Informatique quantique 101

Même si l'information quantique existe depuis longtemps, on commence à en parler davantage dans les médias. Nous vous proposons un guide d'initiation sur quelques sujets :

- Qu'est-ce que l'informatique quantique?
- Superposition et intrication
- Pourquoi les effets quantiques ont-ils de l'importance?
- Qu'est-ce qui est possible pour un ordinateur quantique et impossible pour un ordinateur classique?
- Mais je n'ai pas besoin de factoriser de grands nombres
- Un ordinateur quantique pourrait faire intrusion dans mes données confidentielles?
- Comment la mécanique quantique peut-elle créer des clés ultrasecrètes?
- Que peut-on faire d'autre avec la mécanique quantique?
- Où puis-je me procurer un ordinateur quantique?
- Que faut-il pour construire un ordinateur quantique?
- Quand y aura-t-il un véritable ordinateur quantique?
- Donc, la technologie quantique n'est pas pour demain?

Vous voulez en savoir plus? Parcourez notre boîte à outils quantique.

Qu'est-ce que l'informatique quantique?

L'informatique quantique consiste essentiellement à maîtriser et à exploiter les lois étonnantes de la mécanique quantique pour traiter de l'information. Un ordinateur classique utilise de longues chaînes de bits, dont chacun représente l'une des valeurs 0 ou 1. Par contre, un ordinateur quantique utilise des bits quantiques, appelés qubits. Quelle est la différence? Un qubit est un système quantique qui représente les 0 et les 1 dans 2 états quantiques que l'on peut distinguer. Mais comme les qubits se comportent de manière aléatoire, cela permet de profiter des phénomènes de « superposition » et d'« intrication ».

Superposition et intrication? Pardon?

C'est normal d'être un peu déconcerté par ces notions, dont nous ne faisons pas l'expérience dans notre vie quotidienne. Ce n'est qu'à l'échelle des plus petites particules quantiques — atomes, électrons, photons, etc. — que se manifestent des phénomènes fascinants tels que la superposition et l'intrication.

La superposition est essentiellement la capacité d'un système quantique d'être dans plusieurs états en même temps : quelque chose peut être à la fois « ici » et « là », ou à la fois « en haut » et « en bas ».

L'intrication est une corrélation extrêmement forte entre particules quantiques — si forte que 2 ou plusieurs particules quantiques peuvent être inextricablement liées dans un unisson parfait, même si de grandes distances les séparent. Ces particules sont liées de manière intrinsèque, comme si elles « dansaient » à l'unisson, de manière instantanée, même si elles sont à des extrémités opposées de l'univers. Ce lien en apparence impossible a amené Einstein à qualifier l'intrication d'« effrayante action à distance ».

Pourquoi les effets quantiques ont-ils de l'importance?

Tout d'abord, ils sont fascinants. Mieux encore, ils seront extrêmement utiles pour l'avenir des technologies de l'information et des communications.

Grâce à la superposition et à l'intrication, un ordinateur quantique peut effectuer simultanément un grand nombre de calculs. On peut voir cela de la manière suivante : alors qu'un ordinateur classique travaille sur des 0 et des 1, un ordinateur quantique a l'avantage d'utiliser des 0, des 1 et des « superpositions » de 0 et de 1. Certaines tâches difficiles que l'on a longtemps considérées comme impossibles (ou comme des problèmes insolubles) pour des ordinateurs classiques seront accomplies de manière rapide et efficace par un ordinateur quantique.

Qu'est-ce qui est possible pour un ordinateur quantique et impossible pour un ordinateur classique?

Tout d'abord, la factorisation de grands nombres. N'importe quel ordinateur peut facilement multiplier 2 grands nombres. Mais la décomposition d'un très grand nombre (p. ex. un nombre de 500 chiffres) en facteurs premiers est réputée impossible pour tout ordinateur classique. En 1994, Peter Shor, mathématicien à l'Institut de technologie du Massachusetts (MIT) — et qui était à l'époque chez AT&T —, a montré qu'un ordinateur quantique fonctionnel pourrait facilement factoriser de grands nombres.

