Quantum Information and Computation for Dummies

Peter Samuelsson, Mathematical Physics

Outline

1. What is quantum information?
2. What is a quantum computer?
3. Why build a quantum computer?
4. How to build a quantum computer?

Outline

1 What is quantum information?

2 What is a quantum computer?

3 Why build a quantum computer?

4 How to build a quantum computer?

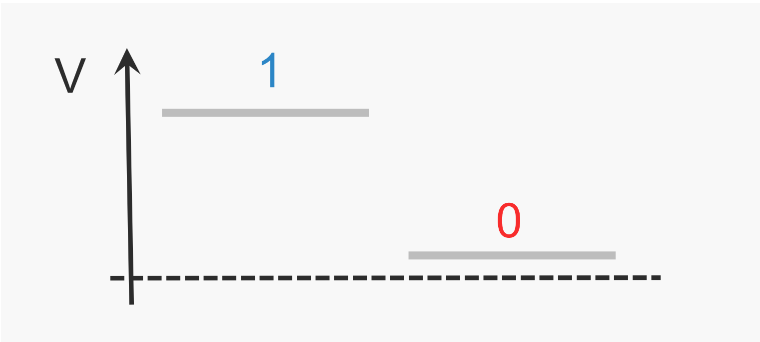
Definition

"Quantum information is physical information that is held in the state of a quantum system" - *wikipedia*

