

Introduction à l'informatique quantique

Semaine du numérique et des sciences informatiques

Gabriel Chênevert

4 décembre 2024

JUNIA ISEN



Gabriel Chênevert

<https://isen.junia.ovh/gch>

Responsable département JUNIA
Computer Science & Mathematics

Théorie de l'information / Cybersécurité :

- traitement de signal
- compression
- correction d'erreur
- cryptographie
- calcul quantique

Le quantique à JUNIA

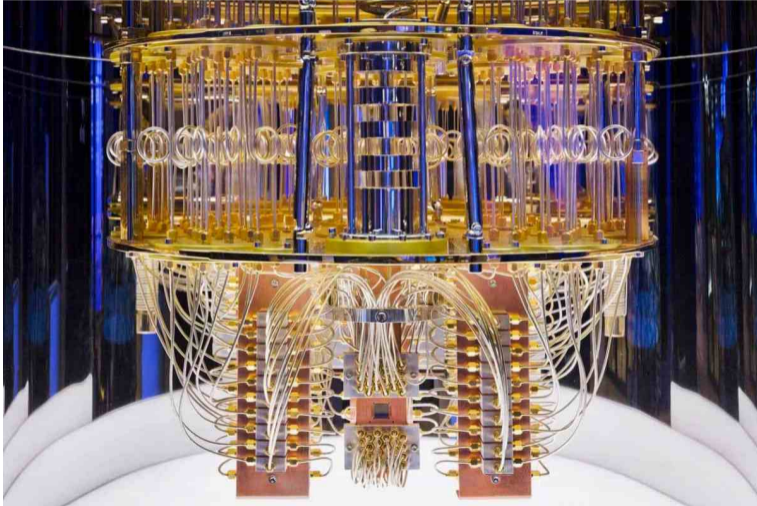
Enseignement (modules du cycle ingénieur ISEN) :

- Mécanique quantique
- Communication quantique
- Calcul et algorithmes quantiques


Recherche (en partenariat avec l'IEMN) :

- nanomatériaux
- optimisation combinatoire quantique
- cryptographie post-quantique

Qu'est-ce que c'est ?




Révolution ou menace ?


 L'Express

Les incroyables promesses de l'informatique quantique pour notre économie, par Nicolas Bouzou

Une technologie à large spectre. L'application la plus médiatisée de la physique quantique concerne l'informatique. L'informatique quantique...



25 mai 2024

 Unite.AI

Le grand pas de Microsoft vers l'informatique quantique tolérante aux pannes avec Azure Quantum

L'informatique quantique, avec sa promesse de résoudre des problèmes complexes avec lesquels les ordinateurs classiques sont aux prises,...



13 mai 2024

 Le Monde.fr

« 2024 pourrait bien être l'an I du bouleversement de l'informatique quantique »

CHRONIQUE. La société française Pasqal a franchi la barre des 1 000 atomes piégés en une seule opération. Une étape technologique majeure...




9 juil. 2024


 lebigdata.fr

IBM : le quantique va provoquer un Armageddon de cybersécurité

L'informatique quantique pourrait déclencher une catastrophe en matière de cybersécurité, avertit IBM. Il faut s'y préparer.




22 janv. 2024

 L'Express

Comment l'informatique quantique menace les secrets militaires et nos paiements

Ce terme désigne le jour où un ordinateur quantique sera suffisamment puissant pour ne faire qu'une bouchée des indispensables algorithmes de...



21 avr. 2024

 Forbes France

Menace quantique : si votre entreprise n'est pas préparée, il est déjà trop tard

"L'informatique quantique remet à plat l'informatique telle qu'on la connaît aujourd'hui. Par ses capacités de calculs sans précédent,..."



23 avr. 2024

La base de l'informatique : le bit

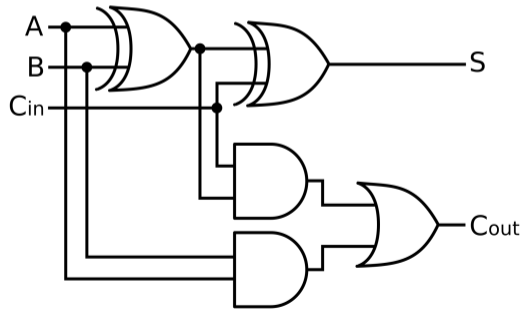
Toute donnée informatique (classique) est représentée en mémoire par une suite de symboles 0 ou 1 appelés *bits* :

- nombres (ex.: $42 = 101010$)
- caractères (ex. A = 01000001)
- fichiers texte, images, audio, vidéo, ...
- exécutable, bibliothèques, ...
- identifiants, adresses, ...

Traitements

À bas niveau, les opérations sont effectuées sur les bits en utilisant des *portes logiques* (OU, ET, NON, XOR, ...)

