SCIENCES INFORMATIQUES

Les algorithmes à l'ère du calcul quantique

Yassine Hamoudi

LaBRI université de BORDEAUX

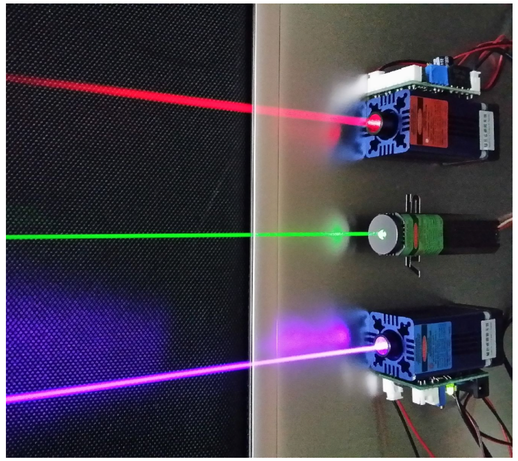
→ 08/10/2025

Qu’est-ce qu’un ordinateur quantique ?

Machines à « effets quantiques »

Émission stimulée

- Laser
- Horloge atomique, GPS



Effet tunnel

- Mémoire flash
- Microscope à effet tunnel



Résonance magnétique

- IRM
- Spectroscopie RMN



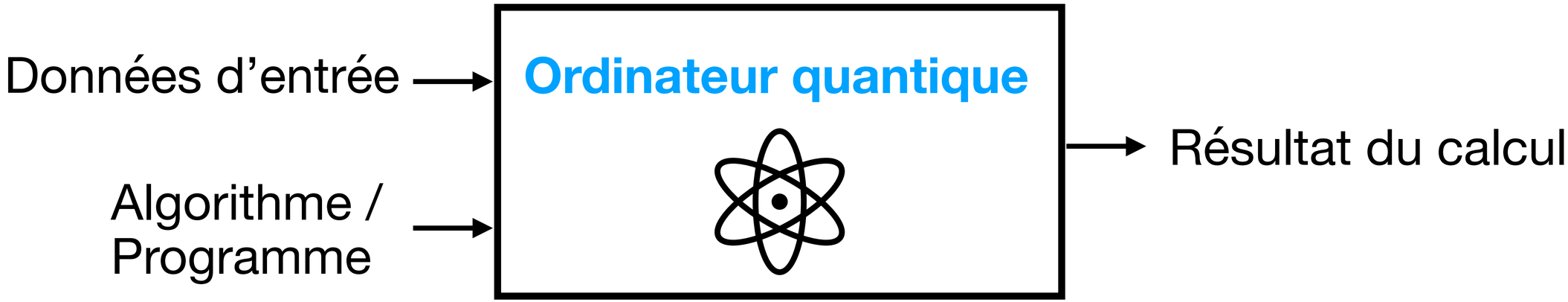
Effets photoélectrique & photovoltaïque

- Panneau solaire
- Capteur photographique CCD



L’ordinateur quantique

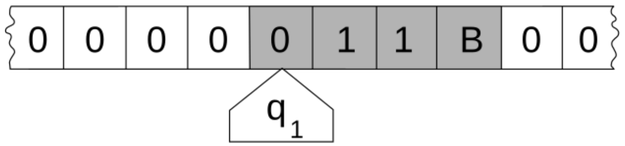
Un dispositif physique qui exploite les lois de la mécanique quantique pour effectuer des calculs sur des données



Exemples de tâches calculatoires : trouver les solutions entières de l’équation $x^2 - 511y^2 = 1$, simuler la molécule FeMoco, trouver les facteurs premiers de $2^{1550019073} - 1$

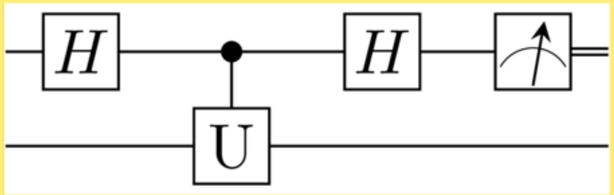
Comment construire (*mathématiquement*) un ordinateur quantique ?