Basic unit of information

0 1

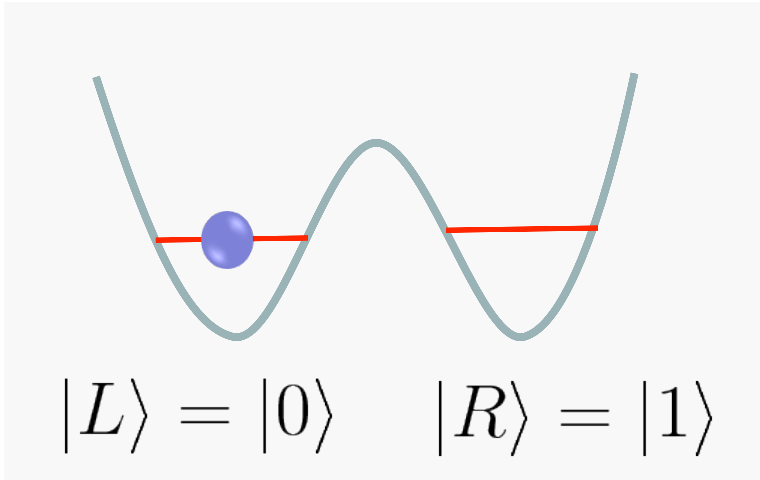
Classical bit



Two-state classical system

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

Quantum bit - *qubit*

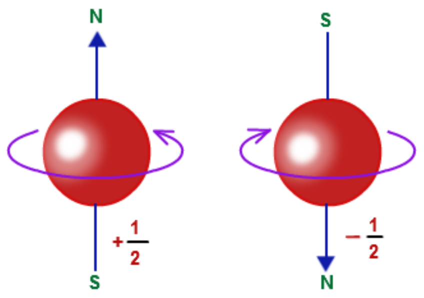


Two-state quantum system

More qubit "hardware" examples

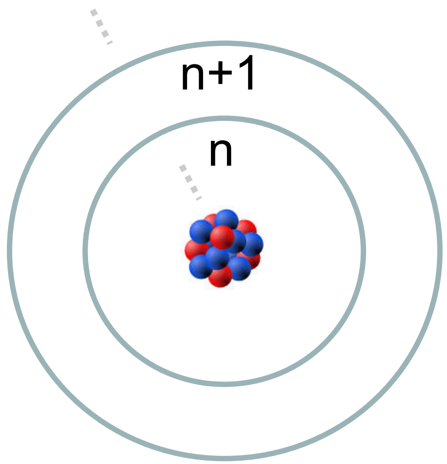
Electrons

spin



$$|\uparrow\rangle = |1\rangle \qquad |\downarrow\rangle = |0\rangle$$

atomic level

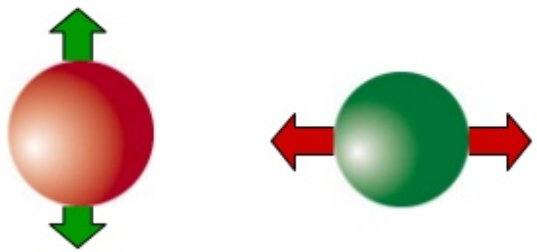


$$|n+1\rangle = |1\rangle$$

$$|n\rangle = |0\rangle$$

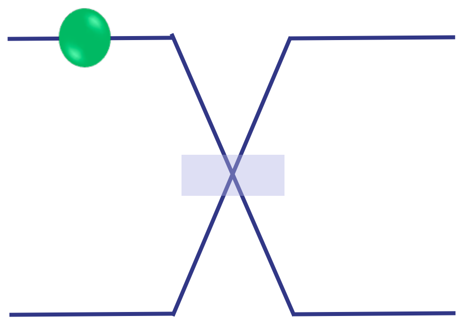
Photons

polarization



$$|V\rangle = |1\rangle \qquad |H\rangle = |0\rangle$$

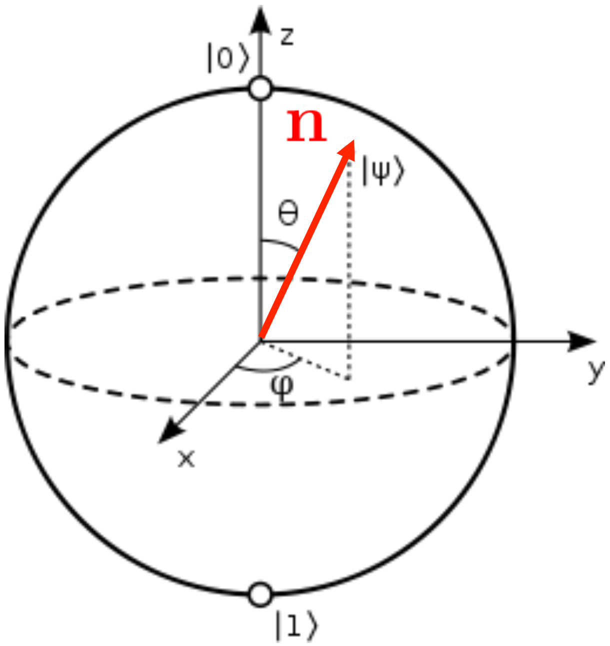
position



$$|U\rangle = |1\rangle$$

$$|D\rangle = |0\rangle$$

Bloch sphere representation



State parametrization

$$|\Psi\rangle = \underbrace{\cos(\theta/2)}_{\alpha}|0\rangle + \underbrace{e^{i\varphi}\sin(\theta/2)}_{\beta}|1\rangle$$

Vector on the unit sphere

$$\mathbf{n} = [\sin\theta\cos\varphi, \sin\theta\sin\varphi, \cos\theta]$$

θ, φ - *”analog information”*

More qubits

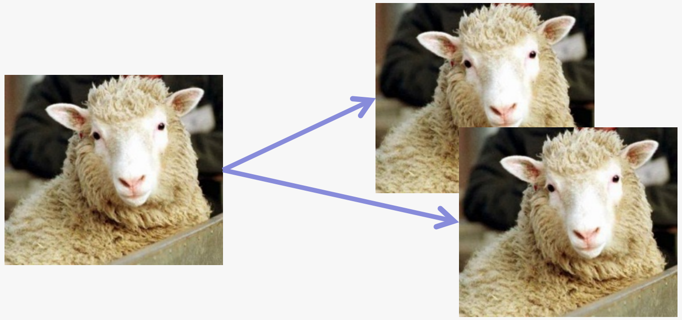
2 $$|\Psi\rangle = c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle$$

- classical 00,01,10,11

N $$|\Psi\rangle = \sum_{i_1 i_2 \ldots . i_N} c_{i_1 i_2 \ldots i_N} |i_1 i_2 .. i_N\rangle$$

Quantum vs classical

Copy information



No cloning theorem

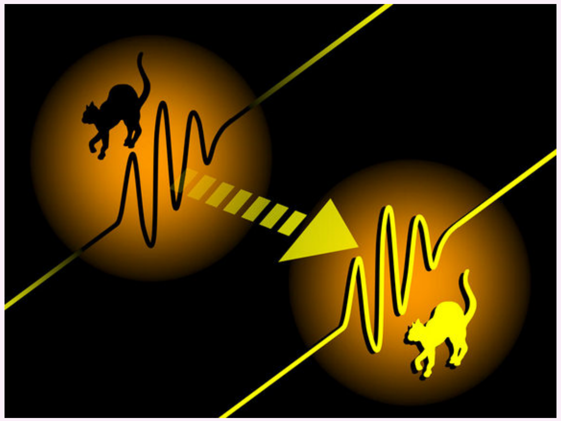
$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

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

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

Teleportation

Quantum teleportation



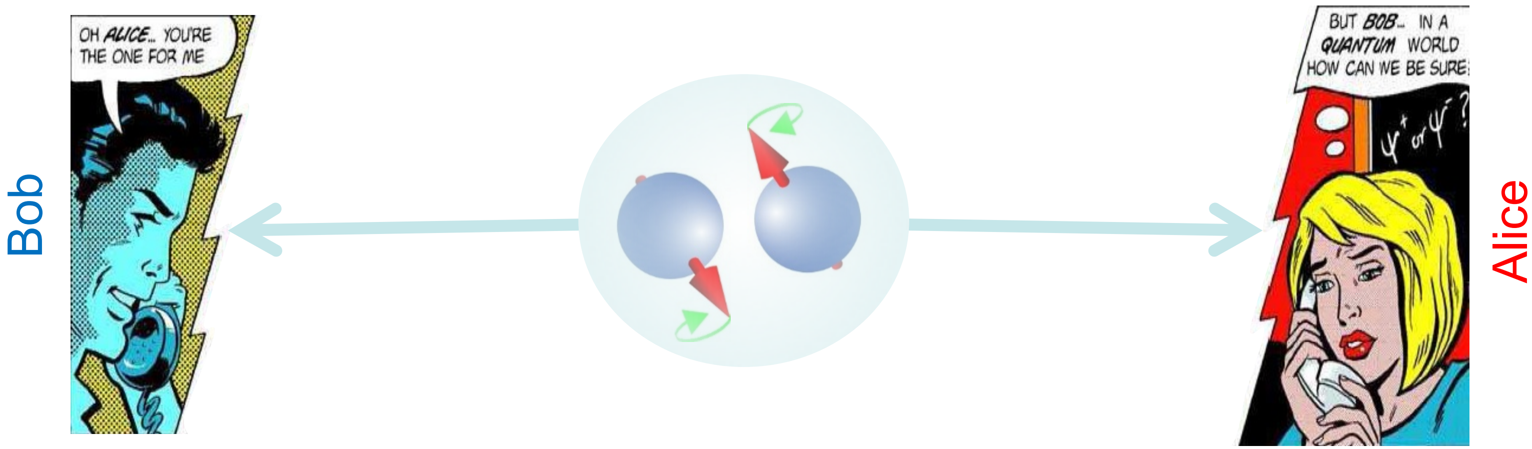
Entanglement

Qubit A and B

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left[|0_A 0_B\rangle + |1_A 1_B\rangle\right]$$

