

L'utilité de l'informatique quantique dans les TIC

Introduction à l'informatique quantique

KOBENAN Ali Ouattara
Speaker

Institut National Polytechnique Félix Houphouet Boigny

19 Septembre 2023

Plan

- 1 Quelques notions fondamentales de la mécanique quantique

Plan

- 1 Quelques notions fondamentales de la mécanique quantique
- 2 Informatique quantique

Plan

- 1 Quelques notions fondamentales de la mécanique quantique
- 2 Informatique quantique
- 3 L'informatique quantique et les besoins actuels

Plan

- 1 Quelques notions fondamentales de la mécanique quantique
- 2 Informatique quantique
- 3 L'informatique quantique et les besoins actuels
- 4 Conclusion

Mécanique quantique

Principes fondamentaux

- En mécanique quantique, toute matière est à la fois particule et onde : c'est la *dualité onde-particule*;
- Deux lois fondamentales gouvernent la mécanique quantique:
 - L'intrication;
 - La superposition.

Intrication quantique

Approche définitionnelle

- Les particules n'ont pas d'état cinématique fixe;

Intrication quantique

Approche définitionnelle

- Les particules n'ont pas d'état cinématique fixe;
- L'intrication phénomène par lequel deux particules ou groupes de particules préalablement en relation forment un système (lié) l'un de l'autre quelle que soit la distance qui les sépare;

Intrication quantique

Approche définitionnelle

- Les particules n'ont pas d'état cinématique fixe;
- L'intrication phénomène par lequel deux particules ou groupes de particules préalablement en relation forment un système (lié) l'un de l'autre quelle que soit la distance qui les sépare;
- Ces particules sont dites alors intriquées ou elles sont dans un état intriqué.

La loi de conservation du système intriqué

- «Quand on “touche” un objet d'une paire d'objets intriqués, le deuxième tressaille, malgré la distance», Nicolas Gisin, physicien suisse.

La loi de conservation du système intriqué

- «Quand on “touche” un objet d'une paire d'objets intriqués, le deuxième tressaille, malgré la distance», Nicolas Gisin, physicien suisse.
- L'intrication quantique se réfère à l'existence d'un lien invisible entre deux particules qui ont été émises en même temps, quelle que soit la distance qui les sépare.

Superposition quantique

Approche définitionnelle de la superposition

- Richard Feynman (Prix Nobel de Physique en 1965):
« si pour vous un électron tourne autour d'un noyau comme un satellite tourne autour d'une planète, c'est que votre vision de l'atome est restée bloquée en 1915 »;

Superposition quantique

Approche définitionnelle de la superposition

- Richard Feynman (Prix Nobel de Physique en 1965):
« si pour vous un électron tourne autour d'un noyau comme un satellite tourne autour d'une planète, c'est que votre vision de l'atome est restée bloquée en 1915 »;
- Un même état quantique peut posséder plusieurs valeurs pour une certaine quantité observable.

Approche de la notion de l'informatique quantique

- L'un des domaines multidisciplinaire qui comprend de l'informatique, la physique, les mathématiques qui utilise les principes de la **mécanique quantique** pour résoudre les problèmes complexes plus rapidement que l'informatique classique;

Approche de la notion de l'informatique quantique

- L'un des domaines multidisciplinaire qui comprend de l'informatique, la physique, les mathématiques qui utilise les principes de la **mécanique quantique** pour résoudre les problèmes complexes plus rapidement que l'informatique classique;
- Elle utilise une catégorie de bits appelés bits quantiques ou qbits;

Approche de la notion de l'informatique quantique

- L'un des domaines multidisciplinaire qui comprend de l'informatique, la physique, les mathématiques qui utilise les principes de la **mécanique quantique** pour résoudre les problèmes complexes plus rapidement que l'informatique classique;
- Elle utilise une catégorie de bits appelés bits quantiques ou qbits;
- Les ordinateurs utilisés dans ce domaine possèdent des propriétés mettant en application l'usage des qbits: ce sont les ordinateurs quantiques.

