Introduction à l'informatique quantique

ADRIAN TANASĂ

LABRI

Talence

Plan du cours d'aujourd'hui

- Aperçu du cours "Introduction à l'informatique quantique"
- Motivation pour l'informatique quantique
- Un peu d'historique
- Plan du cours

C'est quoi l'information quantique et le calcul quantique ?

Le calcul quantique et l'information quantique sont l'étude de taches de traitement de l'information qui peuvent être accomplie en utilisant de systèmes quantiques

plutôt simple, n'est-ce pas ? :)

idée simple mais très profonde

Important :

un ordinateur quantique n'est pas simplement un ordinateur plus rapide sur lequel on va faire tourner son système d'exploitation préféré, mais un ordinateur qui permet une nouvelle manière de concevoir les algorithmes - *les algorithmes quantiques*

Ordinateurs classiques et bits

Un ordinateur classique - utilisation du binaire (0 ou 1)

bit - facile à représenter de point de vue électrique :

1. si le courant passe : 1
2. si le courant passe pas : 0

Tout calcul effectué par un ordinateur se décompose en une suite d'opérations qui agissent sur l'état de quelques bits à la fois

algorithme : suite d'instructions permettant de traiter et de manipuler de bits
les portes logiques : les briques de base pour manipuler l'information sous forme binaire - opération élémentaires qui permet d'agir sur le bits
la porte NOT : inverse la valeur du bit
une entrée (E) et une sortie (S)

E	S
0	1
1	0

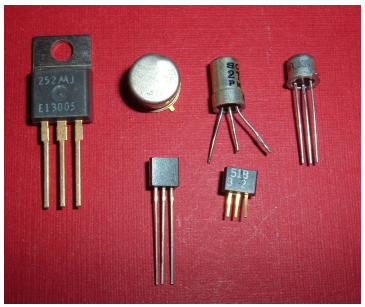
(1)

la porte ET : deux entrées (E_1 et E_2) et une sortie (S)

E_1	E_2	S
0	0	0
0	1	0
1	0	1
1	1	1

avec quelques types de portes on peut faire un ordinateur

on sait fabriquer physiquement les portes logiques (en utilisant notamment de transistors)



Par ArnoldReinhold — Travail personnel, CC BY-SA 3.0,

https ://commons.wikimedia.org/w/index.php ?curid=409337

exemple : une porte logique AND est réalisé avec 2 transistors

les microprocesseurs peuvent contenir jusqu'à plusieurs milliards de transistors

limitation ordinateurs classiques : les systèmes physiques peuvent être dans une seule état à la fois

Avant le bit quantique, le bit probabiliste

$$(p, q)$$

$$p, q \in [0, 1]$$

$$p + q = 1$$

Ordinateur quantique et qubits

un ordinateur classique manipule des bits, qui valent 0 ou 1
l'ordinateur quantique manipule de *bits quantiques* ou de *qubits*,
de bits qui obéissent aux lois de la mécanique quantique

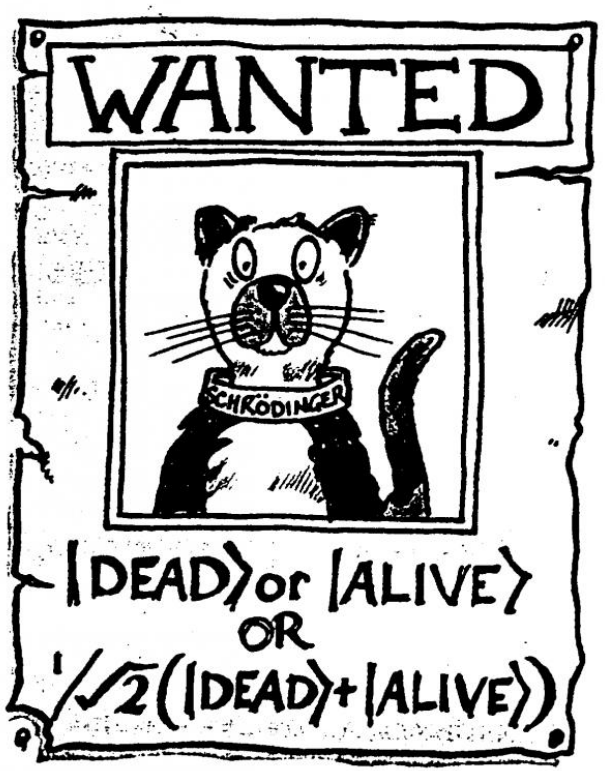
Principe de superposition

Les qubits obéissent principalement à un principe fondamental, le principe de superposition

Principe de superposition : un objet quantique peut se retrouver en super-position de plusieurs états - le qubit n'est pas seulement soit dans l'état 0 soit dans l'état 1, mais il peut être dans une superposition de ces deux états ("dans les deux états à la fois")

Le chat de Schrödinger

Le chat de Schrödinger - "à la fois mort et vivant"



il faut pas prendre cela littéralement - les chats sont trop gros pour être des objets quantique

