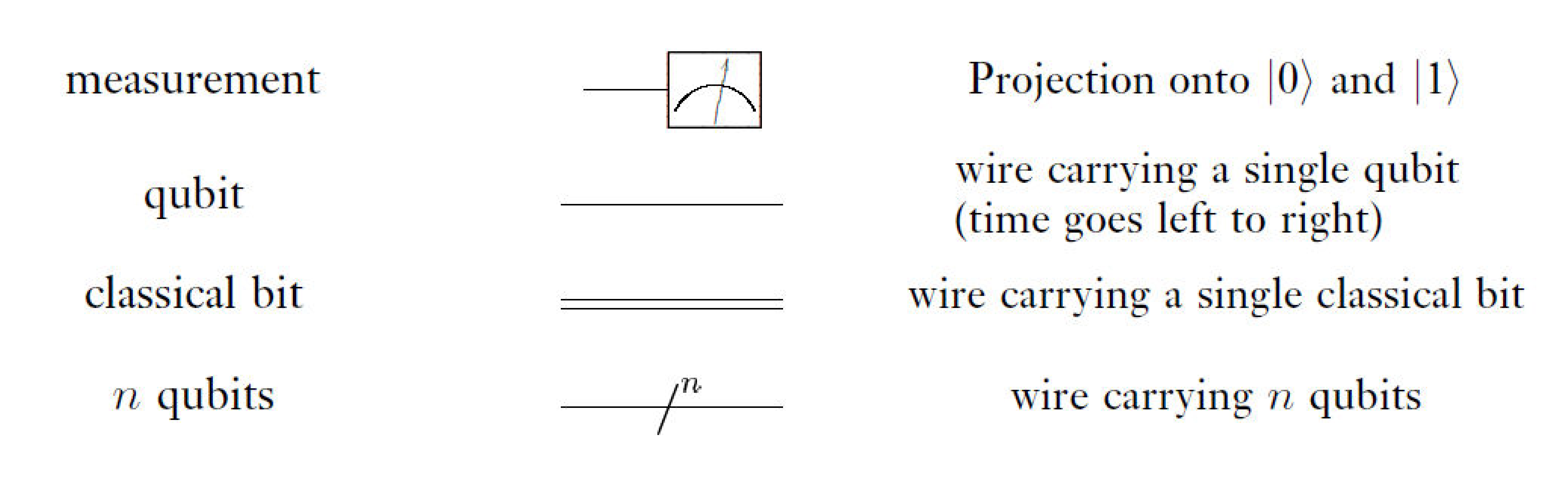
$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Fredkin (controlled-swap)



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

典型的量子线路表示



measurement		Projection onto $\|0\rangle$ and $\|1\rangle$
qubit		wire carrying a single qubit (time goes left to right)
classical bit		wire carrying a single classical bit
n qubits	$/^{n}$	wire carrying n qubits

Decomposing single qubit operations

Arbitrary 2 × 2 unitary matrix may be decomposed as

$$U = e^{i\alpha} \left[\begin{array}{cc} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{array} \right] \left[\begin{array}{cc} \cos\frac{\gamma}{2} & -\sin\frac{\gamma}{2} \\ \sin\frac{\gamma}{2} & \cos\frac{\gamma}{2} \end{array} \right] \left[\begin{array}{cc} e^{-i\delta/2} & 0 \\ 0 & e^{i\delta/2} \end{array} \right]$$

where α, β, γ, and δ are real-valued.

Swap gate

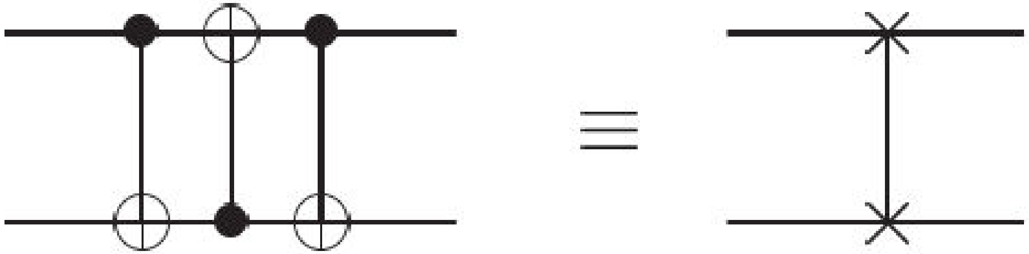


Figure 1.7. Circuit swapping two qubits, and an equivalent schematic symbol notation for this common and useful circuit.

$$
\begin{aligned}
|a, b\rangle &\longrightarrow |a, a \oplus b\rangle \\
&\longrightarrow |a \oplus (a \oplus b), a \oplus b\rangle = |b, a \oplus b\rangle \\
&\longrightarrow |b, (a \oplus b) \oplus b\rangle = |b, a\rangle \,,
\end{aligned}
$$

Control-U gate

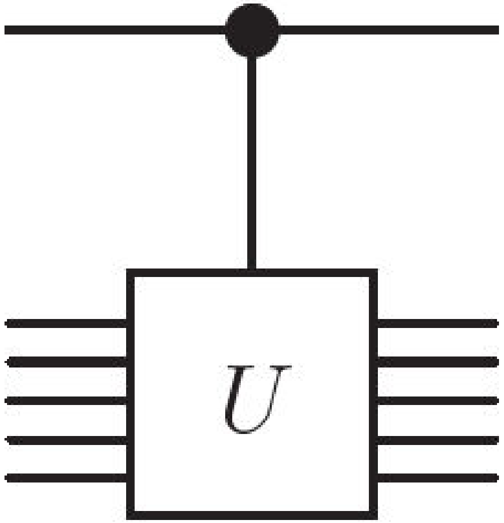


Figure 1.8. Controlled-U gate.

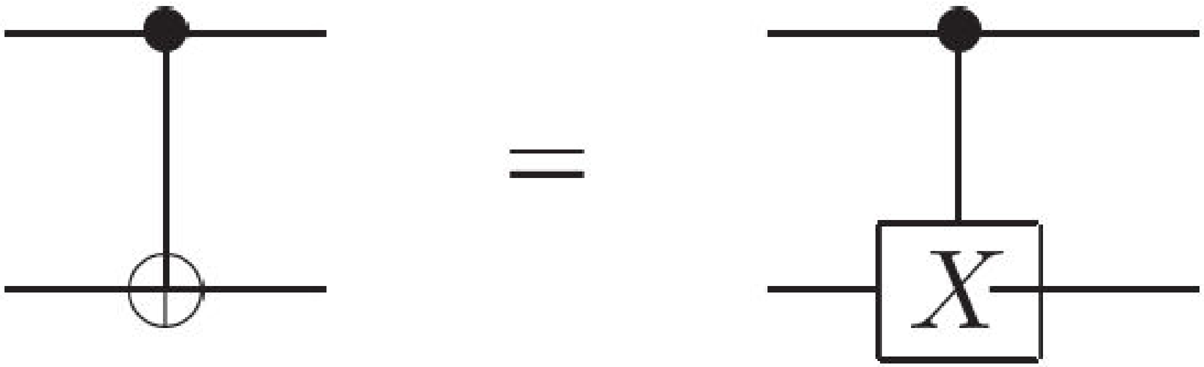


Figure 1.9. Two different representations for the controlled-NOT.

第六章 量子计算

1. 经典计算机发展
2. 量子计算机简介
3. 量子计算实现准则
4. 量子计算的物理实现、商业化进程
5. 量子比特表示、量子线路
6. **量子协议的线路实现**
7. 典型量子算法
8. 单向量子计算
9. 量子算法总结

Circuit for measurement

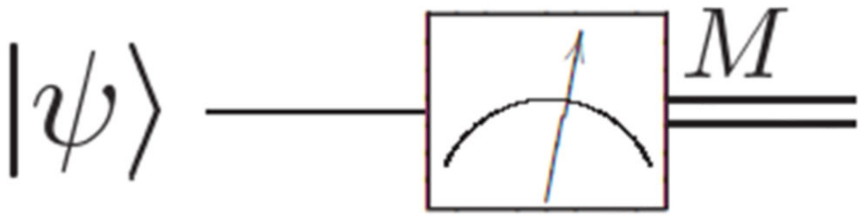
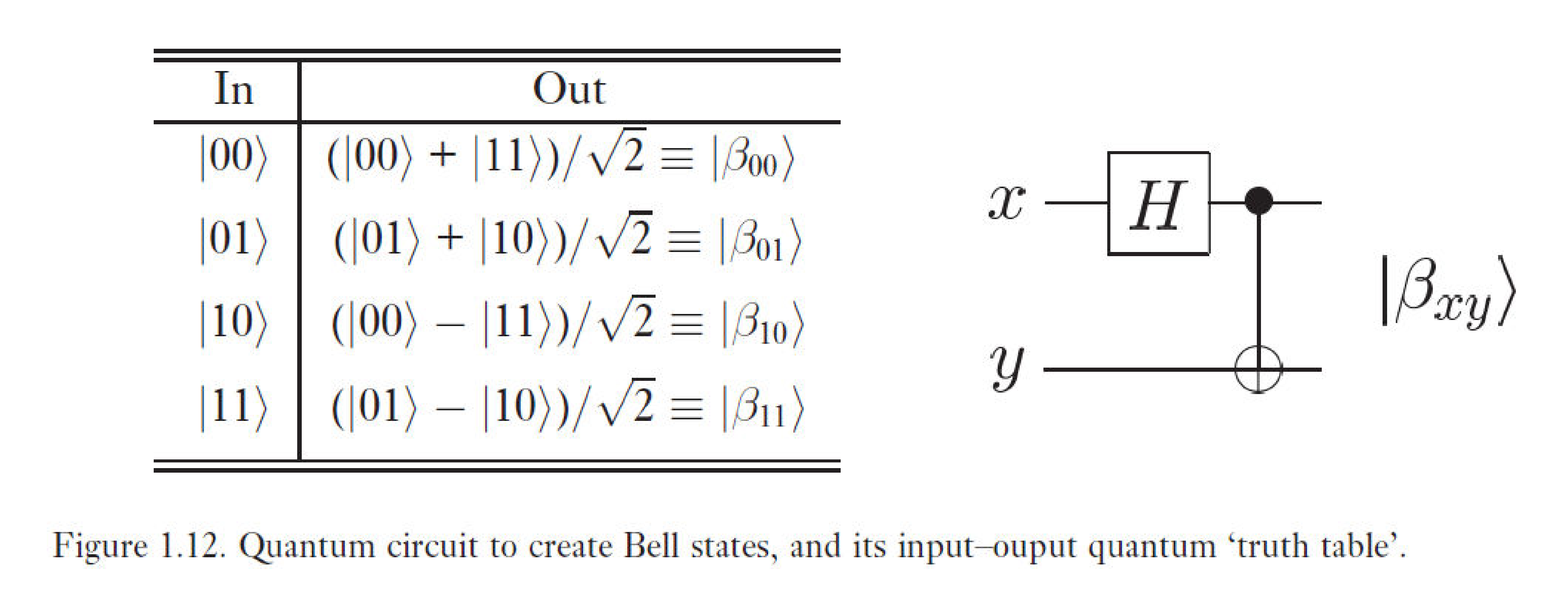


Figure 1.10. Quantum circuit symbol for measurement.

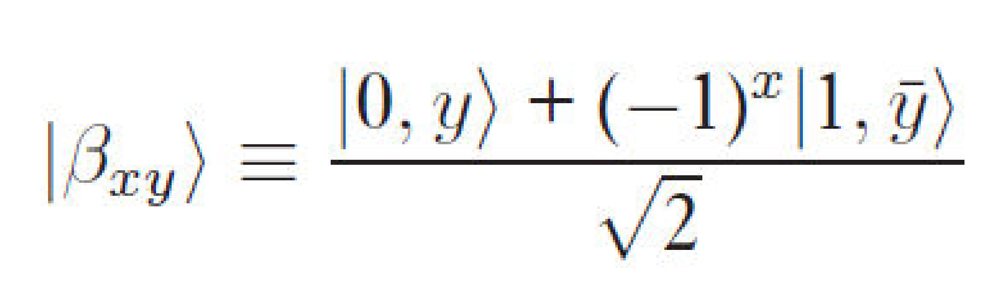
This operation converts a single qubit state $/\psi> = a/0> +\beta/1>$ into a probabilistic classical bit M (distinguished from a qubit by drawing it as a double-line wire), which is 0 with probability $/a/^2$, or 1 with probability $/\beta/^2$.

