Tout comprendre sur l'informatique quantique

Google a frappé un grand coup médiatique en début de semaine avec la parution d'informations de presse faisant état de ses bonds de géants dans le domaine de l'informatique quantique. L'heure est certainement donc venue de revenir sur ce concept qui peut paraître nébuleux à maints égards.

Pour commencer, soulignons que le but de la recherche en informatique quantique est de découvrir un moyen d'accélérer l'exécution de longues vagues d'instructions. Pour ce faire, les chercheurs spécialisés ont recours à des phénomènes observé en mécanique quantique qui sont d'un ordre complètement différent de tout ce que l'espèce humaine a jamais construit.

Leur objectif consiste à construire une ordinateur quantique surpassant de loin tout ce qu'un superordinateur peut faire aujourd'hui. De quoi résoudre des problèmes mathématiques qui nécessitent aujourd'hui des jours de calcul sur n'importe quel supercalculateur. Certains de ces problèmes n'ont toujours pas de solution, et pourraient alors être résolus de manière instantanée.

Les modèles de changement climatique, les estimations de la probabilité de la présence d'exoplanètes dans la galaxie observable ou encore les modèles de la capacité du système immunitaire à détruire les cellules cancéreuses pourraient soudainement donner des résultats dans l'heure qui suit le lancement du programme. Si ces résultats pourraient ne pas se présenter sous la forme d'une solution complète, mais plutôt sous la forme d'un tableau de probabilité indiquant les solutions les plus probables, ils constituerait toutefois un bond de connaissance sans précédent dans l'histoire de l'humanité.

Ce que peut l'informatique quantique

Si vous avez déjà programmé une macro Excel, alors vous avez certainement vécu ce qui suit : vous ajoutez des lignes de saisie au bas d'une feuille de calcul dont les colonnes servent d'entrées pour une formule longue. Chaque fois que la formule se recalcule, le temps de calcul se fait de plus en plus long. Si vous travaillez sur un ordinateur assez lent, vous pouvez être témoin de ce phénomène par vous-même : comme le nombre de lignes d'entrée augmente linéairement, le temps consommé par la macro croît de façon exponentielle.

Maintenant, si vous faites partie des chanceux à avoir déjà écrit un programme pour un superordinateur, vous avez pu être également témoin du même phénomène. L'échelle peut être différente, mais l'effet est le même. Et si vous lisez les journaux de log du superordinateur, vous pouvez vérifier personnellement cette observation. Pour résumer : il vient un moment où chaque algorithme, aussi simple soit-il, devient tout simplement inapplicable en raison du poids écrasant de ses données d'entrée.

C'est là que l'informatique quantique entre en jeu. En supprimant purement et simplement ce phénomène d'allongement des durées de calcul. En théorie, un ordinateur quantique pleinement fonctionnel deviendra en effet plus performant de façon exponentielle. Comment ? Tout simplement en mettant à l'échelle sa capacité de calcul de façon linéaire. Par conséquent, pour chaque augmentation du nombre d'étapes d'un algorithme quantique, la quantité de temps consommée pendant l'exécution des calculs augmentera d'une plus petite quantité, jusqu'à ce que l'écart de temps entre des charges de travail exponentiellement différentes devienne si infime qu'il ne pourra plus être mesuré.

"Cela signifie tout simplement la fin de la différence entre les problèmes faciles et les problèmes difficiles" a indiqué le chercheur John Preskill, professeur de physique théorique à l'université Caltech lors d'un discours prononcé en 2017. Avec l'informatique quantique, "la différence entre les problèmes que nous pourrons résoudre un jour avec des technologies avancées et les problèmes que nous ne pourrons jamais résoudre car ils sont tout simplement hors de notre portée n'existera plus car nous serons passé d'un monde régi par des règles classiques à un monde régi par des règles quantiques".

Les compromis quantiques

Pour être très clair : il serait inexact de dire qu'un ordinateur quantique exécute des programmes plus rapidement qu'un PC ou un serveur x86. Un "programme" pour un ordinateur quantique s'avère tout simplement d'un ordre différent de tout ce qui a jamais été produit pour un processeur binaire. Il y a un monde entre la traduction d'un problème mathématique intelligible par les professeurs d'université en un programme binaire et la traduction du même problème en un programme d'ordinateur quantique.