Décohérence

Décohérence : passage du monde quantique au monde classique

plus un système physique interagit avec son environnement (comme c'est le cas pour les objets macroscopiques), plus les phénomènes quantiques s'estompent

Représentation d'un qubit - sphère de Bloch

$|\psi>$ - un état d'un système quantique à 2 niveaux (tel qu'un qubit)
décomposition du vecteur :

$$|\psi>=\alpha|0>+\beta|1>$$

avec

$$\alpha^2+\beta^2=1, \text{ et } \alpha,\beta\in\mathbb{C}$$

Représentation d'un qubit - sphère de Bloch

un nombre complexe est donnée par un module et une phase

les facteurs de phase n'affectent pas l'état physique d'un système, sans perte de généralité : α réel positif

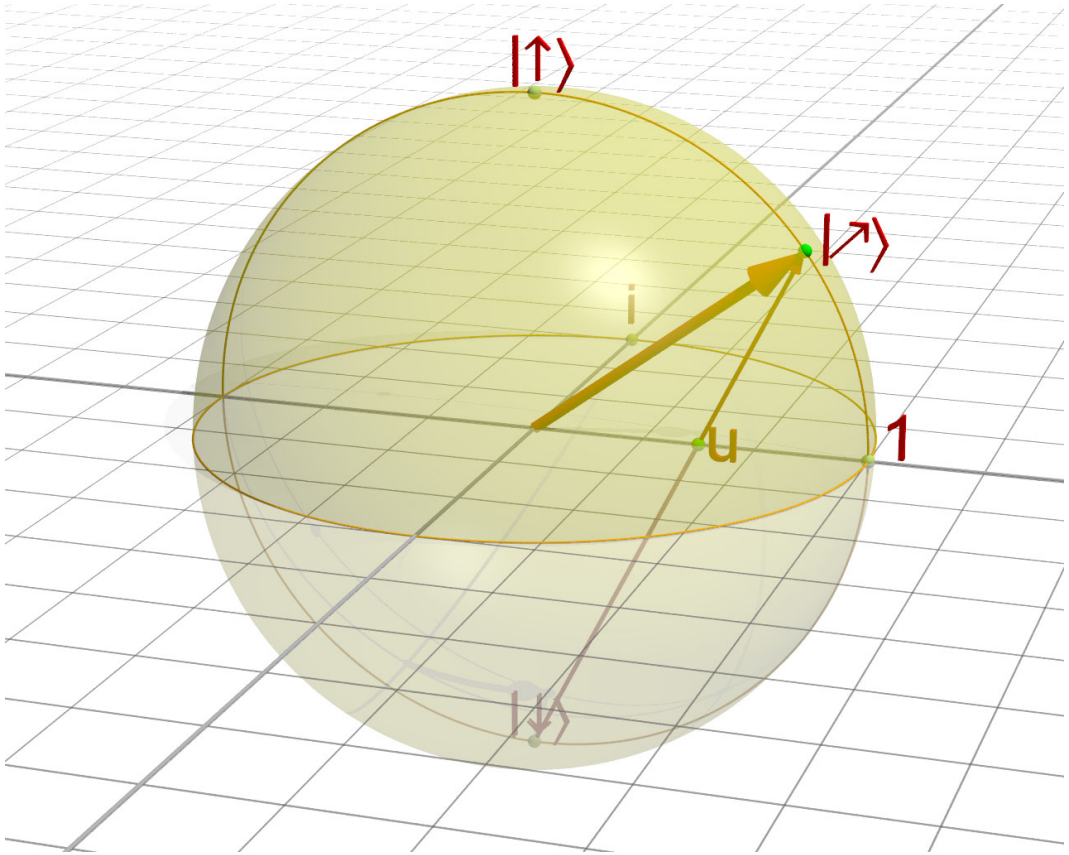
$$|\psi>= \cos\frac{\theta}{2}|0> + e^{\imath\phi}\sin\frac{\theta}{2}|1> \text{ avec } 0 \leq \theta \leq \pi,\ 0 \leq \phi \leq 2\pi$$

spécification de manière unique d'un point sur le sphere unité de $\mathbb{R}^3$

coordonnées cartésiennes :

$$\begin{aligned} x &= \sin\theta \times \cos\phi, \\ y &= \sin\theta \times \sin\phi, \\ z &= \cos\theta \end{aligned} \tag{2}$$

Représentation d'un qubit - sphère de Bloch



Exemple d'objets quantiques - l'électron

propriété quantique - le spin

pour l'électron, 2 possibilités

$\longrightarrow$ un spin peut faire office de qubit : il peut être dans un état, dans l'autre, ou dans une superposition de ces deux états

notation en mécanique quantique :
les vecteurs d'un espace sont appelés de kets :

$$|X>$$

superposition de deux états :

$$|X_1> + |X_2>$$

un ordinateur classique utilise de registres
exemple :
registre de 4 bits - plusieurs configurations : $0000, 0001, \ldots, 1111$
(16 états possibles pour le registre - permet de représenter de nombres entre 0 et 15)

Registre quantique

exemple - registre quantique fait de 4 qubits
superposition de 16 états
$|0000> + |0001> + \ldots + |1111>$
(on peut mettre de coefficients sur les états)
16 calculs en parallèle
registre de N qubits
2^N états