Bell态产生



In	Out
$\|00\rangle$	$(\|00\rangle + \|11\rangle)/\sqrt{2} \equiv \|\beta_{00}\rangle$
$\|01\rangle$	$(\|01\rangle + \|10\rangle)/\sqrt{2} \equiv \|\beta_{01}\rangle$
$\|10\rangle$	$(\|00\rangle - \|11\rangle)/\sqrt{2} \equiv \|\beta_{10}\rangle$
$\|11\rangle$	$(\|01\rangle - \|10\rangle)/\sqrt{2} \equiv \|\beta_{11}\rangle$

Figure 1.12. Quantum circuit to create Bell states, and its input–ouput quantum ‘truth table’.



$$|\beta_{xy}\rangle \equiv \frac{|0, y\rangle + (-1)^x |1, \bar{y}\rangle}{\sqrt{2}}$$

Quantum teleportation

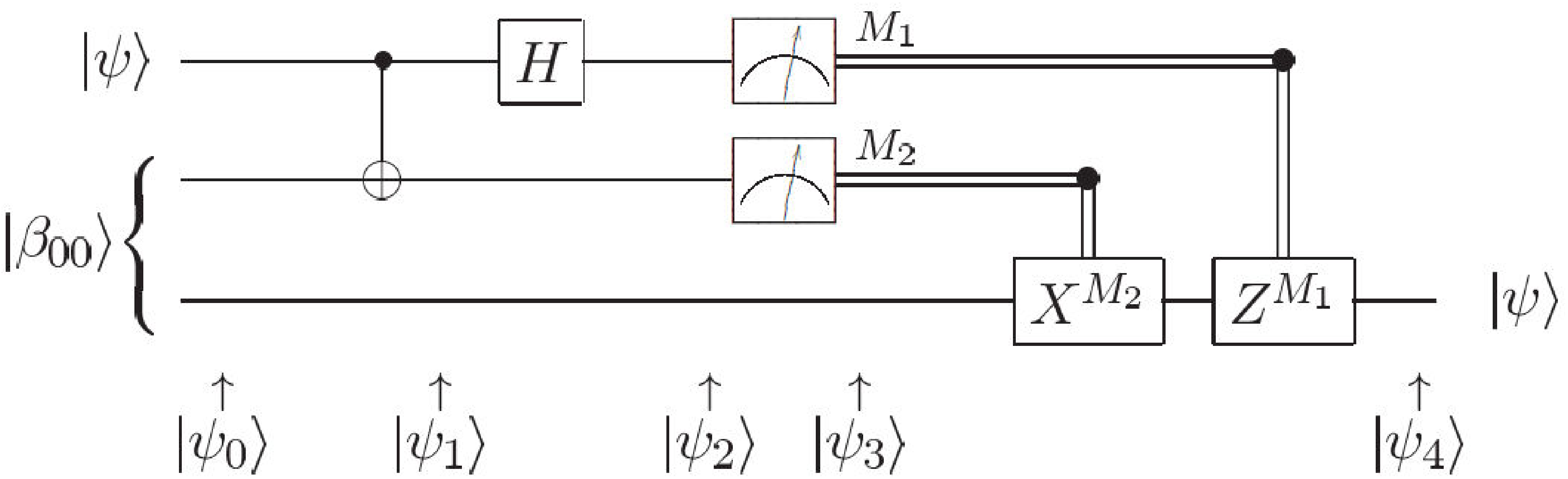
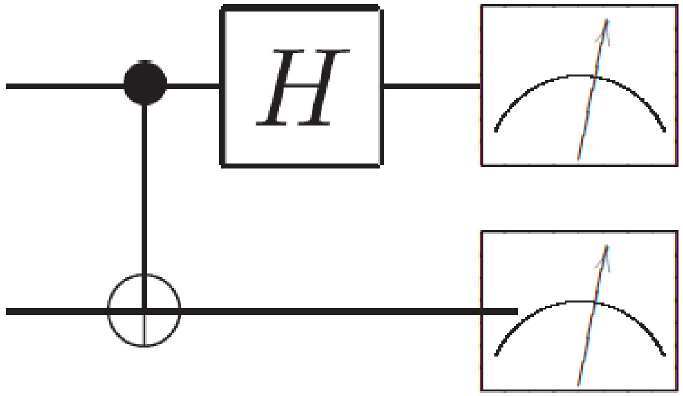
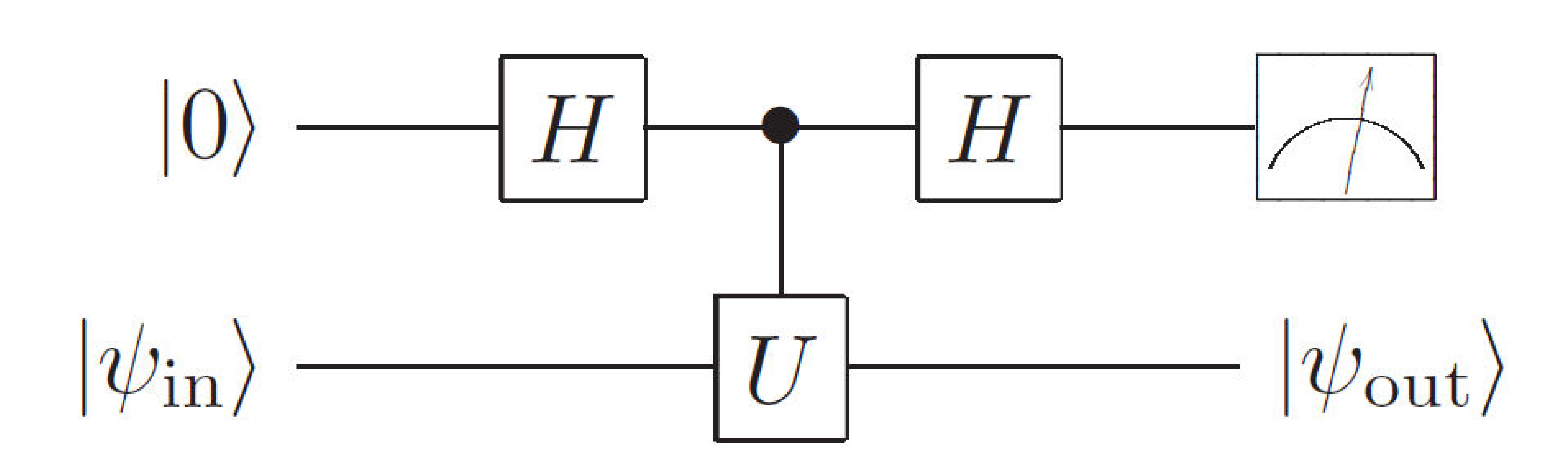


Figure 1.13. Quantum circuit for teleporting a qubit. The two top lines represent Alice's system, while the bottom line is Bob's system. The meters represent measurement, and the double lines coming out of them carry classical bits (recall that single lines denote qubits).



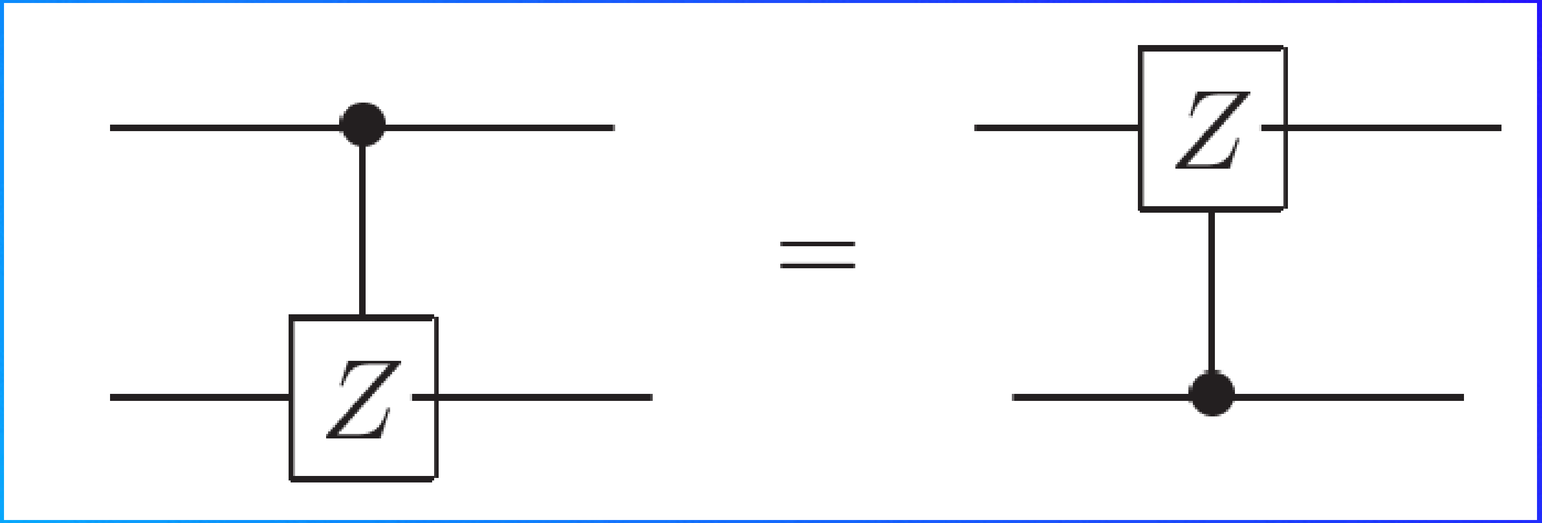
Measurement in the basis of the Bell states

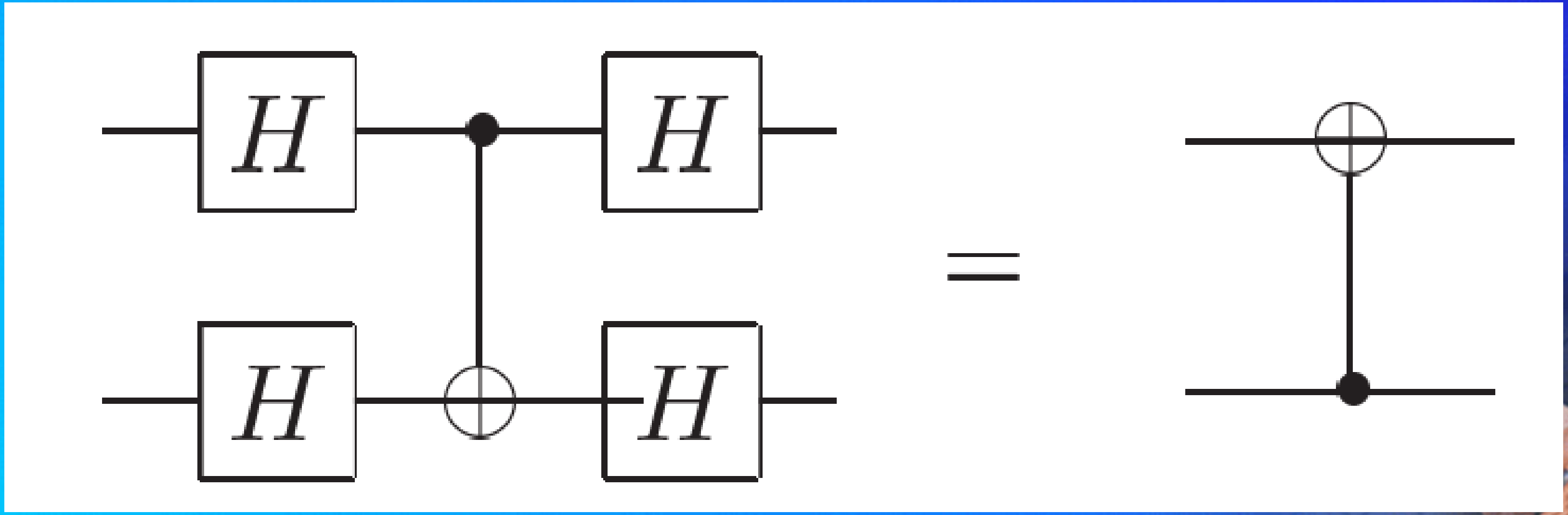
Measuring an operator



Suppose we have a single qubit operator U with eigenvalues ±1, so that U is both Hermitian and unitary, so it can be regarded both as an observable and a quantum gate. Suppose we wish to measure the observable U. That is, we desire to obtain a measurement result indicating one of the two eigenvalues, and leaving a post-measurement state which is the corresponding eigenvector. How can this be implemented by a quantum circuit? Show that the following circuit implements a measurement of U.

