Quantum algorithms 2021/2022

Benoit.vermersch@lpmmc.cnrs.fr
http://bvermersch.github.io

IBMQ Practicals with Julien Renard

Today’s lecture

Elements of context in computer science

Basic ideas of quantum computing

Organization of the course

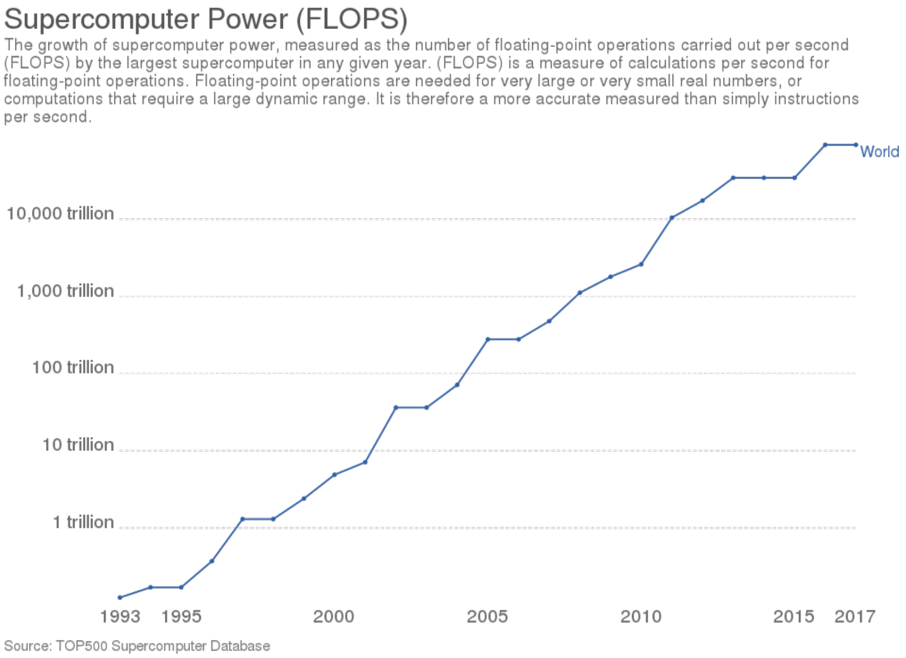
Part 1: Quantum circuits

Real quantum computers

Modern supercomputers

Exponential rise of supercomputer power

→ we may reach soon technological/financial/environmental barriers

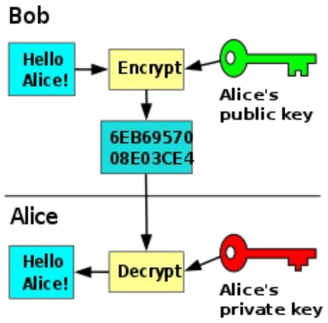


Rank	Rmax Rpeak (PFLOPS)	Name	Model
1 ▲	415.530 513.855	Fugaku	Supercomputer Fugaku
2 ▼	148.600 200.795	Summit	IBM Power System AC922
3 ▼	94.640 125.712	Sierra	IBM Power System S922LC
4 ▼	93.015 125.436	Sunway TaihuLight	Sunway MPP

Fugaku: 1 billion USD...

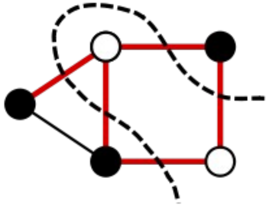
Some tough problems for computers

Factorization

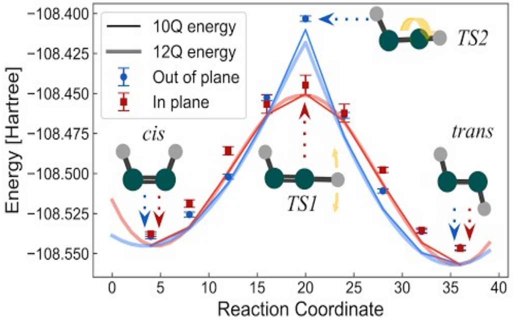


Search algorithms

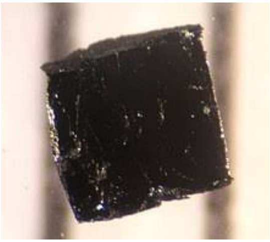
Optimization problems



Quantum chemistry

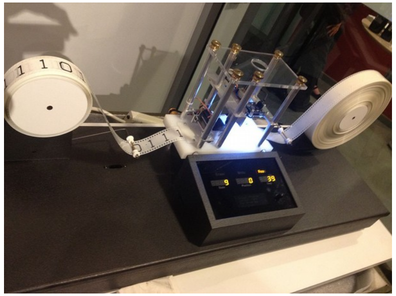


Strongly correlated quantum materials



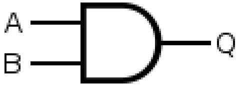
Basic concepts of computer science

- Original ideas: **Turing Machine (1936)**



- Useful formulation of models of computation: circuits of **logic gates** with **classical bits (b in [0,1])**

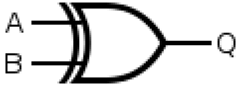
AND



INPUT		OUTPUT
A	B	Q
0	0	0
0	1	0
1	0	0
1	1	1

Q=AB

XOR



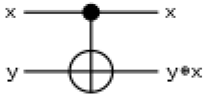
INPUT		OUTPUT
A	B	Q
0	0	0
0	1	1
1	0	1
1	1	0

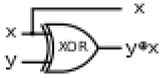
$$Q = A \oplus B$$

Basic concepts of computer science

Reversible gates: a’,b’ = f(a,b), f invertible
→ No erasure of information → no increase of entropy

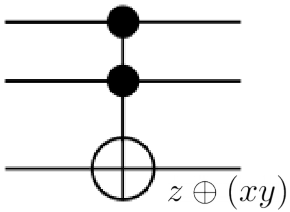
Reversible **XOR** gate
(known as CNOT in the quantum case)





input		output	
x	y	x	y+x
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

Toffoli gate



INPUT			OUTPUT		
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

The Toffoli gate is **universal** for classical computation:
Any Boolean operation on n bits can be written as a sequence of Toffolis (see TD1)

Basic concepts of computer science

Classical computational complexity: number of elementary operations to run an algorithm (on a given model of computation, ex: Turing Machine, Boolean circuit, etc)

→ **Adding two n-bit numbers:** O(n)

Example 4+7

n-bit additions

0100

0111

1011 → 11

→ Complexity O(n)

→ **Sorting n entries :** O(n^2) (comparing pairs), O(n log(n)) (Heapsort)

→ **Integer factorization of a n-bit integer:** $O\left(\exp\left[\sqrt[3]{\frac{64}{9}n\log^2(n)}\right]\right)$

Basic concepts of computer science

The complexity hierarchy of decision problems

→ Decision problems have **a yes/no answer**

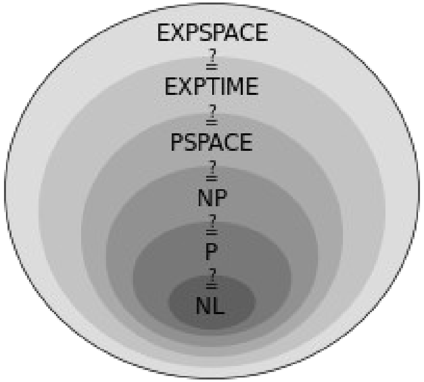
Complexity: scaling of resources (for a deterministic Turing machine)

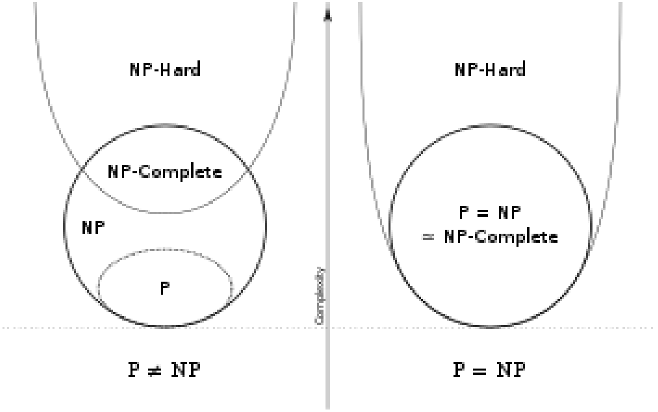
Open problem: P=NP?