Mais je n'ai pas besoin de factoriser de grands nombres…

Personne ne veut factoriser de très grands nombres! Parce que c'est très difficile — même pour les meilleurs ordinateurs actuels. De fait, la difficulté de factoriser de grands nombres est aujourd'hui à la base d'une grande partie de la cryptographie. Celle-ci est fondée sur des problèmes mathématiques trop difficiles pour être résolus. Le chiffrement RSA, employé pour crypter votre numéro de carte de crédit lorsque vous faites des achats en ligne, repose entièrement sur le problème de la factorisation. Le site Web où vous vous apprêtez à faire un achat vous fournit un grand nombre agissant comme une clé « publique » (accessible à tous) pour coder les données de votre carte de crédit.

Cette clé est le produit de 2 très grands nombres premiers, que seul le commerçant connaît. La seule manière dont quelqu'un pourrait intercepter vos données serait de connaître ces 2 nombres premiers qui sont multipliés entre eux pour donner la clé. Comme la factorisation est très difficile, aucun intrus ne peut accéder à votre carte de crédit, et votre compte est en sécurité. À moins que quelqu'un ait construit un ordinateur quantique et exécute l'algorithme de Peter Shor!

Attendez… Un ordinateur quantique pourrait faire intrusion dans mes données confidentielles? Ça, ce n'est pas bon.

Ne vous en faites pas : la cryptographie classique n'est pas totalement compromise. Même si certains aspects de la cryptographie seraient menacés par l'informatique quantique, la mécanique quantique permet aussi un nouveau type de cryptographie ultrasûre.

Prenons un protocole répandu de cryptographie appelé masque jetable : les interlocuteurs A et B (appelons-les Alice et Bob) utilisent en commun une longue suite aléatoire de 0 et de 1 — la clé secrète. À condition d'utiliser cette clé une seule fois et d'être les seuls à connaître cette clé, ils peuvent s'envoyer un message secret qu'aucun intrus ne pourra déchiffrer. La principale difficulté du masque jetable réside dans la transmission des clés elles-mêmes. Dans le passé, des gouvernements envoyaient des personnes porter des livres pleins de données aléatoires destinées à servir de clés. Évidemment, cette manière de procéder est peu pratique et imparfaite. C'est là que la mécanique quantique est à nouveau bien commode : la distribution quantique de clés (DQC) permet de transmettre à distance des clés entièrement aléatoires.

Comment la mécanique quantique peut-elle créer des clés ultrasecrètes?

La distribution quantique de clés repose sur une autre propriété intéressante de la mécanique quantique : toute tentative d'observation ou de mesure d'un système quantique perturbe le système en question.

L'Institut d'informatique quantique (IQC) possède l'un des rares prototypes de DQC au monde. L'appareil baptisé Alice, situé au siège de l'IQC, reçoit un photon de chaque paire de photons intriqués (fortement corrélés) produit par un laser sur le toit d'un bâtiment de l'Université de Waterloo. L'appareil baptisé Bob, situé à l'Institut Périmètre, non loin de là, reçoit l'autre photon de chaque paire.

Les photons possèdent une propriété mesurable distinctive appelée polarisation (les connaisseurs en matière de lunettes de soleil reconnaîtront ce terme).

Comme la polarisation de chaque photon individuel est aléatoire, il n'y a aucun moyen de connaître à l'avance les propriétés propres à chaque photon. C'est là où l'intrication devient intéressante : si Alice et Bob mesurent la polarisation des photons intriqués qu'ils reçoivent, ils obtiendront les mêmes résultats (rappelez-vous que des particules intriquées sont fortement corrélées, même à de grandes distances). Selon la polarisation de chaque photon, Alice et Bob attribuent un 1 ou un 0 à chaque photon qu'ils reçoivent. Par conséquent, si Alice reçoit une suite de photons codée 010110, Bob reçoit aussi 010110. Si un intrus tente d'espionner le signal, il perturbe du même coup le système, et Alice et Bob remarquent instantanément que leurs clés ne correspondent plus.

Alice et Bob continuent de recevoir des photons jusqu'à ce que leurs clés soient assez longues tout en étant identiques, et ils disposent alors d'un moyen ultrasûr de crypter leurs communications.

