Quantum Computing
---
an introduction for computing scientists

CPPM, 3 February 2020, Marseille

Bogdan Vulpescu

Laboratoire de Physique de Clermont

Service Informatique

At CERN

- CERN OpenLab, “Quantum Computing for High Energy Physics Workshop”
  5-6 November 2018, CERN
  https://indico.cern.ch/event/719844/
  D-Wave, Rigetti, IBM, Google, Intel, Microsoft, ProjectQ, Strangeworks, …

  “A contribution to the particle physics strategy update 2018-2020”
  https://indico.cern.ch/event/765096/contributions/3295802/attachments/1785308/2906350/QC-HEP-2020.pdf

Quantum Computing for HEP

CERN openlab — a public-private partnership between CERN and leading companies driving ICT innovation — organised a highly successful workshop on this topic at CERN in November 2018, attended by more than 400 representatives of the HEP community and of major research laboratories, experts in IQCT and the leading companies working at the development of IQCT solutions.

It is the common consensus of the signees of this document that, given the projected deficit of HEP computing and the potential promise of QICT, the HEP community should invest in the exploration of these technologies.

At IN2P3

- Working Group at IN2P3 (within GT09) on quantum information technology:
  6 September 2019, Michel-Ange, Paris (a report on the CERN workshop)
  https://indico.in2p3.fr/event/19662/

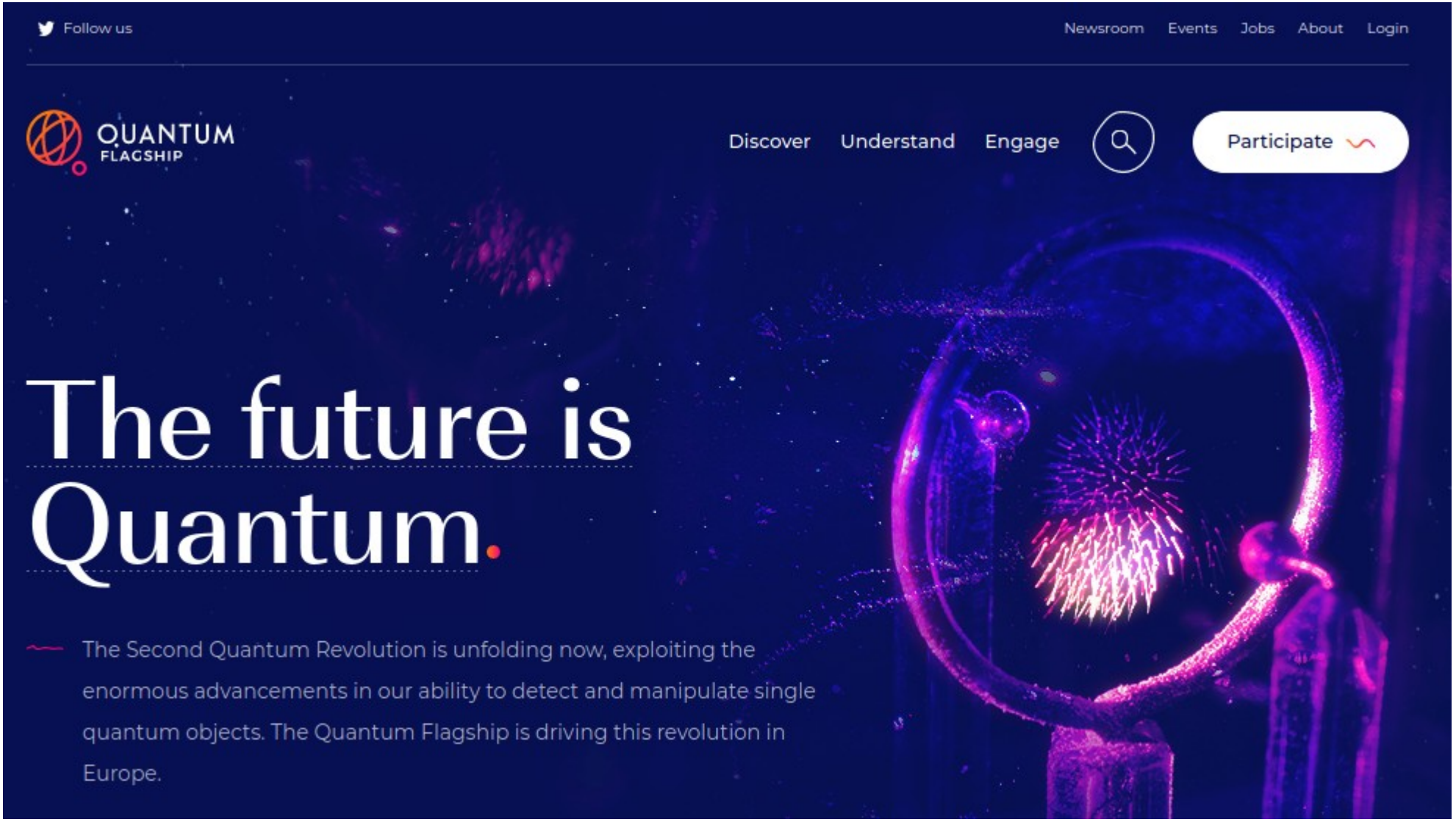
- “Prospectives CNRS/IN2P3 Calcul Algorithmes et Données”
  17-18 October 2019, Clermont-Ferrand
  https://indico.in2p3.fr/event/19733/
  https://webcast.in2p3.fr/container/journees-prospectives-calcul-algorithmes-et-donnees

- “Journées thématiques IN2P3 – Quantum computing: state of the art and applications”
  2-3 December 2019, IPNO, Orsay
  https://indico.in2p3.fr/event/19917/
  CEA, Atos, ...

And at CNRS

- “Les débuts de l’ordinateur quantique: principes, promesses, réalisations et défis”, by Pascale Senellart-Mardon (C2N, Center for Nanoscience and Nanotechnology)
  14 January 2020, IJCLab, Orsay
  https://indico.lal.in2p3.fr/event/5907

In Europe: Quantum Flagship https://qt.eu



Summary of the talk

- Classical bits and classical computing
- Quantum mechanics and quantum bits (qubits)
- Manipulating qubit states, unitary errors
- Quantum gates and circuits
- Quantum teleportation
- Quantum Fourier Transformation
- Quantum cryptography
- IBM Q experience

- Classical bits and classical computing
- Quantum mechanics and quantum bits (qubits)
- Manipulating qubit states, unitary errors
- Quantum gates and circuits
- Quantum teleportation
- Quantum Fourier Transformation
- Quantum cryptography
- IBM Q experience

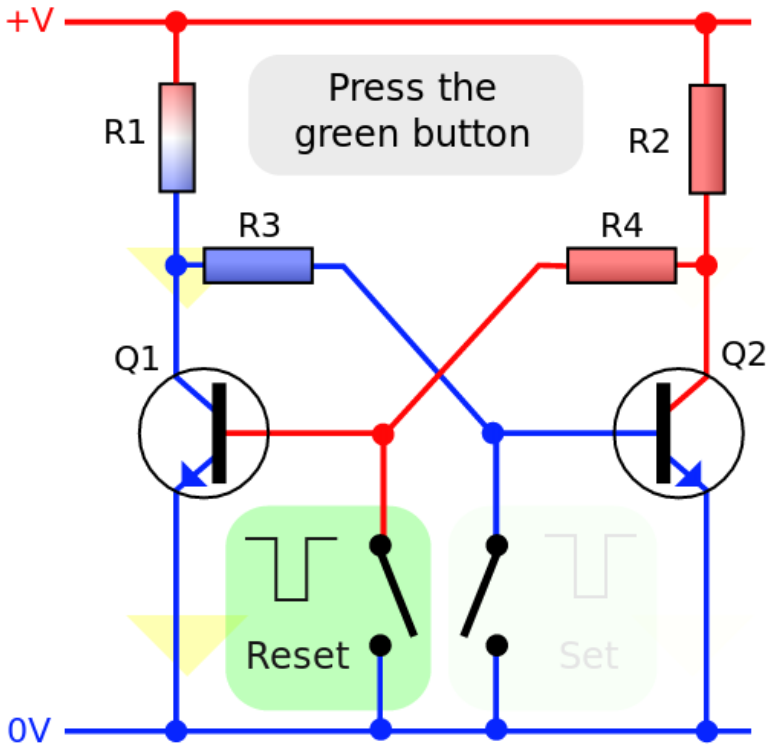
Semiconductors

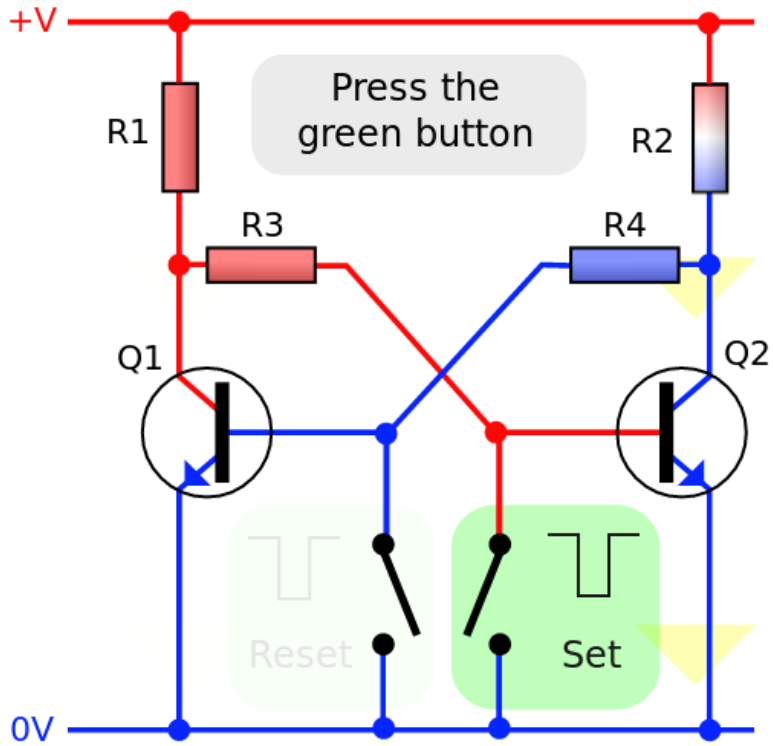
their conductivity can be controlled by doping and gating with electric fields

a silicon crystal

The flip-flop circuit (a bi-stable circuit)

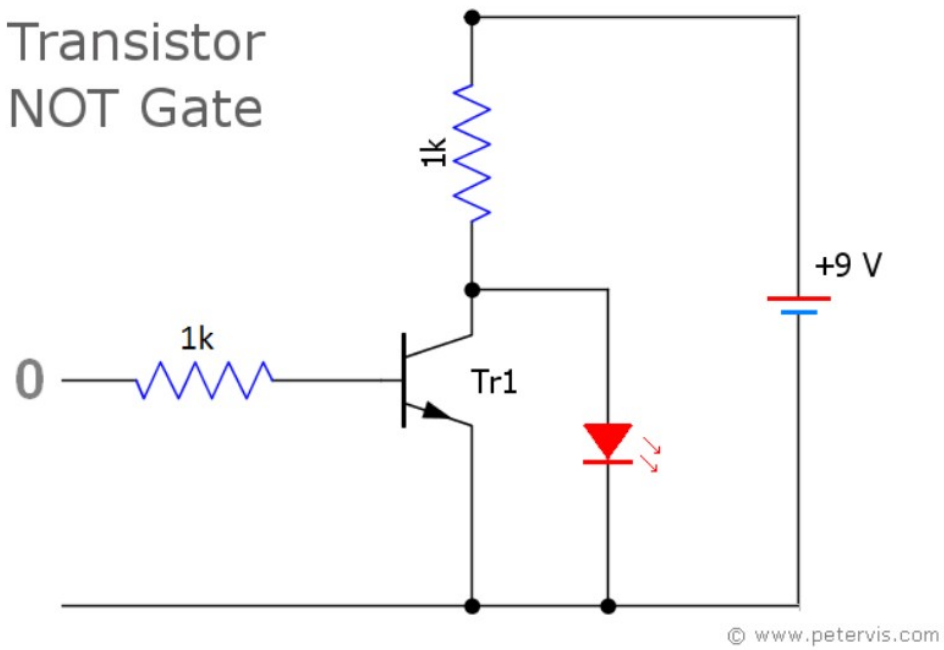
a device that can store a single bit of data (0 or 1)

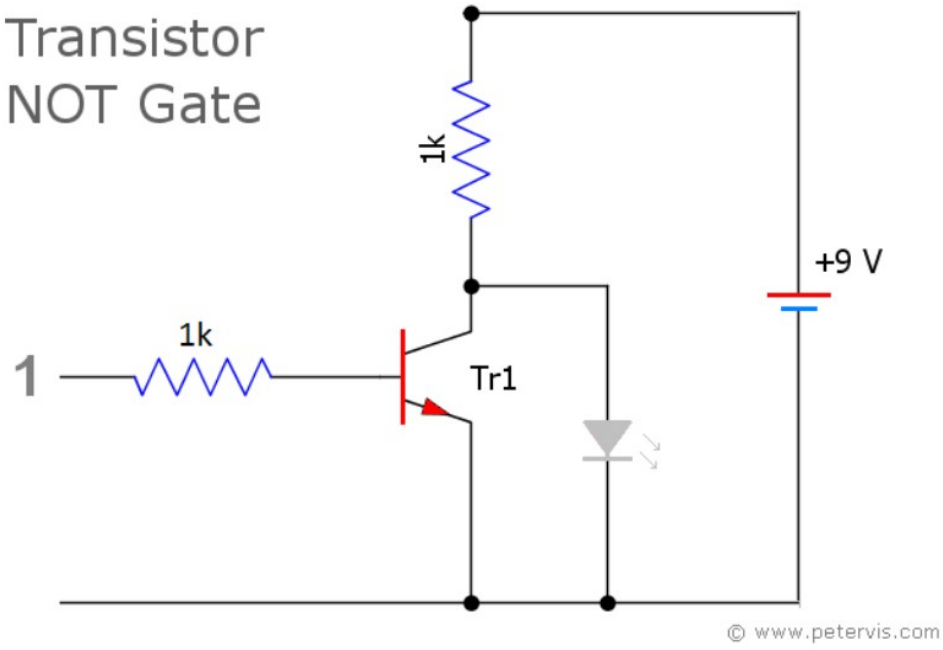




https://en.wikipedia.org/wiki/Flip-flop_(electronics)

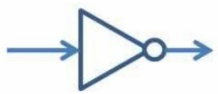
Inverter (0 ⇒1, 1 ⇒ 0) with transistor-transistor logic (TTL)

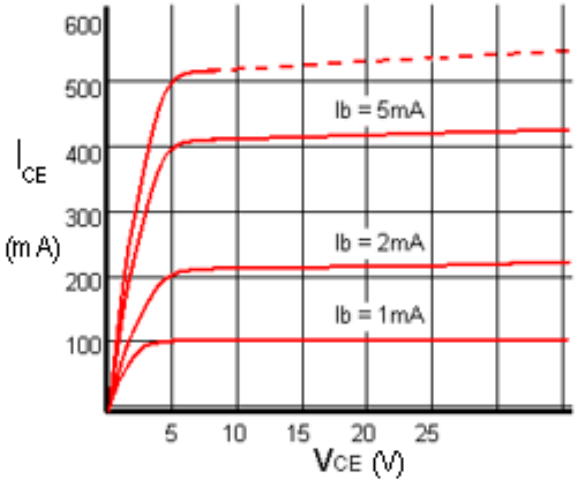




NOT

x	F
0	1
1	0



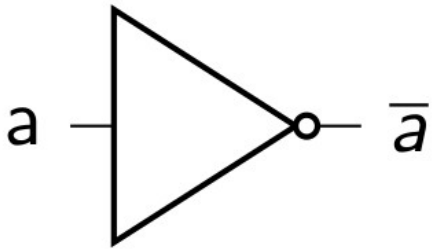


Elementary logic gates: one-bit logic gates

$$f : \{0,1\} \rightarrow \{0,1\}$$

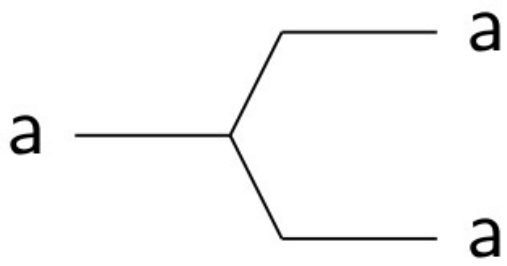
NOT

$$\bar{a} = 1 - a$$



a	$\bar{a}$
0	1
1	0

FANOUT (COPY)