Important classes

P: Problem solved in polynomial time
NP: A yes answer can be verified in polynomial time
PSPACE: Problem solved with polynomial resources
EXPTIME: Problem solved in exponential time

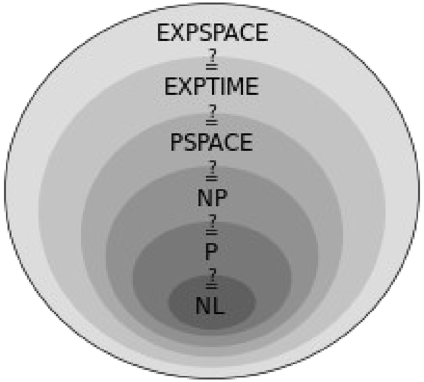
NP-HARD: Every problem in NP can be transformed into this problem in polynomial time
NP-COMPLETE: A problem that is both NP and NP-HARD





Basic concepts of computer science

Example: Factorization decision problem (F) : can a given number be factorized?



→ No polynomial time known → We do not know if F is in P

→ Solutions can be checked `easily' → F is in NP

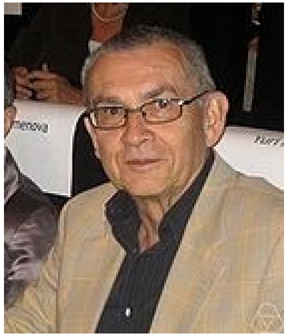
Quantum computing offers additional complexity classes

Example: **BQP** bounded-error quantum polynomial time. F is in BQP (Shor's Algorithm)

What is a quantum computer ?

Paul Benioff

Richard Feynman



Yuri Manin

David Deutsch

A quantum machine that could imitate any quantum system, including the physical world

Why can a quantum computer be powerful?

1 classical bit

$$|\psi\rangle = |0\rangle$$
$$|\psi\rangle = |1\rangle$$

1 quantum bit (qubit)

$$|\psi\rangle = c_0\,|0\rangle + c_1\,|1\rangle$$

N classical bits

$$|\psi\rangle = |00000000\rangle$$

$$|\psi\rangle = |11111111\rangle$$

2^N configurations

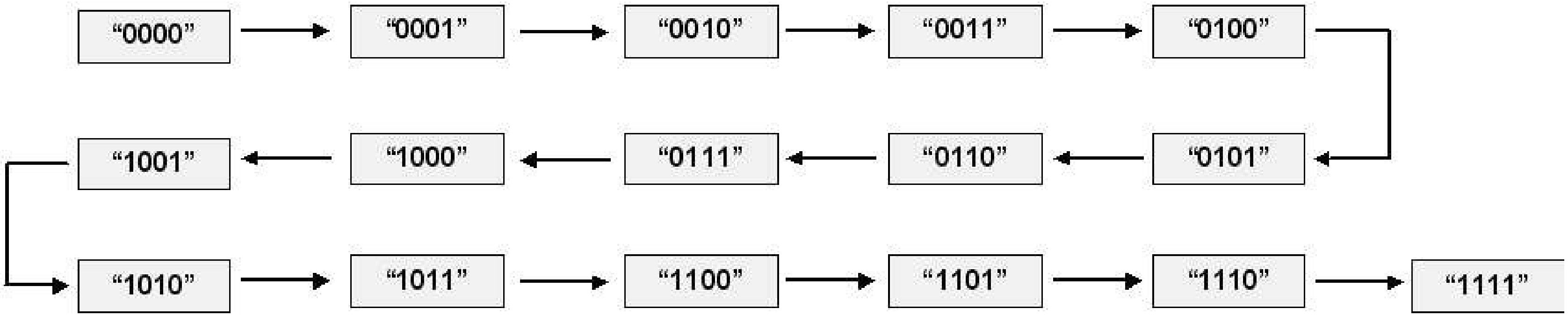
N qubits

$$|\psi\rangle = c_0\,|00000000\rangle + \cdots + c_{2^N-1}\,|11111111\rangle$$

2^N configurations
'simultaneously'