等价的量子线路





Rotation operators

The Pauli matrices give rise to three useful classes of unitary matrices when they are exponentiated, the *rotation operators* about the *x*, *y*, and *z* axes, defined by the equations:

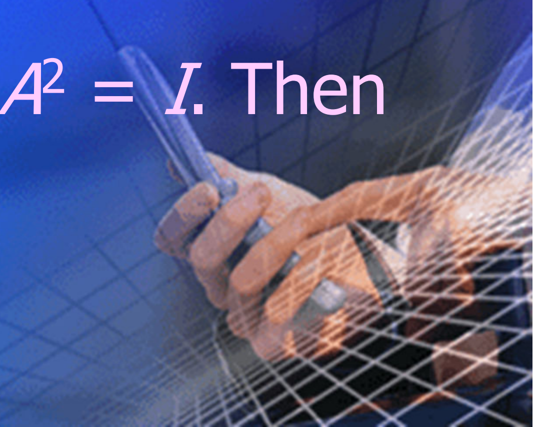
$$R_x(\theta) \equiv e^{-i\theta X/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}X = \begin{bmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$$

$$R_y(\theta) \equiv e^{-i\theta Y/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Y = \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$$

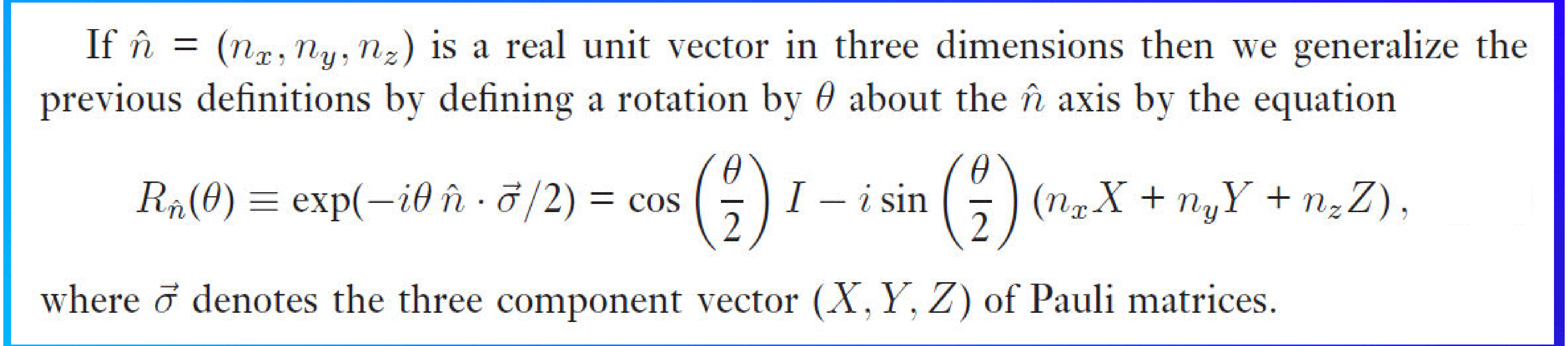
$$R_z(\theta) \equiv e^{-i\theta Z/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Z = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix}.$$

Let *x* be a real number and *A* a matrix such that $A^2 = I$. Then

$$\exp(iAx) = \cos(x)I + i\sin(x)A$$



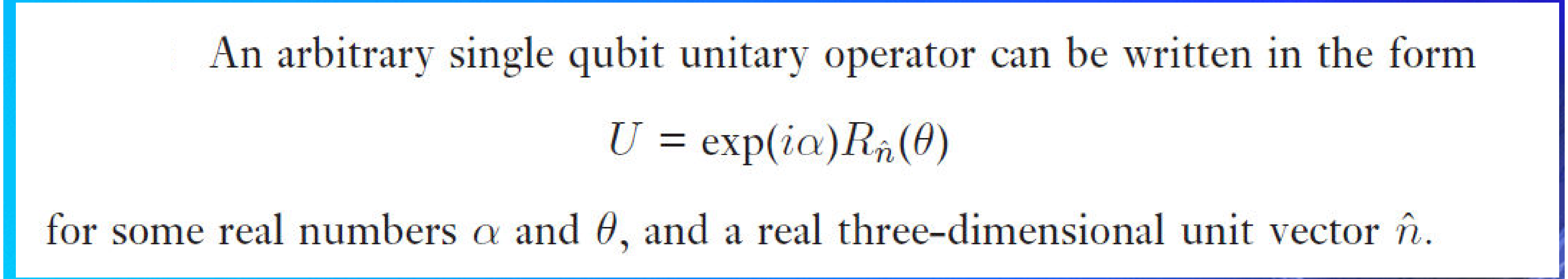
Rotation operators



If $\hat{n} = (n_x, n_y, n_z)$ is a real unit vector in three dimensions then we generalize the previous definitions by defining a rotation by θ about the $\hat{n}$ axis by the equation

$$R_{\hat{n}}(\theta) \equiv \exp(-i\theta\,\hat{n}\cdot\vec{\sigma}/2) = \cos\left(\frac{\theta}{2}\right) I - i\sin\left(\frac{\theta}{2}\right)(n_x X + n_y Y + n_z Z),$$

where $\vec{\sigma}$ denotes the three component vector (X, Y, Z) of Pauli matrices.



An arbitrary single qubit unitary operator can be written in the form

$$U = \exp(i\alpha)R_{\hat{n}}(\theta)$$

for some real numbers α and θ, and a real three-dimensional unit vector $\hat{n}$.

第六章 量子计算

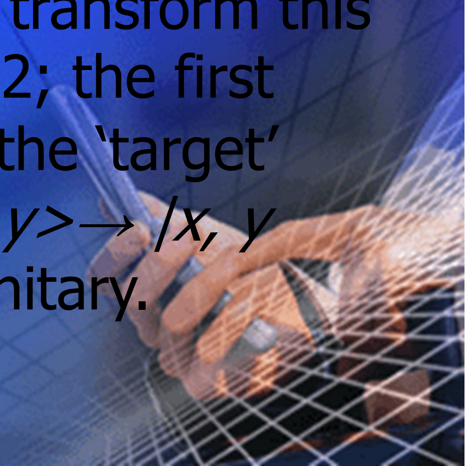
1. 经典计算机发展
2. 量子计算机简介
3. 量子计算实现准则
4. 量子计算的物理实现、商业化进程
5. 量子比特表示、量子线路
6. 量子协议的线路实现
7. **典型量子算法**
8. 单向量子计算
9. 量子算法总结

Quantum parallelism

Quantum parallelism is a fundamental feature of many quantum algorithms. Heuristically, and at the risk of over-simplifying, quantum parallelism allows quantum computers to evaluate a function $f(x)$ for many *different* values of x simultaneously.

Suppose $f(x) : \{0, 1\} \to \{0, 1\}$ is a function with a one-bit domain and range.

A convenient way of computing this function on a quantum computer is to consider a two qubit quantum computer which starts in the state $/x, y>$. With an appropriate sequence of logic gates it is possible to transform this state into $/x, y \oplus f(x)>$, where $\oplus$ indicates addition modulo 2; the first register is called the ‘data’ register, and the second register the ‘target’ register. We give the transformation defined by the map $/x, y> \to /x, y \oplus f(x)>$ a name, U_f, and note that it is easily shown to be unitary.



A quantum computer

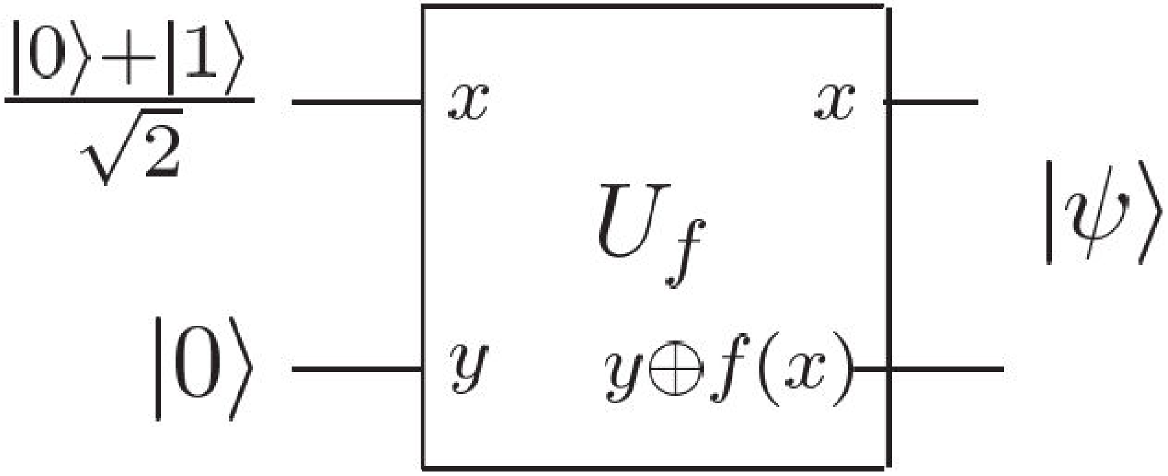


Figure 1.17. Quantum circuit for evaluating $f(0)$ and $f(1)$ simultaneously. U_f is the quantum circuit which takes inputs like $|x, y\rangle$ to $|x, y \oplus f(x)\rangle$.

The resulting state is

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

多体推广

This procedure can easily be generalized to functions on an arbitrary number of bits, by using a general operation known as the *Hadamard transform*, or sometimes the *Walsh–Hadamard transform*. This operation is just *n* Hadamard gates acting in parallel on *n* qubits.

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

$$\frac{1}{\sqrt{2^n}} \sum_x |x\rangle$$

Prepare the $n + 1$ qubit state /0>$^{\otimes n}$/0>, then apply the Hadamard transform to the first *n* qubits, followed by the quantum circuit implementing U_f . This produces the state

