English Course : Presentation

THE QUANTUM COMPUTING

ABAK-KALI Nizar
ROUSSEAU Sylvain

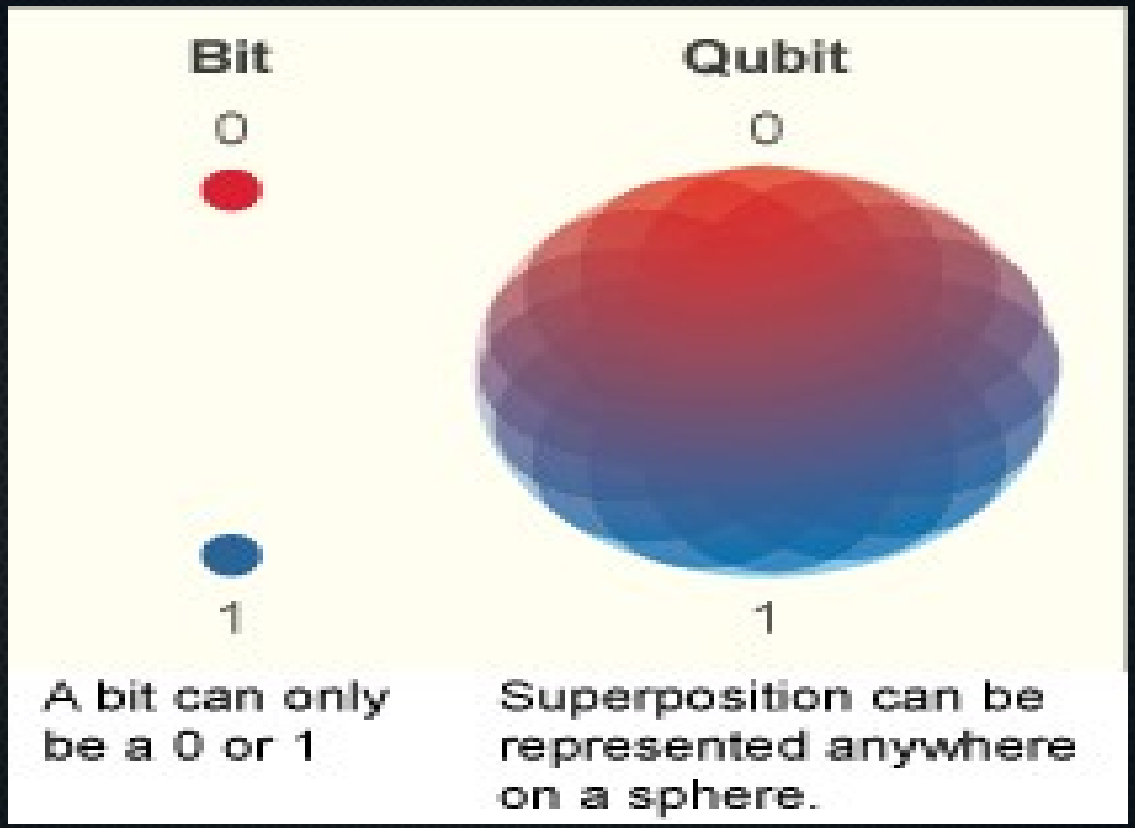
2014-2015

Introduction

Presentation Outline

- The Qubits vs the bits
- How a Qubit work ?
- The States of a Qubit
- Computation with Qubits
- Quantum algorithms
- Shor's algorithm
- Quantum computers simulators
- D-Wave Systems
- Conclusion