Il existe en effet plusieurs compromis fondamentaux à prendre en compte lorsqu'on entre dans le domaine de l'informatique quantique. Dont certains s'avèrent pour le moins intimidants. L'informatique quantique arrive rarement à élaborer une réponse exacte ou définitive à un problème donné. En informatique quantique, il n'existe en effet pas, ou peu, de solution unique pour laquelle tout autre résultat serait une erreur. Au lieu de cela, un ordinateur quantique aura tendance à rendre des ensembles de réponses avec leurs probabilités respectives.

Vous êtes encore là ? OK.

Pensez maintenant à cela : l'appareil au niveau atomique qui effectue les calculs quantiques s'autodétruira lorsque sa tâche sera terminée. Un mécanisme d'informatique quantique se présente en effet comme une machine qui construit automatiquement le dispositif informatique à partir d'atomes (les atomes de calcium sont de bons candidats pour cela). Il maintient les conditions de fonctionnement de ce dispositif pour la durée de son programme, applique le programme, lui permet de s'exécuter, interprète l'état final des registres comme la table de probabilité finale des résultats puis se rétablit pour reconstruire un mécanisme complètement différent.

Imaginez si l'incroyable machine Enigma d'Alan Turing (à télécharger ici) s'effondrait après chaque décodage de code. Maintenant, imaginez si ce dernier, au regard de son génie, reconstruisait cette machine à partir de nouvelles pièces, tous les jours. Chaque ingénieur en informatique quantique a fait plus qu'imaginer un tel schéma, mais a construit un plan pour un tel dispositif à l'échelle quantique. En effet, de tels schémas hypothétiques "sur papier" sont appelés "machines de Turing". Bref, les ingénieurs quantiques croient que leurs ordinateurs peuvent fonctionner et fonctionneront, parce que leurs expériences sur les machines de Turing leur donnent des raisons de le croire.

Les avantages d'un ordinateur quantique

Navigation : un système GPS ne peut pas fonctionner partout sur la planète, et en particulier sous l'eau. Un ordinateur quantique exige pour son fonctionnement que les atomes soient sur-refroidis et en suspension, dans un état qui les rend particulièrement sensibles. Pour tirer parti de cette hypersensibilité, des équipes de scientifiques s'affairent aujourd'hui à mettre au point une sorte d'accéléromètre quantique qui pourrait produire des données très précises sur les mouvements.

Le laboratoire français de Photonique Numérique et Nanosciences réalise actuellement des travaux pour construire un composant hybride qui associe un accéléromètre quantique à un accéléromètre classique, puis utilise un filtre passe-haut pour soustraire les données classiques des données quantiques. Le résultat de leurs recherches pourrait se présenter sous la forme d'un compas

quantique extrêmement précis qui éliminerait les dérives de biais et de facteurs d'échelle couramment associées aux composants gyroscopiques.

Sismologie : cette même sensibilité extrême peut également être exploitée pour détecter la présence de gisements de pétrole et de gaz, ainsi qu'une activité sismique potentielle, dans des endroits où les capteurs conventionnels n'ont pas encore pu être explorés. C'est du moins ce que pense QuantIC, le centre de technologie d'imagerie quantique dirigé par l'Université de Glasgow.

Il a démontré, en juillet 2017, en collaboration avec le fournisseur commercial d'outils photoniques M Squared, comment un gravimètre quantique détecte la présence d'objets profondément enfouis en mesurant les perturbations dans le champ gravitationnel. Si un tel dispositif devient non seulement pratique mais portable, l'équipe estime qu'il pourrait devenir inestimable dans un système d'alerte rapide pour prédire les événements sismiques et les tsunamis.

Produits pharmaceutiques : dans leurs recherches portant sur le traitement de la maladie d'Alzheimer ou de la sclérose en plaques, les scientifiques utilisent des logiciels qui modélisent le comportement des anticorps artificiels au niveau moléculaire. L'an dernier, la société de neurosciences Biogen s'est associée à Accenture, cabinet de conseil en informatique, et à 1QBit, société de recherche en informatique quantique, pour concevoir un nouveau modèle de simulation moléculaire qui pourra être exécuté sur des plateformes classiques, ainsi que sur des plateformes quantiques actuelles et futures.