The power of quantum parallelism

Example :Exhaustive search on 4 bit keys



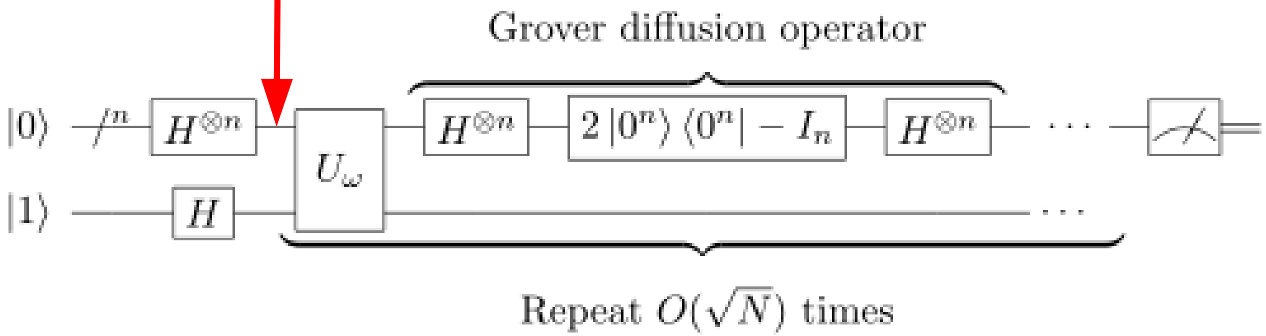
Complexity : $O(2^N)$

The power of quantum parallelism

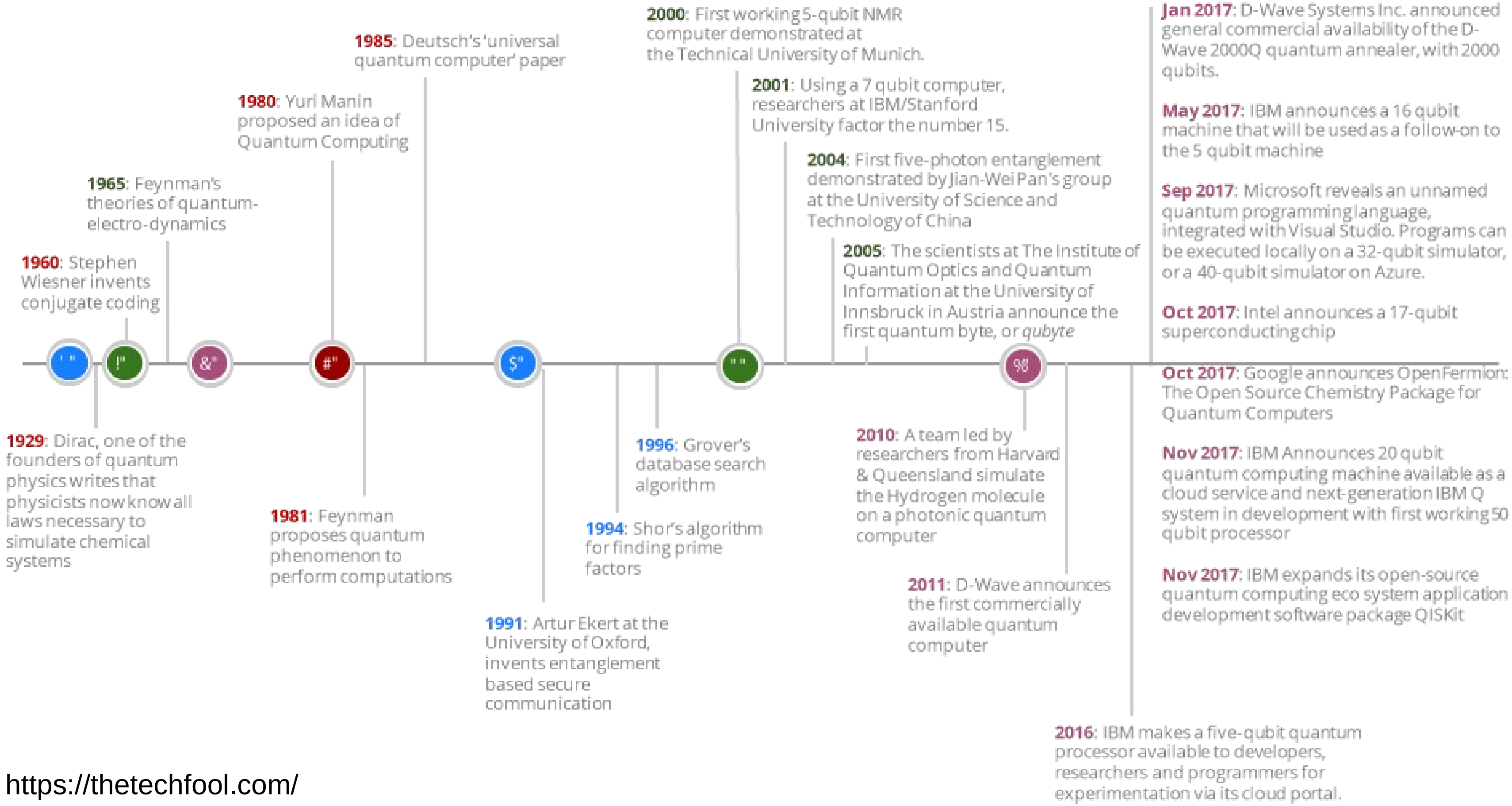
The quantum way

$$|s\rangle = \sqrt{\frac{1}{2^N}}\left(|0000\rangle + \cdots + |1111\rangle\right)$$

Grover's algorithm : We test all states simultaneously (see lecture 2)



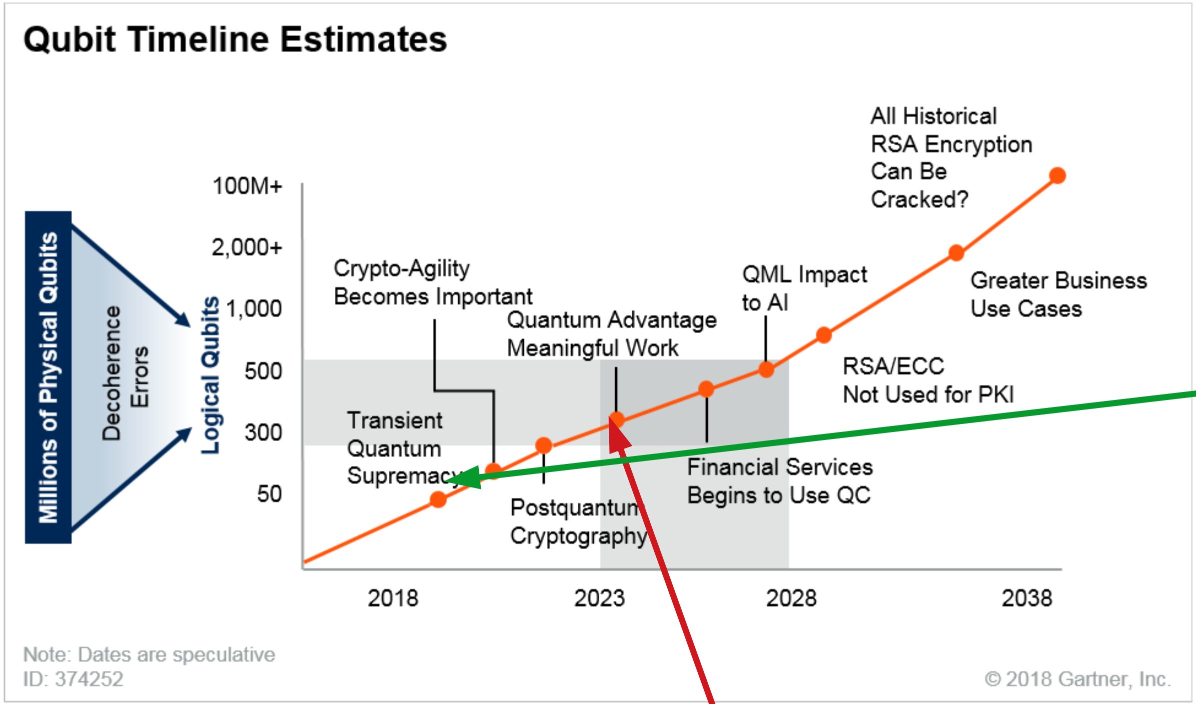
The first era of quantum computing



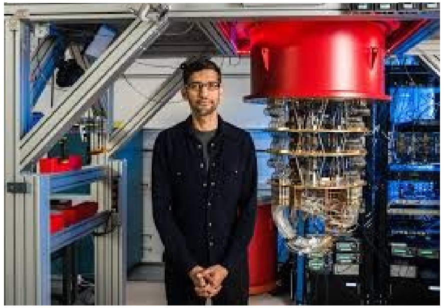
Credit: https://thetechfool.com/

The NISQ Era and beyond (2018-)