- Resource for quantum information processing
- Hotly debated non-local properties

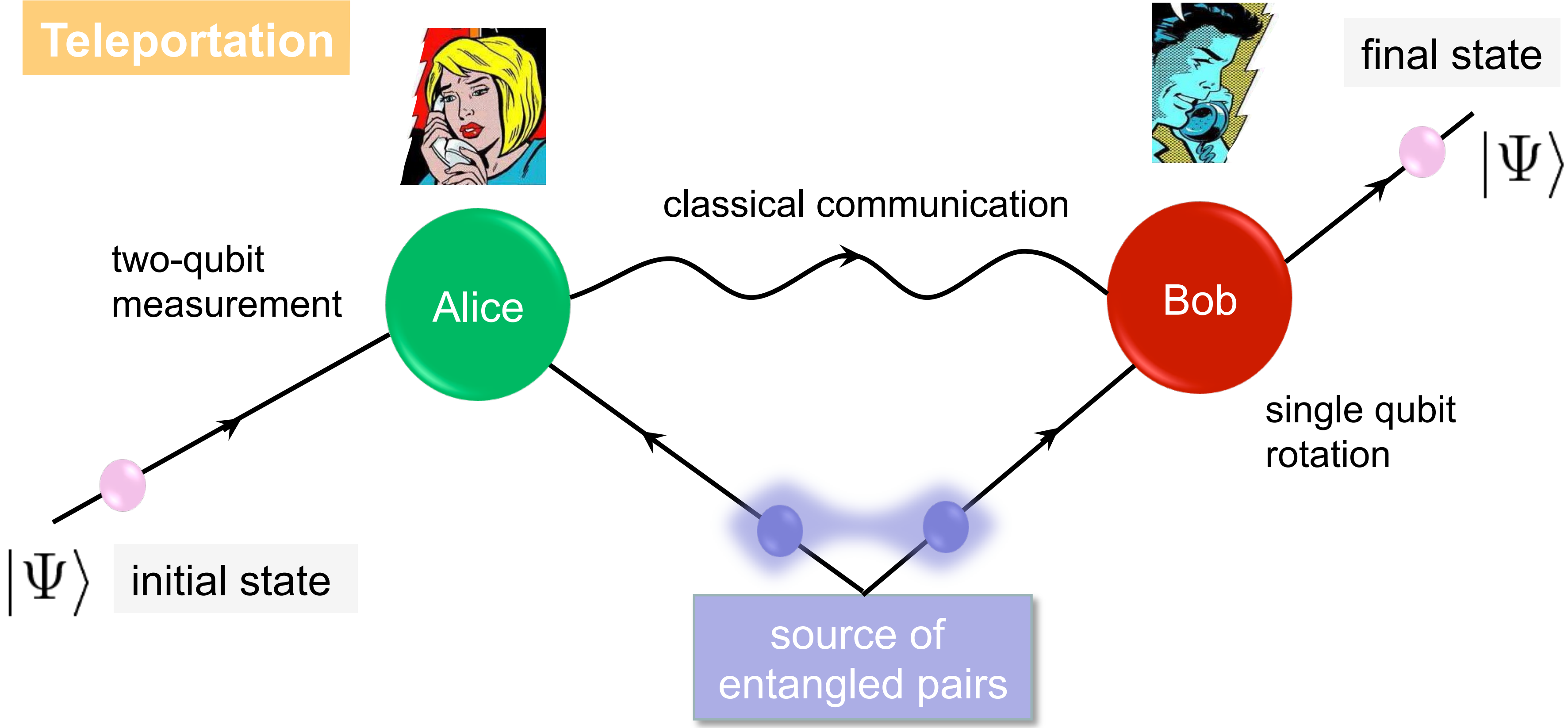
$$|\Psi\rangle \neq |\Psi_A\rangle \otimes |\Psi_B\rangle$$



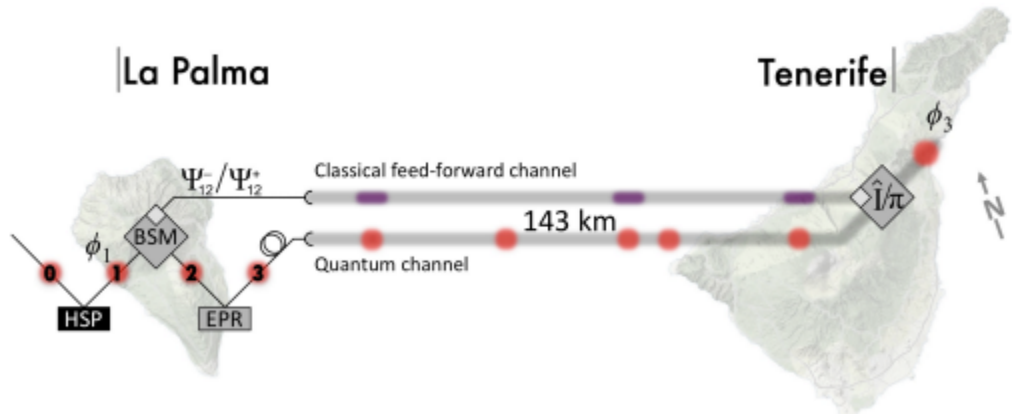
Alice measures $|0_A\rangle$ / $|1_A\rangle$ → Bob must measure $|0_B\rangle$ / $|1_B\rangle$