Une méthodologie mise au point par les chercheurs de 1QBit consiste à traduire des diagrammes moléculaires traditionnels en graphiques remplis de points, de lignes et de courbes qui, bien qu'apparemment plus confus en surface, s'appliquent plus directement à un modèle quantique et pourrait donner des résultats thérapeutiques révolutionnaires.

Passons maintenant à la question plus controversée : supposons que quelqu'un a construit un mécanisme qui a réussi à franchir les obstacles imposés par la physique quantique, produisant un ordinateur quantique complet capable d'exécuter toutes les tâches actuellement reléguées au domaine de la théorie et de la simulation.

Selon les experts dans ce domaine, qu'est-ce qu'un ordinateur quantique devrait alors être capable de faire, en supposant que chaque phénomène que les physiciens ont théorisé et que les scientifiques ont observé et vérifié, est exploitable en fin de compte ?

Physique : Celle-ci devrait être assez évidente. C'est en fait la raison d'être même du concept. Lors d'un discours prononcé en 1981 au Caltech, le professeur Richard Feynman, père de l'électrodynamique quantique (QED), a suggéré que la seule façon de construire une simulation réussie du monde physique au niveau quantique serait via une machine qui obéirait aux lois de la mécanique quantique.

C'est au cours de ce discours que le chercheur a expliqué qu'il ne suffirait pas qu'un ordinateur génère une table de probabilité et, pour ainsi dire, lance des dés. Il lui faudrait de plus un mécanisme qui se comporterait de la même façon que le comportement qu'il prétendrait simuler, pour produire des résultats que les physiciens eux-mêmes n'auraient pas imaginé.

Machine Learning : les systèmes quantiques peuvent être conçus pour "apprendre" des modèles d'états en vagues simultanées énormes plutôt qu'en balayages successifs et séquentiels. Mais si les mathématiques peuvent circonscrire un ensemble de résultats quantiques probables, ils ne peuvent pour l'heure pas simuler comment ces résultats peuvent être atteints. De quoi douter de l'imminence d'un Machine Learning quantique, qui prendra des années à se développer.

Décryptage : ce qui rend les codes de chiffrement si difficiles à déchiffrer, même pour les superordinateurs modernes, c'est le fait qu'ils sont basés sur des facteurs de nombres extrêmement élevés, nécessitant un temps excessif pour être isolés par "force brute".

Un ordinateur quantique opérationnel devrait isoler et identifier ces facteurs en quelques instants seulement, rendant le système de codage RSA obsolète. En 1994, Peter Shor, professeur au MIT, a mis au point un algorithme quantique pour factoriser les valeurs, que les expérimentateurs qui

construisent des systèmes quantiques à faible débit ont déjà testé avec succès, bien qu'avec des quantités plutôt faibles. Lorsque les ordinateurs quantiques à large qubit seront réalité, peu de chercheurs doutent de la puissance de l'algorithme de Shor pour démolir toute la cryptographie actuelle.

Chiffrement : pour certains, il s'agit là d'une réelle opportunité. Un concept appelé distribution de clés quantiques (QKD - quantum key distribution) permet d'espérer théoriquement que les clés publiques et privées que nous utilisons aujourd'hui pour chiffrer les communications pourront bientôt être remplacées par des clés quantiques soumises aux effets de l'intrication.

Théoriquement, toute tierce partie brisant la clé et tentant de lire le message détruirait immédiatement le message pour tout le monde. La théorie de la QKD est basée sur une hypothèse énorme qui doit encore être testée dans le monde réel : que les valeurs produites avec des qubits enchevêtrés sont elles-mêmes enchevêtrées et sujettes à des effets quantiques partout où elles vont.

Qui sont aujourd'hui les acteurs de l'informatique quantique ?

Malgré la remise en cause actuelle de la mondialisation et l'isolationnisme en vogue dans certains pays, l'économie moderne reste mondialisée. Les laboratoires, les universités et les fabricants qui s'intéressent au quantum ont leurs propres intérêts à travers le monde. Il n'y a donc pas de véritable "course aux armements" entre pays pour construire le premier ordinateur quantique complet.