NISQ : noisy intermediate scale quantum



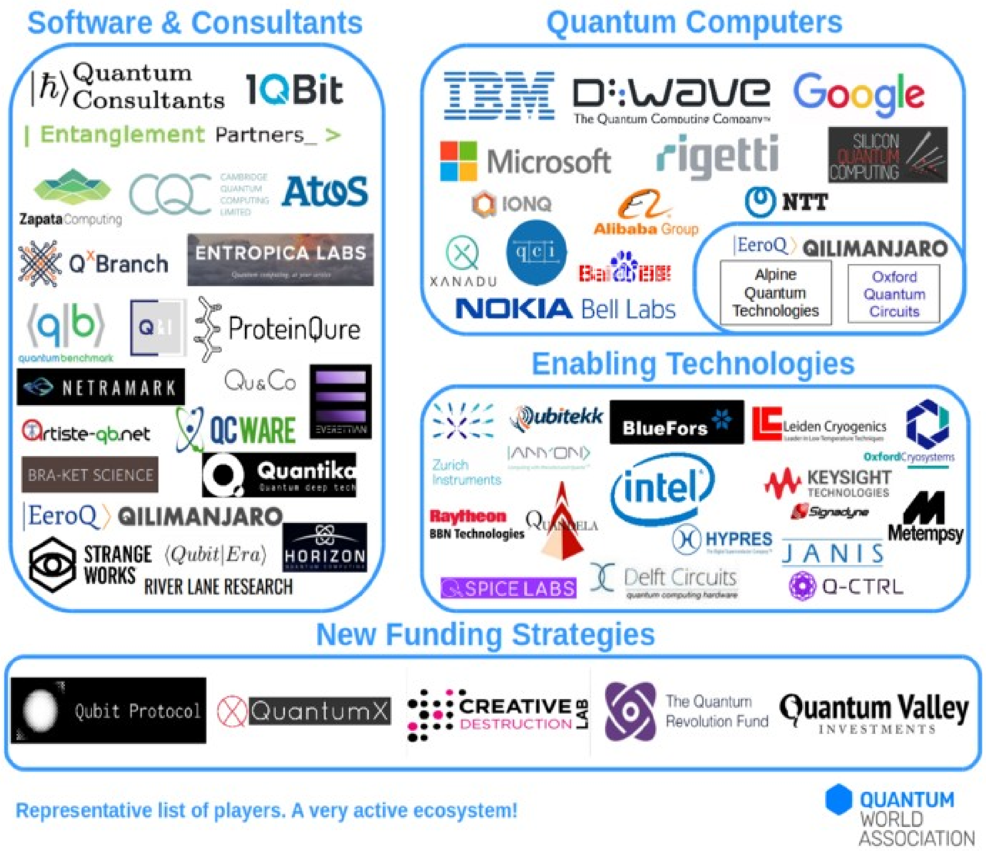
Google AI Quantum

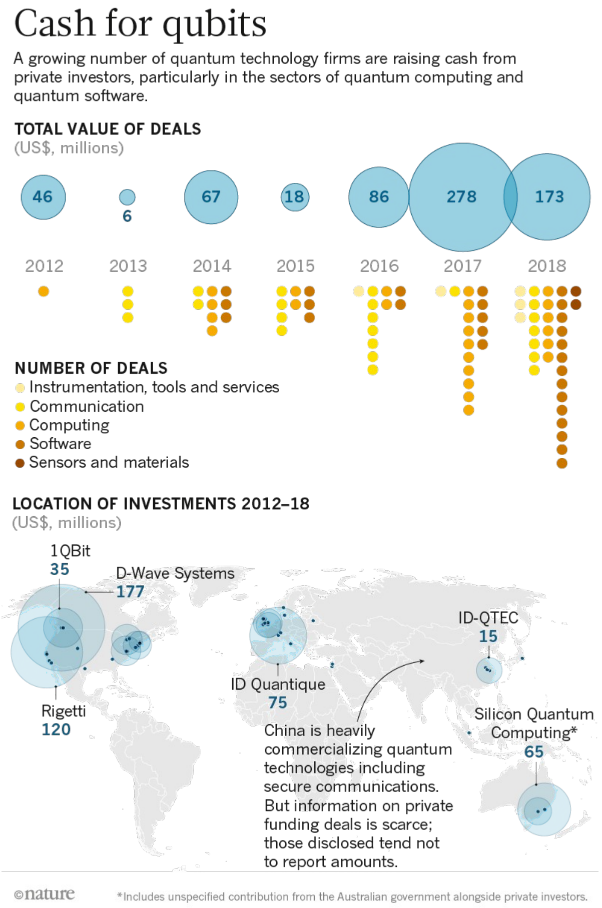


See lecture 4

The new challenge...

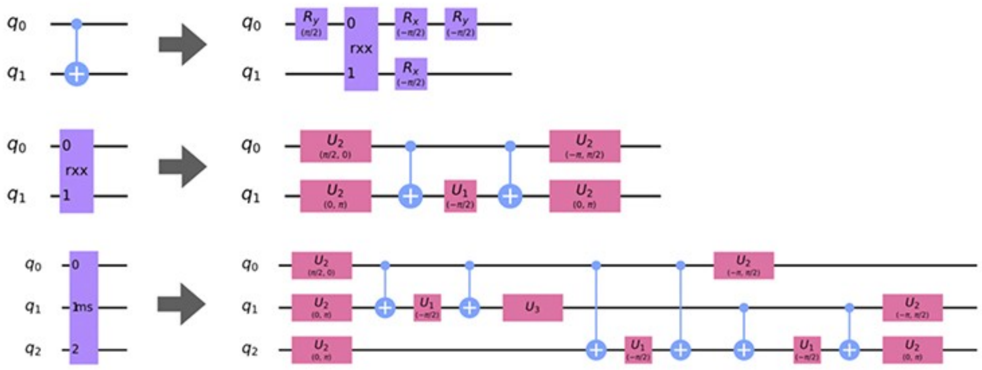
The NISQ Era and beyond (2018-)





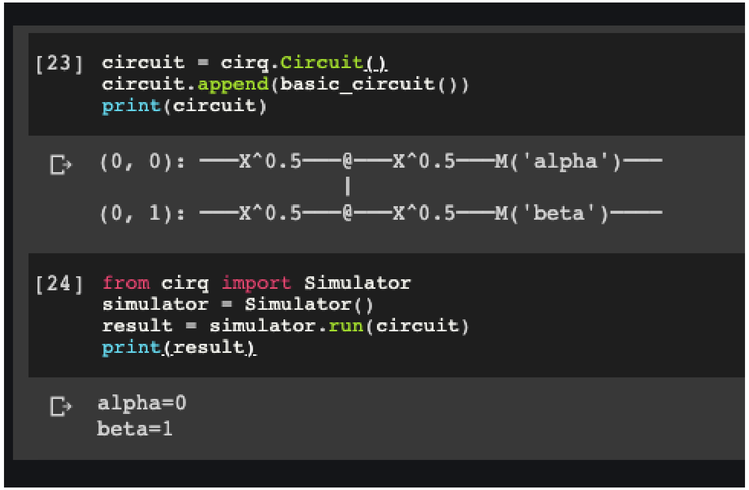
Quantum softwares

Qiskit
Elements for building a quantum future

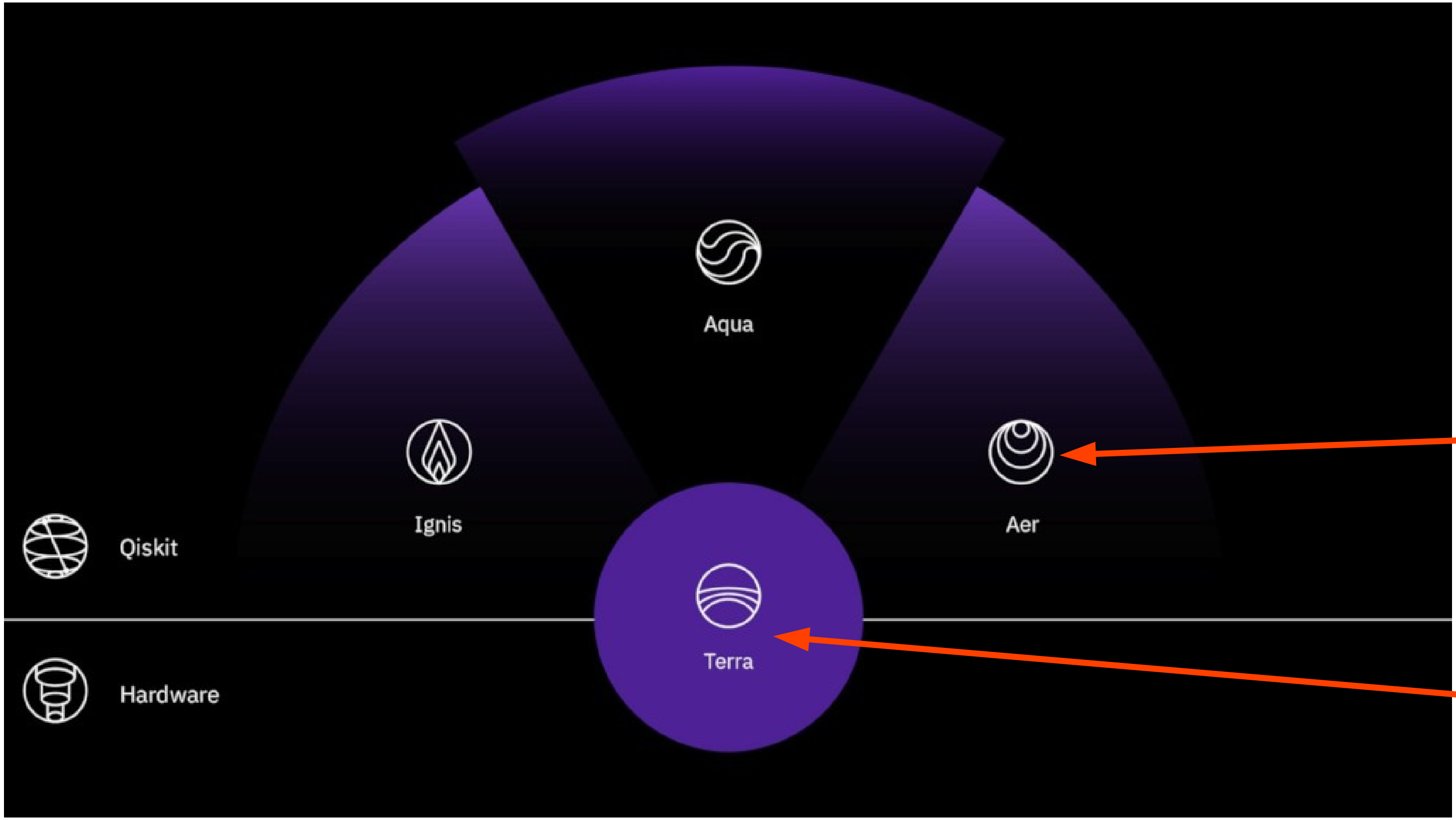


→ **IBMs practicals with Julien Renard**

Cirq



Qiskit architecture



« Simulator »