$$\frac{1}{\sqrt{2^n}} \sum_x |x\rangle |f(x)\rangle$$

Quantum algorithms
Deutsch algorithm

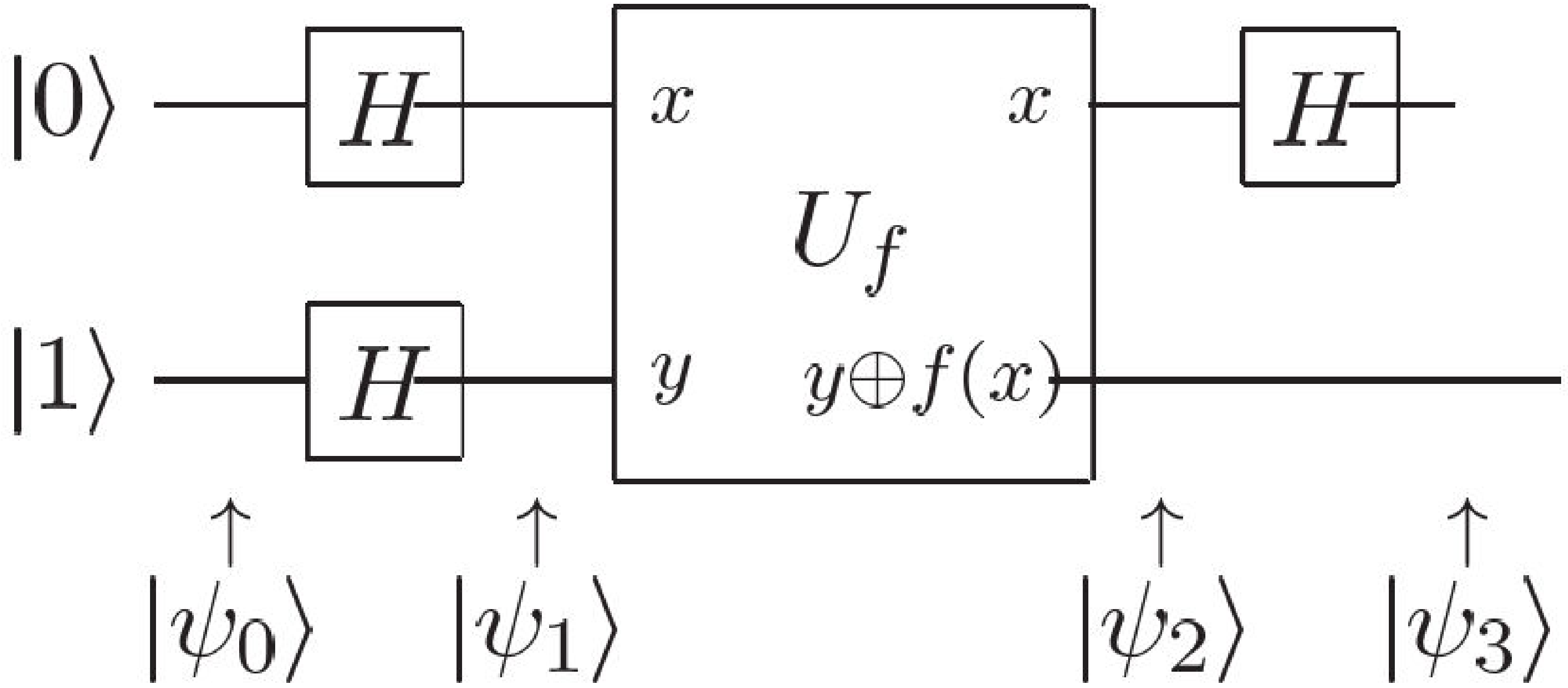
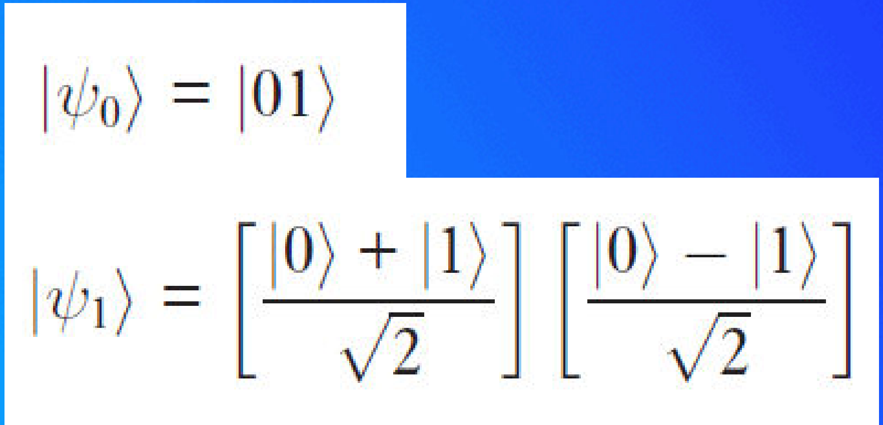


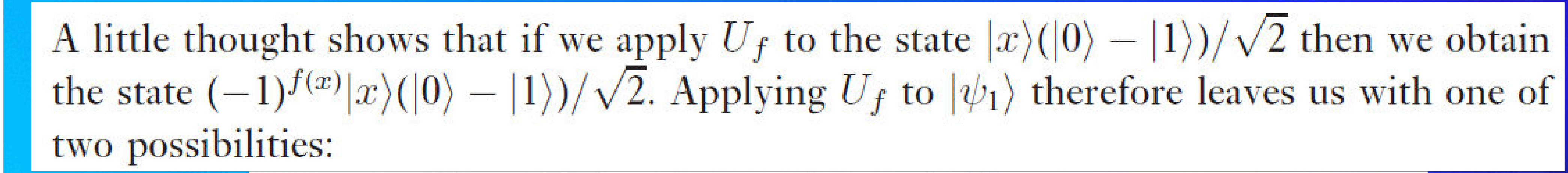
Figure 1.19. Quantum circuit implementing Deutsch's algorithm.

Deutsch algorithm

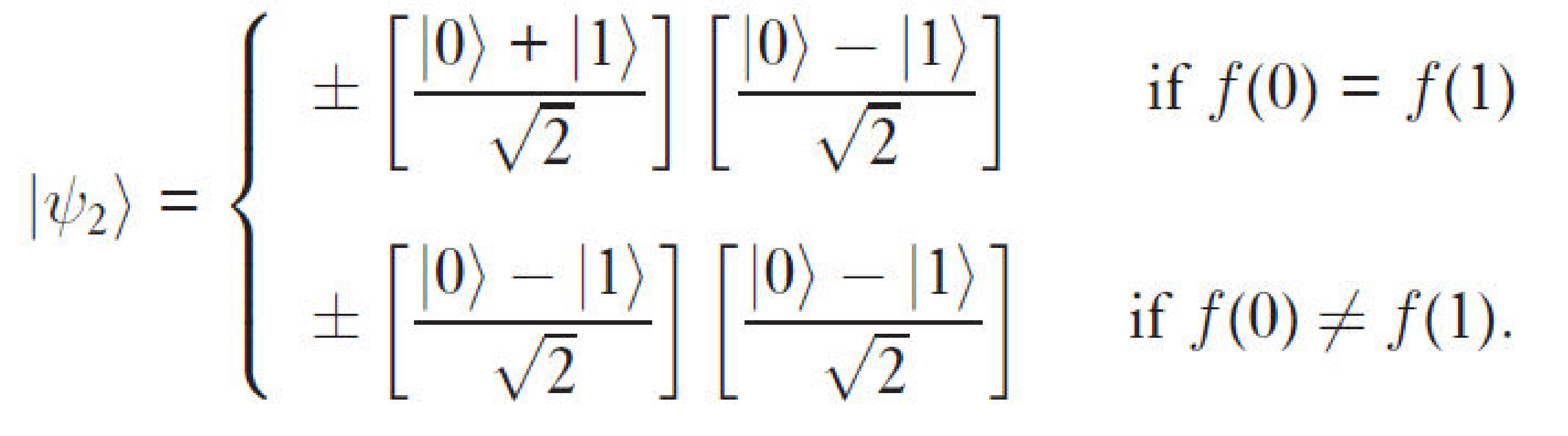


$$|\psi_0\rangle = |01\rangle$$

$$|\psi_1\rangle = \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$



A little thought shows that if we apply U_f to the state $|x\rangle(|0\rangle - |1\rangle)/\sqrt{2}$ then we obtain the state $(-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle)/\sqrt{2}$. Applying U_f to $|\psi_1\rangle$ therefore leaves us with one of two possibilities:



$$|\psi_2\rangle = \begin{cases} \pm\left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{if } f(0) = f(1) \\ \pm\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{if } f(0) \neq f(1). \end{cases}$$

Deutsch algorithm

The final Hadamard gate on the first qubit thus gives us

$$|\psi_3\rangle = \begin{cases} \pm|0\rangle\left[\dfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & \text{if } f(0)=f(1) \\[2em] \pm|1\rangle\left[\dfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & \text{if } f(0)\neq f(1). \end{cases}$$

Realizing that $f(0) \oplus f(1)$ is 0 if $f(0) = f(1)$ and 1 otherwise, we can rewrite this result concisely as

$$|\psi_3\rangle = \pm|f(0)\oplus f(1)\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$$

Deutsch algorithm

By measuring the first qubit we may determine $f(0) \oplus f(1)$. This is very interesting indeed: the quantum circuit has given us the ability to determine a *global property* of $f(x)$, namely $f(0)\oplus f(1)$, using only *one* evaluation of $f(x)$! This is faster than is possible with a classical apparatus, which would require at least two evaluations.

Naively, one might think that the state $/0>/f(0)> + /1>/f(1)>$ corresponds rather closely to a probabilistic classical computer that evaluates $f(0)$ with probability one-half, or $f(1)$ with probability one-half. The difference is that in a classical computer these two alternatives forever exclude one another; in a quantum computer it is possible for the two alternatives to interfere with one another to yield some global property of the function f, by using something like the Hadamard gate to recombine the different alternatives, as was done in Deutsch’s algorithm. The essence of the design of many quantum algorithms is that a clever choice of function and final transformation allows efficient determination of useful global information about the function – information which cannot be attained quickly on a classical computer.

Deutsch-Jozsa algorithm

Alice, in Amsterdam, selects a number x from 0 to $2^n - 1$, and mails it in a letter to Bob, in Boston. Bob calculates some function $f(x)$ and replies with the result, which is either 0 or 1. Now, Bob has promised to use a function f which is of one of two kinds; either $f(x)$ is *constant* for all values of x, or else $f(x)$ is *balanced*, that is, equal to 1 for exactly half of all the possible x, and 0 for the other half. Alice's goal is to determine with certainty whether Bob has chosen a constant or a balanced function, corresponding with him as little as possible. How fast can she succeed?

Deutsch-Jozsa algorithm

Boolean function $f : \{0,1\}^N \rightarrow \{0,1\}$

Promise: ***f* is constant or balanced.**

Task: Determine which.

Classical: Roughly 2^{N-1} +1 function calls are required to be certain.

Quantum: Only 1 function call is needed.

Deutsch-Jozsa algorithm

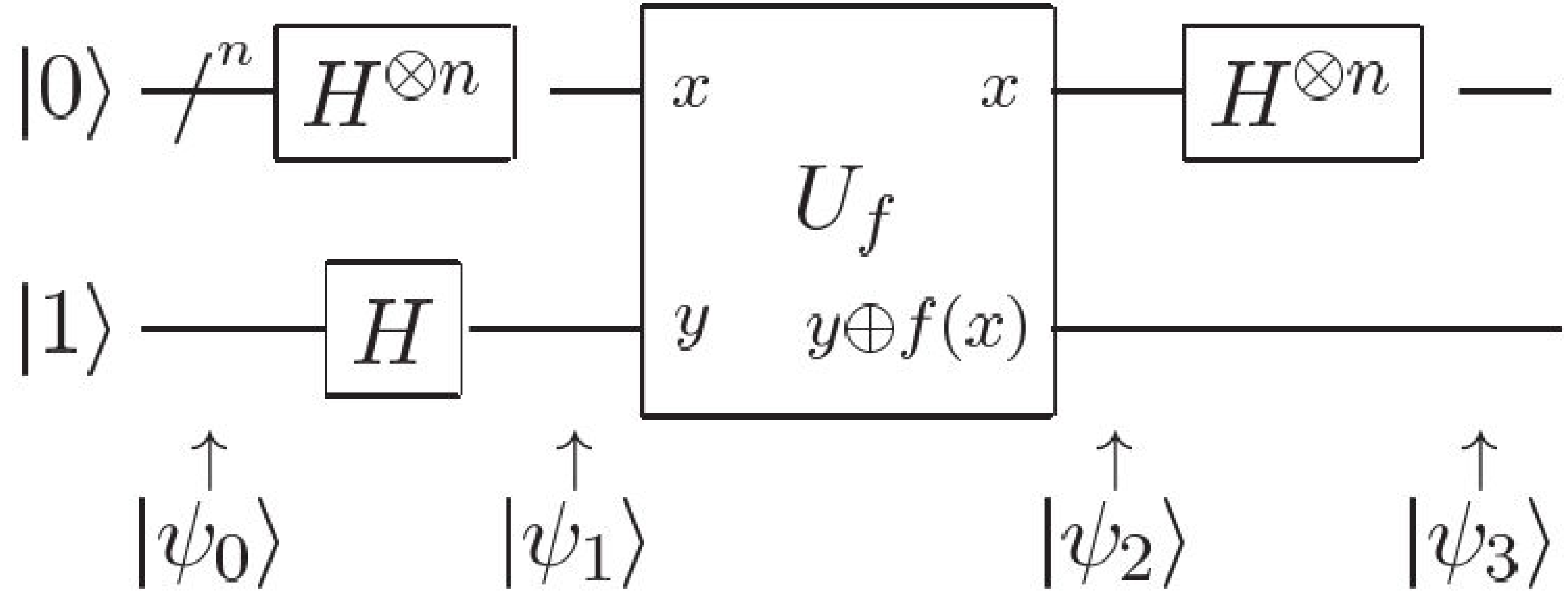


Figure 1.20. Quantum circuit implementing the general Deutsch–Jozsa algorithm. The wire with a '/' through it represents a set of n qubits, similar to the common engineering notation.

$$|\psi_0\rangle = |0\rangle^{\otimes n}|1\rangle$$

Deutsch-Jozsa algorithm

After the Hadamard transform on the query register and the Hadamard gate on the answer register we have

$$|\psi_1\rangle = \sum_{x \in \{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$$

Next, the function *f* is evaluated (by Bob) using U_f : $|x, y> \rightarrow |x, y \oplus f(x)>$, giving

$$|\psi_2\rangle = \sum_{x} \frac{(-1)^{f(x)} |x\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$$

Deutsch-Jozsa algorithm

利用

$$H|x\rangle = \sum_z (-1)^{xz}|z\rangle/\sqrt{2}$$

我们有

$$H^{\otimes n}|x_1,\ldots,x_n\rangle = \frac{\sum_{z_1,\ldots,z_n}(-1)^{x_1z_1+\cdots+x_nz_n}|z_1,\ldots,z_n\rangle}{\sqrt{2^n}}$$

$$H^{\otimes n}|x\rangle = \frac{\sum_z(-1)^{x\cdot z}|z\rangle}{\sqrt{2^n}}$$

where *x* · *z* is the bitwise inner product of *x* and *z*, modulo 2.