D-Wave Systems

Citons d'abord D-Wave Systems, une entreprise privée qui travaille avec des organismes gouvernementaux américains pour produire des appareils qui effectuent une forme d'informatique quantique, appelée recuit quantique. Aujourd'hui, D-Wave produit un système commercial qui, selon elle, est capable de supporter 2 048 qubits, soit beaucoup plus que ce qui existe actuellement.

Bien que certains continuent de contester l'existence de tels appareils et mettent en doute le caractère "quantique" de ses résultats, il convient de noter que les partenaires de D-Wave au Quantum Artificial Intelligence Laboratory (QuAIL) sont la NASA et Google, tandis que ses partenaires au Quantum Computation Center (QCC) sont Lockheed Martin et l'University of Southern California.

Microsoft

Microsoft participe de son côté à des laboratoires de recherche quantique dans le monde entier, cela dans tous les domaines. Le géant américain finance et soutient activement la recherche en informatique quantique par l'intermédiaire de son groupe QuArC (Quantum Architectures and Computation).

Pour promouvoir les concepts d'algorithmes quantiques, Microsoft a lancé en décembre 2017 un simulateur quantique et un kit de développement, avec un langage de programmation spécifique au domaine appelé Q#, qui sont tous téléchargeables gratuitement et peuvent être intégrés avec Visual Studio ou VS Code.

IBM

Pour sa part, IBM prétend à juste titre avoir construit plusieurs dispositifs de traitement quantique fonctionnels, bien que limités à l'heure actuelle à un réseau de 20 qubits au mieux. Tout comme Microsoft, IBM propose un kit de développement open source appelé Qiskit, et invite les particuliers à expérimenter la production d'algorithmes quantiques à l'aide de son simulateur 32 qubit.

Le géant américain souhaite mener en 2019 des expériences de construction d'ordinateurs quantiques à son laboratoire Thomas J. Watson, en se basant sur des expérimentations récemment synthétisées par des chercheurs de l'Université de Princeton et de l'Université du Wisconsin.
Intel

Intel a travaillé à la fabrication de dispositifs d'informatique quantique comme le prototype de 17 qubits, en utilisant des procédés qui ne seraient pas très différents de la fabrication des supraconducteurs classiques. Le problème est qu'Intel chercherait à remplacer le modèle conventionnel du qubit, qui est supraconducteur et nécessite donc un sur-refroidissement, par une alternative plus tolérante à la température qu'il appelle un qubit de spin.

En juin dernier, la firme américaine a produit une puce d'essai qui, selon elle, est capable de supporter des qubits à la température beaucoup plus douce que -273 degrés Celsius. Une telle puce ne peut cependant pas encore être considérée comme un processeur quantique complet.
L'Union européenne

En avril 2016, l'Union européenne a lancé un projet qu'elle appelle Quantum Technologies Flagship, dans le but de stimuler la recherche et le développement en informatique quantique en Europe. En octobre dernier, cette structure a annoncé le lancement d'une vingtaine de projets connexes, dont l'Alliance Internet Quantum (QIA). Son but n'est rien de moins que la conceptualisation d'un réseau global totalement enchevêtré, permettant théoriquement la transmission instantanée des qubits entre stations répétitives.
Comment pourrait se présenter un ordinateur quantique ?

Comment se présenteront les futurs ordinateurs quantiques ? Il ne s'agira pas d'un ordinateur au sens classique du terme, avec son système de refroidissement, son processeur et sa mémoire. Pour rappel, tout ordinateur électronique classique exploite le comportement naturel des électrons pour produire des résultats conformes à la logique booléenne, qui veut que pour deux états d'entrée spécifiques se trouve un certain état de sortie. Ici, l'unité de base de la transaction est le chiffre binaire ("bit"), dont l'état est 0 ou 1. Dans un semi-conducteur conventionnel, ces deux états sont représentés par des niveaux de basse et haute tension dans les transistors.

A contrario, la structure d'un ordinateur quantique s'avèrera radicalement différente. Son unité de base d'enregistrement d'état est le qubit, qui s'appuie également sur un état 0 et/ou 1. Toutefois, au lieu de transistors, un ordinateur quantique obtient ses qubits en bombardant les atomes de champs électriques perpendiculaires les uns aux autres, ce qui a pour effet d'aligner les ions mais aussi de les maintenir séparés de manière pratique et équivalente. Lorsque ces ions sont séparés par juste assez d'espace, leurs électrons en orbite deviennent, si vous voulez, les adresses personnelles des qubits.