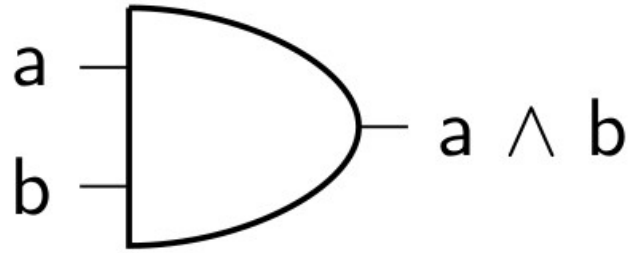


IDENTITY

$$a = a$$

Elementary logic gates: two-bit logic gates

$$f : \{0,1\}^2 \rightarrow \{0,1\}$$



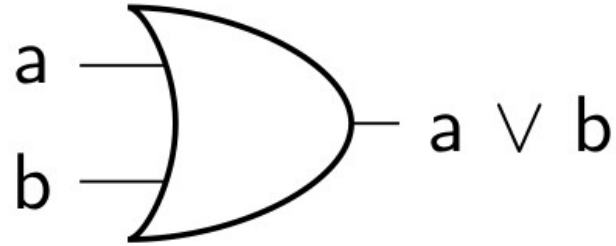
the AND gate:

$$a \wedge b \;=\; ab$$

a	b	a ∧ b
0	0	0
0	1	0
1	0	0
1	1	1

Elementary logic gates: two-bit logic gates

$$f : \{0,1\}^2 \rightarrow \{0,1\}$$



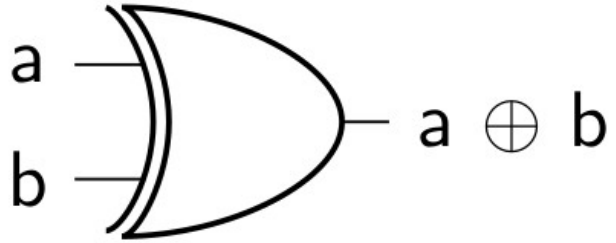
the OR gate:

$$a \vee b \;=\; a + b - ab$$

a	b	a ∨ b
0	0	0
0	1	1
1	0	1
1	1	1

Elementary logic gates: two-bit logic gates

$$f : \{0,1\}^2 \rightarrow \{0,1\}$$



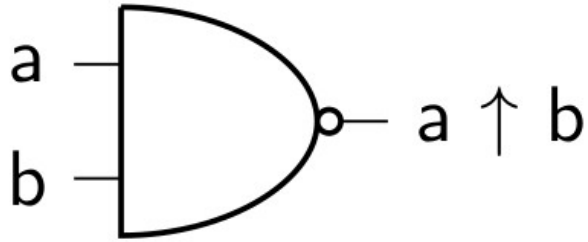
the XOR (exclusive OR) gate:

$$a \oplus b \;=\; a+b \quad (mod\,2)$$

a	b	a ⊕ b
0	0	0
0	1	1
1	0	1
1	1	0

Elementary logic gates: two-bit logic gates

$$f : \{0,1\}^2 \rightarrow \{0,1\}$$



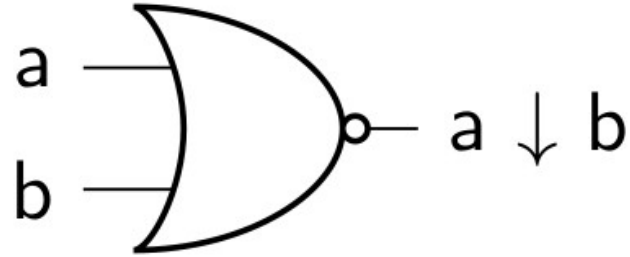
the NAND (negated AND) gate:

$$a \uparrow b \;=\; \overline{a \wedge b} \;=\; \overline{ab} \;=\; 1 - ab$$

a	b	a ↑ b
0	0	1
0	1	1
1	0	1
1	1	0

Elementary logic gates: two-bit logic gates

$$f : \{0,1\}^2 \rightarrow \{0,1\}$$

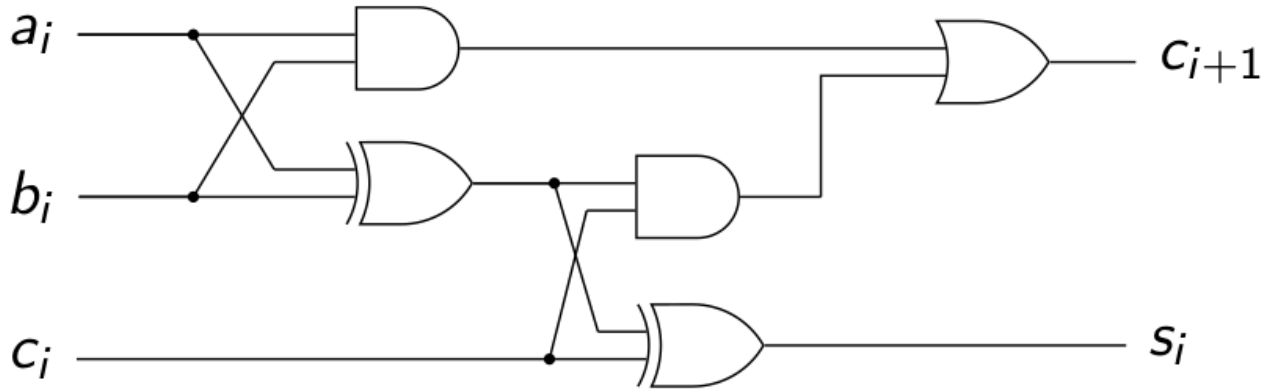


the NOR (negated OR) gate:

$$a \downarrow b = \overline{a \vee b} = \overline{a + b - ab}$$
$$= 1 - a - b + ab$$

a	b	a ↓ b
0	0	1
0	1	0
1	0	0
1	1	0

A circuit for computing the sum (with carry bit)



Given the binary representations $a = (a_{n-1}, \ldots, a_1, a_0)$ and $b = (b_{n-1}, \ldots, b_1, b_0)$, the i-th bit of the sum is

$$s_i = a_i + b_i + c_i \pmod 2$$

where c_i is the carry over from the sum $a_{i-1} + b_{i-1} + c_{i-1}$. The carry over is set to one if two or more of the input bits a_i, b_i and c_i are 1 and 0 otherwise. This circuit can be built with the following elementary gates: 2 AND, 1 OR, 2 XOR and 4 FANOUT.

Universal (classical) gates

Any function $f:\{0,1\}^m \rightarrow \{0,1\}^n$ can be constructed from the elementary gates:

AND, OR, NOT and FANOUT !

We say that AND, OR, NOT and FANOUT constitute **a universal set of gates** for the classical computation.

A smaller universal set is NAND and FANOUT:

OR can be obtained from NOT and AND: $a \vee b = \overline{\bar{a} \wedge \bar{b}}$ (De Morgan's identities)

and NOT can be obtained from NAND and FANOUT:

$$a \uparrow a = \overline{a \wedge a} = 1 - a^2 = 1 - a = \bar{a}$$

here we have FANOUT and NAND

Classical reversible computing

It is possible top embed any irreversible function into a reversible function:

irreversible function: $f:\{0,1\}^m \rightarrow \{0,1\}^n \qquad m>n$

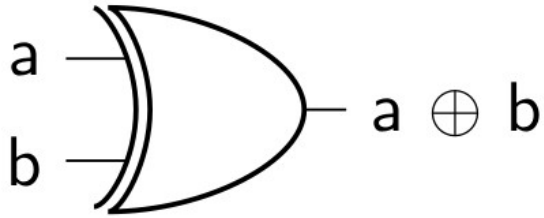
reversible function: $\tilde{f}:\{0,1\}^{m+n} \rightarrow \{0,1\}^{m+n}$

defined such that: $\tilde{f}(x,y) = (x,[y+f(x)](mod\,2^n))$

where **x** represents **m** bits, while **y** and **f(x)** represent **n** bits. Since the embedding function is **bijective**, it will be **reversible**! So at the logic level it is possible, with the price of introducing more dimensions in the calculations (**ancillary** bits **y**).

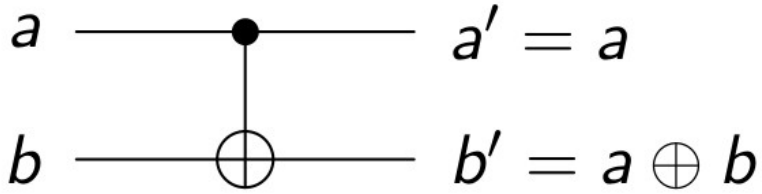
A simple reversible classical gate: the controlled-NOT (CNOT)

The exclusive-OR function (XOR):



a	b	a ⊕ b
0	0	0
0	1	1
1	0	1
1	1	0

The CNOT gate:

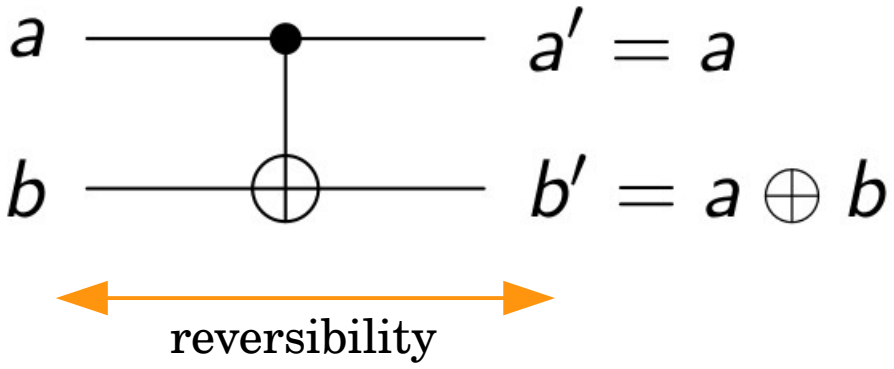


a	b	a'	b'
0	0	**0**	0
0	1	**0**	1
1	0	**1**	1
1	1	**1**	0

The circuit representation of the classical CNOT gate

the control bit:

the target bit:



two CNOT gates, applied one after the other:

$$(a,b) \rightarrow (a,a\oplus b) \rightarrow (a,a\oplus(a\oplus b))=(a,b)$$

so CNOT is self-inverse:

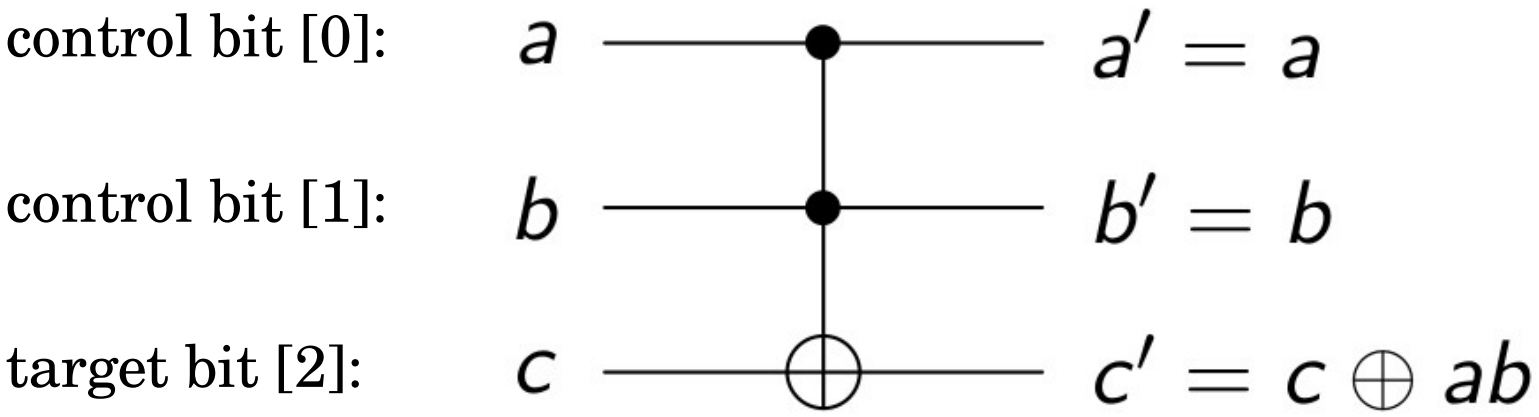
$$(CNOT)^2=I \quad , \quad CNOT^{-1}=CNOT$$

If the target bit is set to 0 (b=0) then CNOT becomes the FANOUT gate:

$$(a,0) \rightarrow (a,a)$$

... but two-bit reversible gates are not enough for universal computation !
We can not construct the NAND gate ...

Three-bit reversible gates: the Toffoli gate (controlled-controlled-NOT, or C^2NOT)



The Toffoli gate is a universal gate!

NOT: $a=b=1 \quad , \quad c'=\bar{c}$

AND: $c=0 \quad , \quad c'=a\wedge b$

OR: $a\to\bar{a} \quad , \quad b\to\bar{b} \quad , \quad c=1 \quad , \quad c'=a\vee b$

- Classical bits and classical computing
- Quantum mechanics and quantum bits (qubits)
- Manipulating qubit states, unitary errors
- Quantum gates and circuits
- Quantum teleportation
- Quantum Fourier Transformation
- Quantum cryptography
- IBM Q experience

Quantum bits (qubits)

A **qubit** is a quantum object: a microscopic system whose state and evolution are governed by the laws of quantum mechanics. In order to keep a good resemblance with the classical bit, this system will be chosen to have only two possible states, corresponding to some (measurable) physical property.

The two states are **orthogonal** and any arbitrary state the system can be described as a linear combination (superposition) of those two states:

$$|\psi\rangle = \alpha\ |0\rangle + \beta\ |1\rangle \qquad |\alpha|^2+|\beta^2|=1 \qquad \alpha,\beta\in\mathbb{C}$$

The 1st postulate of quantum mechanics

The state vector (or wave function) completely describes the state of the physical system.

The evolution in time of the state vector is governed by the Schrödinger equation:
(H is the Hamiltonian, a self-adjoint operator)

$$i\hbar\frac{d}{dt}|\psi(t)\rangle = H|\psi(t)\rangle$$

the 6th postulate

The coefficients α and β multiplying the vectors of the computational basis are functions of time:

$$|\psi(t)\rangle = \alpha(t)|0\rangle + \beta(t)|1\rangle$$

$$\hbar \approx 6.626\times10^{-34}\, Joule\cdot sec$$

$$i=\sqrt{-1}$$

Vector algebra with qubits

Since we describe our space with two coordinates, we can write the two basis vectors:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

and their superposition in the state vector: $|\psi\rangle = \alpha\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$

The vectors of the computational basis are normalized orthogonal vectors:

$$\langle 0|0\rangle = (1 \;\; 0)\begin{pmatrix} 1 \\ 0 \end{pmatrix} = 1 \quad , \quad \langle 0|1\rangle = (1 \;\; 0)\begin{pmatrix} 0 \\ 1 \end{pmatrix} = 0$$

$$\langle 1|0\rangle = (0 \;\; 1)\begin{pmatrix} 1 \\ 0 \end{pmatrix} = 0 \quad , \quad \langle 1|1\rangle = (0 \;\; 1)\begin{pmatrix} 0 \\ 1 \end{pmatrix} = 1$$

The 2nd postulate of quantum mechanics

We associate with any observable a **self-adjoint operator** on the Hilbert space of the states. The only possible outcome of a measurement is one of the eigen-values of the corresponding operator (3rd postulate).