Includes
quantum hardware
(TPs with J. Renard)

Outline

- 12 Lectures/Exercices (Monday 10:15-12:15)

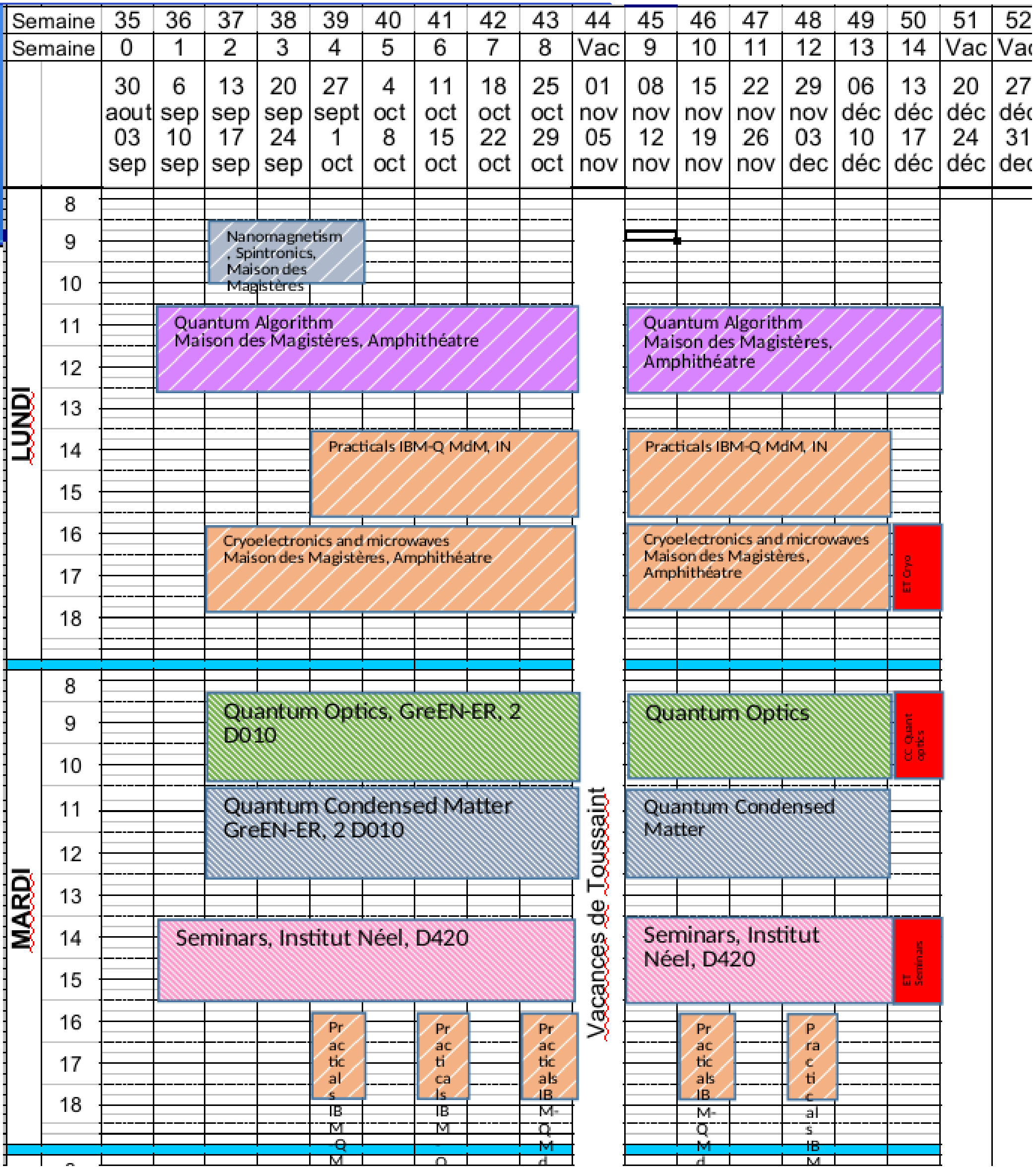
Part 1: Quantum circuits

Part 2: Quantum algorithms

Part 3: Quantum error correction

Part 4: Quantum simulation
Quantum optimization

- 5 Practical IBMQs
(4 Groups, 1 Group with J. Renard)



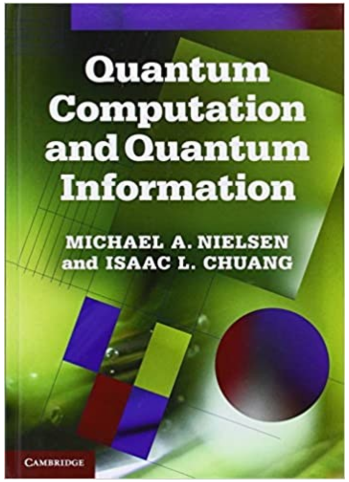
Useful references

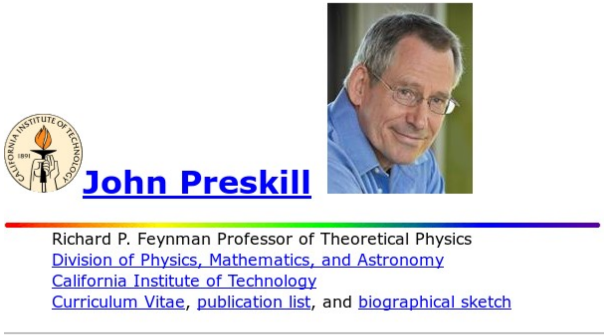
- **Quantum computation and quantum information**
  (Nielsen and Chuang)

- **John Preskill's quantum information course:**
  http://theory.caltech.edu/~preskill/ph219/index.html

- **Scott Aaronson's quantum information course:**
  https://www.scottaaronson.com/qclec.pdf

- **Quantum world II** (Zoller and Gardiner)





Moodle

Quantum algorithms

Tableau de bord › Mes cours › Quantum algorithms

Informations

Benoit Vermersch (benoit.vermersch@lpmmc.cnrs.fr)

Course start

Monday 6th of September, CNRS campus, Maison des Magistères, Mag amphitheater

Thematic and interdisciplinary project: IBM-Q practicals

Tableau de bord › Mes cours › Thematic and interdisciplinary project: IBM-Q practicals

Informations

Contacts:

Benoit Vermersch (benoit.vermersch@lpmmc.cnrs.fr)

Nicolas Roch (nicolas.roch@neel.cnrs.fr)