Par exemple, on réalise l'addition de deux entiers à n bits en chaînant n blocs :



La base de l'informatique quantique : le qubit

Bit

(Classical Computing)

0

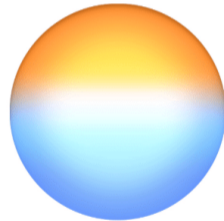


1

Qubit

(Quantum Computing)

0



1

Version simplifiée : le p -bit

Comme un qubit, un p -bit (bit probabiliste) peut être dans une *superposition d'états* : à la fois 0 et 1, dans différentes proportions (ou probabilités).

0



1

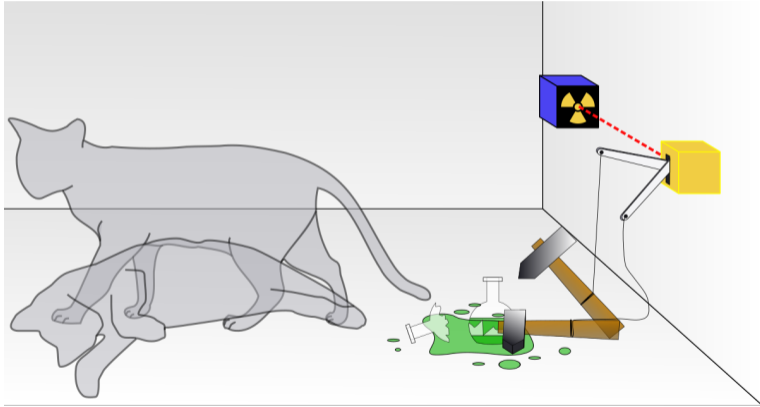
Par exemple :

$$\frac{1}{10} [0] + \frac{9}{10} [1]$$

Lorsqu'on mesure ce p -bit, on a

- 10% de chances d'observer un 0
- 90% de chances d'observer un 1

Le chat de Schrödinger : $\frac{1}{2}$ [vivant] + $\frac{1}{2}$ [mort]



Portes logiques

Si on met des p -bits en entrées, on aura des p -bits en sortie :

$$\text{NON}\left(\frac{1}{3} [0] + \frac{2}{3} [1]\right) = \frac{2}{3} [0] + \frac{1}{3} [1]$$

$$\left(\frac{1}{3} [0] + \frac{2}{3} [1]\right) \text{ ET } \left(\frac{1}{4} [0] + \frac{3}{4} [1]\right) = \text{ET}\left(\frac{1}{12} [00] + \frac{1}{4} [01] + \frac{1}{6} [10] + \frac{1}{2} [11]\right)$$

$$= \left(\frac{1}{12} + \frac{1}{4} + \frac{1}{6}\right)[0] + \frac{1}{2} [1] = \frac{1}{2} [0] + \frac{1}{2} [1]$$

Registre de p -bits

Un registre à 2 p -bits peut être dans une superposition des 4 états [00], [01], [10], [11]

⋮

Un registre à n p -bits peut être dans une superposition de 2^n états.

Cela permet de faire plusieurs calculs en même temps !

Par exemple : si

$$a = \frac{1}{3} [000] + \frac{1}{3} [010] + \frac{1}{3} [100] \quad \text{et} \quad b = \frac{1}{2} [000] + \frac{1}{2} [010]$$

alors

$$a + b = \frac{1}{6} [000] + \frac{1}{3} [010] + \frac{1}{3} [100] + \frac{1}{6} [110]$$

Intrication

Certains états de p -registres ne peuvent pas être décomposés en p -bits individuels.

Par exemple :

$$\frac{1}{2} [00] + \frac{1}{2} [11]$$

Si on mesure chaque p -bit, on aura 50 % de chances de voir 0 ou 1.

Mais on a 100 % de chances de mesurer la même valeur sur chacun !

Ces états sont dits *intriqués*.

Les échecs quantiques

Jeu développé pour se familiariser avec certains concepts contre-intuitifs de la mécanique quantique, notamment la *superposition* et l'*intrication*



Mécanique de jeu

Les pièces sont les mêmes qu'aux échec classiques, avec les règles de déplacement et de prise habituelles.

Classiquement : chaque pièce est dans un état (vivante ou morte) bien définie et à une position précise

Déplacement standard : on sélectionne une case de départ et une case d'arrivée admissibles.

Aux échecs quantiques : on peut être dans une superposition d'états !

Déplacements quantiques

Deux types de déplacements spéciaux, possibles pour toutes les pièces sauf les pions :

- *scindements*

On sélectionne une case de départ et *deux* cases d'arrivée admissibles

⇒ la pièce se retrouve dans une superposition équiprobable d'états

- *fusions*

On sélectionne *deux* cases de départ et une case d'arrivée admissibles

⇒ les fragments de pièces se rassemblent

Mesure et intrication

Les états superposés persistent jusqu'à ce qu'une *mesure* (tentative de prise par une pièce superposée) soit effectuée

⇒ une des issues est alors sélectionnée selon sa probabilité.

Lors du déplacement d'une pièce glissante (tour, fou, reine), les cases traversées doivent être libres

⇒ il est possible de se retrouver avec plusieurs pièces *intriquées* (dont les états possibles dépendent les unes des autres).

Au jeu !