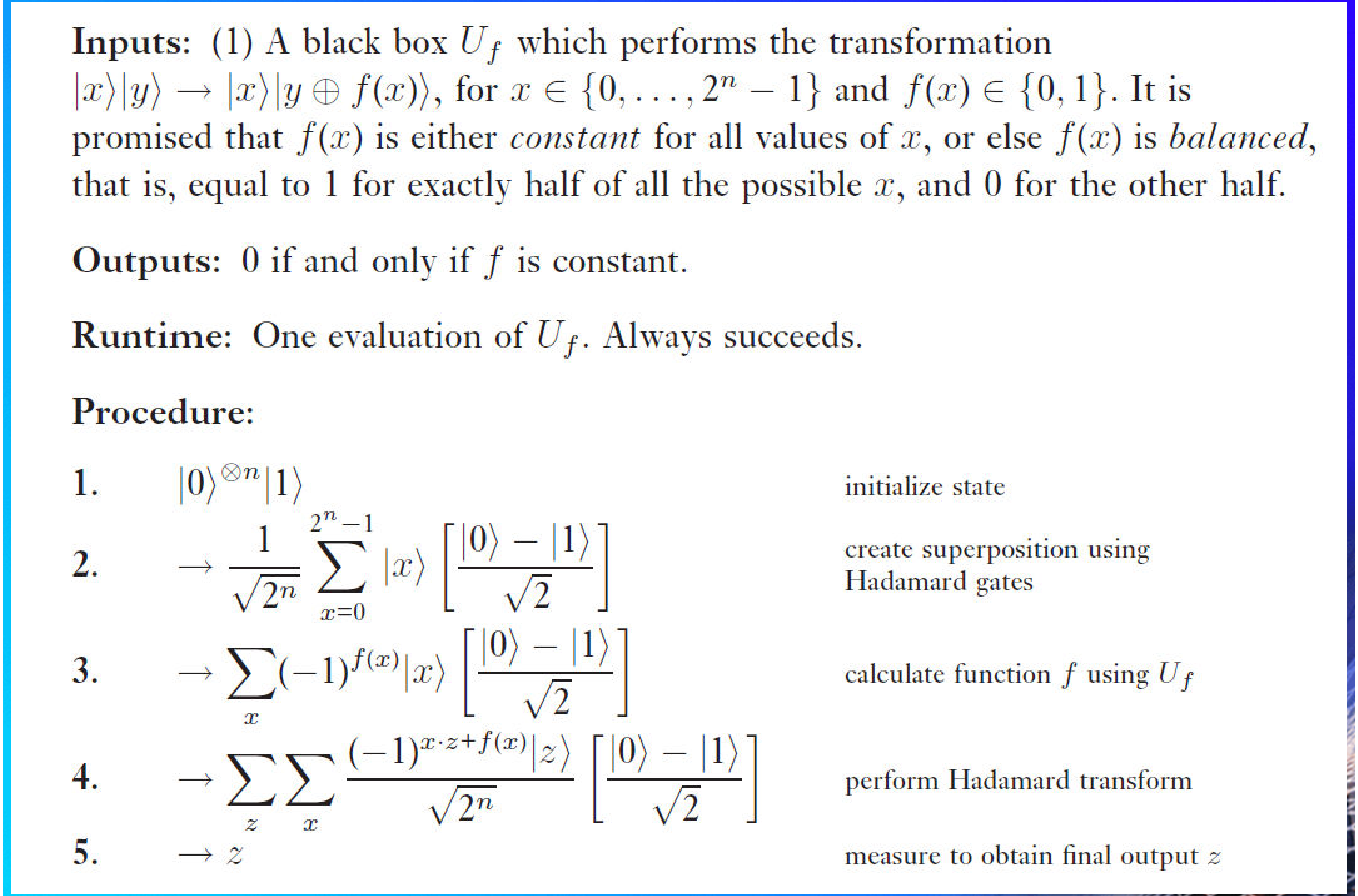
Deutsch-Jozsa algorithm

利用上页结果，我们进一步有

$$|\psi_3\rangle = \sum_z \sum_x \frac{(-1)^{x\cdot z + f(x)}|z\rangle}{2^n}\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

Note that the amplitude for the state /0>$^{\otimes n}$ is $\sum_x (-1)^{f(x)}/2^n$. Let's look at the two possible cases – *f* constant and *f* balanced – to discern what happens. In the case where *f* is constant the amplitude for /0>$^{\otimes n}$ is +1 or −1, depending on the constant value *f*(*x*) takes. Because /ψ_3> is of unit length it follows that all the other amplitudes must be zero, and an observation will yield 0s for all qubits in the query register. If *f* is balanced then the positive and negative contributions to the amplitude for /0>$^{\otimes n}$ cancel, leaving an amplitude of zero, and a measurement must yield a result other than 0 on at least one qubit in the query register. Summarizing, if Alice measures all 0s then the function is constant; otherwise the function is balanced. The Deutsch–Jozsa algorithm is summarized below.

Deutsch-Jozsa algorithm



Inputs: (1) A black box U_f which performs the transformation $|x\rangle|y\rangle \to |x\rangle|y \oplus f(x)\rangle$, for $x \in \{0, \ldots, 2^n - 1\}$ and $f(x) \in \{0, 1\}$. It is promised that $f(x)$ is either *constant* for all values of x, or else $f(x)$ is *balanced*, that is, equal to 1 for exactly half of all the possible x, and 0 for the other half.

Outputs: 0 if and only if f is constant.

Runtime: One evaluation of U_f. Always succeeds.

Procedure:

1. $|0\rangle^{\otimes n}|1\rangle$ initialize state

2. $\to \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$ create superposition using Hadamard gates

3. $\to \sum_x (-1)^{f(x)}|x\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$ calculate function f using U_f

4. $\to \sum_z \sum_x \frac{(-1)^{x\cdot z + f(x)}|z\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$ perform Hadamard transform

5. $\to z$ measure to obtain final output z

Quantum interference in the Deutsch-Jozsa algorithm

Quantum interference allows one to distinguish the situation where half the amplitudes are +1 and half -1 from the situation where all the amplitudes are +1 or -1 (this is the information one wants) without having to determine all amplitudes (this information remains inaccessible).

Variational quantum algorithms

Variational quantum algorithms (VQAs) have emerged as the leading strategy to obtain quantum advantage on NISQ devices. Accounting for all of the constraints imposed by NISQ computers with a single strategy requires an optimization-based or learning-based approach, precisely what VQAs use. VQAs are arguably the quantum analogue of highly successful machine-learning methods, such as neural networks. Moreover, VQAs leverage the toolbox of classical optimization, since they use parameterized quantum circuits to be run on the quantum computer, and then outsource the parameter optimization to a classical optimizer. This approach has the added advantage of keeping the quantum circuit depth shallow and hence mitigating noise, in contrast to quantum algorithms developed for the fault-tolerant era

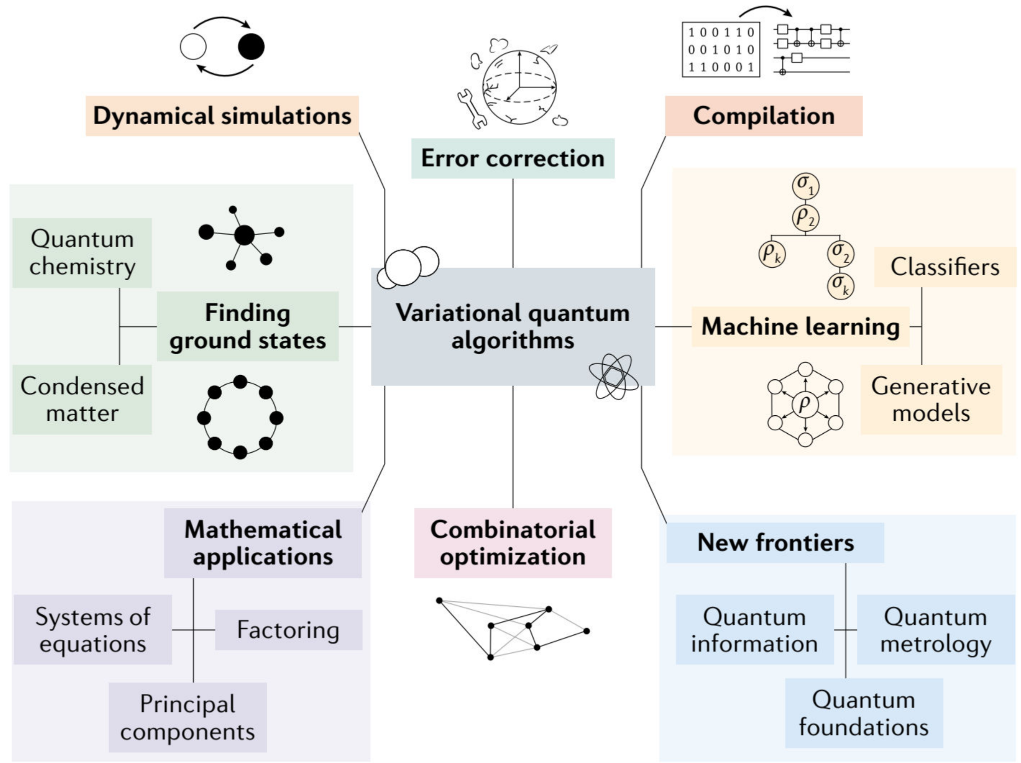
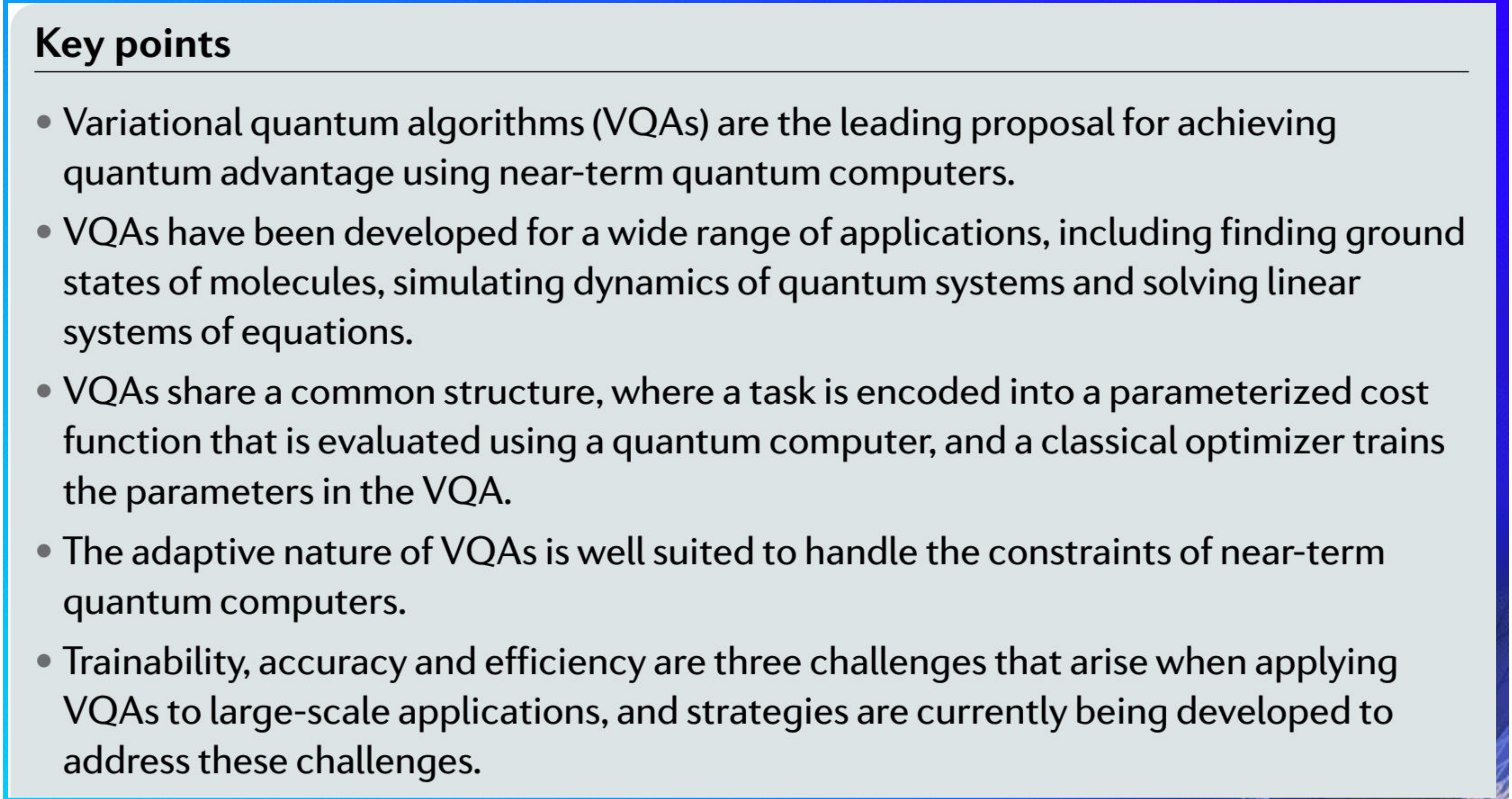


Fig. 1 | **Applications of variational quantum algorithms.** Many applications have been envisaged for variational quantum algorithms. Here we show some of the key applications that are discussed in this Review.