Plusieurs modèles mathématiques très précis pour exprimer le comportement attendu des ordinateurs quantiques :



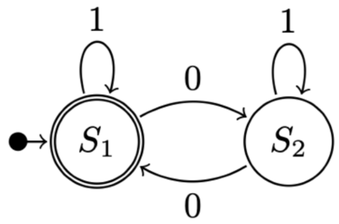
Machines de Turing quantiques

(~1980-85)



Circuits quantiques

(~1989-93)



Automates finis quantiques

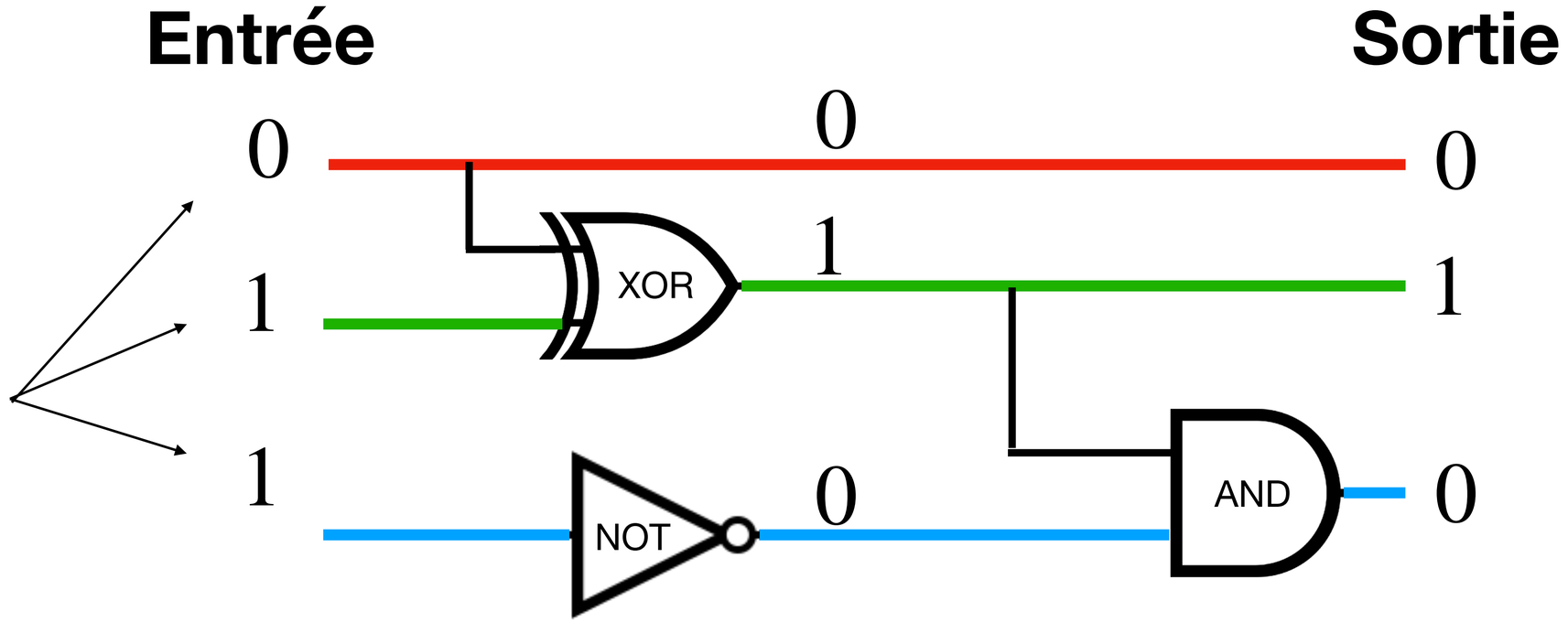
(~1997-2000)

…

Les circuits classiques

Un ordinateur classique peut être modélisé comme une suite d'opérations booléennes agissant sur des bits de mémoire