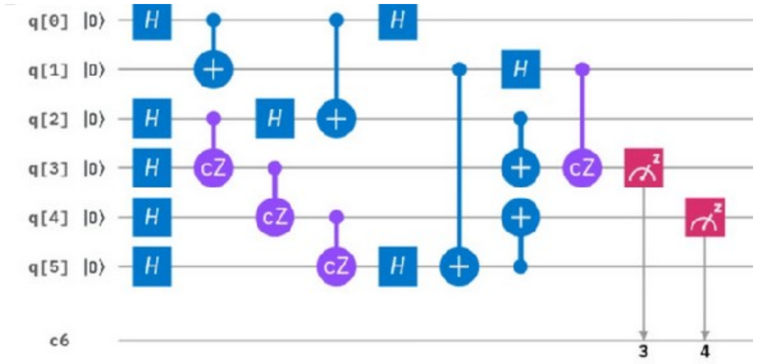
Julien Renard(julien.renard@neel.cnrs.fr)

Annonces

Course’s material also on bvermersch.github.io

Lecture 1 : Quantum Circuits

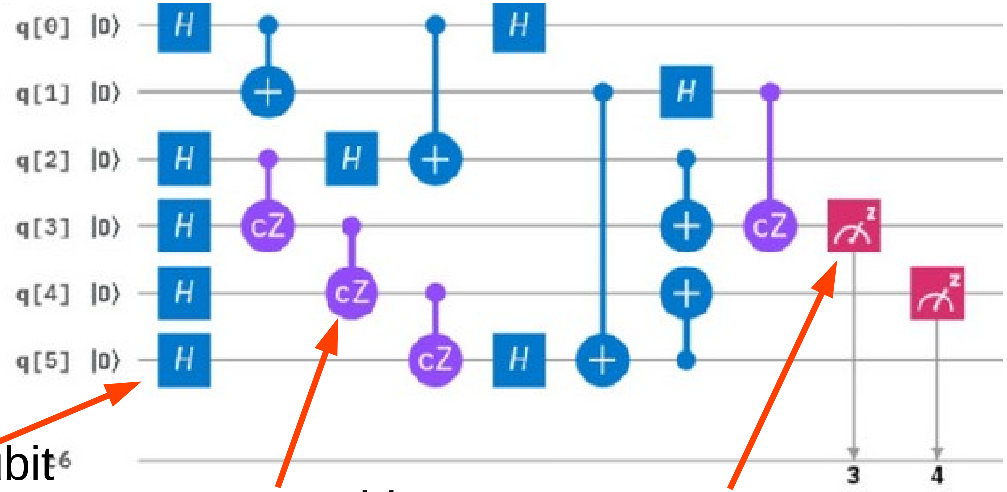
- Presentations of a quantum circuit
- Single qubit : structure and operation (gates)
- Multi-qubit case : Universal set of gates
- The Measurement
- Physical realizations



What is a quantum circuit ?

A quantum circuit executes the most common type of **quantum algorithms**

Qubits



Single qubit gate

Two-qubit gate

Measurement

time

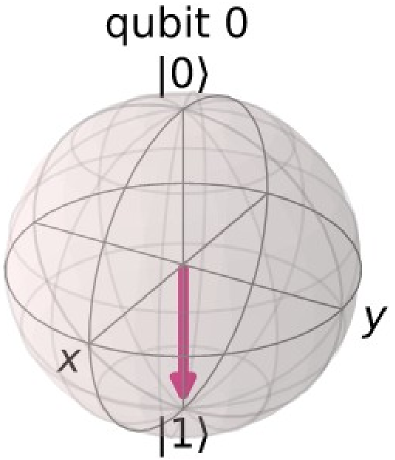
There exists other types! e.g., quantum annealing/analog quantum simulation (see Lecture 4)

Single qubit : structure and operation (gates)

A qubit is a two-level quantum system (e.g., a two-level atom)

$$|\psi\rangle = c_0\,|0\rangle + c_1\,|1\rangle = \begin{bmatrix} c_0 \\ c_1 \end{bmatrix}$$

The state of a pure single qubit state can be represented by a Bloch vector **on the Bloch sphere**

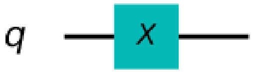


$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + \sin\left(\frac{\theta}{2}\right)e^{i\phi}\,|1\rangle$$

Classical bits are limiting cases of a qubit

Single qubit gates

A single qubit gate converts a single qubit state to another single qubit state

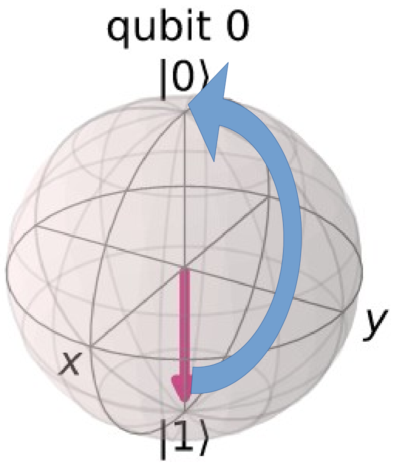


$$\longrightarrow \; |\psi'\rangle = X\,|\psi\rangle$$

It is described by a unitary 2x2 matrix

$$UU^\dagger = 1$$

Or, equivalently, by a rotation on the Bloch sphere



Important Single qubit gates

Pauli-X (X)	$-\boxed{\mathbf{X}}-$	$-\oplus-$	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \lvert 1\rangle\langle 0\rvert + \lvert 0\rangle\langle 1\rvert$
Pauli-Y (Y)	$-\boxed{\mathbf{Y}}-$		$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z (Z)	$-\boxed{\mathbf{Z}}-$		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \lvert 0\rangle\langle 0\rvert - \lvert 1\rangle\langle 1\rvert$
Hadamard (H)	$-\boxed{\mathbf{H}}-$		$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Phase (S, P)	$-\boxed{\mathbf{S}}-$		$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$ (T)	$-\boxed{\mathbf{T}}-$		$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$

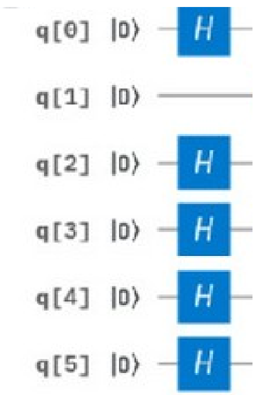
Question: How can I create an equal-weight superposition state from the logical state |0> ?

Concatenation: from left to right

Multi-qubit case

Single qubit gates can act on parallel in a tensor product space

$$|0\rangle\,|0\rangle\,|0\rangle\,|0\rangle\,|0\rangle\,|0\rangle \rightarrow H\,|0\rangle\,|0\rangle\,H\,|0\rangle\,H\,|0\rangle\,H\,|0\rangle\,H\,|0\rangle$$



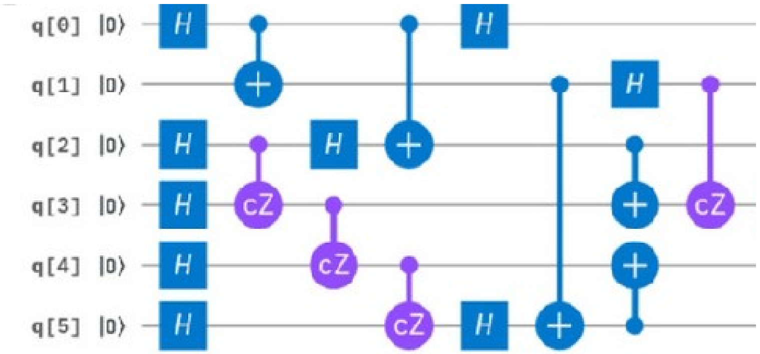
However, for a **universal quantum computer**, every global unitary operation of the 2^Nx2^N Hilbert space must be available

→ **Entangling operations required**

Multi-qubit case

Deutsch (1989):

A universal quantum computer can be realized with a set of single qubit and two qubit gates



The number of gates required to realize a certain operation is not necessarily small

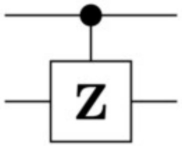
Efficient algorithms are the one that a require polynomial number of gates

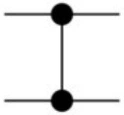
Important two-qubit gates

Controlled Not (CNOT, CX)

$$\begin{array}{cccc} |00\rangle & |01\rangle & |10\rangle & |11\rangle \end{array}$$
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = |0\rangle\langle 0| \otimes 1 + |1\rangle\langle 1| \otimes X$$

Controlled Z (CZ)





$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} = |0\rangle\langle 0| \otimes 1 + |1\rangle\langle 1| \otimes Z$$

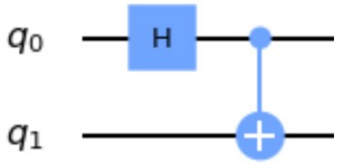
CNOT: I flip the target qubit if the control qubit is 1

CZ: minus sign if both qubits are 1

Two qubit gates generate entanglement

Creation of a Bell state

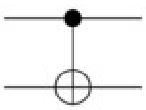
Two ingredients: Hadamard and CNOT



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

We have created a maximally entangled state!