Portes quantiques

Les portes quantiques permet de manipuler de qubits et de faire avec eux de manipulations qu'on pourrait pas faire avec un ordinateur classique

Porte de Hadamard

entrée : 1 qubit
sortie : 1 qubit

$$|0> \rightarrow \frac{1}{\sqrt{2}}(|0> + |1>)$$
$$|0> \rightarrow \frac{1}{\sqrt{2}}(|0> - |1>)$$

Portes quantiques

il existe toute une zoologie de portes quantiques, qui permet de prendre en entrée $1, 2$ *etc.* qubits

mathématiquement, on représente une porte quantique par une matrice unitaire U
(ie $U \cdot U^\dagger = U^\dagger U = 1$,
$U^\dagger$ est la matrice transposée conjugué de la matrice carré complexe U)

Factorisation de nombres entières

factorisation : trouver la décomposition en produit de nombres premiers
exemple : $70 = 2 \times 5 \times 7$,

$$48279 = 3 \times 7 \times 11^2 \times 19$$

pas trop dur, car les facteurs premiers sont petits
par contre, le problème se complique quand les facteurs premiers sont grands :

$$56153 = 233 \times 241$$

pas simple à trouver

algorithmes de cryptographie se basent sur la factorisation

Algorithme de Shor

En 1994, Peter Shor a trouvé un algorithme quantique pour la factorisation, algorithme qui se base sur l'assemblage de portes quantiques

sa complexité est meilleure que celle de la complexité du meilleur algorithme classique dont on dispose

plus le nombre de départ est grand, plus l'avantage de l'algorithme quantique est notable (l'algorithme quantique est exponentiellement meilleur) !

Réalisation pratiques de qubits

ordinateur classique : utilisation du courant électrique (le courant passe, 1 ou le courant passe pas, 0)

pour réaliser un qubit, il faut un système physique suffisamment petit pour obéir aux lois de la mécanique quantique (pour pouvoir avoir des états superposées)

objets physiques susceptibles de réaliser un qubit : le spin d'un électron ou d'un noyau atomique, polarisation d'un photon, circuits supraconducteur *etc.*

complications techniques :

1. en avoir suffisamment pour un registre quantique assez grand
2. les maintenir isolés du monde extérieur pour qu'il soit stables et qu'ils restent dans un état superposé suffisamment longtemps pour qu'on puisse faire le calcul sur lequel on travaille

Décohérence : passage du monde quantique au monde classique

plus un système physique interagit avec son environnement (comme c'est le cas pour les objets macroscopiques), plus les phénomènes quantiques s'estompent

l'état de superposition d'une particule est détruit dès que ses propriétés sont observées par un appareil de mesure ; la particule se trouve alors dans un état déterminé

Suprématie quantique

résoudre avec un ordinateur quantique quelque chose qu'on arrive pas à résoudre avec un ordinateur classique

Un peu d'histoire

- début des années 80 avec des suggestions d'ordinateurs quantiques analogiques par Richard Feynman (Caltech)
- 1985 : David Deutsch a défini le machine de Turing quantique universelle
- développement des premiers algorithmes quantique par Deutsch et Jozsa
- développement de la théorie de la complexité quantique par Bernstein et Vazirani
- 1994 : découverte très surprenante de Peter Shor d'algorithmes quantiques efficaces pour les problèmes de factorisation des nombres entiers
- une forme quantique de cryptographie due à Bennett et Brassard

3 motivations pour l'étude de l'informatique quantique

Motivation pour l'étude de l'informatique quantique I

Le processus de miniaturisation qui a rendu les ordinateurs classiques actuels si puissants et bon marché, a déjà atteint des micro-niveaux où se produisent des effets quantiques. Les fabricants de puces ont tendance à se donner beaucoup de mal pour supprimer ces effets quantiques, mais on pourrait aussi essayer de travailler avec les effets quantiques, permettant une miniaturisation plus poussée.

Motivation pour l'étude de l'informatique quantique II

L'utilisation des effets quantiques permet d'accélérer énormément certains calculs (certains fois de manière exponentielle (exemple : algorithme de Shor) et permet même certaines choses qui sont impossibles pour les ordinateurs classiques (suprématie quantique)

Motivation pour l'étude de l'informatique quantique III

On peut dire que le but principal de l'informatique théorique est "d'étudier le pouvoir et les limites des dispositifs de calcul les plus puissants que la nature nous permet". Puisque notre compréhension actuelle de la nature est quantique, l'informatique théorique devrait sans doute étudier la puissance des ordinateurs quantiques, et non seulement des ordinateurs classiques.

Plan du cours

Plan du cours :

1. Le monde quantique : notation de Dirac, téléportation quantique *etc.*
2. L'intrication quantique
3. Le calcul quantique : algorithmes de Deutsch-Jozsa, algorithme de Simon
4. L'algorithme de factorisation de Schor
5. Codes correcteurs quantiques
6. Classe inverse : présentations étudiants (sujets choisit) - dernière semaine