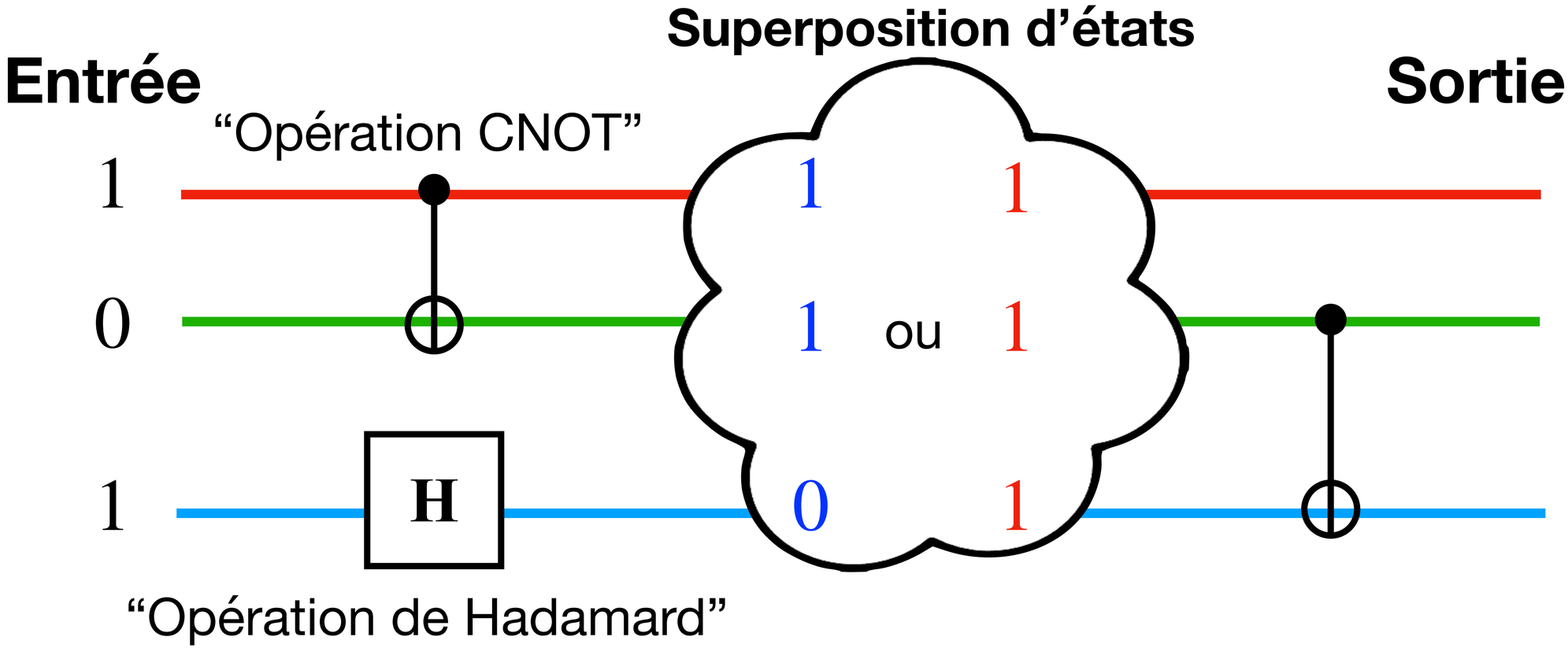
Chaque ligne représente un bit de mémoire



Les circuits quantiques

quantique

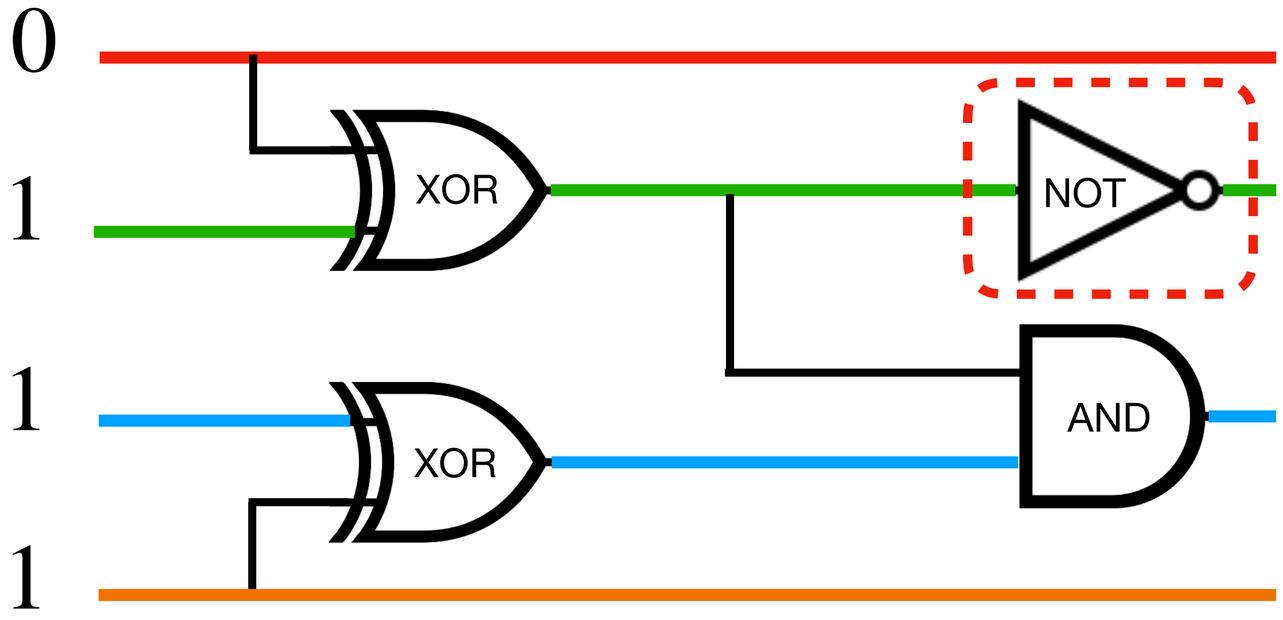
Un ordinateur ~~classique~~ peut être modélisé comme une suite d'opérations ~~booléennes~~ unitaires agissant sur des ~~bits~~ qubits de mémoire