A single-qubit operator can be represented by a 2x2 matrix: $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
(described within a given orthonormal vector base)

$$\sigma_z |0\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = +1 |0\rangle$$

$$\sigma_z |1\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ -1 \end{pmatrix} = -1 |1\rangle$$

$|0\rangle$ and $|1\rangle$ are eigen-vectors of the operator σ_z with eigen-values “+1” and “-1”

The probability of a given measurement outcome (the 4th postulate)

If we expand the state vector over the orthonormal basis formed by the eigen-vectors of the operator corresponding to the observable:

$$|\psi(t)\rangle = \alpha(t)\,|0\rangle + \beta(t)\,|1\rangle$$

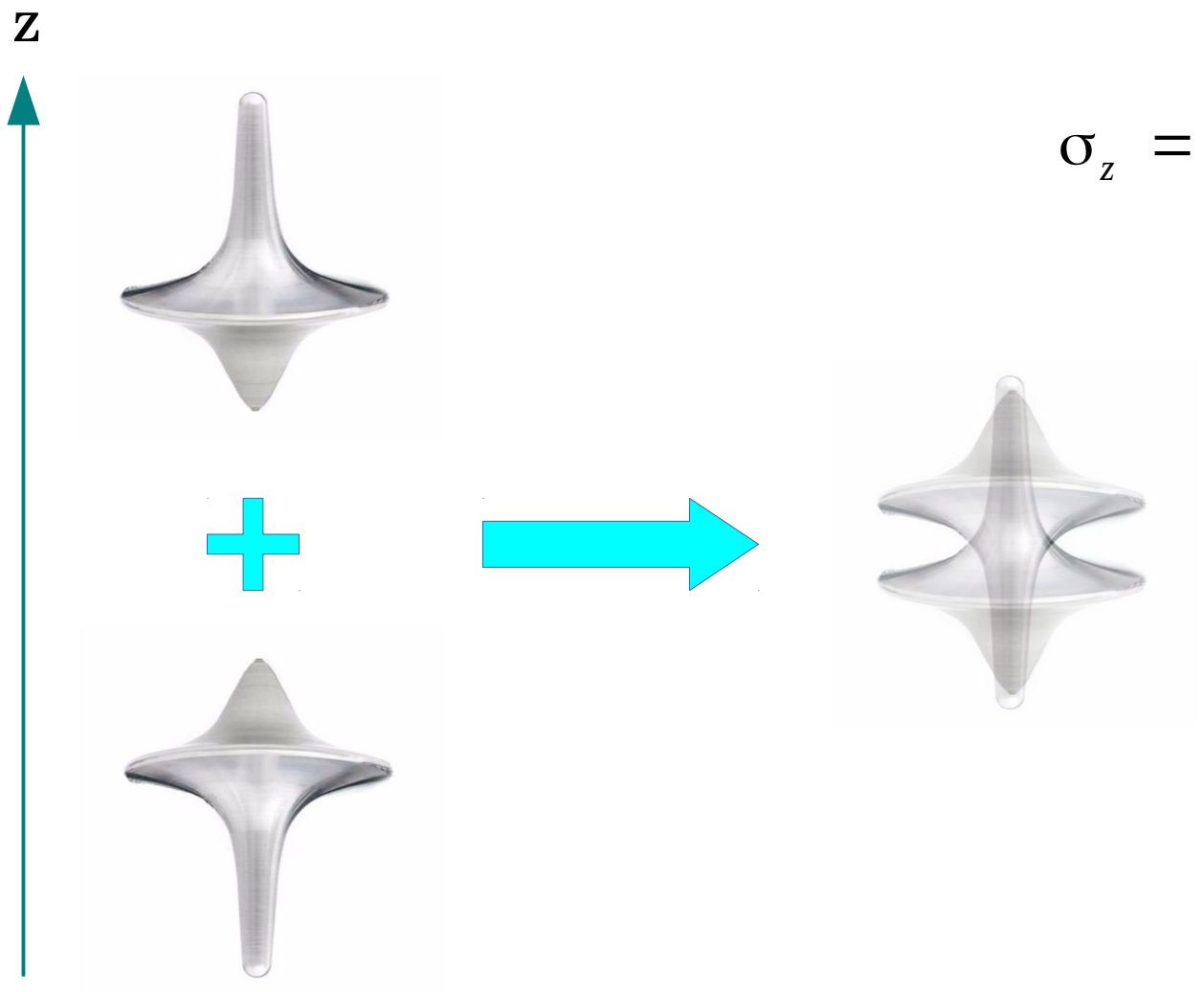
then the probability that a measurement at time t results in outcome "+1" or "-1" is given respectively by:

$$p_{+1}(t) = |\,\langle 0|\psi(t)\rangle\,|^2 = |\alpha(t)|^2$$

$$p_{-1}(t) = |\,\langle 1|\psi(t)\rangle\,|^2 = |\beta(t)|^2$$

Note: global phase factors $|\psi'\rangle = e^{i\theta}\,|\psi\rangle$ do not affect physical predictions!

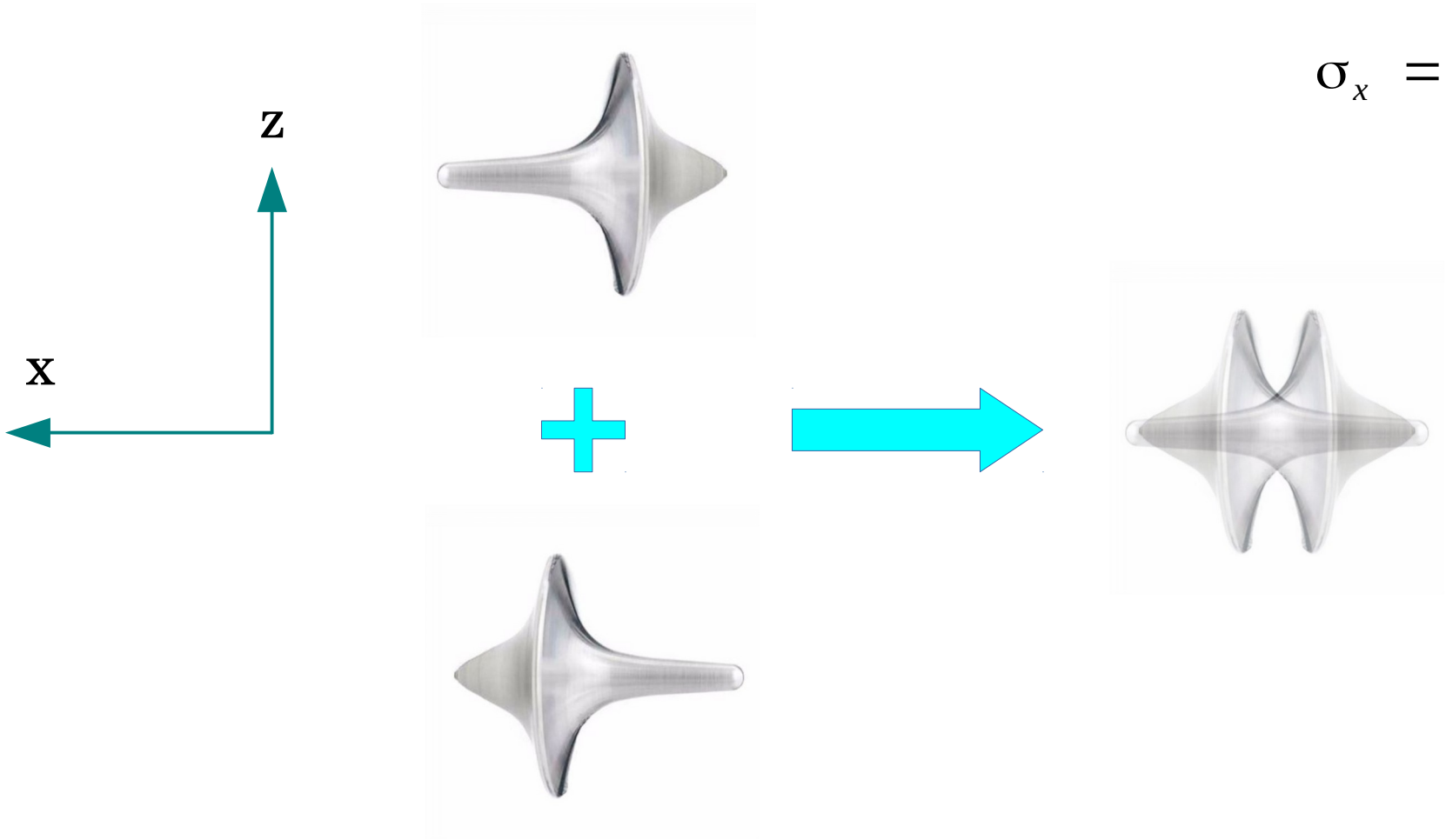
The quantified spin and the choice of the direction of the measurement



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

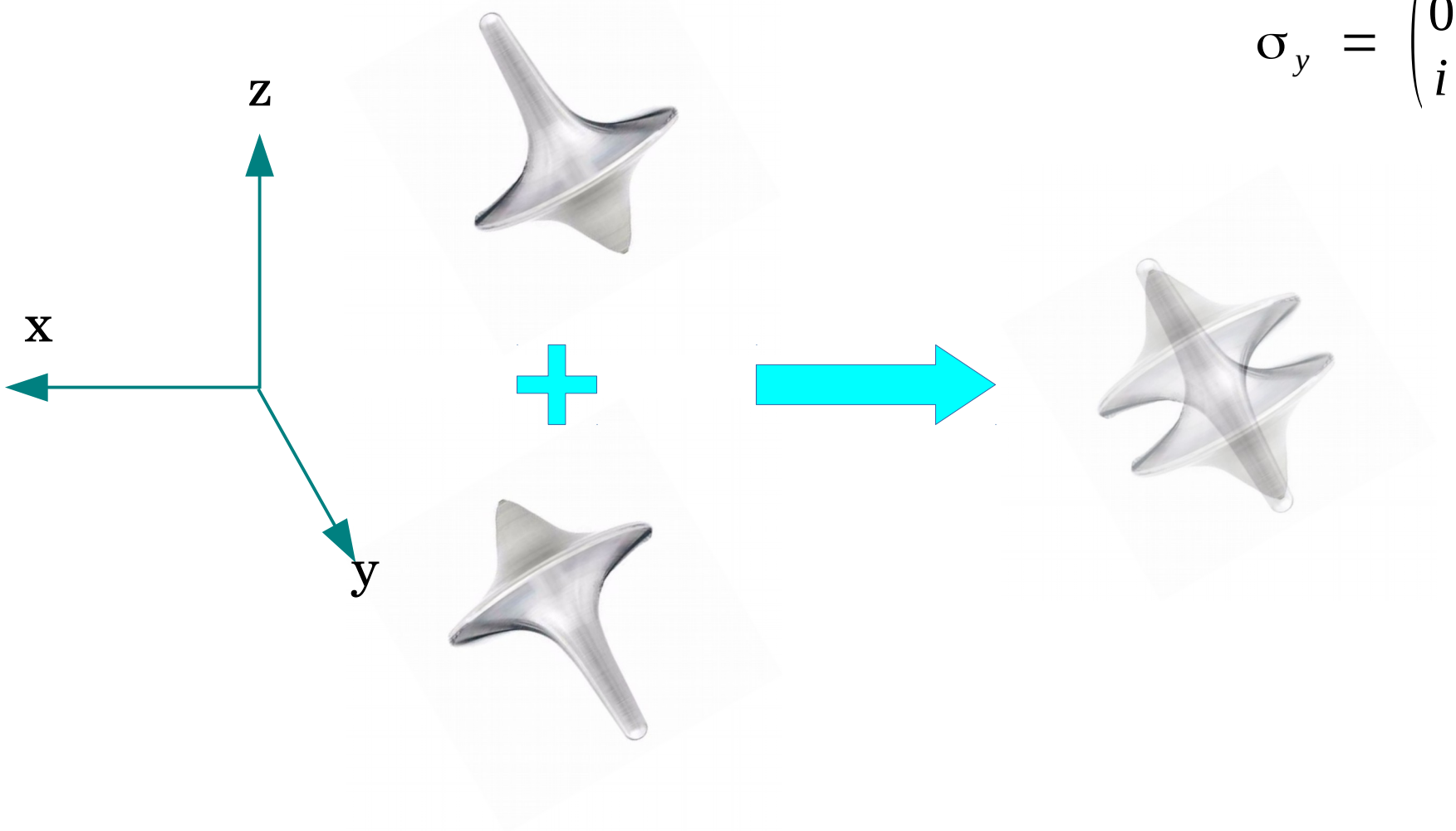
The quantified spin and the choice of the direction of the measurement

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

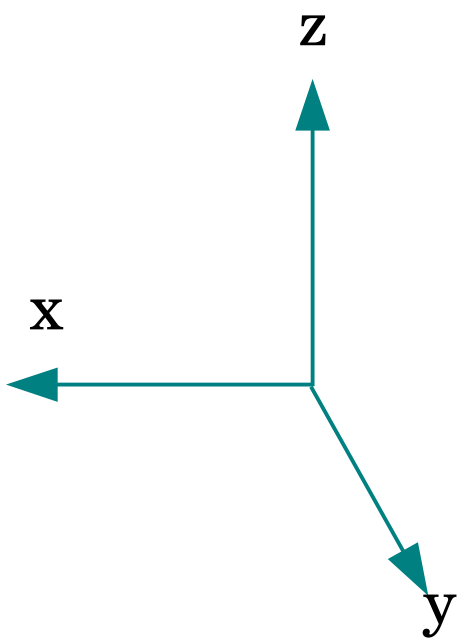


The quantified spin and the choice of the direction of the measurement

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



The quantified spin and the choice of the direction of the measurement



σ_x , σ_y , σ_z = Pauli matrices (operators), also σ_1 , σ_2 , σ_3

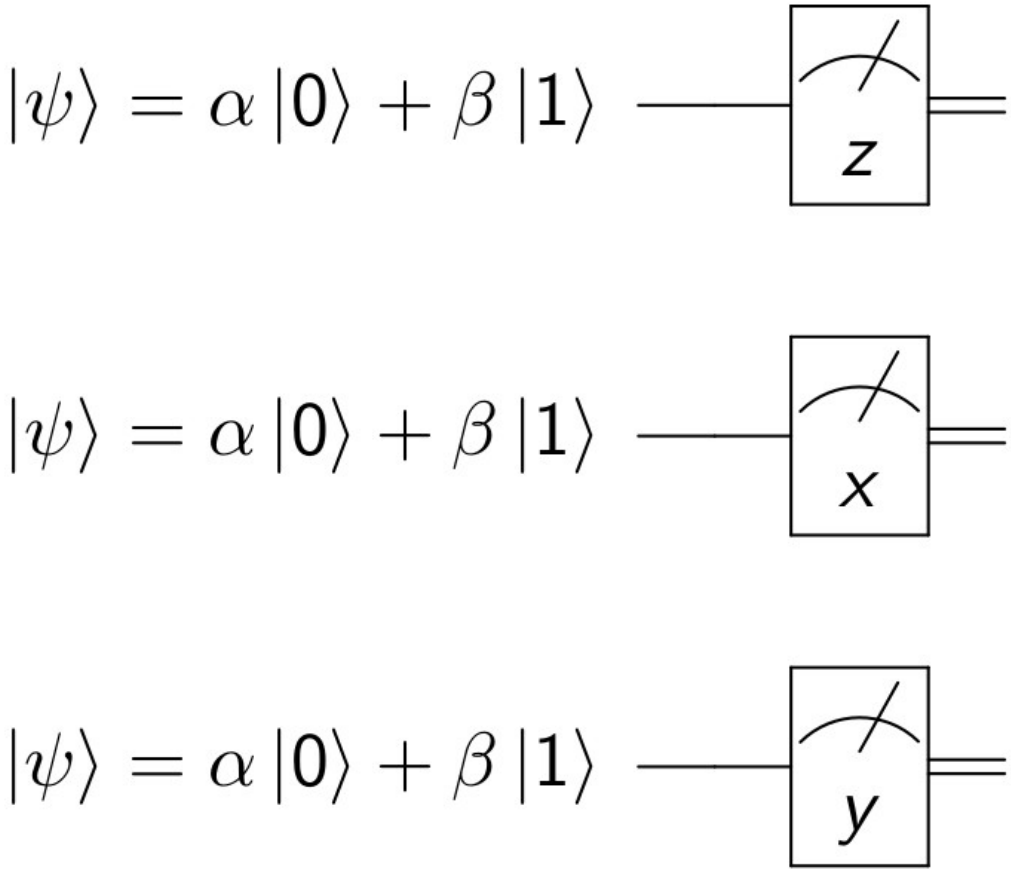
The eigen-vectors of the spin operators (Pauli) corresponding to eigen-values “+1” and “-1”

$$\sigma_x : \qquad |+\rangle_x = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad , \quad |-\rangle_x = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$\sigma_y : \qquad |+\rangle_y = \frac{1}{\sqrt{2}}(|0\rangle + i\,|1\rangle) \quad , \quad |-\rangle_y = \frac{1}{\sqrt{2}}(|0\rangle - i\,|1\rangle)$$

$$\sigma_z : \qquad |+\rangle_z = |0\rangle \quad , \quad |-\rangle_z = |1\rangle$$

Circuit symbol representation for a measurement



Note: double line means that this is a classical information (a bit).