No information is transferred

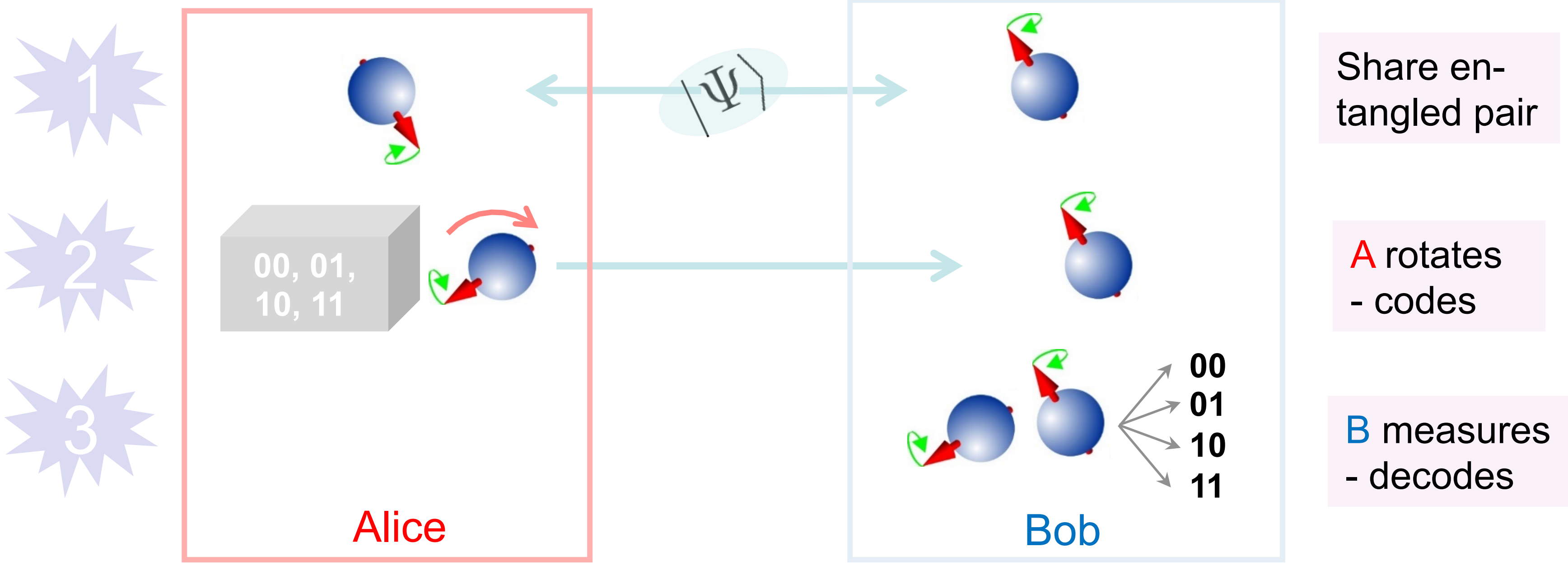
Teleportation



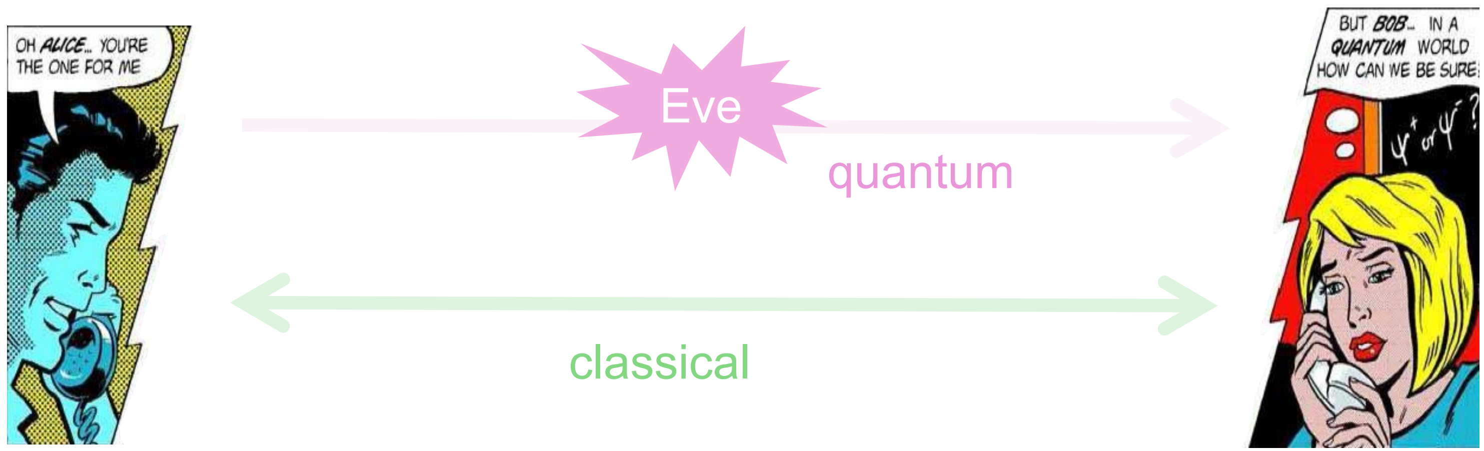
Photon experiment



Superdense Coding - sending 2 classical bits in 1 qubit



Cryptography - quantum key distribution



Outline

1 What is quantum information?

2 What is a quantum computer?

3 Why build a quantum computer?

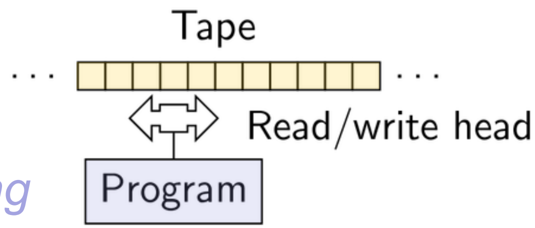
4 How to build a quantum computer?