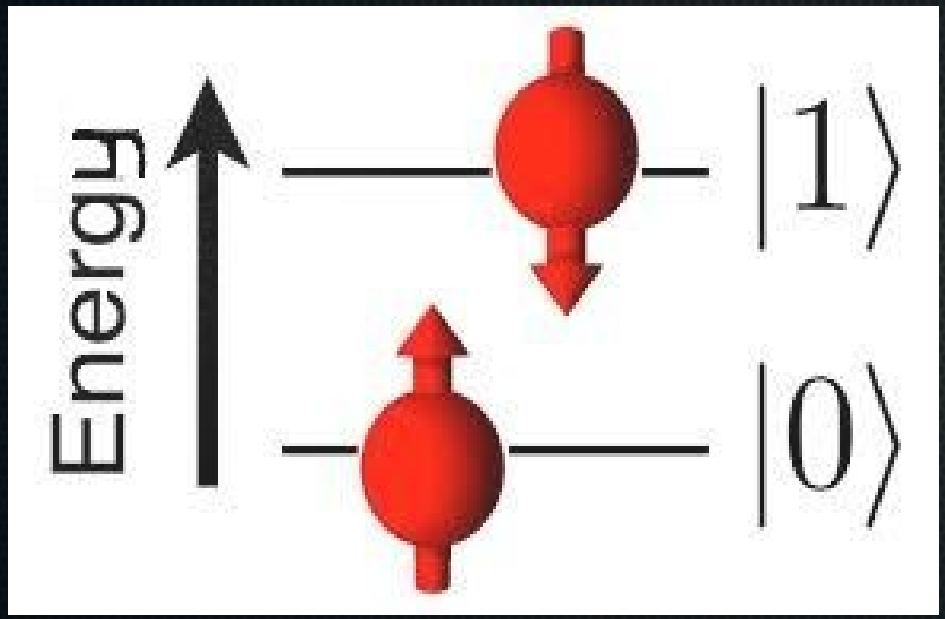
The Qubits vs the bits

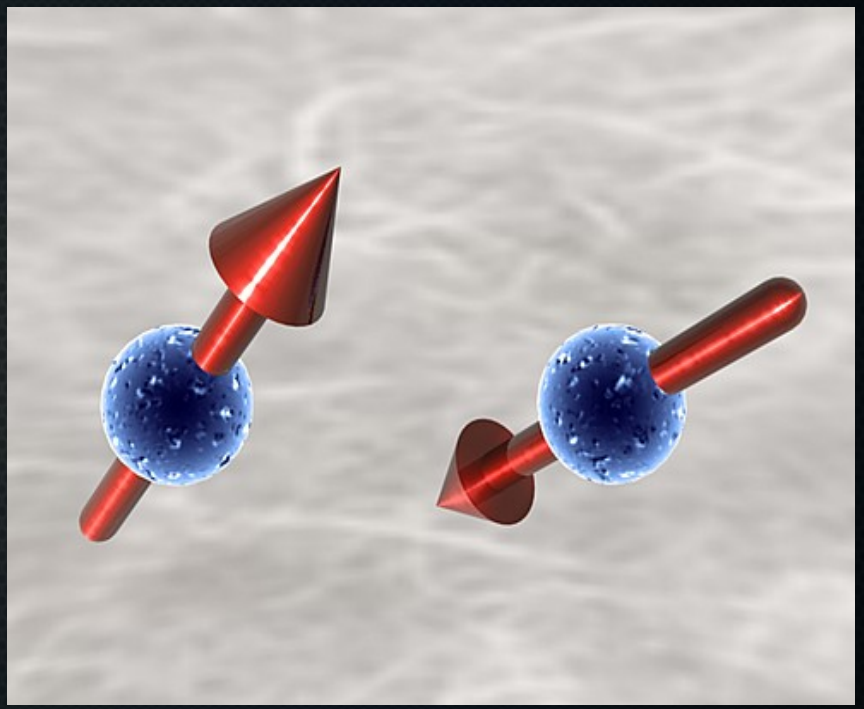


A Photon, an electron, or a nucleus are often used as qubit.

How a Qubit work ?