La mécanique quantique permet donc de violer et de créer des codes. Y a-t-il autre chose? Beaucoup d'autres choses. À titre d'exemple, les ordinateurs quantiques seront capables de simuler d'une manière efficace des systèmes quantiques. C'est ce que le célèbre physicien Richard Feynman a proposé en 1982, donnant effectivement le coup d'envoi du domaine de l'informatique quantique. La simulation de systèmes quantiques est qualifiée de « saint graal » de l'informatique quantique, car elle permettra d'étudier avec un niveau de détail remarquable les interactions entre atomes et molécules.

Cela pourrait aider à concevoir des médicaments ainsi que des matériaux nouveaux, par exemple des supraconducteurs fonctionnant à la température ambiante. Parmi les nombreuses tâches pour lesquelles un ordinateur quantique est intrinsèquement plus rapide qu'un ordinateur classique est la recherche de la meilleure solution dans un espace de solutions potentielles. Des chercheurs travaillent constamment sur de nouveaux algorithmes et applications quantiques. Mais le potentiel réel des ordinateurs quantiques n'a probablement pas encore été complètement imaginé. Les inventeurs du laser n'avaient sûrement pas envisagé les lecteurs de codes à barres, les lecteurs de disques compacts et la chirurgie oculaire. De la même manière, les utilisations futures des ordinateurs quantiques ne sont limitées que par l'imagination.

Très bien! Où puis-je me procurer un ordinateur quantique?

Pas si vite! Même si on a démontré en théorie le potentiel extraordinaire des ordinateurs quantiques, et même si des scientifiques travaillent à l'IQC et dans le monde entier à réaliser ce potentiel, il y a encore beaucoup à faire avant que des ordinateurs quantiques soient offerts sur le marché.
Que faut-il pour construire un ordinateur quantique?

La réponse simple est qu'il faut des qubits qui se comportent comme on le souhaite. Ces qubits peuvent être faits de photons, d'atomes, d'électrons, de molécules ou peut-être de quelque chose d'autre. Les scientifiques de l'IQC font des recherches sur de nombreuses possibilités de réalisation pratique d'ordinateurs quantiques. Mais les qubits sont notoirement difficiles à manipuler, car toute perturbation leur fait perdre leur état quantique (c'est ce que l'on appelle la décohérence). La décohérence est le talon d'Achille de l'informatique quantique, mais cet obstacle n'est pas insurmontable. Le domaine de la correction d'erreurs quantiques vise à pallier la décohérence et à combattre d'autres erreurs. Chaque jour, des chercheurs de l'IQC et d'ailleurs dans le monde découvrent de nouvelles manières de dompter les qubits.

Quand y aura-t-il un véritable ordinateur quantique?

Cela dépend de la définition qu'on en donne. Il y a déjà des ordinateurs quantiques, mais ils ne sont pas assez puissants pour remplacer les ordinateurs classiques. Une équipe de chercheurs de l'IQC et du MIT détient le record mondial actuel du plus grand nombre de qubits utilisés dans une expérience (12). Alors que des technologies quantiques concrètes voient déjà le jour — p. ex. des capteurs, actionneurs et autres dispositifs hautement efficaces —, il faudra attendre encore des années avant d'avoir un véritable ordinateur quantique qui puisse surpasser un ordinateur classique. Les théoriciens trouvent continuellement de meilleures manières de vaincre la décohérence, et les expérimentateurs maîtrisent de mieux en mieux le monde quantique en faisant appel à divers moyens techniques et instruments. Le travail de pionnier accompli aujourd'hui ouvre la voie à l'ère quantique de l'avenir.

Donc, la technologie quantique n’est pas pour demain?

Des technologies quantiques sont déjà utilisées! La DQC est commercialisée et bénéficiera grandement de nouvelles recherches (des scientifiques de l’IQC travaillent actuellement sur le cryptage quantique avec transmission par satellite). Même si un ordinateur quantique entièrement fonctionnel demeure un objectif à long terme, la recherche en informatique quantique a donné lieu à de nombreuses découvertes théoriques et pratiques. Les capteurs et actionneurs quantiques permettront aux scientifiques de naviguer dans le monde nanométrique avec une précision et une sensibilité remarquables. Ces outils seront précieux pour la mise au point de véritables processeurs d’information quantique. La révolution quantique est déjà en marche, et les possibilités qui s’annoncent sont illimitées.