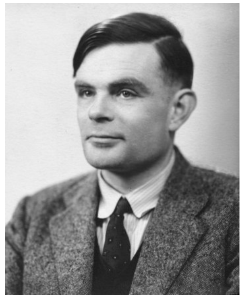
Definition

"A quantum computer make use of quantum-mechanical phenomena, such as superposition and entanglement, to perform operations on data." - *wikipedia*

Fundamentals

1 Any algorithm can be implemented on a (classical) Turing machine – *Church, Turing*





2

A reversible Turing machine can perform the same operations as a standard Turing machine – *Bennett*

3 Any operation on a reversible Turing machine can be simulated quantum mechanically – *Benioff*

4

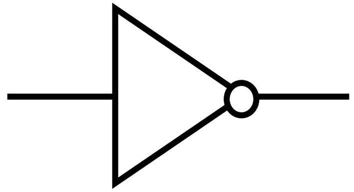
Quantum computers can be programmed to carry out the same operations as classical computers – *Deutsch*

One bit gates

★ Classical one-bit gate

NOT

a

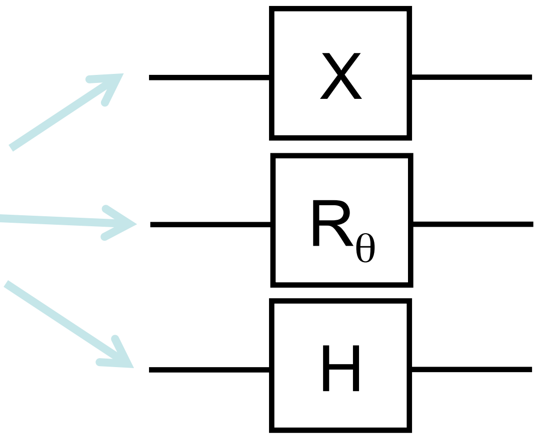


c = NOT a

a	c
0	1
1	0

★ Single qubit gates

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

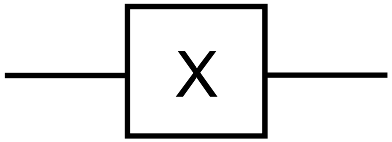


$$\beta|0\rangle + \alpha|1\rangle$$

$$\alpha|0\rangle + e^{i\theta}\beta|1\rangle$$

$$\frac{\alpha+\beta}{\sqrt{2}}|0\rangle + \frac{\alpha-\beta}{\sqrt{2}}|1\rangle$$

Quantum mechanics



gate

$$|1\rangle\langle 0| + |0\rangle\langle 1|$$

operator

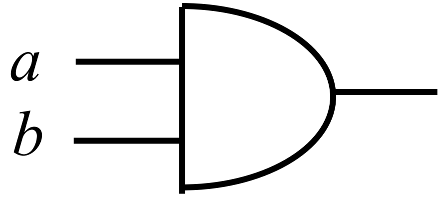
$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

unitary transformation

Two qubit gates

★ Classical two-bit gate

AND



$c = a$ AND b

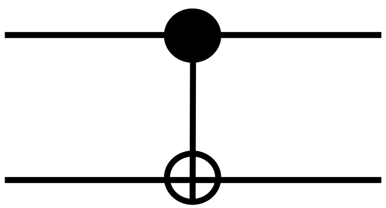
a	b	c
0	0	0
0	1	0
1	0	0
1	1	1

…. also AND, OR, XOR, NAND,

★ Two qubit gate

$|\Psi_A\rangle$

$|\Psi_B\rangle$



$|\Psi_A\rangle$

$|\Psi_A\rangle \oplus |\Psi_B\rangle$

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

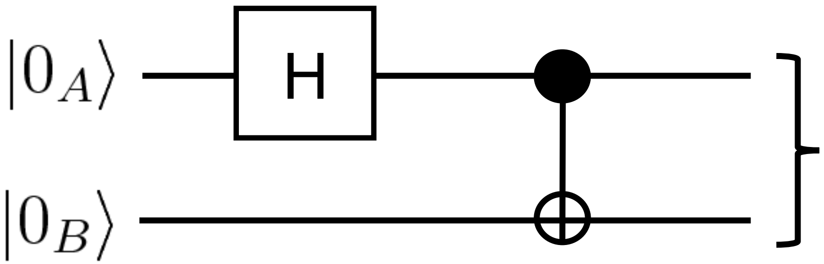
Controlled NOT

$$|0_A\rangle : \quad \begin{array}{l} |0_B\rangle \rightarrow |0_B\rangle \\ |1_B\rangle \rightarrow |1_B\rangle \end{array}$$

$$|1_A\rangle : \quad \begin{array}{l} |0_B\rangle \rightarrow |1_B\rangle \\ |1_B\rangle \rightarrow |0_B\rangle \end{array}$$

Circuits

Entangler

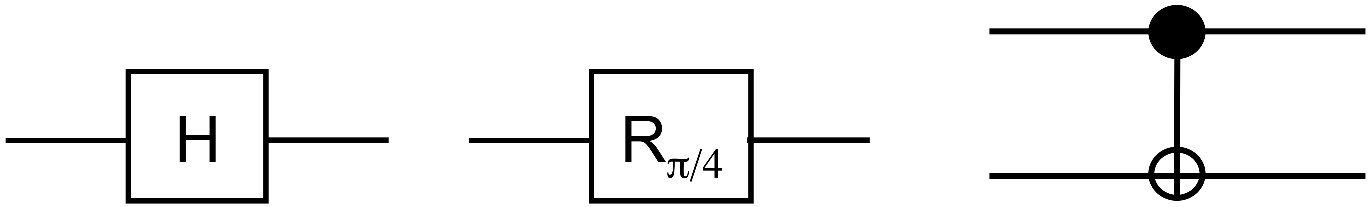


$$\frac{1}{\sqrt{2}}\left[|0_A 0_B\rangle + |1_A 1_B\rangle\right]$$

… and multi qubit circuits

Universal computation

With (for example)