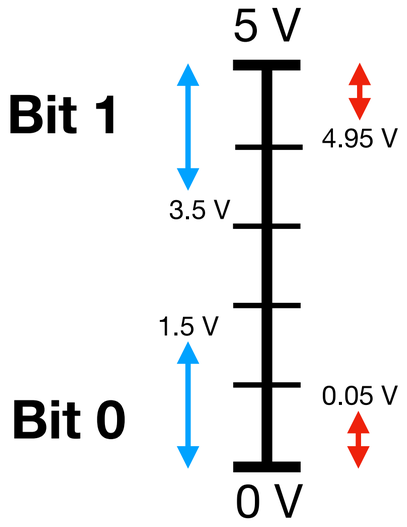
Comment construire (*physiquement*) un ordinateur quantique ?

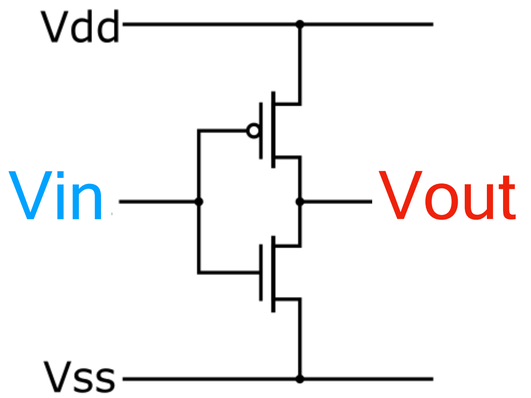
L’ordinateur classique

Plusieurs technologies sont capables de simuler très précisément les modèles mathématiques (ex : les transistors)



Opération NOT





Inverseur CMOS

L’ordinateur quantique

Pas encore de technologies permettant de reproduire
les modèles mathématiques à grande échelle

Des défis majeurs :

- imperfections dans l’implémentation des qubits et des opérations (bruit)
- effets de décohérence (perte incontrôlée des propriétés quantiques)

… à la fois en recherche théorique, expérimentale et ingénierie

- trouver des codes correcteurs d’erreurs quantiques efficaces
- construire des qubits de bonne qualité
- …

Les promesses du calcul quantique

Propriétés prédites par les modèles mathématiques :

1. Résolution plus rapide de certains problèmes grâce aux algorithmes quantiques
2. Nouvelles tâches cryptographiques impossibles à réaliser sur des ordinateurs classiques (échange de clé, protection contre les copies…)
3. Réseaux informatiques améliorés (communications plus sécurisées, meilleurs algorithmes distribués…)

…

Un exemple plus en détails :

La simulation de systèmes quantiques

Objectif : Simuler un système physique qui évolue suivant les lois de la mécanique quantique et prédire ses propriétés

Une des grandes motivations originelles du calcul quantique :

“If you want to make a simulation of Nature,
you’d better make it quantum mechanical.”

Feynman, 1981

Nombreuses applications: chimie (conception de médicaments, matériaux pour batteries…), physique de la matière condensée, physique des hautes énergies…

Équations fondamentales

Mécanique classique

État classique : $(\vec{x}(t), \vec{v}(t))$

Position Vitesse

Deuxième loi de Newton

$$\sum_k F_k = \frac{d\vec{v}(t)}{dt} \quad \text{et} \quad \vec{v}(t) = \frac{d\vec{x}(t)}{dt}$$

Forces extérieures

Mécanique quantique

État quantique : $\vec{\psi}(t)$

Fonction d'onde

Équation de Schrödinger

$$i\frac{d\vec{\psi}(t)}{dt} = H\ \vec{\psi}(t)$$

Hamiltonien du système
(énergie totale)

Simulation hamiltonienne

Équation de Schrödinger

$$i\frac{d\vec{\psi}(t)}{dt} = H\ \vec{\psi}(t)$$

Solution

$$\vec{\psi}(t) = e^{-iHt}\ \vec{\psi}(0)$$

Matrice

En général, les ordinateurs classiques ont besoin d'un temps exponentiel pour calculer la solution (exponentiation de matrice) :

Système composé de n particules/qubits $\Rightarrow$ H est une matrice $2^n \times 2^n$

Lorsque l'hamiltonien H est « raisonnable », il existe un circuit quantique qui construit une représentation quantique de $\vec{\psi}(t)$ très rapidement

(*temps polynomial en n et t*)