L'ordinateur quantique

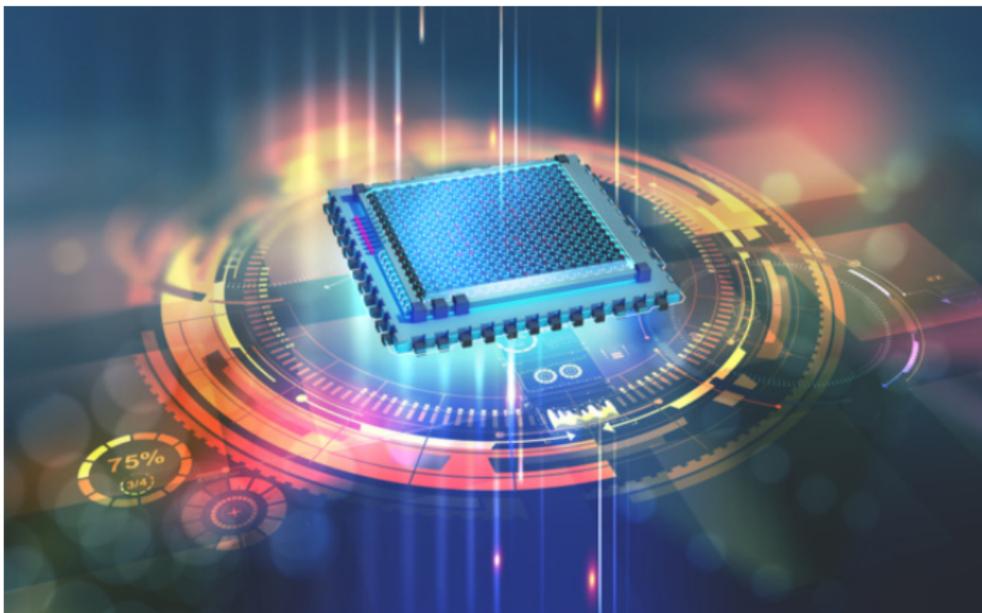


Figure 1: L'ordinateur quantique

Les bits et les qbits

- Le bit est la représentation et l'unité de traitement d'une information stockée en mémoire en informatique classique;
- Un bit classique ne peut que prendre deux états représentés par 0 et 1;
- Une information est caractérisée par un train de bits (le mot binaire);
- Les états des bits sont pris de manière séquentielle;
- Le traitement d'une information représentée par le mot binaire utilise la combinaison des deux états de chaque bit constituant le mot binaire à chaque séquence d'exécution d'horloge.

Les bits et les qbits

- Les ordinateurs quantiques utilisent les qbits comme symboles de traitement de l'information et unités de stockage;
- Les bits quantiques (qbits) peuvent prendre à la fois plusieurs états simultanément en une seule séquence d'horloge;
- Les bits quantiques utilisent la notion de la superposition d'états;
- L'état d'un qbit est représenté par $|0\rangle, |1\rangle$;
- L'utilisation de la superposition des états des qbits dans les mots permet d'avoir plusieurs résultats en une seule séquence d'opérations et accélère le traitement de l'information.

Les bits et les qbits

Les Opérations avec qbits

- Le qubit assure le traitement des opérations beaucoup plus performant et rapide, grâce à la mise en parallèle des calculs;

Les bits et les qbits

Les Opérations avec qbits

- Le qubit assure le traitement des opérations beaucoup plus performant et rapide, grâce à la mise en parallèle des calculs;
- Une donnée représentée sur n qbits, nécessite 2^n opérations en parallèle;

Les bits et les qbits

Les Opérations avec qbits

- Le qubit assure le traitement des opérations beaucoup plus performant et rapide, grâce à la mise en parallèle des calculs;
- Une donnée représentée sur n qbits, nécessite 2^n opérations en parallèle;
- Au cours de l'exécution des tâches, le registre de qubits se trouve dans une superposition quantique de tous ses états possibles ($|00\dots 0\rangle$, $|10\dots 0\rangle$, $|11\dots 1\rangle$, $|10\dots 1\rangle$), permettant un calcul parallèle ce qui augmente la rapidité dans l'exécution des opérations.