single qubit gates

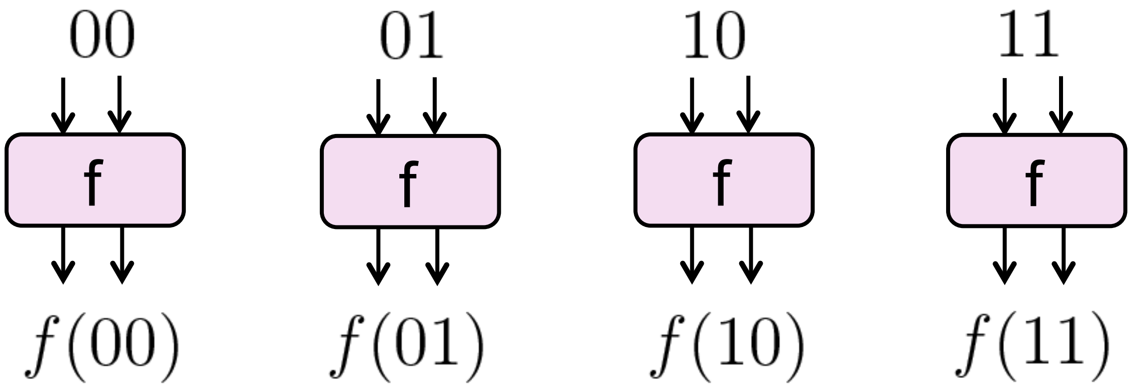
two qubit gate

any multi qubit circuit (*quantum computer*) can be constructed.

Quantum parallelism

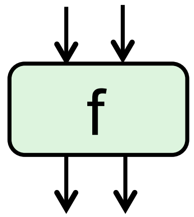
Superposition of computations

- Classical circuit



- Quantum circuit

$$\frac{1}{2}\left[|00\rangle + |01\rangle + |10\rangle + |11\rangle\right]$$



$$\frac{1}{2}\left[f(00)|00\rangle + f(01)|01\rangle + f(10)|10\rangle + f(11)|11\rangle\right]$$

All function evaluations in a single run

Outline

1 What is quantum information?

2 What is a quantum computer?

3 Why build a quantum computer?

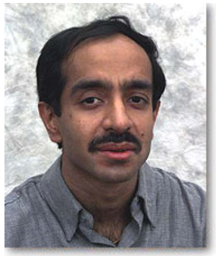
4 How to build a quantum computer?

Motivation

1

Computationally hard problems

Quantum computers can *solve certain problems* much faster than any classical computer



Grover

Shor

Feynman

2

Quantum simulations

Quantum computers can *simulate many-particle systems* much faster than any classical computer

3

Energy saving

Quantum computers are reversible and can consume much less energy than (standard) classical computers

Landauer

Shor's algorithm

Prime factorization problem: Given an integer N, find its prime factors

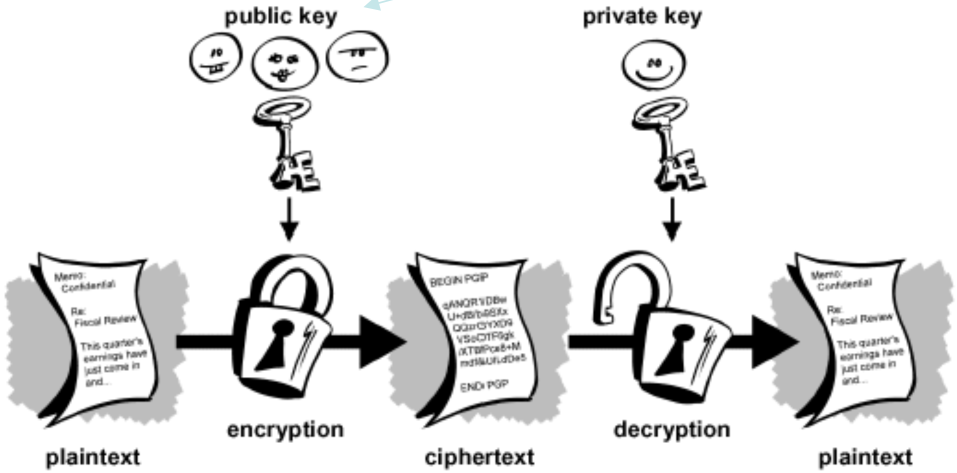
15 = 3 x 5   999999942014077477 = 3162277633 x 3162277669

$$\text{Time to solve: } \begin{cases} 2^{O[\ln(N)^{1/3}]} & \text{classical} \\ O[\ln(N)^2] & \text{quantum} \end{cases}$$

Exponential speed-up

Public key cryptography

Product of two unknown primes



email
transfers
identity
…

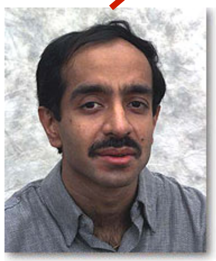
internet security

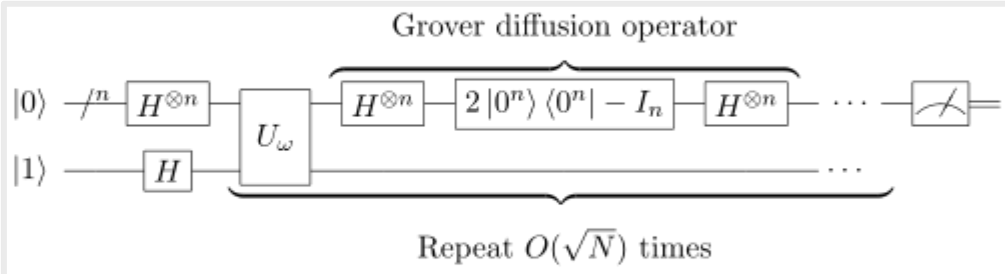
Grovers algorithm

Unsorted data base search: **Find a given element in a data base of size N**

Time to solve:

$$\begin{cases} O(N) & \text{classical} \\ O(N^{1/2}) & \text{quantum} \end{cases}$$