Universal set of gates

Hadamard (H)	**H**	$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$
Phase (S, P)	**S**	$\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}$
$\pi/8$ **(T)**	**T**	$\begin{bmatrix}1 & 0\\ 0 & e^{i\pi/4}\end{bmatrix}$
Controlled Not (CNOT, CX)	 control qubit target qubit	$\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}$

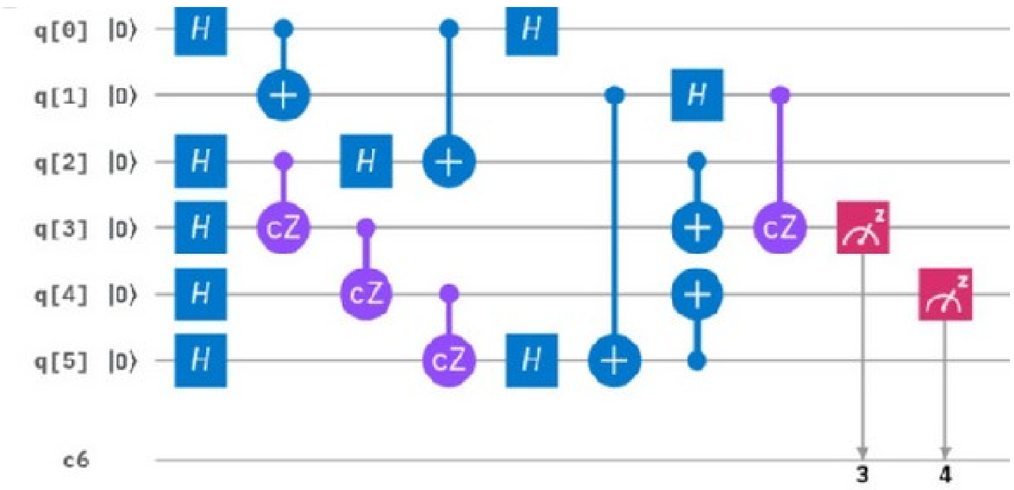
This set is not unique

With one set, I can reach any state up to arbitrary accuracy

Note: phase gate is optional here (but convenient)

Measurement

The measurement is often the last step of a quantum circuit



Mapping of quantum states to classical information (classical registers)

Very crucial step (readout errors)

Quantum operations based on measurement outcomes are possible (ex: error correction lecture 3)

Measurement

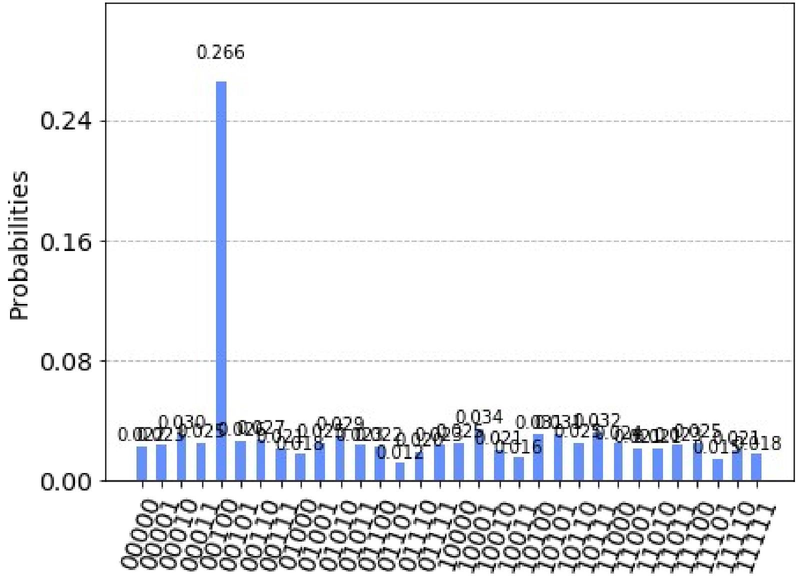
A measurement is described by a set of n measurement outcomes $(a_i)_{i=1,n}$

A quantum state is measured (and projected) in the state $|a_i\rangle$ with probability $|\langle a_i|\psi\rangle|^2$

In a quantum circuit, measurements in the `computational basis’,

Histogram obtained after 1024 repetitions of the circuit

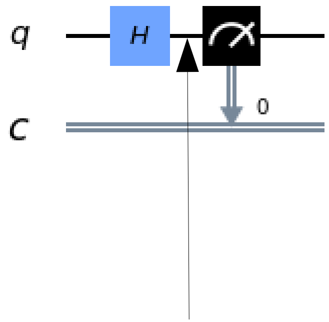
$$|\langle s|\psi\rangle|^2$$



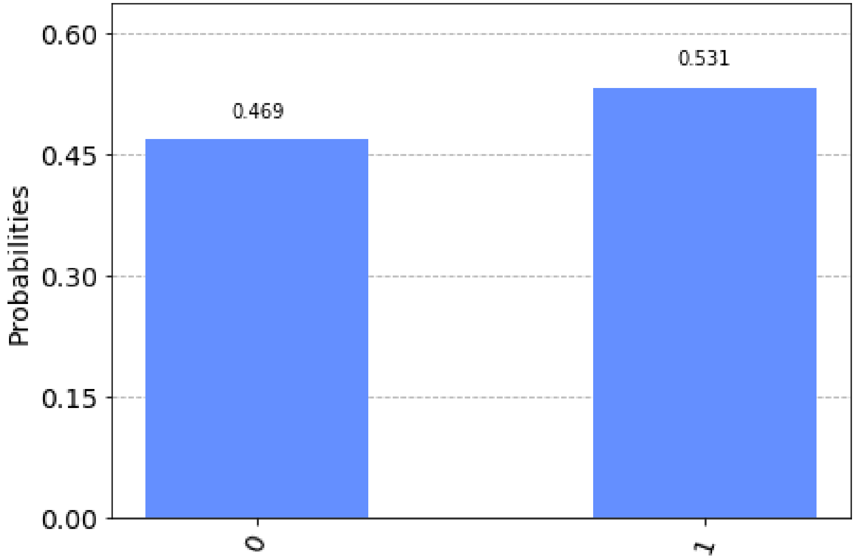
Bit string s

Measurement (examples)

Measurement of **a superposition state** (in the computational basis)



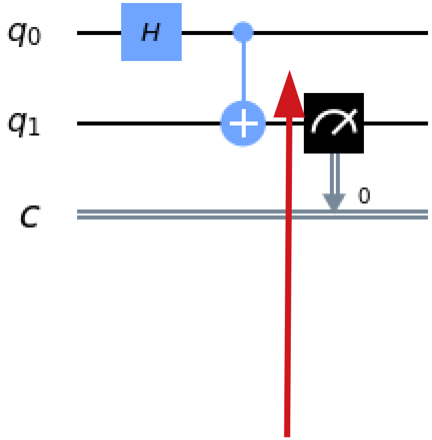
$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$



A single shot is not generically sufficient to characterize a quantum state
A single measurement basis is also not always sufficient

Measurement (examples)

Ancilla-based measurement (very important for the next lectures..)