Les exigences de nouvelles applications

- Nous sommes à l'ère du numérique avec un monde de plus en plus connecté;

Les exigences de nouvelles applications

- Nous sommes à l'ère du numérique avec un monde de plus en plus connecté;
- Les applications actuelles nécessitent de grandes quantités de données avec un traitement demandant plus d'opérations;

Les exigences de nouvelles applications

- Nous sommes à l'ère du numérique avec un monde de plus en plus connecté;
- Les applications actuelles nécessitent de grandes quantités de données avec un traitement demandant plus d'opérations;
- La technologie de l'information et de la communication a des problèmes complexes dont la résolution de ceux-ci dépend de leur complexité.

Les exigences de nouvelles applications

Les exigences de nouvelles applications

- Les ordinateurs classiques utilisés dans les TIC aujourd'hui commencent à montrer leur limite dans cette génération de problèmes;

Les exigences de nouvelles applications

- Les ordinateurs classiques utilisés dans les TIC aujourd'hui commencent à montrer leur limite dans cette génération de problèmes;
- Une solution motivée par les limitations de l'ordinateur classique est l'utilisation de l'ordinateur quantique.

Différents domaines d'applications

Simon Perdrix, chercheur en informatique quantique au CNRS

Quand on arrivera à utiliser pleinement l'ordinateur quantique, bon nombre de problèmes, hors de portée des ordinateurs classiques, pourront être résolus.

Différents domaines d'applications

Intelligence artificielle

Les prévisions météorologiques, financières, de trafic routier et tous les domaines utilisant l'intelligence artificielle seront optimisés. Comme tous ceux qui utilisent le « machine learning », une particularité de l'intelligence artificielle.

Différents domaines d'applications

Intelligence artificielle

Les prévisions météorologiques, financières, de trafic routier et tous les domaines utilisant l'intelligence artificielle seront optimisés. Comme tous ceux qui utilisent le « machine learning », une particularité de l'intelligence artificielle.

Médecine

Investissement dans les laboratoires pharmaceutiques en raison du prix que pourrait valoir cette technologie lors de sa sortie. des diagnostics médicaux plus rapides et plus précis, le développement de molécules thérapeutiques ou la création de nouveaux médicaments nécessitant des temps de calculs et de modélisation très énormes.

Différents domaines d'applications

Cryptographie et sécurité

L'actuel système de cryptographie mondial utilisé par les multinationales, les systèmes d'échanges commerciaux et les banques, etc est le RSA. Vu l'avancée technologique utilisée par les pirates aujourd'hui, les entreprises pourraient avoir recours au code quantique afin d'augmenter la complexité de leur système de sécurité pour rendre leur système difficilement pénétrable.

Différents domaines d'applications

La modélisation mathématique

La modélisation des problèmes actuels de la vie nécessite des puissances de calculs beaucoup plus évoluées. Il est absolument important d'utiliser les techniques adaptées à ce siècle pour une bonne précision des résultats. La modélisation fait partir de la résolution des problèmes complexes qui demandent d'énormes opérations de calculs que les supercalculateurs mettraient assez de temps pour y parvenir.

Bilan général

Synthèse

L'informatique quantique apporte des nombreux avantages aux nouvelles Technologies de l'Information et de la Communication en termes de sécurité, de puissance de calcul et de capacités d'optimisation. Elle ouvre la voie à des solutions innovantes dans cette nouvelle ère en utilisant les principes de la mécanique quantique.

Quelques références

- <https://www.pwc.fr/fr/assets/files/pdf/2019/11/fr-france-pwc-point-of-view-quantum-computing-2019.pdf>
- <https://www.cscience.ca/chroniques/informatique-quantique-et-cybersecurite-une-arme-a-double-tranchant/>
- <https://www.ibm.com/fr-fr/topics/quantum-computing>
- <https://www.zdnet.fr/pratique/tout-comprendre-a-l-informatique-quantique-39891035.htm>

Merci de votre aimable attention !