The 5th postulate of quantum mechanics

If a system is described by the state vector $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ and we measure σ_z obtaining the outcome (spin projection) +1 or -1, then <u>immediately after the measurement the state of the system is given by the eigen-vector corresponding to the eigen-value</u>: $|0\rangle$ or $|1\rangle$ respectively.

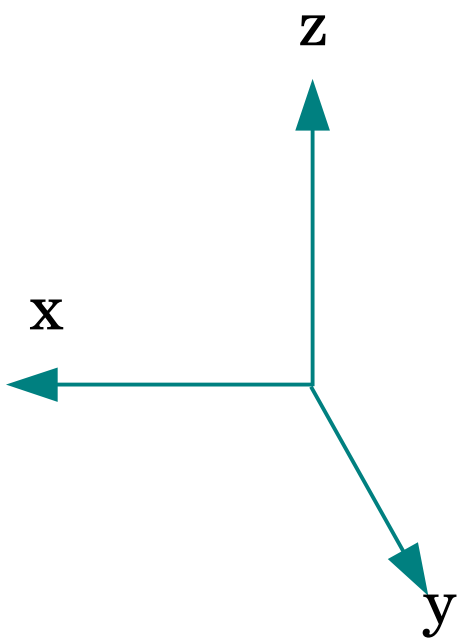
The expected value of an observable will be (4^{th} postulate):

$$\langle\sigma_z\rangle = \sum_n s_n p_n = \sum_n s_n \langle\psi|P_n|\psi\rangle = \langle\psi|(\sum_n s_n P_n)|\psi\rangle = \langle\psi|\sigma_z|\psi\rangle$$

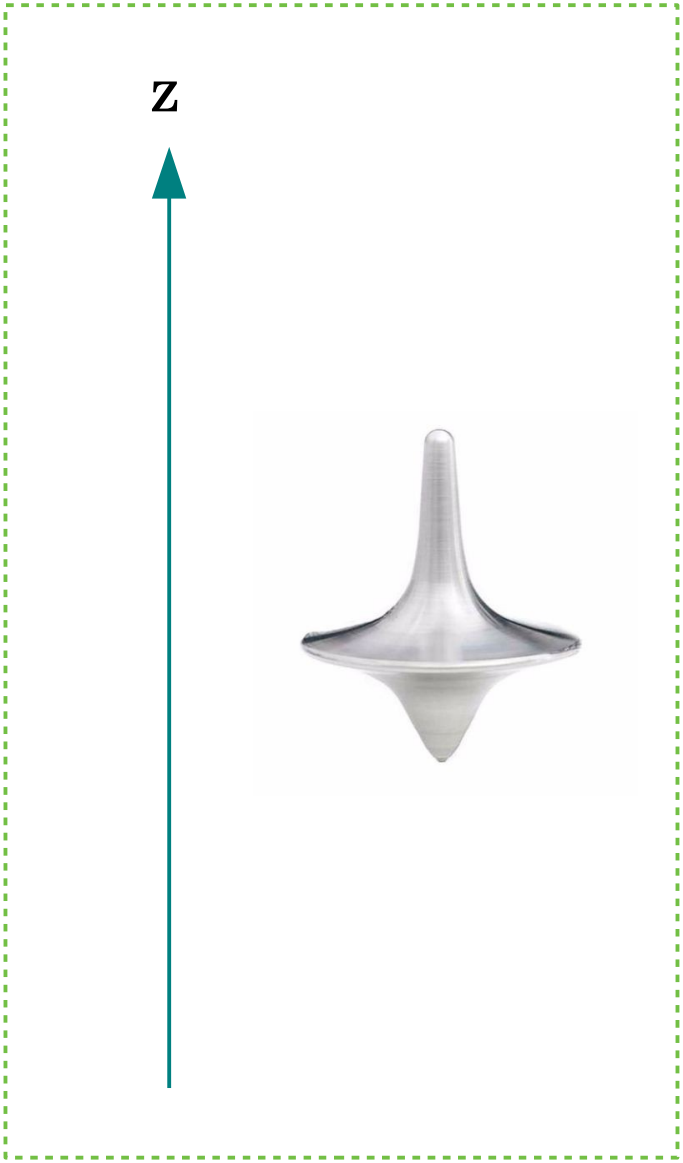
from the outcome probabilities: $p_n = \langle\psi|P_n|\psi\rangle$

with the projector operators: $P_1 = |0\rangle\langle 0| \quad , \quad P_2 = |1\rangle\langle 1|$

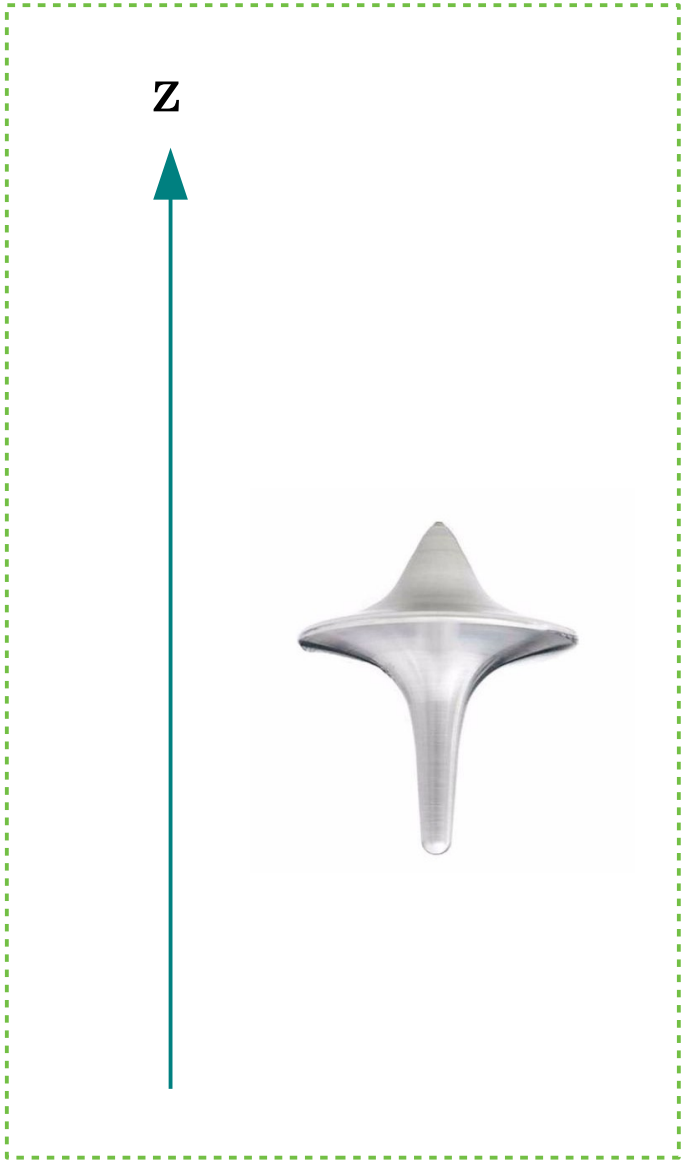
Before the measurement of the z spin component



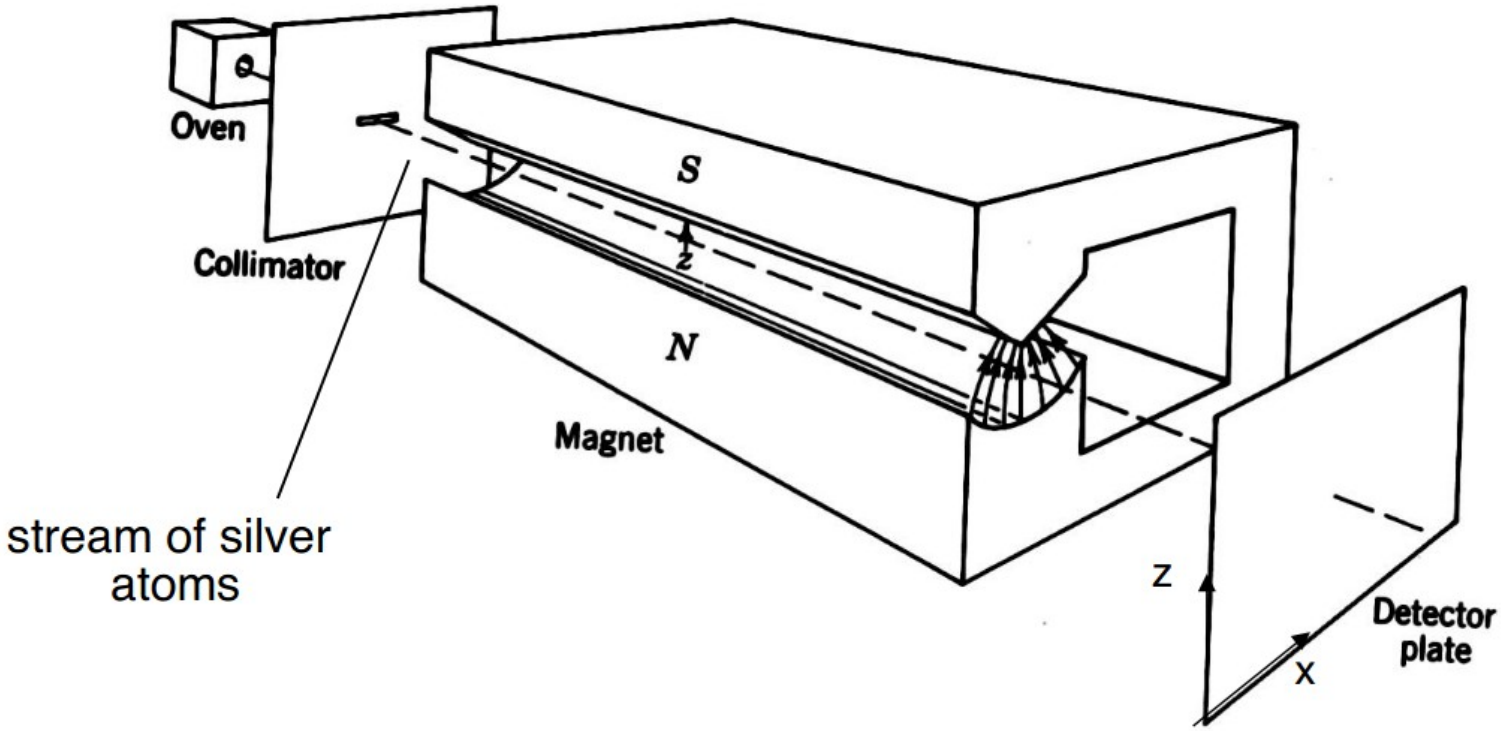
After the measurement



or

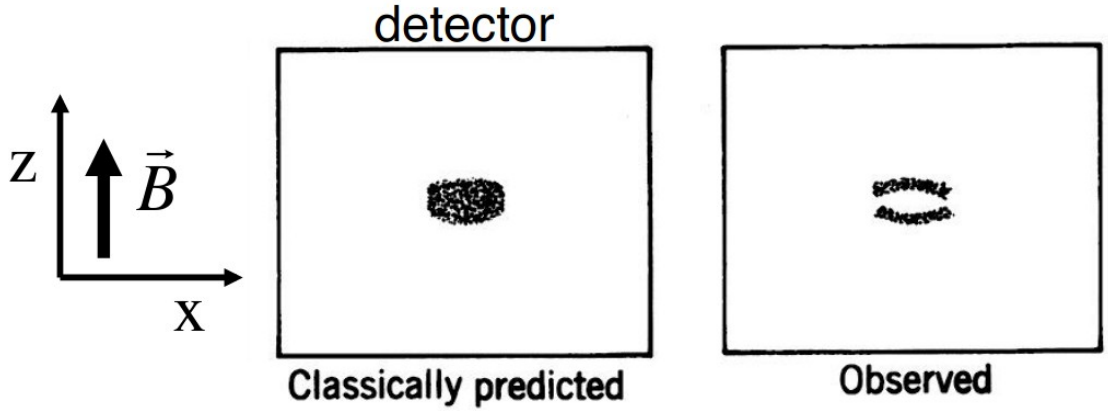


The Stern-Gerlach experiment



Force proportional to the gradient of the magnetic field

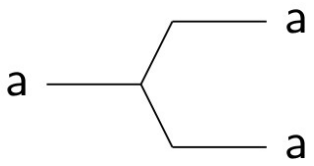
$$F_z = \mu \frac{\partial B_z}{\partial z}$$



http://web.stanford.edu/class/rad226a/Lectures/Lecture5-2017-Quantum-III.pdf

The no-cloning theorem

Contrary to the classical case, it is not possible to clone (COPY or FANOUT) a **generic** quantum state.

The equivalent of this: 

does not exist in the quantum case.

It is impossible to build a machine that operates unitary transformations and is able to clone the generic state of a qubit.

This has important consequences and leads to interesting consequences like the possibility of doing quantum cryptography.

The possibility of cloning would also invalidate the **uncertainty relation of Heisenberg** because it would be possible to simultaneously measure with infinite precision two physical properties of the system on two identical copies of the same quantum state.