Quadratic speed-up

Quantum simulations

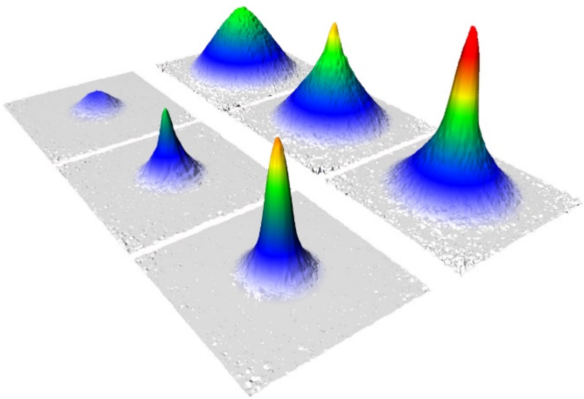
Feynmans observation

Classical computers require exponentially long time to simulate many-particle quantum systems

Quantum computers require polynomial time

Exponential speed-up

Many-body fermion system



Lloyd

Simulate

- Initial state preparation
- Time evolution
- Charge density
- Correlation functions
- ….

Bosonic systems, chemical reactions, …

Outline

1 What is quantum information?

2 What is a quantum computer?

3 Why build a quantum computer?

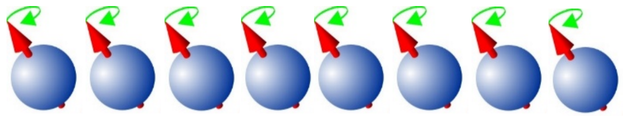
4 How to build a quantum computer?

Di Vincenzo criteria

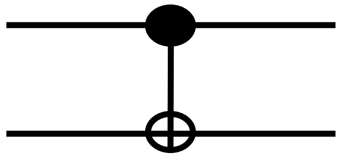
Requirement on physical system (hardware)