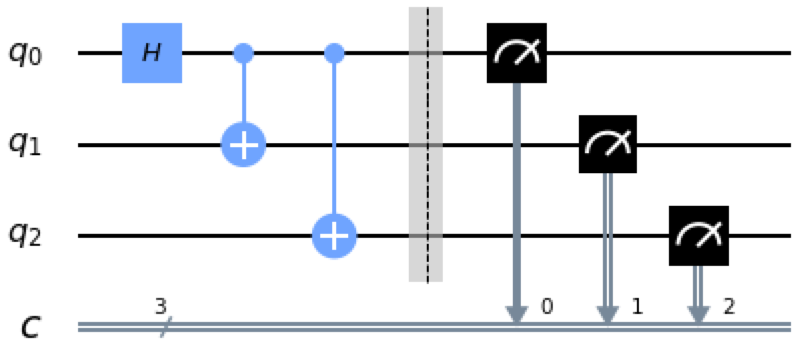


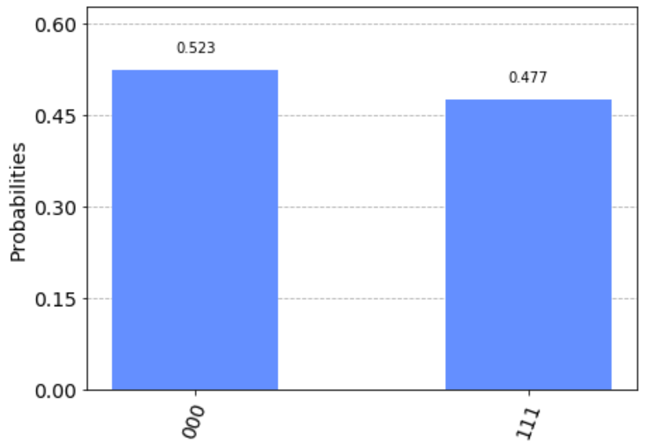
Question :
What is the final state of the first qubit q0 ???

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$ Bell state

Measurement (examples)

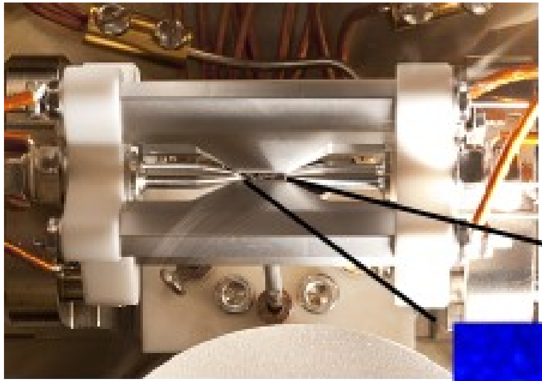
Full measurement of a multi qubit state in the computational basis

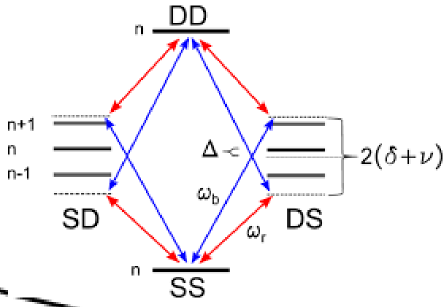


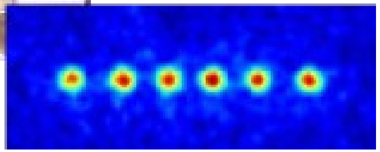


Entertainment : Real quantum computers

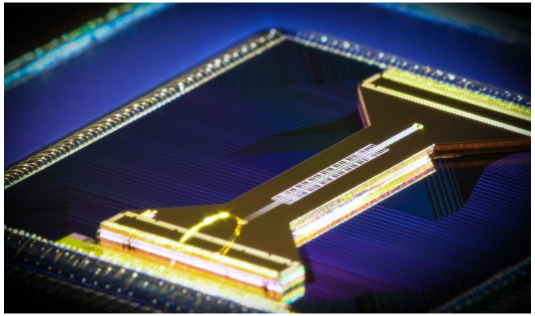
Ion traps







University of Innsbruck



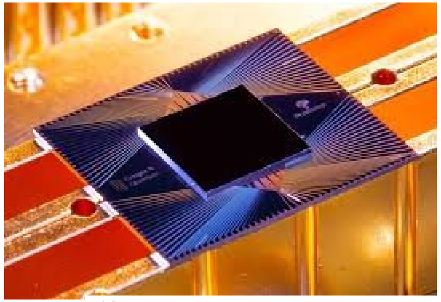
Honeywell

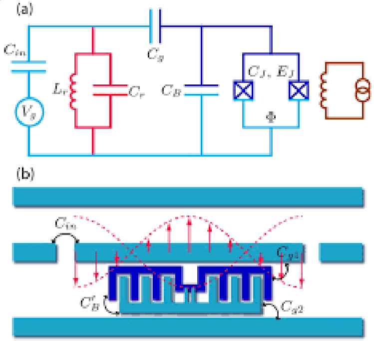
The physics of these devices can be understood from atomic physics and quantum optics

Entertainment : Real quantum computers

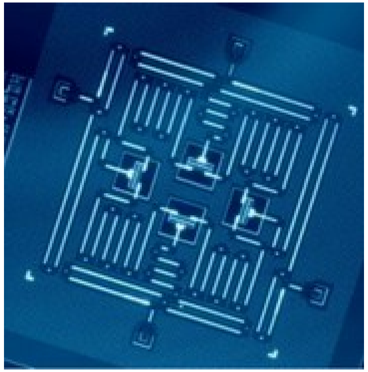
Superconducting quantum circuits

IBM Q





Google AI Quantum



The physics of these devices can be understood from solid-state physics and quantum optics

Many other platforms : NMR qubits, silicon qubits, Rydberg atoms

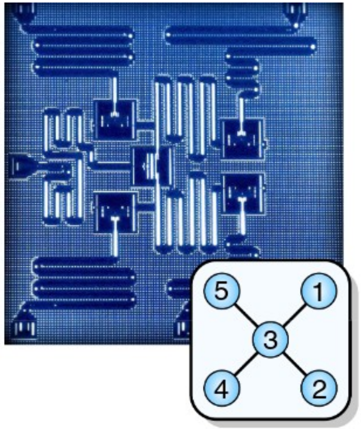
Grenoble is an important place: N. Roch, O. Buisson, T. Meunier, M. Vinet,.. **https://quantum.univ-grenoble-alpes.fr/**

Real quantum computers

Performances

Table 2. Summary of the achieved success probabilities for the implemented circuits, in percentages

Connectivity	Star shaped			Fully connected		
Hardware	Superconducting			Ion trap		
Success probability/%	Obs	Rand	Sys	Obs	Rand	Sys
Margolus	74.1(7)	82	75	90.1(2)	91	81
Toffoli	52.6(8)	78	59	85.0(2)	89	78
Bernstein–Vazirani	72.8(5)	80	74	85.1(1)	90	77
Hidden shift	35.1(6)	75	52	77.1(2)	86	57



Experimental Comparison of Two Quantum Computing Architectures," N. M. Linke, D. Maslov, M. Roetteler, S. Debnath, C. Figgatt, K. A. Landsman, K. Wright, C. Monroe, Proc. Natl. Acad. Sci. 114, 13 (2017).

Performance : Remarquable exprimental progressess, quantum computers do exist (since 2005)!

Speed : 1 Hz for trapped ions, ~10 kHz for superconducting circuits

Summary Lecture 1

- **Quantum circuits** are an architecture for developing quantum algorithms
- Basic ingredients : **qubits**, single qubit **gates** and two qubit gates (sufficient for universal quantum computation), and **measurement**
- **Different physical platforms** can now implement quantum circuits : trapped ion, superconducting quantum circuits, etc