- Classical bits and classical computing
- Quantum mechanics and quantum bits (qubits)
- Manipulating qubit states, unitary errors
- Quantum gates and circuits
- Quantum teleportation
- Quantum Fourier Transformation
- Quantum cryptography
- IBM Q experience

Flipping a qubit using a constant magnetic field

The Schrödinger equation: $i\hbar\frac{d}{dt}|\psi(t)\rangle = H|\psi(t)\rangle$

The time-evolution operator:

$$|\psi(t)\rangle = U(t,t_0)|\psi(t_0)\rangle \quad , \quad U(t,t_0) = \exp\left[-\tfrac{i}{\hbar}H(t-t_0)\right]$$

and in this particular case U is a unitary operator: $UU^\dagger = U^\dagger U = I$

The Hamiltonian of a spin interacting with a magnetic field is:

$$H = -\mu\mathcal{H}\cdot\sigma \quad , \quad \mathcal{H} = (\mathcal{H}_x, \mathcal{H}_y, \mathcal{H}_z) \quad , \quad \sigma = (\sigma_x, \sigma_y, \sigma_z)$$

Flipping a qubit with a constant magnetic field

Using the notations:

$$n = \frac{1}{\sqrt{\mathcal{H}_x^2 + \mathcal{H}_y^2 + \mathcal{H}_z^2}} (\mathcal{H}_x, \mathcal{H}_y, \mathcal{H}_z) \quad , \quad n = (n_x, n_y, n_z)$$

$$\alpha(t) = \frac{\mu t}{\hbar} \sqrt{\mathcal{H}_x^2 + \mathcal{H}_y^2 + \mathcal{H}_z^2}$$

We obtain for the time-evolution operator this:

$$U(t) = \begin{bmatrix} \cos\alpha + i\ n_z \sin\alpha & (n_y + i\ n_x)\sin\alpha \\ (-n_y + i\ n_x)\sin\alpha & \cos\alpha - i\ n_z \sin\alpha \end{bmatrix}$$

Flipping a qubit with a constant magnetic field

For instance, with a magnetic field: $\mathcal{H} = (\mathcal{H}_x, 0, 0) \quad , \quad n = (1, 0, 0)$

We can flip the state $|0\rangle$ into the state $|1\rangle$:

$$\begin{bmatrix} 0 \\ 1 \end{bmatrix} = U \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \cos\alpha(t_{01}) & i \ \sin\alpha(t_{01}) \\ \\ i \ \sin\alpha(t_{01}) & \cos\alpha(t_{01}) \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

Which is fulfilled if:

$$\cos\alpha(t_{01}) = 0 \quad , \quad t_{01} = \frac{\pi\hbar}{2\mu|\mathcal{H}_x|}$$

Unitary errors

Any quantum computation is given by a sequence of quantum gates applied to some initial state:

$$|\psi_n\rangle = \prod_{i=1}^{n} U_i \, |\psi_0\rangle$$

If the errors are unitary (no coupling to the environment, but any realistic implementation of a unitary operation will involve some error, since unitary operators form a continuous set), instead of operators U_i we apply slightly different operators V_i:

$$|\psi_i\rangle = U_i \, |\psi_{i-1}\rangle \quad \longrightarrow \quad V \, |\psi_{i-1}\rangle = |\psi_i\rangle + |E_i\rangle$$

Unitary errors

For instance, in the previous qubit flip example

instead of $|\psi_1\rangle = |0\rangle \quad , \quad |\psi_2\rangle = U(t_{01})\,|\psi_1\rangle = |1\rangle$

we will have $|\psi_2'\rangle = |1\rangle + (\epsilon_0\,|0\rangle + \epsilon_1\,|1\rangle)$

Back to the general case, after n iterations we obtain:

$$|\widetilde{\psi_n}\rangle = |\psi_n\rangle + |E_n\rangle + V_n V_{n-1}\,|E_{n-2}\rangle + \cdots + V_n V_{n-1} \ldots V_2\,|E_1\rangle$$

with a limit of the error: $\left\| |\widetilde{\psi_n}\rangle - |\psi_n\rangle \right\| < n\epsilon$

In the "classical" case we have: $\sigma^2 = \sum_{i=1}^{n} \sigma_i^2 \quad \rightarrow \quad \sigma < \sqrt{n}\ \epsilon$

- Classical bits and classical computing
- Quantum mechanics and quantum bits (qubits)
- Manipulating qubit states, unitary errors
- Quantum gates and circuits
- Quantum teleportation
- Quantum Fourier Transformation
- Quantum cryptography
- IBM Q experience

Single-qubit gates σ_x , σ_y , σ_z

(Pauli operators)

$$\sigma_x |0\rangle = |1\rangle$$

$$\sigma_x |1\rangle = |0\rangle$$

$$\sigma_y |0\rangle = i |1\rangle$$

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

$$\sigma_z |0\rangle = |0\rangle$$

$$\sigma_z |1\rangle = -|1\rangle$$

The Hadamard gate

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \equiv |+\rangle_x$$

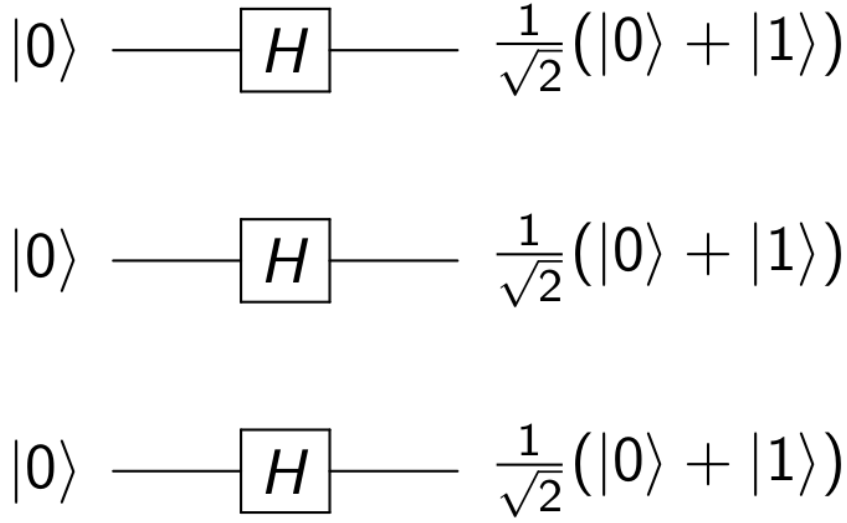
$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \equiv |-\rangle_x$$

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

$|x\rangle$ —— $\boxed{H}$ —— $(-1)^x|x\rangle + |1-x\rangle$, $|x\rangle = \{|0\rangle, |1\rangle\}$

Transforms the computational basis: $|0\rangle, |1\rangle \rightarrow |+\rangle_x, |-\rangle_x$

The exponential power of the states superposition



A network of 3 qubits:
the application of the 3 Hadamard gates is synchronized and in the total product state we have a superposition of the values from 0 to 7.

$$= \frac{1}{2^{3/2}}(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle)$$

$$= \frac{1}{2^{3/2}}(|0\rangle + |1\rangle + |2\rangle + |3\rangle + |4\rangle + |5\rangle + |6\rangle + |7\rangle)$$

The generic state of a qubit in spherical coordinates

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle = \begin{bmatrix} \cos\frac{\theta}{2} \\ e^{i\phi}\sin\frac{\theta}{2} \end{bmatrix}$$

We can write this because:

- the two coefficients α and β are complex
- we have the total probability normalization condition
- a state vector is defined only up to a global phase of no physical significance (we can take one of the coefficients pure real)

$$p_{+1,z} = |\langle 0,\psi\rangle|^2 = \cos^2\frac{\theta}{2} \quad , \quad p_{-1,z} = |\langle 1,\psi\rangle|^2 = \sin^2\frac{\theta}{2}$$

The phase-shift gate

$$R_z(\delta) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\delta} \end{bmatrix}$$

$$R_z(\delta)\,|\psi\rangle = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\delta} \end{bmatrix} \begin{bmatrix} \cos\frac{\theta}{2} \\ e^{i\phi}\sin\frac{\theta}{2} \end{bmatrix} = \begin{bmatrix} \cos\frac{\theta}{2} \\ e^{i(\phi+\delta)}\sin\frac{\theta}{2} \end{bmatrix}$$

$$|x\rangle \longrightarrow \boxed{R_z(\delta)} \longrightarrow e^{ix\delta}\,|x\rangle \qquad , \qquad |x\rangle = \{|0\rangle, |1\rangle\}$$

Universality of Hadamard and phase-shift gates

Any unitary operation on a single qubit can be constructed using only Hadamard and phase-shift gates. In particular, the generic state can be reached starting from $|0\rangle$ in the following way:

$$e^{i\frac{\theta}{2}}\,|\psi\rangle = e^{i\frac{\theta}{2}}(\cos\tfrac{\theta}{2}\,|0\rangle + e^{i\phi}\sin\tfrac{\theta}{2}\,|1\rangle) = R_z(\tfrac{\pi}{2}+\phi)\;H\;R_z(2\theta)\;H\;\;|0\rangle$$

Two-qubit states and gates

$$|\psi\rangle = \alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|10\rangle + \delta\,|11\rangle$$

$$|ij\rangle \equiv |i\rangle\,|j\rangle \equiv |i\rangle \otimes |j\rangle \qquad i = \{0,1\}\ ,\ j = \{0,1\}$$

$$\alpha^2+\beta^2+\gamma^2+\delta^2=1$$

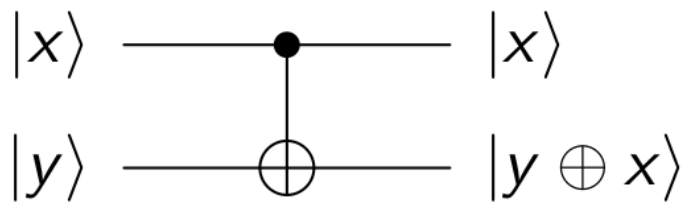
The total vector space of the two qubits is the result of a tensor product, the computational base of the resulting space is given by the 4 possible combinations by tensor product of the computational basis of each of the two qubits.

The quantum (two-qubit) CNOT gate

It acts on the computational basis of the system of two qubits like this:

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

The circuit diagram:

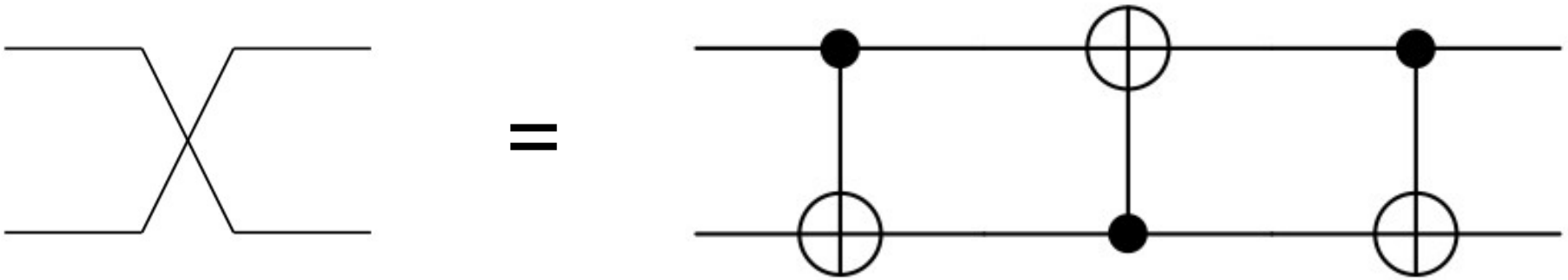


The 4×4 unitary matrix:

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

The state of target qubit (y) flips only if the control qubit (x) is in the $|1\rangle$ state.

Obtaining a SWAP gate from CNOT gates



The CNOT gate generates entanglement of two qubits

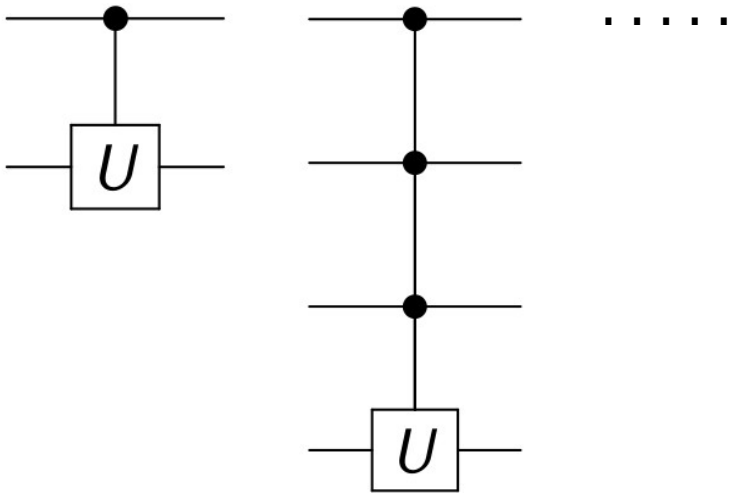
$$CNOT(\alpha\,|0\rangle + \beta\,|1\rangle) \otimes |0\rangle = \alpha\,|0\rangle \otimes |0\rangle + \beta\,|1\rangle \otimes |1\rangle$$

(the final state is non-separable, can not be expressed as a single product of two single qubit states)

Universal quantum gates

Any unitary operation in the Hilbert space of *n* qubits, $U^{(n)}$ can be decomposed into one-qubit gates and two-qubit CNOT gates.

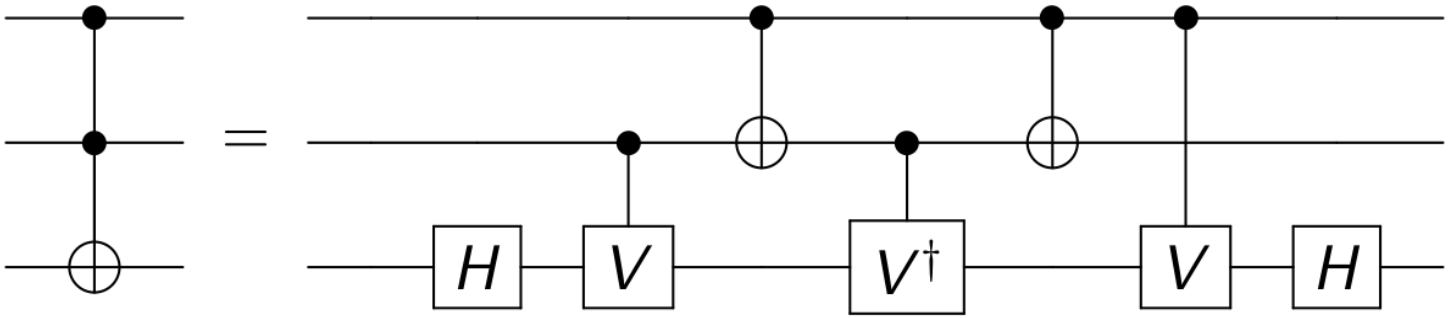
- we need few more special gates, like the controlled-U gate, where the U operator is applied to the target qubit only if the control qubit is in the $|1\rangle$ stat.



- the controlled-U gate can be generalized to the C^k-U gate, with k control qubits.

- a particular C^k-U is the C^2-NOT gate, or Toffoli gate; implementing the Toffoli gate can be done using CNOT, Hadamard and the unitary operator V

Implementing the Toffoli gate



where $V = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$

Universal quantum gates

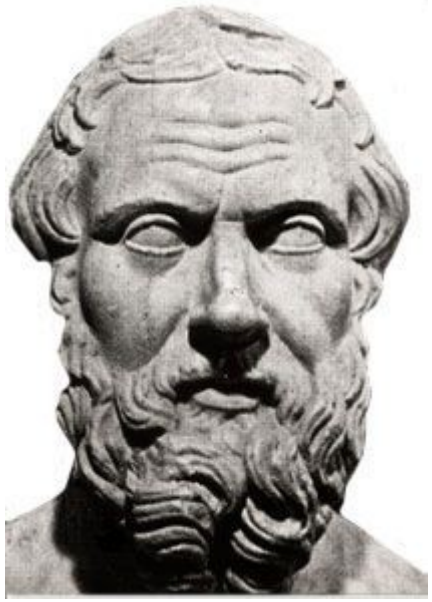
Finally we come to the following conclusion:

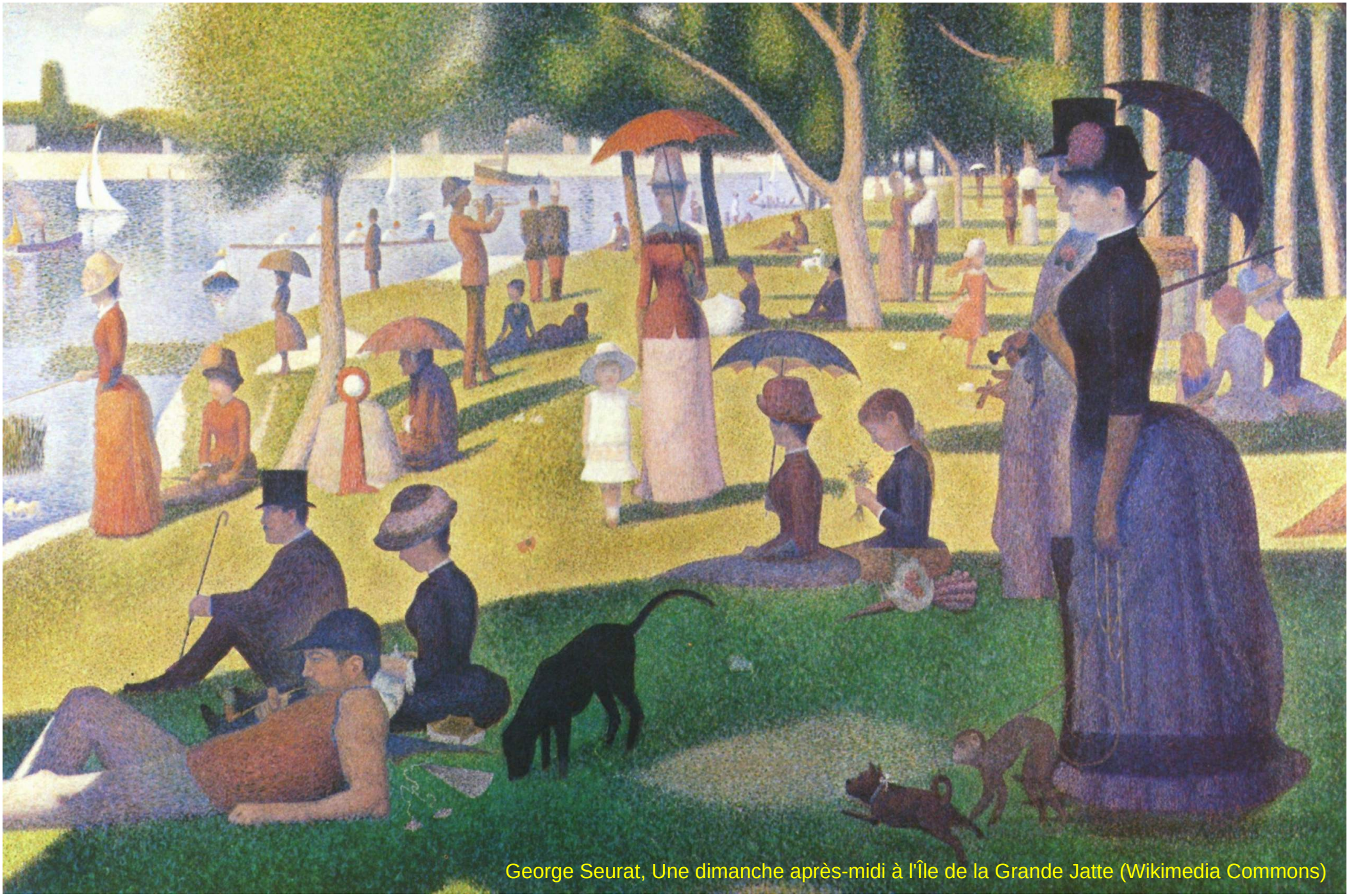
- a generic operator $U^{(n)}$ can be decomposed by means of C^k-U gates
- any C^k-U gate ($k > 2$) can be decomposed into Toffoli and controlled-U gates
- the C^2-NOT gate (Toffoli) can be implemented using CNOT, controlled-U and Hadamard gates
- for any single-qubit rotation U, the controlled-U operation can be decomposed into single-qubit and CNOT gates

- Classical bits and classical computing
- Quantum mechanics and quantum bits (qubits)
- Manipulating qubit states, unitary errors
- Quantum gates and circuits
- Quantum teleportation
- Quantum Fourier Transformation
- Quantum cryptography
- IBM Q experience

Un précurseur de la théorie atomique

"Si tout corps est divisible à l'infini, de deux choses l'une : ou il ne restera rien ou il restera quelque chose. Dans le premier cas la matière n'aurait qu'une existence virtuelle, dans le second cas on se pose la question : que reste-t-il ? La réponse la plus logique, c'est l'existence d'éléments réels, indivisibles et insécables appelés donc atomes."
(Démocrite / vers 460-370 avant JC)

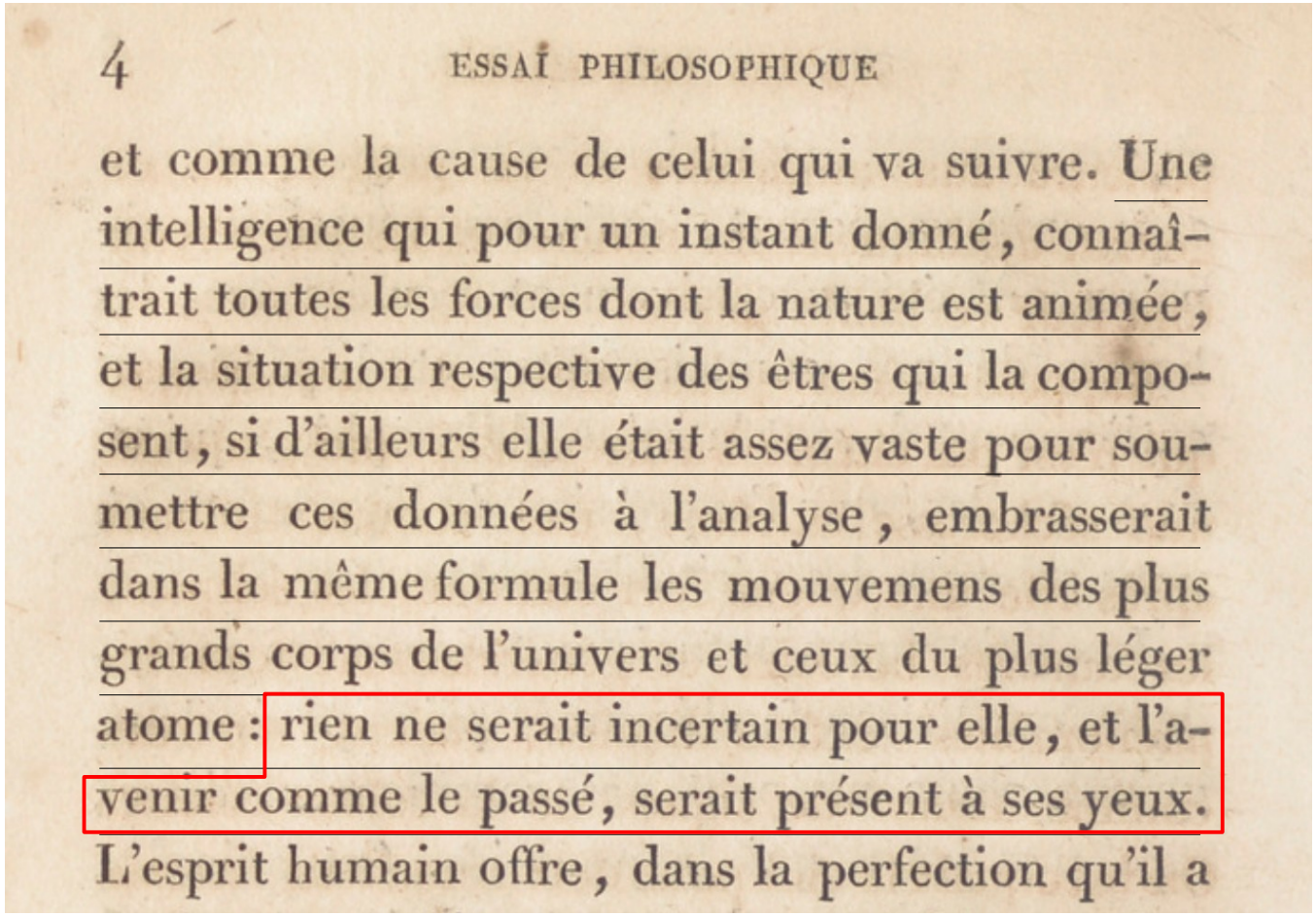




George Seurat, Une dimanche après-midi à l'Île de la Grande Jatte (Wikimedia Commons)

Smithsonian Libraries

Essai Philosophique sur les Probabilités, 1814



4 ESSAI PHILOSOPHIQUE

et comme la cause de celui qui va suivre. Une intelligence qui pour un instant donné, connaîtrait toutes les forces dont la nature est animée, et la situation respective des êtres qui la composent, si d'ailleurs elle était assez vaste pour soumettre ces données à l'analyse, embrasserait dans la même formule les mouvemens des plus grands corps de l'univers et ceux du plus léger atome : rien ne serait incertain pour elle, et l'avenir comme le passé, serait présent à ses yeux. L'esprit humain offre, dans la perfection qu'il a

gallica.bnf.fr

Quantum information: teleportation

Alice owns a two level system in some unknown state: $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ and wishes to send this qubit state to Bob using only a classical communication channel (we know that Alice can not clone that state into a quantum copy).

Alice can not simply measure the state, because it will immediately destroy that state with the price of obtaining only one bit of information (describing the generic state requires an infinite amount of classical information).

Quantum teleportation is possible, providing that Alice and Bob share an **entangled pair of qubits**.

For instance, starting from the computational basis we can create the entangled state of two qubits in this way:

$$CNOT(H \otimes I)\,|01\rangle = |\psi^+\rangle \quad \Rightarrow \quad |\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

(Bell pair)

Quantum information: teleportation

The three qubit state obtained by putting in the same register the two qubits and the qubit to be cloned is given by the tensor product:

$$|\psi\rangle \otimes |\psi^+\rangle = \frac{\alpha}{\sqrt{2}}(|001\rangle + |010\rangle) + \frac{\beta}{\sqrt{2}}(|101\rangle + |110\rangle)$$

Alice will let her qubit interact with her half of the Bell pair, which means that she will perform a measurement not in the computational basis but in the Bell basis.

Quantum information: teleportation

The three-qubit state can be written in the Bell basis after some transformations:

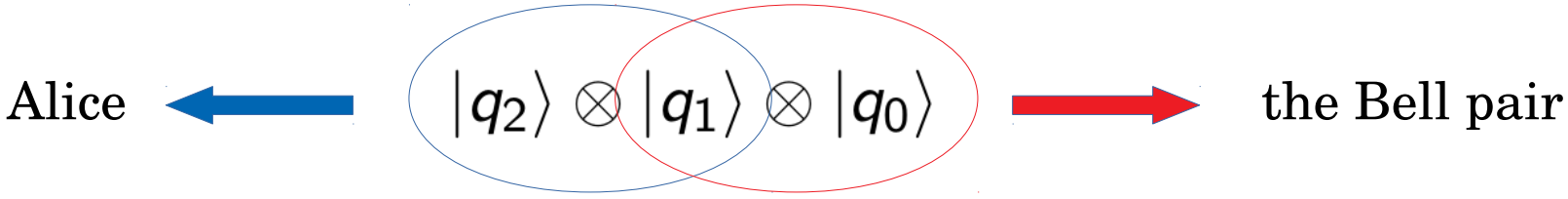
$$|\psi\rangle \otimes |\psi^+\rangle = \frac{1}{2}|\psi^+\rangle(\alpha|0\rangle + \beta|1\rangle) + \frac{1}{2}|\psi^-\rangle(\alpha|0\rangle - \beta|1\rangle)$$

$$+\frac{1}{2}|\phi^+\rangle(\alpha|1\rangle + \beta|0\rangle) + \frac{1}{2}|\phi^-\rangle(\alpha|1\rangle - \beta|0\rangle)$$

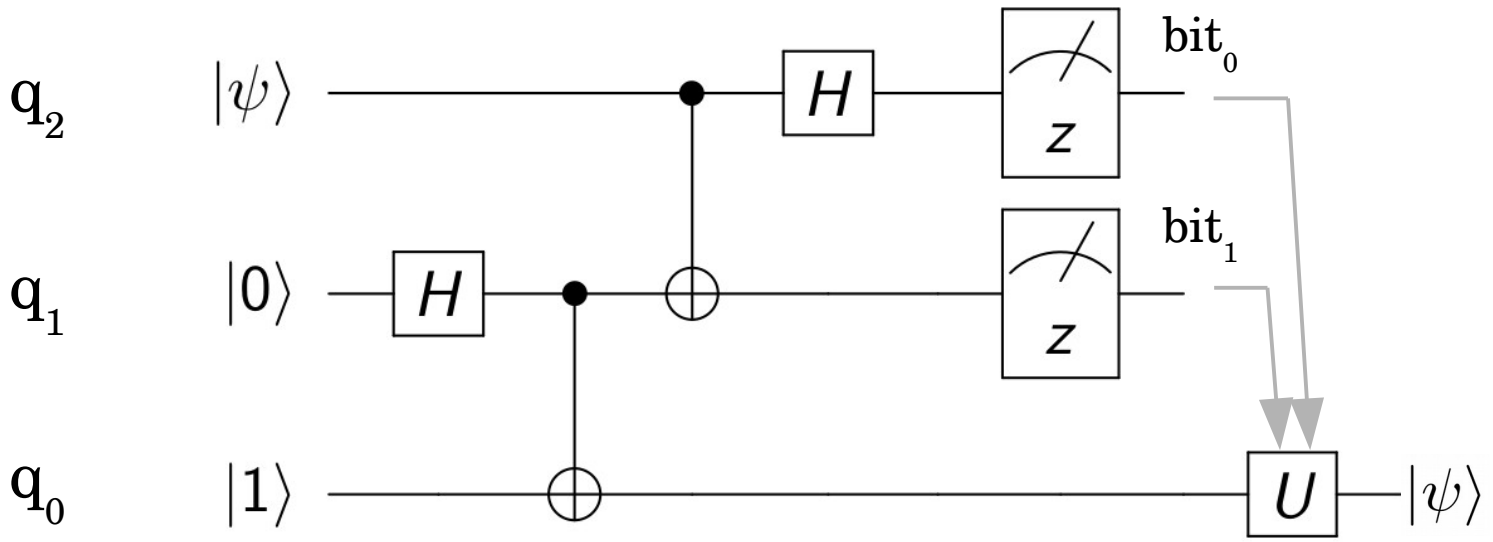
and after the application of the two last gates $(H \otimes I)CNOT$ we obtain:

$$|\psi\rangle \otimes |\psi^+\rangle = \frac{1}{2}|01\rangle(\alpha|0\rangle + \beta|1\rangle) + \frac{1}{2}|11\rangle(\alpha|0\rangle - \beta|1\rangle)$$

$$+\frac{1}{2}|00\rangle(\alpha|1\rangle + \beta|0\rangle) + \frac{1}{2}|10\rangle(\alpha|1\rangle - \beta|0\rangle)$$



Quantum information: teleportation



Finally, Alice makes a measurement on his two qubits and sends the result to Bob, in the form of two classical bits (0, 1) which correspond to the computational basis.

Quantum information: teleportation

If Bob chooses to apply a unitary operator U to his qubit according to the pair of bits sent by Alice as in next table, he will obtain exactly the initial generic state which Alice wanted to transmit:

Alice measures	Bob gets the bits	and applies to his qubit
$\|01\rangle$	0,1	I
$\|11\rangle$	1,1	σ_z
$\|00\rangle$	0,0	σ_x
$\|10\rangle$	1,0	$i\sigma_y$

- Classical bits and classical computing
- Quantum mechanics and quantum bits (qubits)
- Manipulating qubit states, unitary errors
- Quantum gates and circuits
- Quantum teleportation
- Quantum Fourier Transformation
- Quantum cryptography
- IBM Q experience

The Fourier Transformation, continuous and discrete

$$F(\omega) = \int_{-\infty}^{\infty} f(t) e^{-i\omega t} dt$$

direct, time domain to frequence domain

$$f(t) = \frac{1}{2\pi} \int_{-\infty}^{\infty} F(\omega) e^{i\omega t} d\omega$$

inverse, frequence domain to time domain

$$X_k = \sum_{n=0}^{N-1} x_n \mathrm{e}^{-i2\pi kn/N} \quad k = 0, \ldots, N-1$$

$$x_n = \frac{1}{N} \sum_{k=0}^{N-1} X_k \mathrm{e}^{i2\pi kn/N} \quad n = 0, \ldots, N-1$$

(DFT)

The Fast Fourier Transformation (FFT)

The discrete Fourier transform (DFT) is defined by the formula:

(1)
$$X_k = \sum_{n=0}^{N-1} x_n e^{-\frac{2\pi i}{N} nk}, \qquad \longrightarrow \; O\left(N^2\right) \text{ complexity}$$

where k is an integer ranging from 0 to $N-1$.