中国科学技术大学 陈凯

Variational quantum algorithms, M. Cerezo, Andrew Arrasmith, Ryan Babbush, Simon C. Benjamin, Suguru Endo, Keisuke Fujii, Jarrod R. McClean, Kosuke Mitarai, Xiao Yuan, Lukasz Cincio & Patrick J. Coles, *Nature Reviews Physics 3, 625–644 (2021)*

Variational quantum algorithms



Key points

- Variational quantum algorithms (VQAs) are the leading proposal for achieving quantum advantage using near-term quantum computers.
- VQAs have been developed for a wide range of applications, including finding ground states of molecules, simulating dynamics of quantum systems and solving linear systems of equations.
- VQAs share a common structure, where a task is encoded into a parameterized cost function that is evaluated using a quantum computer, and a classical optimizer trains the parameters in the VQA.
- The adaptive nature of VQAs is well suited to handle the constraints of near-term quantum computers.
- Trainability, accuracy and efficiency are three challenges that arise when applying VQAs to large-scale applications, and strategies are currently being developed to address these challenges.

Variational quantum algorithms, M. Cerezo, Andrew Arrasmith, Ryan Babbush, Simon C. Benjamin, Suguru Endo, Keisuke Fujii, Jarrod R. McClean, Kosuke Mitarai, Xiao Yuan, Lukasz Cincio & Patrick J. Coles, *Nature Reviews Physics 3, 625–644 (2021)*

Measurement in quantum circuits

Principle of deferred measurement: Measurements can always be moved from an intermediate stage of a quantum circuit to the end of the circuit; if the measurement results are used at any stage of the circuit then the classically controlled operations can be replaced by conditional quantum operations.

Principle of implicit measurement: Without loss of generality, any unterminated quantum wires (qubits which are not measured) at the end of a quantum circuit may be assumed to be measured.

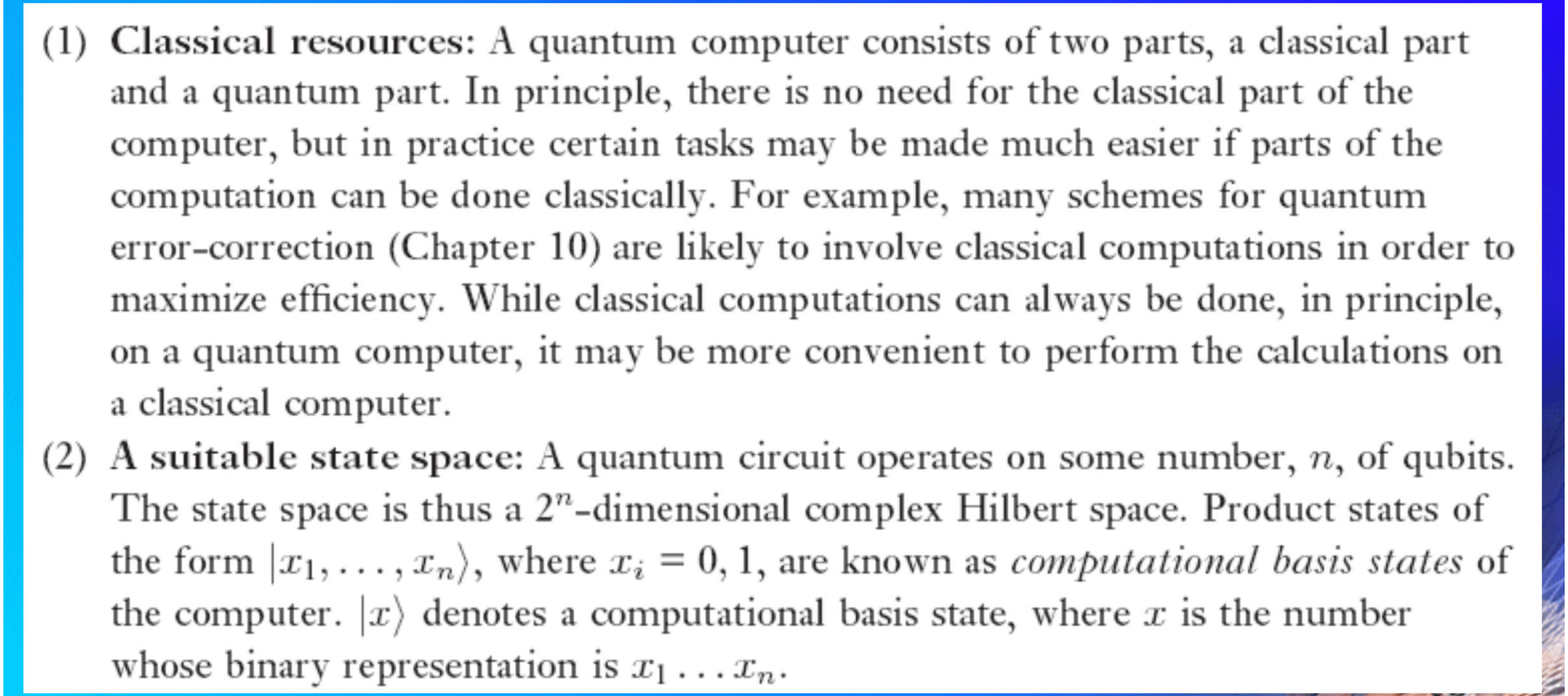
Measurement in quantum circuits

- Measurement is generally considered to be an irreversible operation, destroying quantum information and replacing it with classical information.

- In certain carefully designed cases, however, this need not be true.

- In order for a measurement to be reversible, it must reveal no information about the quantum state being measured!

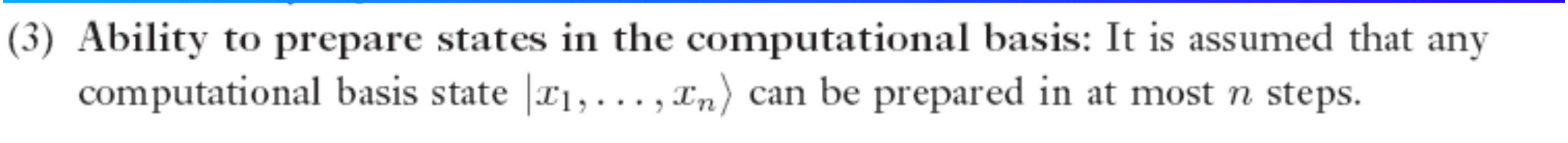
Summary of the quantum circuit model of computation



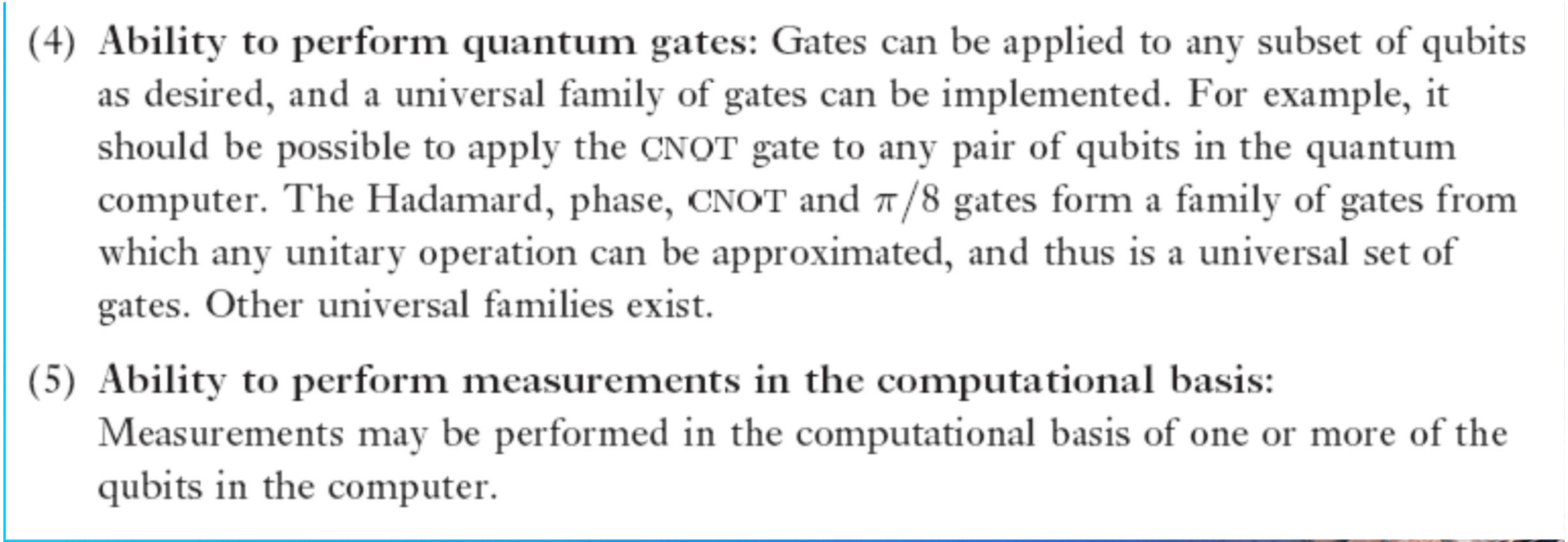
(1) **Classical resources:** A quantum computer consists of two parts, a classical part and a quantum part. In principle, there is no need for the classical part of the computer, but in practice certain tasks may be made much easier if parts of the computation can be done classically. For example, many schemes for quantum error-correction (Chapter 10) are likely to involve classical computations in order to maximize efficiency. While classical computations can always be done, in principle, on a quantum computer, it may be more convenient to perform the calculations on a classical computer.

(2) **A suitable state space:** A quantum circuit operates on some number, n, of qubits. The state space is thus a 2^n-dimensional complex Hilbert space. Product states of the form $|x_1, \ldots, x_n\rangle$, where $x_i = 0, 1$, are known as *computational basis states* of the computer. $|x\rangle$ denotes a computational basis state, where x is the number whose binary representation is $x_1 \ldots x_n$.

Summary of the quantum circuit model of computation



(3) **Ability to prepare states in the computational basis:** It is assumed that any computational basis state $|x_1, \dots, x_n\rangle$ can be prepared in at most n steps.



(4) **Ability to perform quantum gates:** Gates can be applied to any subset of qubits as desired, and a universal family of gates can be implemented. For example, it should be possible to apply the CNOT gate to any pair of qubits in the quantum computer. The Hadamard, phase, CNOT and $\pi/8$ gates form a family of gates from which any unitary operation can be approximated, and thus is a universal set of gates. Other universal families exist.

(5) **Ability to perform measurements in the computational basis:** Measurements may be performed in the computational basis of one or more of the qubits in the computer.