Alors qu'un ordinateur conventionnel se concentre sur la tension, un système quantique est (passivement) concerné par un aspect des électrons au niveau quantique, appelé spin et lié au moment angulaire de l'électron. La raison pour laquelle nous utilisons le terme "quantum" au niveau subatomique de la physique s'appuie sur l'indivisibilité de ce que nous pouvons observer, comme la quantité d'énergie dans un photon (une particule de lumière). Le spin est l'un de ces composants délicieusement indivisibles, représentant le moment angulaire d'un électron lorsqu'il orbite autour du noyau d'un atome.

La rotation d'un électron est toujours, comme le calculent les physiciens, 1/2 ; la seule différence ici est la polarité, qui peut tout simplement être soit "haut" soit "bas". C'est l'état "haut" ou "bas" du spin électronique qui correspond au "1" et au "0" du chiffre binaire typique. Pourtant, c'est ici que l'informatique quantique se transforme en un trou noir logique, à travers un tunnel de bruit blanc, et

nous jette impuissants dans un univers capricieux dont les lois et principes semblent concoctés par l'Université de Toontown.

La superposition et pourquoi vous ne pouvez pas la voir

Un qubit maintient l'état quantique pour un électron. Quand personne ne le regarde, il peut atteindre simultanément l'état "1" et "0". Si vous le regardez, vous ne verrez pas cela se produire, et si cela se produisait avant, cela s'arrête immédiatement. Pourtant, le fait que l'électron du qubit tournait dans les deux sens à la fois, est vérifiable après coup. Il est impossible de voir un électron dans un état de superposition parce que le témoignage exige l'échange même des photons qui provoque l'effondrement d'une telle superposition. Comme l'a sobrement expliqué un professeur de l'université de Fordham : "on ne comprend pas ça, mais on s'y habitue."

Il existe de multiples états de superposition possibles. Voici pourquoi chaque qubit supplémentaire dans un système quantique est plus influent que le précédent. Dans un système à n qubits, le nombre d'états de superposition possibles pour chaque qubit est de 2n. Dans le cadre des ordinateurs binaires, lorsque les processeurs 16 bits ont été remplacés pour la première fois par des processeurs 32 bits, la valeur maximale non signée d'un octet n'était plus 65 535 mais 4 294 967 295. Dans un système quantique, chaque qubit dans un rack de 32 unités d'atomes aurait 4 294 967 296 états de superposition possibles.

Pourquoi cela importe-t-il, si l'état final ne s'effondre qu'à 0 ou 1 de toute façon quand quelqu'un ou quelque chose essaie simplement d'assister au phénomène ? Parce qu'avant cet effondrement, chacun de ces états est une valeur valide et possible. Pendant cette étrange période de boîte noire où il peut fonctionner sans être observé et sans être perturbé, un processeur quantique est capable d'exécuter de véritables fonctions algorithmiques sur des unités qui ressemblent finalement très peu à des chiffres binaires.

Les ingénieurs quantiques ont une façon élégante de représenter les états de spin des qubits, empruntée à un physicien suisse émigré aux Etats-Unis, Felix Bloch, qui a obtenu le prix Nobel de physique en 1952 pour avoir découvert le principe de la résonance magnétique nucléaire. Si vous pouvez imaginer une boule de billard avec un point et une ligne imaginaire à partir du centre de la boule à travers le centre du point et vers l'extérieur comme vecteur, alors vous pouvez imaginer une sphère de Bloch.

Chaque état de superposition qu'un qubit peut prendre peut être représenté par un vecteur dans une sphère de Bloch, auquel vous pouvez penser en termes d'angles sur les axes x et y de la sphère. En utilisant la géométrie ordinaire, le vecteur peut être exprimé en fonction du cosinus de cet angle par rapport à l'axe z, ajouté au sinus de cet angle par rapport à l'axe z.

À quoi ressembleront les premiers programmes quantiques ?