(2)
$$X_k = \sum_{m=0}^{N/2-1} x_{2m} e^{-\frac{2\pi i}{N}(2m)k} + \sum_{m=0}^{N/2-1} x_{2m+1} e^{-\frac{2\pi i}{N}(2m+1)k}$$

(3)
$$X_k = \underbrace{\sum_{m=0}^{N/2-1} x_{2m} e^{-\frac{2\pi i}{N/2} mk}}_{\text{DFT of even-indexed part of } x_n} + e^{-\frac{2\pi i}{N} k} \underbrace{\sum_{m=0}^{N/2-1} x_{2m+1} e^{-\frac{2\pi i}{N/2} mk}}_{\text{DFT of odd-indexed part of } x_n} = E_k + e^{-\frac{2\pi i}{N} k} O_k.$$

(4)
$$\begin{aligned} X_k &= E_k + e^{-\frac{2\pi i}{N} k} O_k \\ X_{k+\frac{N}{2}} &= E_k - e^{-\frac{2\pi i}{N} k} O_k \end{aligned}$$

The QFT

We want to do a discrete transformation of a vector of N complex values :

$$f(0), f(1), \ldots, f(N-1) \quad \rightarrow \quad \tilde{f}(0), \tilde{f}(1), \ldots, \tilde{f}(N-1)$$

We start by building a generic state with n = $\log_2$N qubits, written in the computational basis as :

$$|\psi\rangle = \sum_{j=0}^{2^n-1} f(j)\,|j\rangle \qquad \text{(superposition)}$$

where a vector of the computational basis is the tensor product :

$$|j\rangle = |j_0\rangle \otimes |j_1\rangle \otimes \ldots \otimes |j_{n-1}\rangle \quad , \quad j_m = \{0,1\} \quad , \quad m = 0, \ldots, n-1$$

The QFT

We define the following unitary operator F acting on the states of the computational basis as follows :

$$F(|j\rangle) = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i \frac{jk}{2^n}} |k\rangle$$

such that an arbitrary state is transformed into :

$$|\widetilde{\psi}\rangle = F(|\psi\rangle) = \sum_{k=0}^{2^n-1} \tilde{f}(k) |k\rangle$$

with the coefficients being the discrete transformation :

$$\tilde{f}(k) = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i \frac{jk}{N}} f(j) \qquad , \qquad N = 2^n$$

The QFT

If we introduce the notations for the binary representation of the indices of of the states of the computational basis:

$$j = j_{n-1}j_{n-2}\cdots j_0 = j_{n-1}2^{n-1} + j_{n-2}2^{n-2} + \ldots + j_0 2^0$$

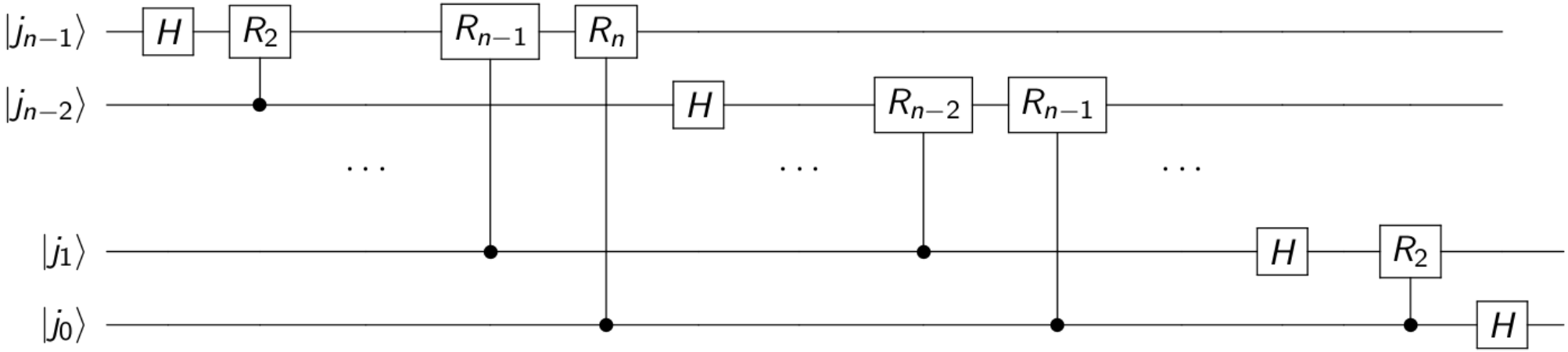
$$0.j_l j_{l+1}\cdots j_m = j_l 2^{-1} + j_{l+1}2^{-2} + \ldots + j_m 2^{-(m-l+1)}$$

then, after few steps, we obtain the product representation of the FT:

$$F(|j\rangle) = \frac{1}{\sqrt{2^n}}(|0\rangle + e^{2\pi i\ 0.j_0}\,|1\rangle)(|0\rangle + e^{2\pi i\ 0.j_1 j_0}\,|1\rangle)\cdots$$
$$\cdots(|0\rangle + e^{2\pi i\ 0.j_{n-1}j_{n-2}\cdots j_0}\,|1\rangle)$$

Note that this state is not entangled, it is factorized in n single qubit states.

The quantum circuit for the QFT



with the operator $R_k = \begin{bmatrix} 1 & 0 \\ 0 & \exp(\frac{2\pi i}{2^k}) \end{bmatrix}$

It is using n Hadamard gates and n(n-1)/2 single qubit gates,

so the computation requires $O(n^2)$ elementary quantum gates.

The FFT on a vector of $N = 2^n$ complex values, needs O(N logN)

elementary operations ! The DFT needs $O(N^2)$ operations.

- Classical bits and classical computing
- Quantum mechanics and quantum bits (qubits)
- Manipulating qubit states, unitary errors
- Quantum gates and circuits
- Quantum teleportation
- Quantum Fourier Transformation
- Quantum cryptography
- IBM Q experience

The RSA public-key cryptosystem (Rivest-Shamir-Adleman, 1977)

It is based on the number theory, in particular on the prime factorization of a very large number used in a trapdoor one-way function.

$$c = m^e \pmod{n} \quad , \quad m = c^d \pmod{n} \quad , \quad ed \equiv 1 \pmod{\Phi(n)}$$

$$\Phi(n) = (p-1)(q-1) \quad , \quad n = pq \quad , \quad p, q \quad \text{prime numbers}$$

e = private key
d = public key

But the realization of an efficient quantum processor would break this inviolability (like the Shor algorithm).

The unbreakable cypher

Gilbert Vernam (1917)

- the text is written as a binary sequence of 0's and 1's

0	0	1	0	1	0	0	1	1

- the secret key is a completely random binary sequence of the same length as the text

1	0	0	1	1	1	0	1	0

1	0	1	1	0	1	0	0	1

- the cypher text is obtained by adding the secret key bitwise module 2 to the plain text

$$c_i = p_i \oplus k_i \quad (i = 1, 2, \ldots, N)$$

Note: a key must not be reused for another message!

and to go back to the text

$$p_i = q_i \oplus k_i \quad (i = 1, 2, \ldots, N)$$

The unbreakable cypher

- the secret key has to be unique for each message
- the secret key must have the same length as the message
- the problem is not the transmission of the cypher text but the distribution of a large number of secret keys
- even by brute force it is impossible to guess the original message

Alice  0 1 1 0 0 1 0 0 0 1 1 1 .... 0 1 0 0 1 1 1 1 0 0  Bob

The BB84 (quantum) protocol
Bennett and Brassard, 1984

BB84 is using four quantum states of a single qubit and it is coding the classical bits into states of a qubit using two alphabets:

$$|0\rangle \quad , \quad |1\rangle \quad , \quad |+\rangle \equiv |0\rangle_x = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad , \quad |-\rangle \equiv |1\rangle_x = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

which are the eigen-states of the Pauli matrices σ_z and σ_x respectively (the z-alphabet and the x-alphabet), a pair on non-commuting observables.

$$0 = \begin{cases} |0\rangle \text{ , z-alphabet} \\ |+\rangle \text{ , x-alphabet} \end{cases} \qquad 1 = \begin{cases} |1\rangle \text{ , z-alphabet} \\ |-\rangle \text{ , x-alphabet} \end{cases}$$

The first part of the BB84 protocol

Alice's data bits	1	0	0	0	1	1	0	1	0	1

1. Alice generates a random sequence of 0's and 1's

The first part of the BB84 protocol

Alice's data bits	1	0	0	0	1	1	0	1	0	1
Alice's alphabet	x	z	x	z	x	x	x	z	z	x

2. Alice encodes each data bit in a qubit, by choosing Randomly between the z- and the x-alphabet

The first part of the BB84 protocol

Alice's data bits	1	0	0	0	1	1	0	1	0	1
Alice's alphabet	x	z	x	z	x	x	x	z	z	x
Transmitted qubits	$\|-\rangle$	$\|0\rangle$	$\|+\rangle$	$\|0\rangle$	$\|-\rangle$	$\|-\rangle$	$\|+\rangle$	$\|1\rangle$	$\|0\rangle$	$\|-\rangle$

3. The resulting string of qubits is sent by Alice and received by Bob (by teleportation)

The first part of the BB84 protocol

Alice's data bits	1	0	0	0	1	1	0	1	0	1
Alice's alphabet	x	z	x	z	x	x	x	z	z	x
Transmitted qubits	$\|-\rangle$	$\|0\rangle$	$\|+\rangle$	$\|0\rangle$	$\|-\rangle$	$\|-\rangle$	$\|+\rangle$	$\|1\rangle$	$\|0\rangle$	$\|-\rangle$
Bob's alphabet	x	z	x	x	z	x	z	x	z	z

4. For each qubit, Bob decides at random which alphabet (axis) to use for the measurement, z or x.

The first part of the BB84 protocol

Alice's data bits	1	0	0	0	1	1	0	1	0	1
Alice's alphabet	x	z	x	z	x	x	x	z	z	x
Transmitted qubits	$\|-\rangle$	$\|0\rangle$	$\|+\rangle$	$\|0\rangle$	$\|-\rangle$	$\|-\rangle$	$\|+\rangle$	$\|1\rangle$	$\|0\rangle$	$\|-\rangle$
Bob's alphabet	x	z	x	x	z	x	z	x	z	z
Bob's measurement	1	0	0	0	0	1	0	0	0	1

If Bob chooses the same alphabet as Alice, he gets the same bit value (if there are no eavesdroppers or noise); this happens on average for half of his choices. When Bob chooses a different axis, the resulting bit will agree with the one of Alice only half of the time, on average.

The first part of the BB84 protocol

Alice's data bits	1	0	0	0	1	1	0	1	0	1
Alice's alphabet	x	z	x	z	x	x	x	z	z	x
Transmitted qubits	$\|-\rangle$	$\|0\rangle$	$\|+\rangle$	$\|0\rangle$	$\|-\rangle$	$\|-\rangle$	$\|+\rangle$	$\|1\rangle$	$\|0\rangle$	$\|-\rangle$
Bob's alphabet	x	z	x	x	z	x	z	x	z	z
Bob's measurement	1	0	0	0	0	1	0	0	0	1
Bob's data bits	1	0	0	0	0	1	0	0	0	1

The first part of the BB84 protocol

5. Bob communicates to Alice over a classical public channel his choices of the alphabet (but not the results of his measurements!)

6. Alice communicates to Bob over a classical public channel which alphabet she used for the transmitted qubits.

7. Alice and Bob delete all bits corresponding to the cases in which they used different alphabets. The remaining bits form the “raw key”.

+ other steps to minimize the effects of **eavesdropping** and especially **noise**.

The first part of the BB84 protocol

Alice's data bits	1	0	0	0	1	1	0	1	0	1
Alice's alphabet	x	z	x	z	x	x	x	z	z	x
Transmitted qubits	$\|-\rangle$	$\|0\rangle$	$\|+\rangle$	$\|0\rangle$	$\|-\rangle$	$\|-\rangle$	$\|+\rangle$	$\|1\rangle$	$\|0\rangle$	$\|-\rangle$
Bob's alphabet	x	z	x	x	z	x	z	x	z	z
Bob's measurement	1	0	0	0	0	1	0	0	0	1
Bob's data bits	1	0	0	0	0	1	0	0	0	1
Raw key	1	0	0			1			0	

The raw key is now: 10010 (in the process, 5 bits out of 10 were lost)

- Classical bits and classical computing
- Quantum mechanics and quantum bits (qubits)
- Manipulating qubit states, unitary errors
- Quantum gates and circuits
- Quantum teleportation
- Quantum Fourier Transformation
- Quantum cryptography
- IBM Q experience

IBM Q

IBM Q:
- quantum computing for researchers, www.ibm.com/quantum-computing/

Qiskit:
- open-source quantum computing software development framework,
- qiskit.org

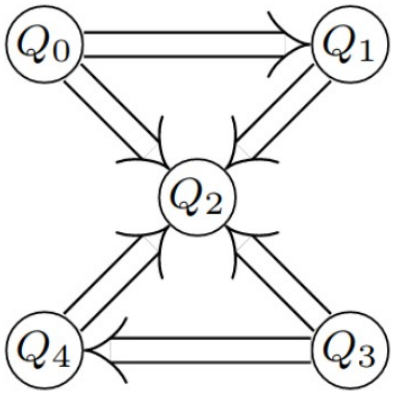
IBM Q account:
- qiskit.org/ibmqaccount

Tutorials:
- github.com/Qiskit/qiskit-iqx-tutorials.git

IBM Q

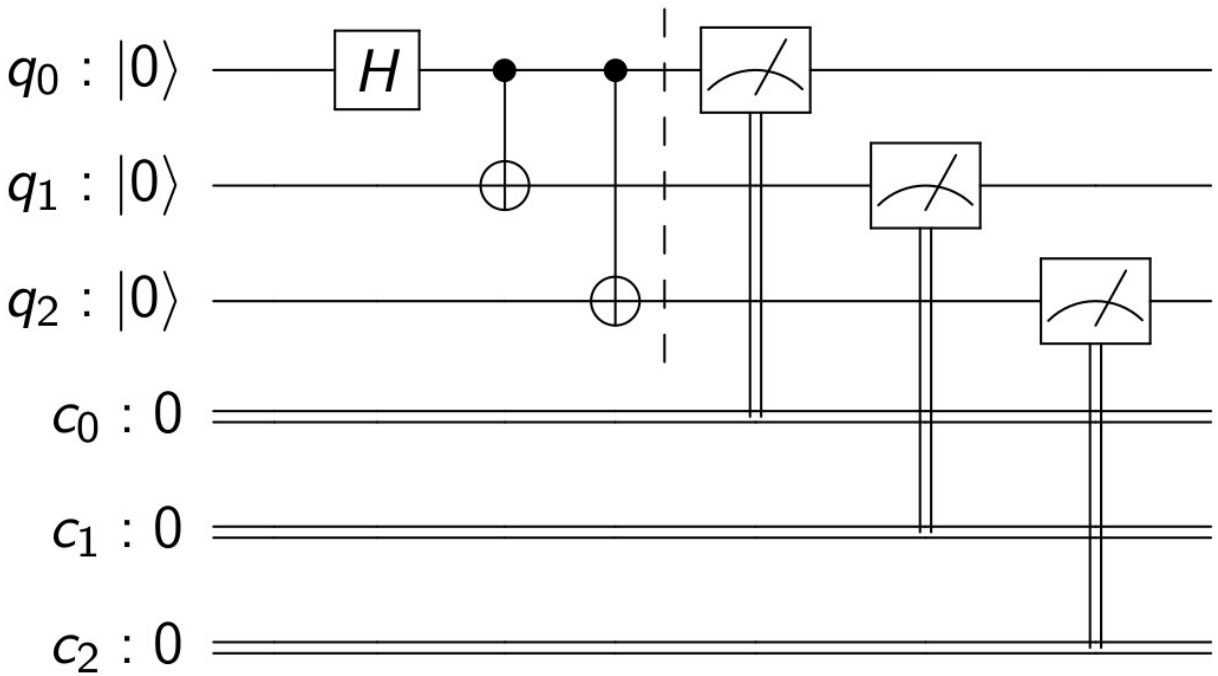
IBM Q backend **ibmqx2**:

- 5 qubits, 1024 shots



(a) *IBM QX2*

arXiv:1712.04722v3

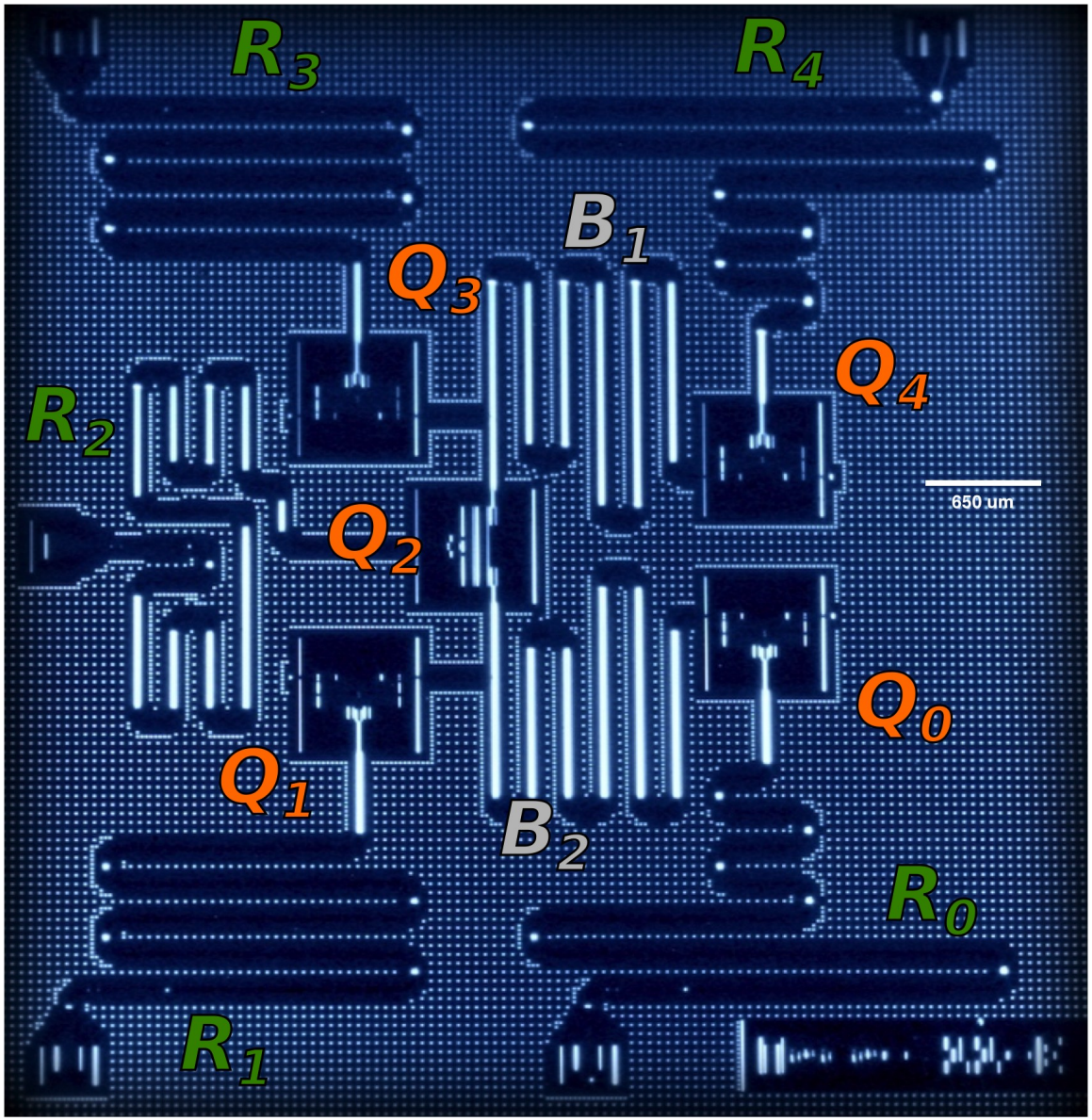


Running an example: create a 3-qubit entangled state GHZ (Greenberger-Horne-Zeilinger):

$$|GHZ\rangle = \frac{|0\rangle^{\otimes 3} + |1\rangle^{\otimes 3}}{\sqrt{2}} = \frac{|000\rangle + |111\rangle}{\sqrt{2}}$$

Device information

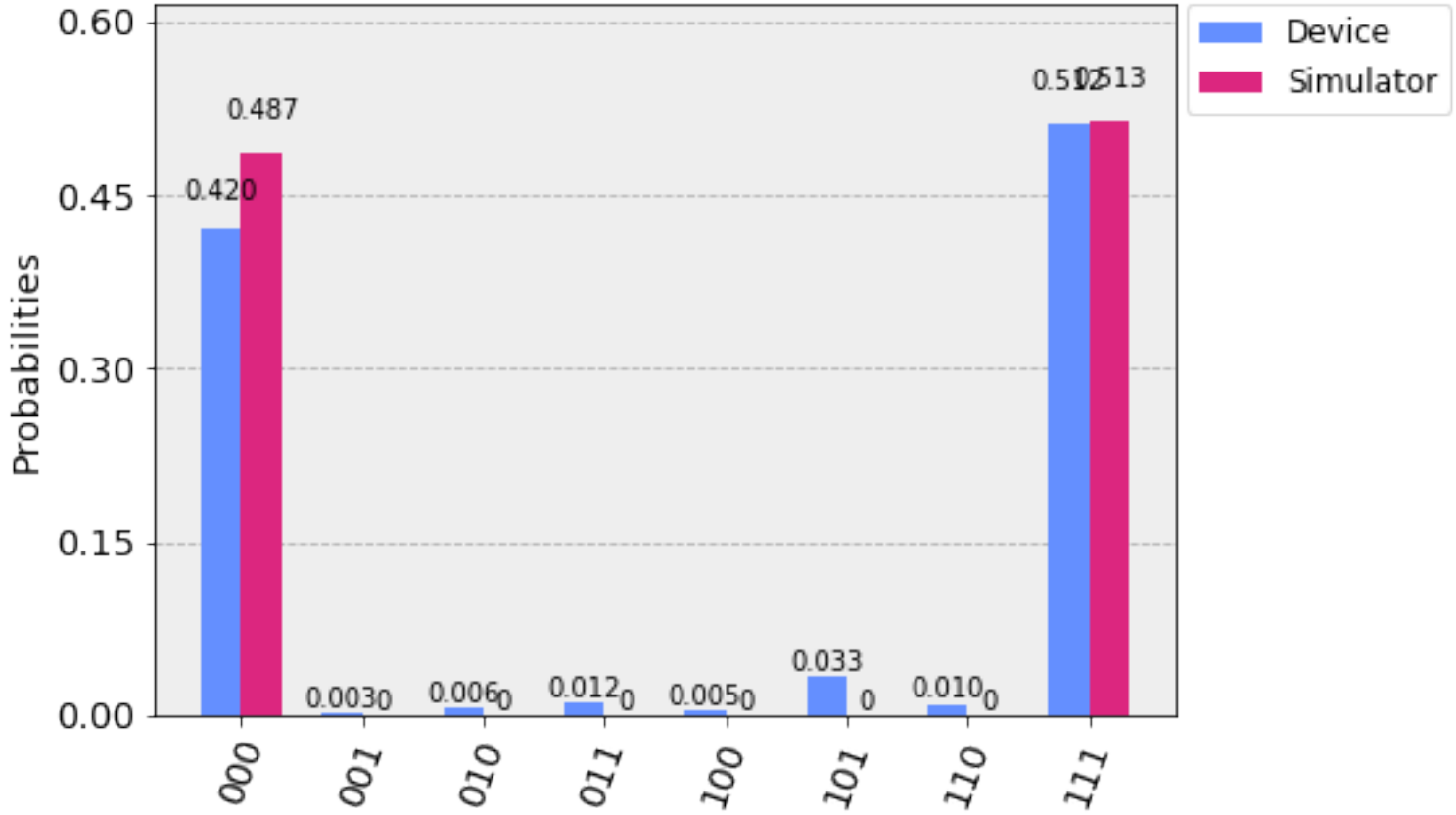
https://github.com/Qiskit/ibmq-device-information/tree/master/backends/yorktown/V1



IBM Q

We should have only states (000) and (111) but in reality we see with small probability other states.

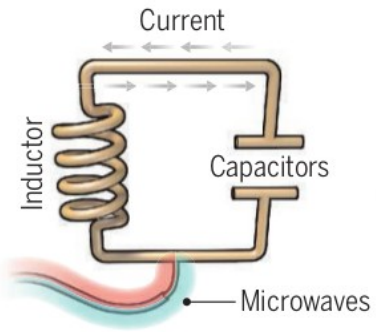
$$|GHZ\rangle = \frac{|0\rangle^{\otimes 3} + |1\rangle^{\otimes 3}}{\sqrt{2}} = \frac{|000\rangle + |111\rangle}{\sqrt{2}}$$

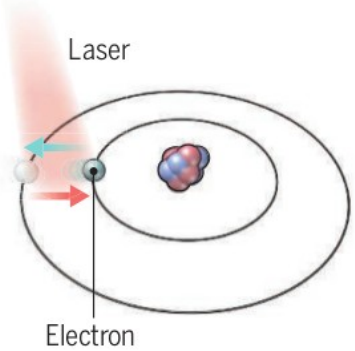


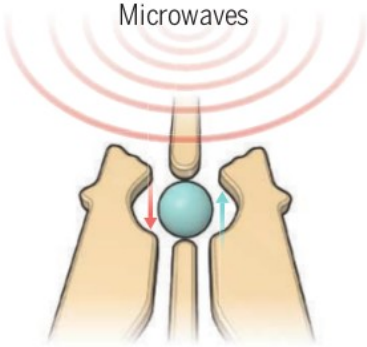
The GHZ state

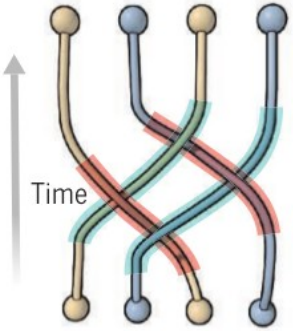
$$|\psi\rangle = \mathbf{T} + \mathbf{h} + \mathbf{a} + \mathbf{n} + \mathbf{k} + \mathbf{Y} + \mathbf{o} + \mathbf{u} + !$$

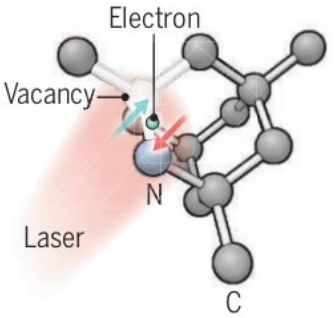
Extra slides











	Superconducting loops	**Trapped ions**	**Silicon quantum dots**	**Topological qubits**	**Diamond vacancies**
	A resistance-free current oscillates back and forth around a circuit loop. An injected microwave signal excites the current into super-position states.	Electrically charged atoms, or ions, have quantum energies that depend on the location of electrons. Tuned lasers cool and trap the ions, and put them in superposition states.	These "artificial atoms" are made by adding an electron to a small piece of pure silicon. Microwaves control the electron's quantum state.	Quasiparticles can be seen in the behavior of electrons channeled through semi-conductor structures. Their braided paths can encode quantum information.	A nitrogen atom and a vacancy add an electron to a diamond lattice. Its quantum spin state, along with those of nearby carbon nuclei, can be controlled with light.
Longevity (seconds)	0.00005	>1000	0.03	N/A	10
Logic success rate	99.4%	99.9%	~99%	N/A	99.2%
Number entangled	9	14	2	N/A	6
Company support	Google, IBM, Quantum Circuits	ionQ	Intel	Microsoft, Bell Labs	Quantum Diamond Technologies
⊕ **Pros**	Fast working. Build on existing semiconductor industry.	Very stable. Highest achieved gate fidelities.	Stable. Build on existing semiconductor industry.	Greatly reduce errors.	Can operate at room temperature.
⊖ **Cons**	Collapse easily and must be kept cold.	Slow operation. Many lasers are needed.	Only a few entangled. Must be kept cold.	Existence not yet confirmed.	Difficult to entangle.

Note: Longevity is the record coherence time for a single qubit superposition state, logic success rate is the highest reported gate fidelity for logic operations on two qubits, and number entangled is the maximum number of qubits entangled and capable of performing two-qubit operations.

Gabriel Popkin, Quest for Qubits, in Science Magazine, December 2016

AND, OR, NOT and FANOUT constitute a universal set of gates for classical computation.

Proof.
The m-bit function is equivalent to m one-bit (or Boolean) functions

$$f_i : \{0,1\}^n \to \{0,1\}, \qquad (i = 1, 2, ..., m)$$

where $f = (f_1, f_2, ..., f_m)$. For any values of the input argument $a = (a_{n-1}, a_{n-2}, ..., a_1, a_0)$, one way to compute the boolean function $f_i(a)$ is to consider the *minterms* $f_i^{(l)}(a)$, defined as

$$f_i^{(l)} = \begin{cases} 1, & \text{if } a = a^{(l)} \\ 0, & \text{otherwise} \end{cases}$$

(cont.)

for instance, if the particular value of $a^{(l)} = 110100\ldots001$, then $f_i^{(l)}$ can be defined as follows

$$f_i^{(l)} = a_{n-1} \wedge a_{n-2} \wedge \bar{a}_{n-3} \wedge a_{n-4} \wedge \bar{a}_{n-5} \wedge \bar{a}_{n-6} \wedge \ldots \wedge \bar{a}_2 \wedge \bar{a}_1 \wedge a_0$$

the one-bit function f_i can be calculated for all possible a values as follows

$$f_i(a) = f_i^{(1)} \vee f_i^{(2)} \vee \ldots \vee f_i^{(k)}$$

as the logical OR of all k minterms, with $0 \leq k \leq 2^n - 1$ (2^n is the number of all possible values of the input a). The FANOUT gate is required to feed the input a to the k minterms.

(cont.)

Consider the Boolean function $f(a)$, where $a = (a_2, a_1, a_0)$ defined as follows

	a	a_2	a_1	a_0	$f(a)$
t	$a^{(1)} = 1$	0	0	1	1
	$a^{(2)} = 3$	0	1	1	1
	$a^{(3)} = 6$	1	1	0	1
	$a^{(4)} = 0$	0	0	0	0
	$a^{(5)} = 2$	0	1	0	0
	$a^{(6)} = 4$	1	0	0	0
	$a^{(7)} = 5$	1	0	1	0
	$a^{(8)} = 7$	1	1	1	0

$$f^{(1)} = \bar{a}_2 \wedge \bar{a}_1 \wedge a_0$$

$$f^{(2)} = \bar{a}_2 \wedge a_1 \wedge a_0$$

$$f^{(3)} = a_2 \wedge a_1 \wedge \bar{a}_0$$

$$f(a) = f^{(1)}(a) \vee f^{(2)}(a) \vee f^{(3)}(a)$$

Note: we may have up to $2^3 = 8$ minterms.

The no-cloning theorem

Let us consider two qubits in the states $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ (generic) and $|\phi\rangle$ (ancillary qubit), the cloning machine in the initial state $|A_i\rangle$ and suppose there is a unitary transformation U such that:

$$U(|\psi\rangle|\phi\rangle|A_i\rangle) = |\psi\rangle|\psi\rangle|A_{f\psi}\rangle = (\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle)|A_{f\psi}\rangle$$

but at the same time we can write:

$$U(|\psi\rangle|\phi\rangle|A_i\rangle) = U((\alpha|0\rangle + \beta|1\rangle)|\phi\rangle|A_i\rangle)$$

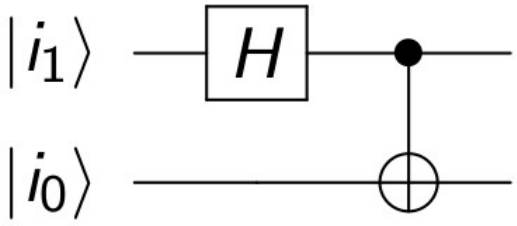
if we invoke the linearity of quantum mechanics we obtain:

$$\alpha U(|0\rangle|\phi\rangle|A_i\rangle) + \beta U(|1\rangle|\phi\rangle|A_i\rangle) = \alpha|0\rangle|0\rangle|A_{f0}\rangle + \beta|1\rangle|1\rangle|A_{f1}\rangle$$

which is the entangled state clearly different from the desired cloned state.

The Bell (EPR) basis

This circuit:



transforms the computational basis states into the Bell states:

$$|00\rangle \to |\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$|10\rangle \to |\phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

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

$$|11\rangle \to |\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

(EPR = Einstein-Podolski-Rosen, a paradox about the quantum nature of the reality)