Les potentialités des ordinateurs quantiques

David Bensoussan

L'auteur est professeur de sciences à l'Université du Québec

Bien des inquiétudes sont actuellement émises au sujet des dangers de l'intelligence artificielle (IA) et la plupart des chercheurs du domaine insistent sur la nécessité d'un code d'éthique. Indépendamment de l'IA, la course à l'ordinateur quantique est lancée. Il s'agit d'un ordinateur superpuissant capable de traiter en parallèle des milliards de possibilités et d'optimiser la solution à retenir.

Une évolution vertigineuse

En 1953, l'invention du transistor a permis de remplacer des tubes électroniques encombrants et de construire des cartes de circuits imprimés contenant des transistors et des composantes électriques. Un grand nombre d'applications, tels des systèmes audio, vidéos et des contrôleurs de tous genres, y compris les circuits logiques qui sont à la base des ordinateurs ont été développés. En 1958, le premier circuit intégré incorporant des transistors et des composantes électriques a vu le jour. Des années 50 aux années 2020, le nombre de transistors intégrés dans les puces électroniques est passé de 1 à près de 16 milliards.

L'ordinateur qui a servi à construire le véhicule Curiosity déployé sur la planète Mars en 2012 avait un processeur opérant à une vitesse de 200 mégahertz, une mémoire vive de 256 mégabits et une mémoire de 2 gigabits. Aujourd'hui, les spécifications respectives des ordinateurs en vente au grand public sont de l'ordre de centaines de gigahertz, de dizaines de gigabits et de plusieurs térabits.

De la règle à calcul aux ordinateurs portables, tant les capacités de calcul que l'envergure des applications qu'il est possible de développer ont été multipliées.

Du bit au qubit

Les ordinateurs actuels traitent des bits représentant des valeurs binaires de 0 et 1 et ces états d'énergie sont mutuellement exclusifs. Par contre, les ordinateurs quantiques traitent des qubits qui peuvent avoir des valeurs simultanées de 1 et de 0, l'état final n'étant connu qu'au moment de la mesure.

La loi de Moore est une loi empirique selon laquelle la puissance de calcul des ordinateurs double chaque année. Il en va de même pour le nombre de transistors contenus dans une puce électronique. Il semble bien que ce soit encore le cas pour le nombre de qubits d'un ordinateur quantique. Il a été annoncé que l'ordinateur quantique chinois Jiuzhang peut effectuer en 200 secondes un calcul qui prendrait plus d'un demi-milliard d'années sur les plus rapides de nos ordinateurs non quantiques.

Les ordinateurs quantiques opèrent à des températures très basses qui approchent le zéro absolu, soit -273^{o} Celsius. Plusieurs solutions concurrentes sont à l'étude, exploitant des super conducteurs, des semiconducteurs, des ions piégés, des impuretés dans les diamants, des atomes froids, des ordinateurs quantiques topologiques ou photoniques… Dans ce dernier cas, l'ordinateur quantique opère à la température ambiante.

Un ordinateur de 100 qubits peut envisager de façon quasi simultanée 2^{100} réalités parallèles. Dans la course à l'ordinateur quantique, aucun pays ou industrie ne voudra se trouver en arrière du peloton.

Une gamme d'applications révolutionnaire

La puissance de calcul des ordinateurs quantiques va permettre d'accélérer la recherche dans de nombreux domaines. La fabrication de nouveaux matériaux sera facilitée par des simulations de molécules complexes. Il en ira de même pour la simulation des interactions entre médicaments qui contribuera à de meilleurs diagnostics et à des traitements médicinaux plus appropriés. Elle facilitera l'amélioration des prédictions météorologiques ou même l'optimisation des options d'achat d'un portefeuille en bourse. La logistique des flux de transport d'énergie, de transport routier ou d'une

chaîne d'assemblage bénéficiera également d'une meilleure analyse des données…

Les possibilités de déchiffrage de communications cryptées les plus sophistiquées à l'aide d'ordinateurs quantiques sont énormes : la méthode de chiffrement la plus sûre aujourd'hui est la méthode RSA qui est basée sur un code de 2048 bits. Il faudrait des milliards d'années pour que les plus puissants des ordinateurs actuels puissent vérifier l'ensemble des possibilités. Par contre, un ordinateur quantique de 2 000 qubits pourrait le faire en moins d'un jour et un ordinateur de 4 000 qubits le ferait en quelques secondes. En d'autres mots, il va être difficile de conserver la confidentialité dans tous les domaines. Par contre, une communication quantique peut être considérée comme sécuritaire, car toute interception de la transmission mettrait fin à la transmission.

Le déterminisme qui existe dans la mécanique classique permet de prédire l'évolution d'un processus vers un état final à partir de la connaissance du processus et de son état initial. À titre d'exemple, un objet lâché tombe vers le bas en raison de la gravité. Cette compréhension intuitive de la mécanique classique fait défaut en mécanique quantique qui est la mécanique qui régit les interactions entre les atomes. Ainsi, tout ce que l'on pourra avancer dans le cas d'une particule, c'est qu'elle se trouve dans deux états (deux positions) simultanément, la position finale ne pouvant être connue qu'avec l'observation.

Un qubit peut représenter un état (la position) d'une particule ou encore la polarisation d'un photon. L'intrication des particules est obtenue en rapprochant des particules créées simultanément lors d'une collision ou encore en les rapprochant de façon à ce qu'elles interagissent. Il en va de même pour l'intrication de deux photons lumineux dont les polarisations sont intriquées.

Il n'est pas possible de connaître l'état final d'une paire de qubits intriqués avant de l'avoir mesuré. Jusque-là, le processus se trouve simultanément dans deux états. La mesure de l'un de ces états a automatiquement un impact sur l'état de l'entité intriquée, indépendamment de la distance qui les

sépare… Tout au plus pourra-t-on se faire une idée de la probabilité de trouver la particule à un endroit donné en fonction du temps.

La téléportation quantique est possible grâce à l'intrication quantique qui permet de transmettre l'état d'une particule à distance. Il est à prévoir que cette information pourra servir à reproduire la matière originale : des molécules, ou même le code génétique ADN…

Les domaines d'intervention des ordinateurs quantiques sont aussi vastes que l'imagination peut concevoir.

Revenons à l'éthique

Indépendamment de l'IA, les ordinateurs quantiques seront capables de modifier substantiellement le vécu dans les domaines privés et publics.

Si l'on se soucie de normes éthiques, le domaine des ordinateurs quantiques n'est pas moins important que celui de l'IA.

Qui plus est, l'intégration de la puissance matérielle des ordinateurs quantiques et de la puissance logicielle de l'IA fera que d'ici deux à trois décennies, il sera possible de dépasser la capacité de traitement de tous les cerveaux humains. Les potentialités de l'apprentissage machine quantique et de l'intelligence artificielle quantique dépassent ce que peut concevoir l'imagination. Un changement de donne radical du mode de vie est à prévoir.

Si l'on tient compte des mégacentres de données qui sont en train d'être accumulées sur le nuage, cette intégration augmentera encore plus les possibilités d'interposition dans la vie privée et publique.

Sera-t-il possible d'assujettir les applications cette intégration de l'IA et des ordinateurs quantiques aux lois constitutionnelles ?

La préoccupation en matière d'éthique n'en est que plus urgente.