NOTE de VEILLE

février 2018

Tous les mois, retrouvez à travers les notes de veille, un dyptique Tendances globales / Actualités locales sur l'innovation et les mondes numériques décrypté par Unitec

L'INFORMATIQUE QUANTIQUE, À L'AUBE D'UNE NOUVELLE ÈRE ?

L'informatique quantique, oui mais encore ?

L'informatique quantique, c'est d'abord de la physique quantique. Elle se différencie de la physique classique du fait de son approche à l'échelle de l'infiniment petit, atomique et subatomique, et des lois physiques qui y régissent ses mondes.

En informatique quantique, on tire parti de deux comportements très différents : la superposition et l'intrication.

La superposition quantique suppose qu'un système quantique, une particule par exemple, peut être dans deux états simultanément, c'est-à-dire posséder plusieurs valeurs pour une certaine quantité observable. Un électron peut disposer par exemple, d'un SPIN (champ magnétique) différent, positif, négatif, ou les deux simultanément.

L'intrication quantique (ou enchevêtrement quantique), est un phénomène impliquant deux particules disposant d'états quantiques dépendants. Cela suppose qu'un changement d'état de l'une de ces particules intriquées, induira automatiquement un changement d'état de son homologue. En reprenant l'exemple de l'électron. Si l'on fabrique 2 électrons dans un état intriqué, la mesure du SPIN négatif de l'un, impliquera obligatoirement un SPIN positif pour l'autre et ce peu importe la distance, remettant en cause le principe de localité et admettant une transmission d'information plus rapide que la lumière.

Ce sont ces deux comportements qui sont à la base de l'informatique quantique, et de toute sa puissance.

> « Si vous croyez comprendre la mécanique quantique, c'est que vous ne la comprenez pas.»
> Richard Feynmann

Quand TIC devient quantique

En informatique classique on manipule l'information sous forme binaire, à l'aide de bits, comptant des 0 et des 1. En informatique quantique, on parle de quantum bit ou Qubit[1], car ils répondent aux lois de la physique quantique et notamment au principe de superposition. La différence est notable, au lieu de disposer de deux états possibles, 0 ou 1, comme on vient de le voir en informatique traditionnelle, ils permettent aux bits d'être 0, 1, voir les deux en même temps. C'est ce procédé qui accélèrerait alors la vitesse de calcul des ordinateurs de façon considérable. En d'autres termes, si un Qubit est dans une quelconque superposition d'états, 2 Qubits permettent de superposer 4 états pour le calcul (2 puissance 2), 10 Qubits permettant de superposer 1024 états (2 puissance 10). Résultat, l'ordinateur quantique peut doubler sa puissance de calcul à chaque Qubit ajouté. Pour 20 Qubits en interactions on atteindrait la puissance théorique d'un ordinateur classique, 40 un supercalculateur, 100...

Une nuance est néanmoins à apporter. S'il se montrera très efficace en matière de factorisation de nombre premier (principe cryptographique sur lequel se base un certain nombre d'algorithmes en sécurité informatique), un ordinateur quantique ne sera pas à même d'être plus rapide pour tous les types de calculs. De fait, s'il est en mesure de traiter plusieurs calculs en parallèle, il ne saura donner qu'un seul résultat et non une analyse d'une multitude de résultats, d'une multitude de calculs comme ça peut être le cas aujourd'hui. De plus, il est nécessaire de créer des algorithmes quantiques à même de gérer cette idée de parallélisme dans les calculs. Il existe donc des problèmes pour lesquels aujourd'hui il n'existe pas d'algorithmes quantiques et qui ne peuvent donc être résolu par l'informatique quantique.

Les défis techniques de l'informatique Quantique

L'ordinateur quantique est soumis à de fortes contraintes. La première vient du phénomène de la décohérence quantique. La **décohérence quantique** stipule que tout acte d'observation sélectionnerait instantanément un seul et unique état parmi l'ensemble des états superposés possibles. En

1 Il existe différentes manières de faire un Qubit. On peut pour cela utiliser le SPIN d'un électron, la polarisation d'un photon ou bien certains circuits supra-conducteurs.

Réalisé par UNITEC en partenariat avec DIGITAL AQUITAINE

d'autres termes, lire un état de Qubit a pour conséquence de détruire sa superposition, il est donc impossible de le lire et sans le lire, il est impossible d'en copier l'information et d'en imaginer une mise à l'échelle. Dès lors, comment programmer un tel ordinateur alors que l'on détruit l'état d'un Qubit quand on le lit et que l'on ne peut pas copier un Qubit ?