L'astuce dans l'écriture d'un algorithme quantique est d'imaginer que vous pouvez réellement voir, ou mesurer, les qubits dans leurs états de superposition, de sorte que vous puissiez leur donner des instructions sur ce qui se passe ensuite et causer des ajustements à ces états. En réalité, l'acte même de tenter d'assister à une superposition entraîne une décohérence - le retour des qubits à leur état classique 0 ou 1. La décohérence finit toujours par se produire dans un système quantique, souvent après quelques minutes, ou si vous avez de la chance, en moins d'une heure.

Tout l'intérêt d'un programme quantique devient de profiter pleinement de la capacité de manipuler de quelle façon toutes ces boules de billard sont pointées alors que personne ne regarde, avant leur décohérence. Il existe deux types de programmes quantiques, qui fonctionnent très différemment l'un de l'autre :

Un programme utilisant des portes quantiques suivant la suggestion originale de Richard Feynman, pour lequel il pourrait exister d'autres formes de logique dans l'espace quantique. Avec un ordinateur binaire, une porte ET ou OU prendrait deux entrées de tension discrètes comme bits et produirait une certaine sortie. Dans un circuit quantique, plusieurs qubits peuvent être utilisés comme entrées, et le résultat peut être une forme d'état de superposition, que la représentation de la sphère de Bloch décompose en valeurs mathématiques - incluant, très probablement, des nombres complexes.

Un système de recuit quantique, tel que celui que produit actuellement l'onde D-Wave, emprunte une voie très différente. Au lieu d'établir un circuit quantique, un recuit traduit des formules (appelées "Hamiltoniennes") qui décrivent l'état physique du système quantique, en états physiques réels. Alors que n'importe quel ordinateur quantique peut utiliser ces formules pour décrire l'état initial, un recuit utilise des formules similaires pour représenter des changements infimes dans l'état désiré du système, par étapes très incrémentielles sur le chemin vers l'état final désiré. Chaque étape bouleverse les qubits, de telle sorte que leur état à l'étape finale représente l'ensemble des probabilités qui forment la solution finale.

Les perspectives réelles d'un écosystème quantique

Si chaque technologie "révolutionnaire" était garantie de succès financier ou commercial, vous tiendriez aujourd'hui dans vos mains un processeur de bord à commande vocale avec des transistors 3D alimentés par un supraconducteur de la taille d'un dixième de dollar d'une durée de vie d'un demi-siècle, plutôt que ce que vous utilisez actuellement.

L'informatique quantique ne réussira pas vraiment à moins qu'il n'existe un modèle d'affaires viable pour elle. Parce qu'un ordinateur quantique complet n'est pas et ne sera jamais portable (contrairement à une boussole quantique, où la détection des perturbations est le but réel), le seul moyen de le rendre commercial est de l'offrir en tant que service, comme les laboratoires et les universités offrent des services de superordinateurs de nos jours.

Ce ne serait pas un "nuage quantique". Le cloud computing implique une sorte de location, une location de capacité de calcul virtuel ou, dans le cas de la technologie dite sans serveur, l'utilisation d'une solution. Il n'y a pas de division de la location dans l'espace quantique ; il établit la situation hamiltonienne, exécute l'algorithme ou le modèle de recuit, laisse le système exploser, et rend les résultats comme probabilités. Le temps n'est pas un facteur ; un problème plus difficile peut ne pas prendre plus de temps qu'un problème plus simple, donc la location à la minute est inutile.

Ce qui laisse une autre option, celle d'une solution sans serveur. Mais comme les solutions sont des probabilités plutôt que des certitudes, et qu'elles sont sujettes à des variations, les clients vont inévitablement s'interroger sur la valeur des solutions qu'ils obtiennent. Il semblerait que les premiers adeptes de l'informatique quantique incluraient probablement tous ceux qui cherchent à démolir la cryptographie à base de RSA à la première occasion.

Mais pour que les fabricants d'ordinateurs quantiques commencent à en tirer profit, ils voudront une clientèle plus stable que les pirates informatiques en herbe. Ils devront favoriser des communautés de développeurs scientifiques et éducatifs désireux d'apprendre les règles et les pratiques d'un univers complètement nouveau, afin de pouvoir apporter des solutions aux problèmes auparavant insondables auxquels notre propre monde est confronté.

Article "Understanding the how, why and when of quantum computers" traduit et adapté par ZDNet.fr

https://www.zdnet.fr/pratique/tout-comprendre-a-l-informatique-quantique-39891035.htm