1. Scalable with well characterized qubits $|0\rangle \; |1\rangle$

2. Initial state preparation



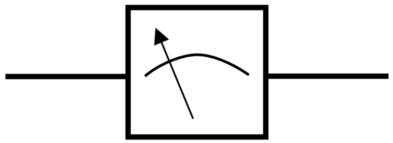
3. A universal set of quantum gates



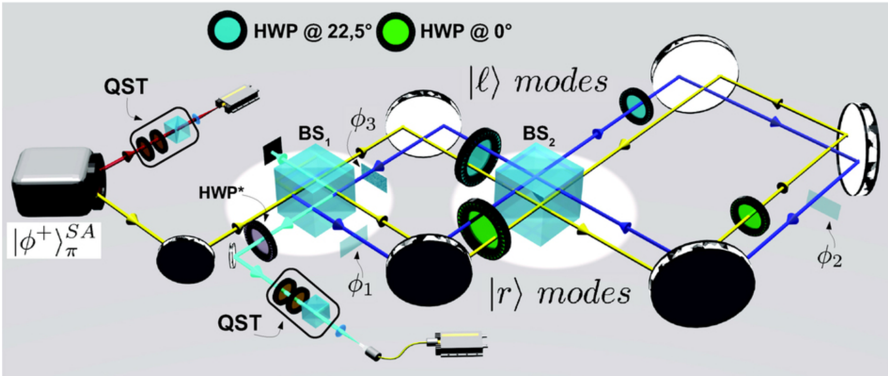
4. Long (relevant) decoherence times

Quantum error correction

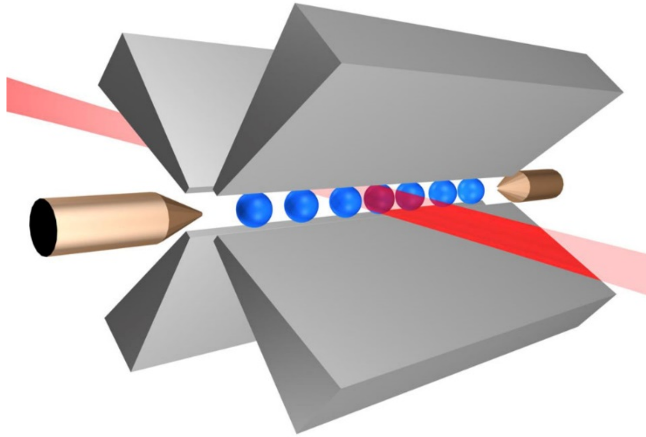
5. Reading out the result



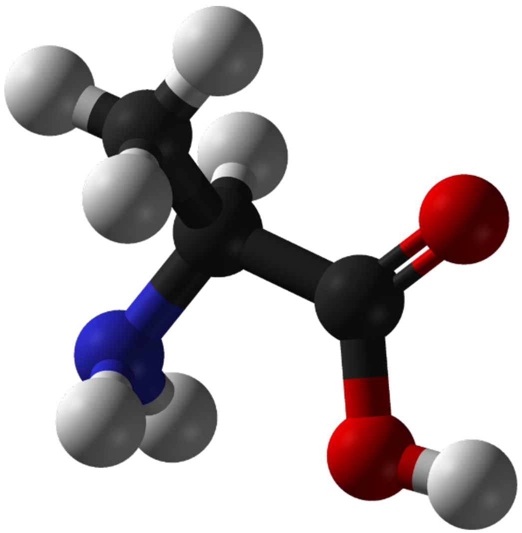
Linear quantum optics



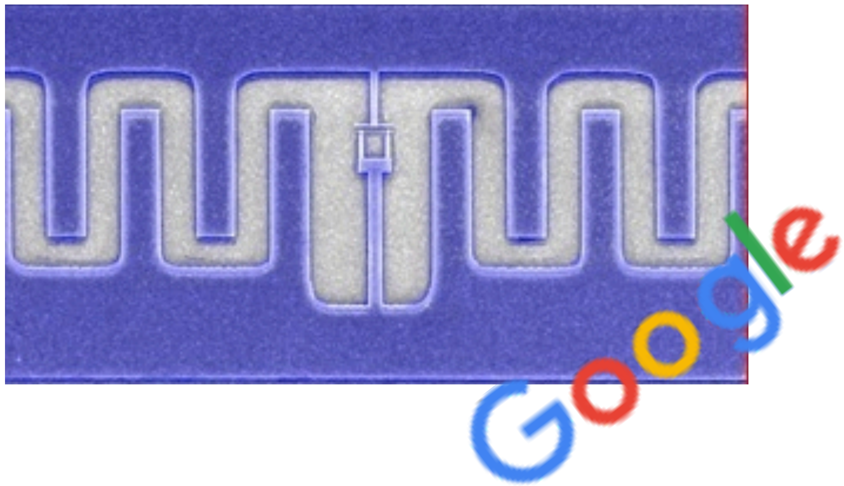
Trapped ions



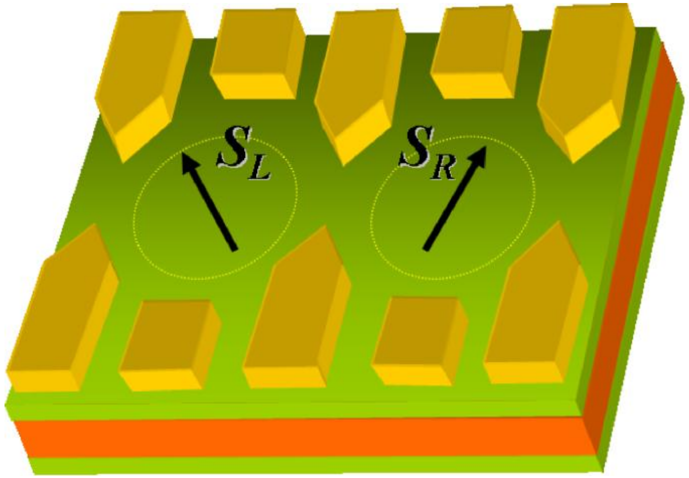
Nuclear magnetic resonance



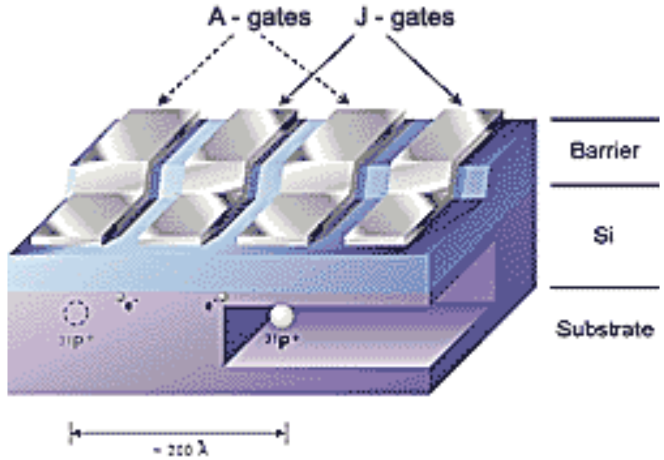
Superconducting circuits



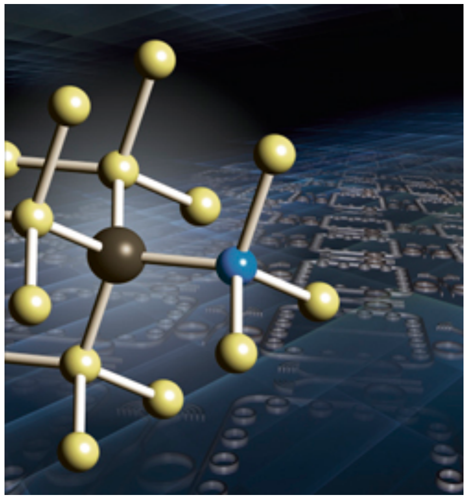
Electrons in solid state



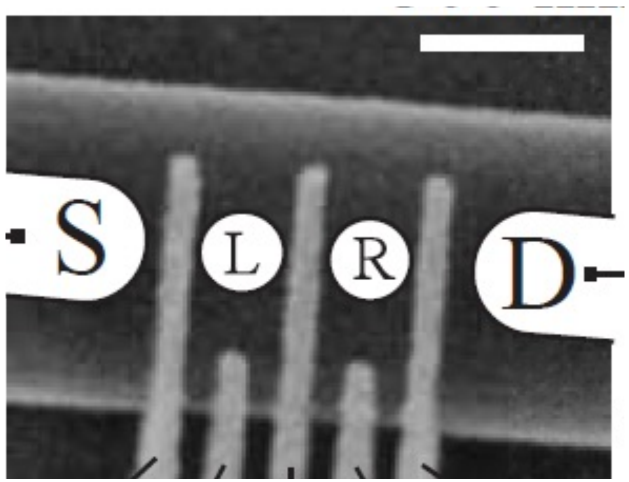
Spins in quantum dots



Dopants in silicon



Nitrogen vacancies in diamond



Charge states in quantum dots

Status and outlook

Achieved to date

- ✓ Controlling & coupling individual qubits
- ✓ Running algorithms with <10 qubits
- ✓ Error correction with <10 qubits
- ✓ Coherent transfer of individual qubits
- ✓ …

Needed to beat classical computers

Full quantum computer : 10^4 - 10^5 qubits

Limited tasks: 10^2 - 10^3 qubits

Still plenty of work to do….