La seconde difficulté est donc matérielle avec la nécessité de maintenir isolés du monde extérieur les qubits, afin qu'ils restent stables dans leur état superposé. Pour ce faire, il faut recourir à un ordinateur cryogénique. Pour fonctionner, et stabiliser les processeurs, il faut en effet, les maintenir à 0.013 Kelvin, soit -273.1 degré Celsius. Soit une température plus froide que celle de l'espace (-270). Le but étant d'obtenir un temps de cohérence, c'est-à-dire le temps où cet état de superposition est maintenu, plus important que le temps de calcul. Il semble donc encore difficile de l'imaginer sur votre bureau demain.

Des avancées notables

Face à ces difficultés, le français Atos au travers de sa solution **Quantum Learning Machine**, propose un émulateur du comportement des bits quantiques. En d'autres termes, c'est un supercalculateur miniature émulant un ordinateur quantique de 40 Qubits. Il apporte ainsi une première réponse, en aidant à la conception d'algorithmes quantiques et aidant ainsi le monde de la programmation à se préparer à cette nouvelle ère. **IBM** aurait de son côté mis au point un algorithme de détection d'erreurs qui couplé à son travail sur des Qubits supraconducteurs pourrait répondre à cette question de stabilité du Qubit. Quand Microsoft pencherait, lui, sur l'élaboration de **Qubit Topologique** jugé plus stable, en s'appuyant sur la découverte récente du **fermion de majorana**, une particule qui possède sa propre antiparticule. Ces Qubits prendraient ainsi la forme de tresses de quasi-particules et limiteraient la décohérence quantique.

Depuis 2002 et la première opération de calcul réussie sur un ordinateur quantique de 7 qubits (factorisation du nombre 15, soit 3*5), des avancées se sont faites jusqu'à la sortie en 2011 du premier ordinateur quantique commercialisable, par la société canadienne D-Wave. Depuis les annonces se succèdent et se multiplient. Dernièrement c'est au CES qu'Intel a dévoilé **une puce quantique de 49 qubits.**

Des perspectives et des enjeux immenses

Si l'on semble aujourd'hui encore très loin d'être parvenu à la réalisation d'un ordinateur quantique opérationnel, il n'en reste pas moins un des sujets de recherche majeurs des grands groupes, grandes institutions et autres startups. Microsoft, IBM, la NASA, NSA, **Rigetti**, ou encore **IonQ**, tous y entrevoient l'avenir et la résolution des grandes questions de l'humanité. Tous veulent atteindre la suprématie quantique, c'est-à-dire créer un ordinateur quantique en mesure de supplanter un ordinateur classique.

De fait, les possibilités entrevues sont nombreuses et certaines miraculeuses. L'informatique quantique pourrait permettre la création de nouvelles matières, d'élaborer de nouveaux matériaux supraconducteurs pour le transport de l'énergie ou son stockage, voir d'autres en mesure de capturer le CO2. Certains y voient la possibilité de créer de nouveaux médicaments et d'améliorer le traitement de maladie aujourd'hui incurable, comme la sclérose en plaques ou Alzheimer. L'Américain **Biogen, Accenture et 1Qubit**, travaillent ainsi à la simulation numérique de nouvelles molécules et tente de prouver l'efficacité de l'ordinateur quantique dans le domaine pharmaceutique.

Mais il serait également le moyen de réaliser des intelligences artificielles sans équivalent ou encore d'optimiser les transports et notamment les transports autonomes. Pour exemple, le constructeur automobile **Volkswagen** s'est positionné sur le sujet et entend proposer une solution quantique à l'optimisation du trafic routier et ainsi réduire les problèmes récurrents de congestion qui sévissent dans les grandes villes.

Cependant, cela soulève également certaines questions. La première à laquelle on pense est celle de la cybersécurité. La majeure partie des clés cryptographiques actuelles n'auront plus d'utilité à l'ère de l'informatique quantique. De nombreux chercheurs travaillent à l'élaboration des solutions de chiffrement en mesure de résister à la puissance de Qubit. L'initiative française **Risq** (Regroupement de l'Industrie française pour la Sécurité Post – Quantique) en est un exemple. Partant du principe que l'avènement d'un ordinateur quantique viendrait perturber la sécurité des données et des échanges numériques, ce regroupement entend proposer une gamme complète d'outils de chiffrement, de logiciels et matériels répondant à ces nouvelles contraintes en termes de sécurité, ainsi que des guides pour accompagner les industriels dans l'intégration de ces nouvelles technologies post-quantiques.

Pour l'heure, la réalité est tout autre, et une longue route reste encore à parcourir.

Maël Le Borgne

Vous pouvez nous suggérer des thèmes que vous souhaiteriez voir traités dans une prochaine Note (ou Dossier) de Veille :

veille@unitec.fr | communication@digital-aquitaine.com

avec le soutien de

BÈGLES · MONTESQUIEU · BORDEAUX MÉTROPOLE · RÉGION Nouvelle-Aquitaine

La Région et l'Union européenne soutiennent le projet Détection et accompagnement de jeunes entreprises innovantes 2017 dans le cadre du « Programme Opérationnel FEDER/FSE 2014-2020 »