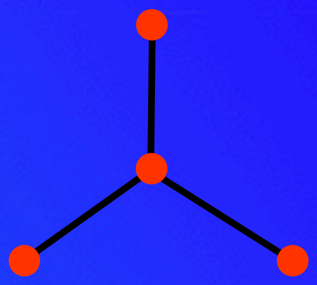
第六章 量子计算

1. 经典计算机发展
2. 量子计算机简介
3. 量子计算实现准则
4. 量子计算的物理实现、商业化进程
5. 量子比特表示、量子线路
6. 量子协议的线路实现
7. 典型量子算法
8. **单向量子计算**
9. 量子算法总结

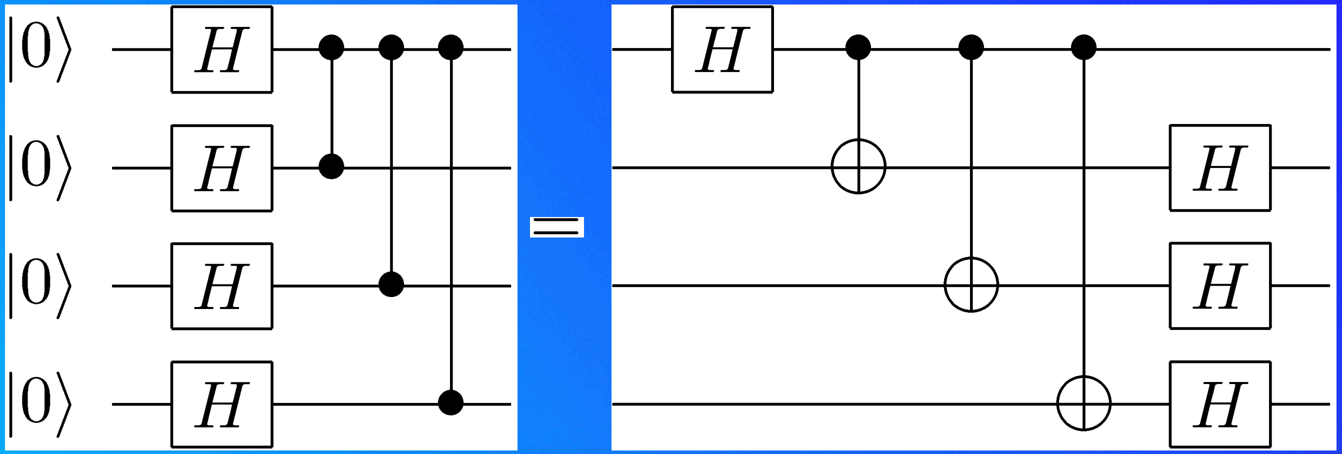
One way quantum computing

Graph states

4-qubit GHZ graph state



$ZIII$
$IZII$
$IIZI$
$IIIZ$



$XZZZ$
$ZXII$
$ZIXI$
$ZIIX$

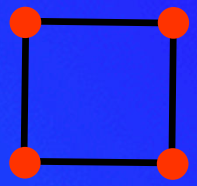
$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\bar{0}\bar{0}\bar{0}\rangle + |1\bar{1}\bar{1}\bar{1}\rangle)$$

From Caves

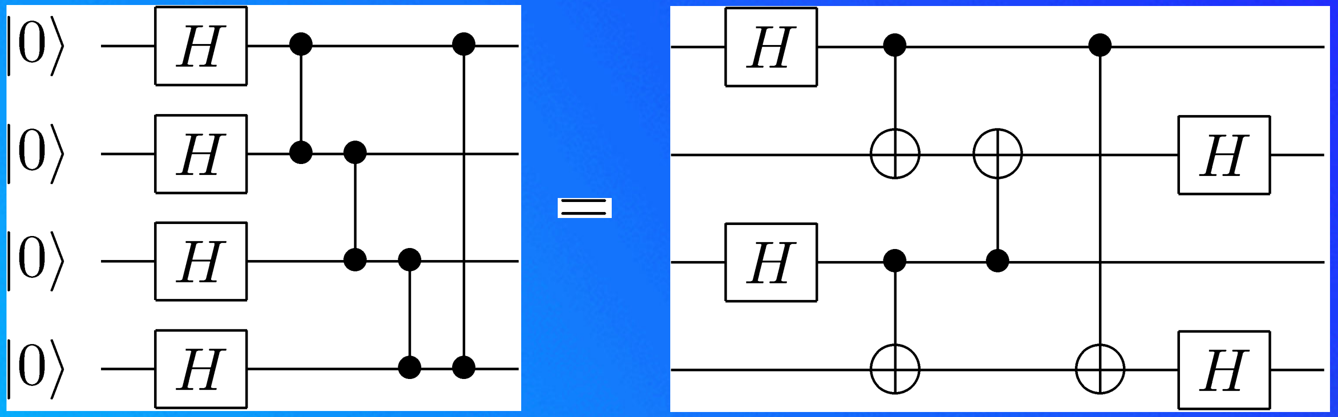
One way quantum computing

Graph states

2 x 2 cluster state



$ZIII$
$IZII$
$IIZI$
$IIIZ$



$XZIZ$
$ZXZI$
$IZXZ$
$ZIZX$

$$|\psi\rangle = \frac{1}{2}\left(|0\bar{0}0\bar{0}\rangle + |1\bar{1}0\bar{1}\rangle + |0\bar{1}1\bar{1}\rangle + |1\bar{0}1\bar{0}\rangle\right)$$

From Caves

One way quantum computing using cluster- and graph states

A cluster state is a collection of qubits that are entangled via nearest-neighbour CZ gates (rectangular lattice).

Horizontal links determine the information flow, while the vertical links furnish the two-qubit gates.

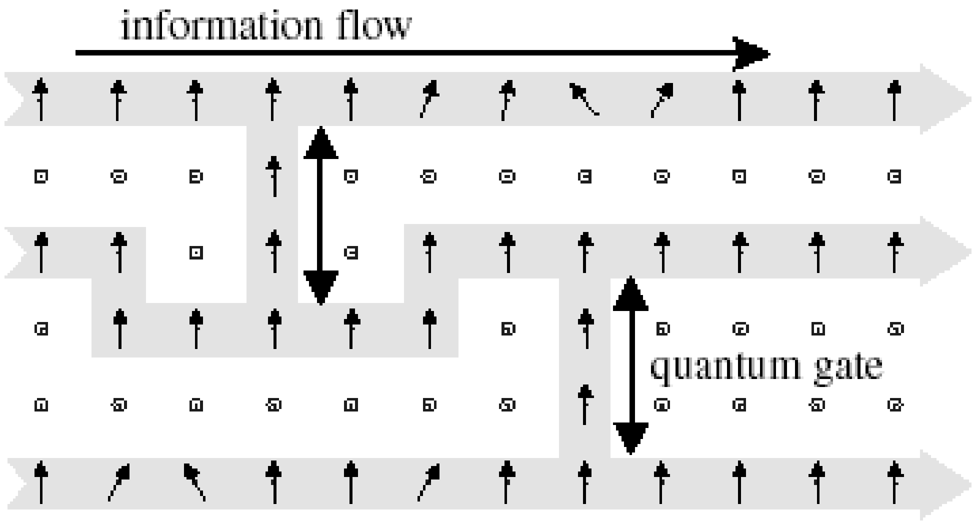
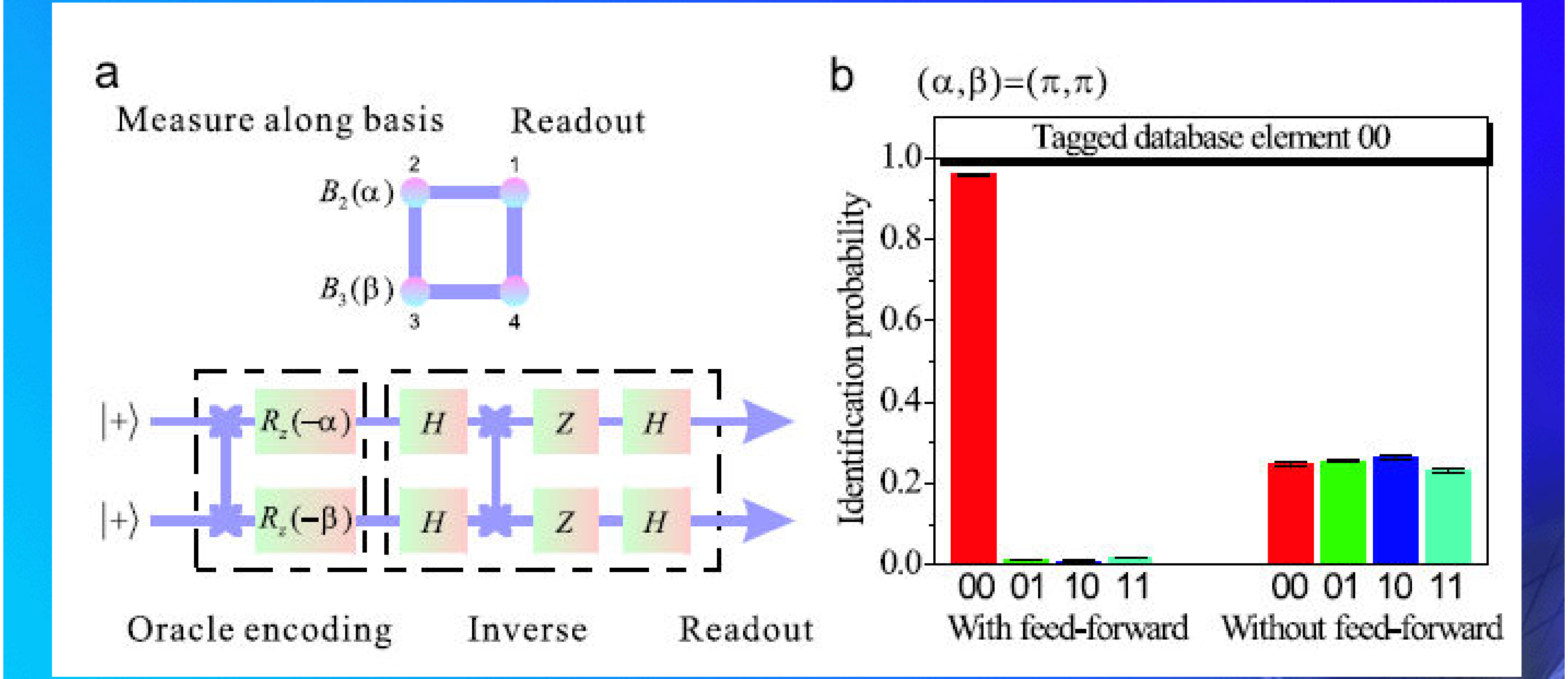


FIG. 1. Quantum computation by measuring two-state particles on a lattice. Before the measurements the qubits are in the cluster state $|\Phi\rangle_C$ of (1). Circles ⊙ symbolize measurements of σ_z, vertical arrows are measurements of σ_x, while tilted arrows refer to measurements in the x-y plane.

Source: Raussendorf & Briegel PRL **86**, 5188 (2001)

One way quantum computing



Kai Chen *et al.*, Experimental Realization of One-Way Quantum Computing with Two-Photon Four-Qubit Cluster States. Phys. Rev. Lett., 99, 120503 (2007).