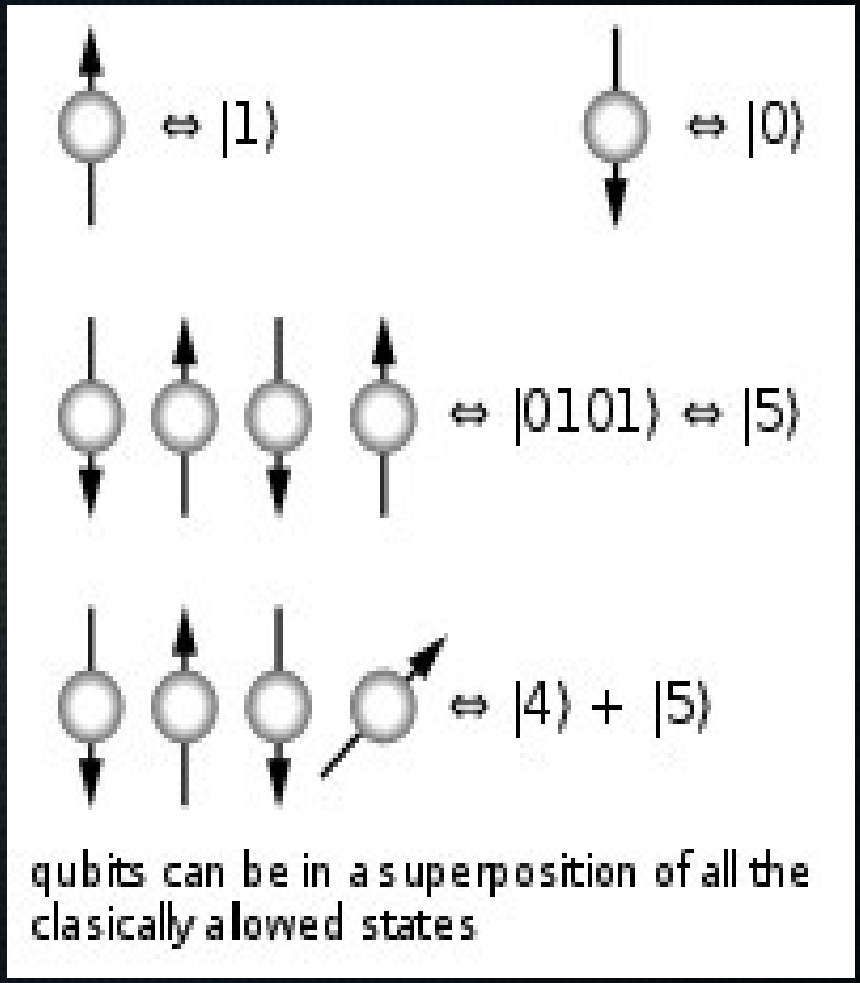
Energy states and spins





The States of a Qubit

- A qubit has the possibility to be either 1 or 0 or both .
- A qubit is a quantic particle, so his state is entangled to the state of another particle or a groupe of particles .
- There is a quantic superposition .



Computation with Qubits

- We don't know the state of a qubit until we mesure it .
- N qubits are equivalent to 2^N bits of information.
- 300 qubits are equivalent to the number of particles in the universe .

Quantum algorithms

- Shor's algorithm : integer factorization in $O((\log(n))^3)$
- Grover's algorithm : searches an unordered list (or database) in $O(\sqrt{N})$
- Quantum Fourier Transform : $O(n \log(n))$

Shor's algorithm

Let N be a composite number

1/ Pick a random number a < N

2/ If gcd(a, N) != 1 we found a factor

3/ Quantum part : find r sush as $a^{x+r} \bmod N \equiv a^{x} \bmod N$ (period)

4/ If r is odd or $a^{r/2} \equiv -1 \pmod N$, pick another a

5/ $\gcd(a^{r/2} \pm 1, N)$ is a nontrivial factor of N

Quantum computers simulators

- Online : http://www.quantumplayground.net/
- C/C++ : CHP, Q++, QCLib, QuIDDPro, Shor's Algorithm Simulation
- CaML : Q-gol

D-Wave Systems

Conclusion

- Qubit will allow us to resolve problems unresolved before, very quickly .
- At the same time, all form of security will be useless .