中国科学技术大学 陈凯

One way quantum computing

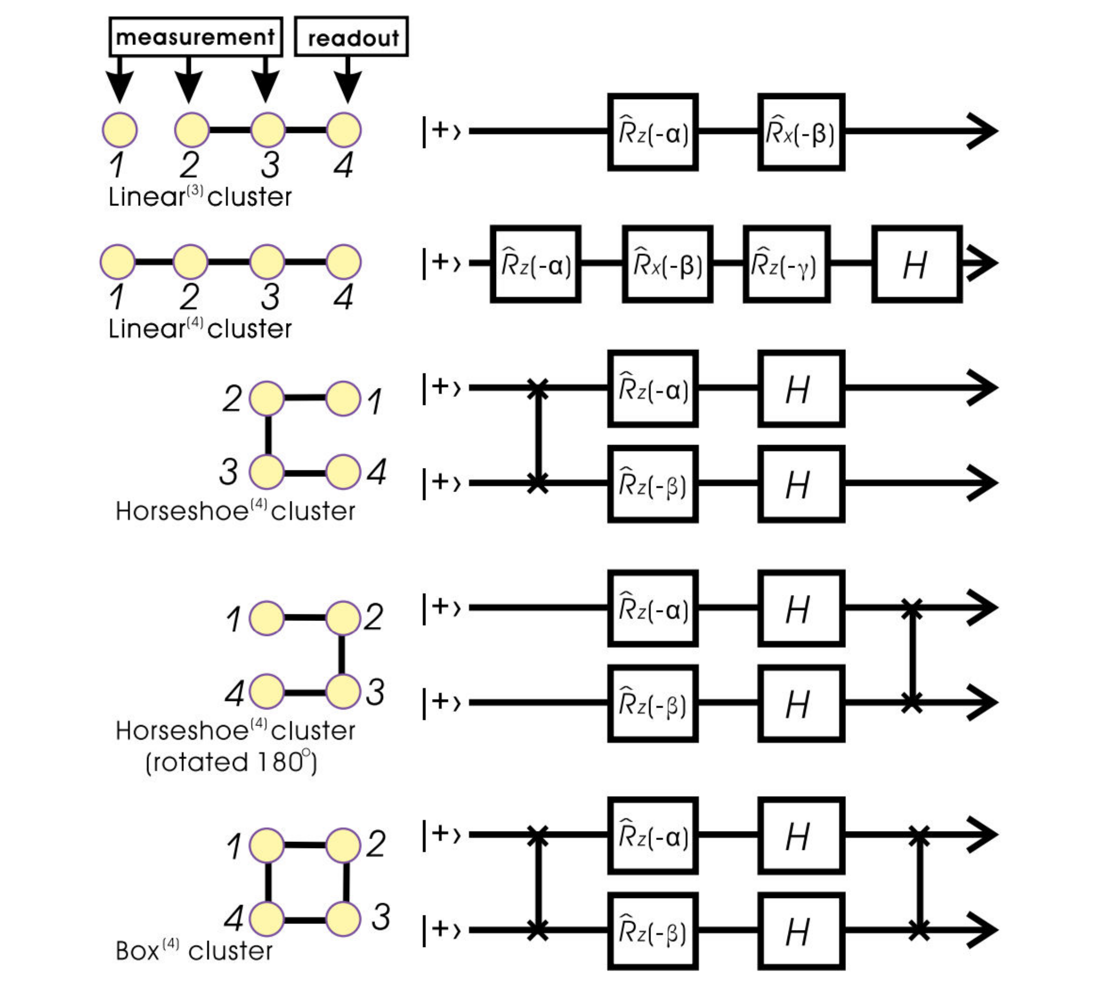


FIG. 37 (color online). Few-qubit cluster states and the quantum circuits they implement. For each three-qubit and four-qubit cluster, its quantum state ($|\Phi_{\text{lin3}}\rangle$, $|\Phi_{\text{lin4}}\rangle$, $|\Phi_{\sqsubset 4}\rangle$, $|\Phi_{\sqsupset 4}\rangle$, or $|\Phi_{\square 4}\rangle$) and the computation carried out in the one-way quantum computer model is shown. Adapted from Walther, Resch, Rudolph *et al.*, 2005.

Experimental one-way quantum computing, P. Walther, K. J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer & A. Zeilinger *Nature 434, 169–176 (2005)*

Jian-Wei Pan *et al.*, Multiphoton entanglement and interferometry *Rev. Mod. Phys.* 84, 777-838 (2012).

第六章 量子计算

1. 经典计算机发展
2. 量子计算机简介
3. 量子计算实现准则
4. 量子计算的物理实现、商业化进程
5. 量子比特表示、量子线路
6. 量子协议的线路实现
7. 典型量子算法
8. 单向量子计算
9. **量子算法总结**

Quantum algorithms: an overview

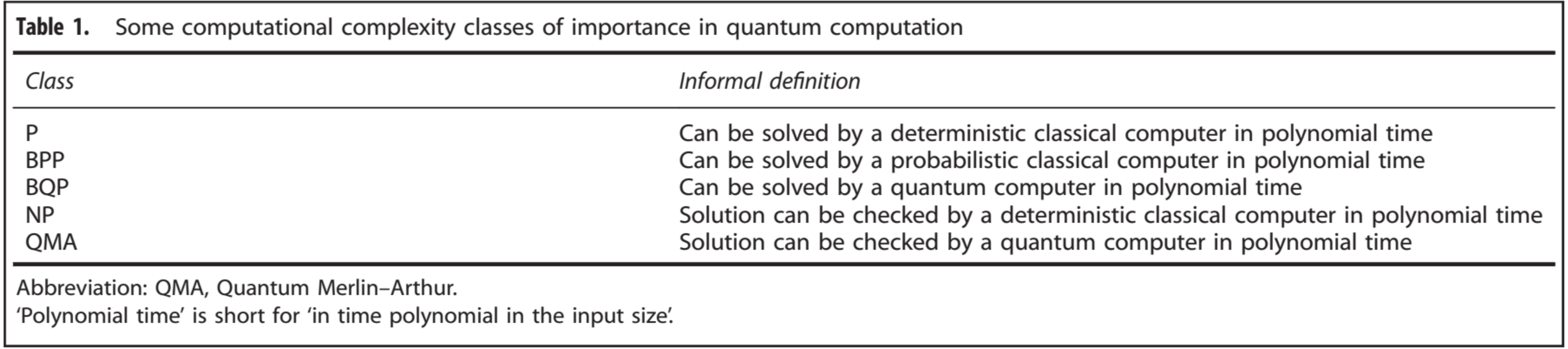


Table 1. Some computational complexity classes of importance in quantum computation

Class	*Informal definition*
P	Can be solved by a deterministic classical computer in polynomial time
BPP	Can be solved by a probabilistic classical computer in polynomial time
BQP	Can be solved by a quantum computer in polynomial time
NP	Solution can be checked by a deterministic classical computer in polynomial time
QMA	Solution can be checked by a quantum computer in polynomial time

Abbreviation: QMA, Quantum Merlin–Arthur.
'Polynomial time' is short for 'in time polynomial in the input size'.

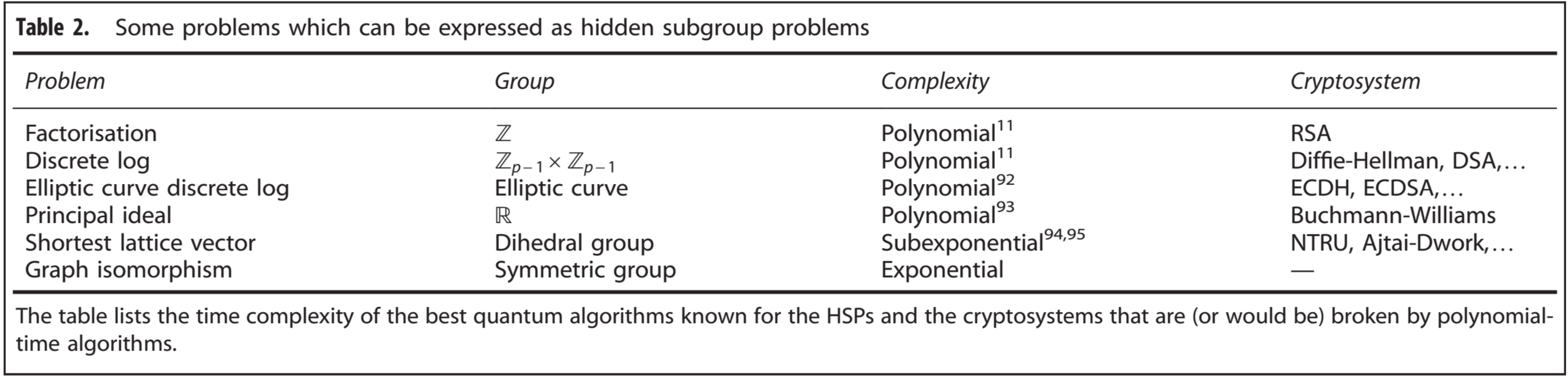


Table 2. Some problems which can be expressed as hidden subgroup problems

Problem	*Group*	*Complexity*	*Cryptosystem*
Factorisation	$\mathbb{Z}$	Polynomial[11]	RSA
Discrete log	$\mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}$	Polynomial[11]	Diffie-Hellman, DSA,…
Elliptic curve discrete log	Elliptic curve	Polynomial[92]	ECDH, ECDSA,…
Principal ideal	$\mathbb{R}$	Polynomial[93]	Buchmann-Williams
Shortest lattice vector	Dihedral group	Subexponential[94,95]	NTRU, Ajtai-Dwork,…
Graph isomorphism	Symmetric group	Exponential	—

The table lists the time complexity of the best quantum algorithms known for the HSPs and the cryptosystems that are (or would be) broken by polynomial-time algorithms.

Ashley Montanaro, *npj Quantum Information (2016) 2, 15023*

Quantum algorithms: an overview

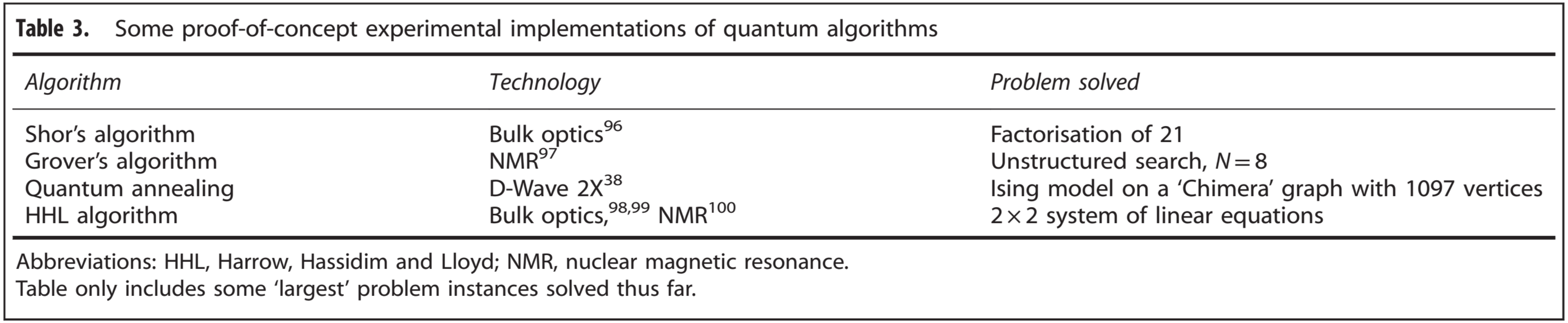


Table 3. Some proof-of-concept experimental implementations of quantum algorithms

Algorithm	*Technology*	*Problem solved*
Shor's algorithm	Bulk optics[96]	Factorisation of 21
Grover's algorithm	NMR[97]	Unstructured search, $N=8$
Quantum annealing	D-Wave 2X[38]	Ising model on a 'Chimera' graph with 1097 vertices
HHL algorithm	Bulk optics,[98,99] NMR[100]	2×2 system of linear equations

Abbreviations: HHL, Harrow, Hassidim and Lloyd; NMR, nuclear magnetic resonance.
Table only includes some 'largest' problem instances solved thus far.

Measuring quantum speedup

What does it mean to say that a quantum computer solves a problem more quickly than a classical computer? As is typical in computational complexity theory, we will generally consider asymptotic scaling of complexity measures such as runtime or space usage with problem size, rather than individual problems of a fixed size. In both the classical and quantum settings, we measure runtime by the number of elementary operations used by an algorithm. In the case of quantum computation, this can be measured using the quantum circuit model, where a quantum circuit is a sequence of elementary quantum operations called quantum gates, each applied to a small number of qubits (quantum bits). To compare the performance of algorithms, we use computer science style notation O(f(n)), which should be interpreted as 'asymptotically upper-bounded by f(n)'.

Ashley Montanaro, *npj Quantum Information (2016) 2, 15023*

Quantum Algorithm Zoo

Algebraic and Number Theoretic Algorithms

Oracular Algorithms

Approximation and Simulation Algorithms

Author:
Stephen Jordan
Microsoft Quantum

https://quantumalgorithmzoo.org/

Quantum Algorithm Zoo 中文版
https://www.qtumist.com/quantum-algorithm-zoo

参考书目和文献

- Quantum computation and quantum information by M.A. Nielsen and I.L. Chuang

  Chapters 1,4,5,6

谢谢