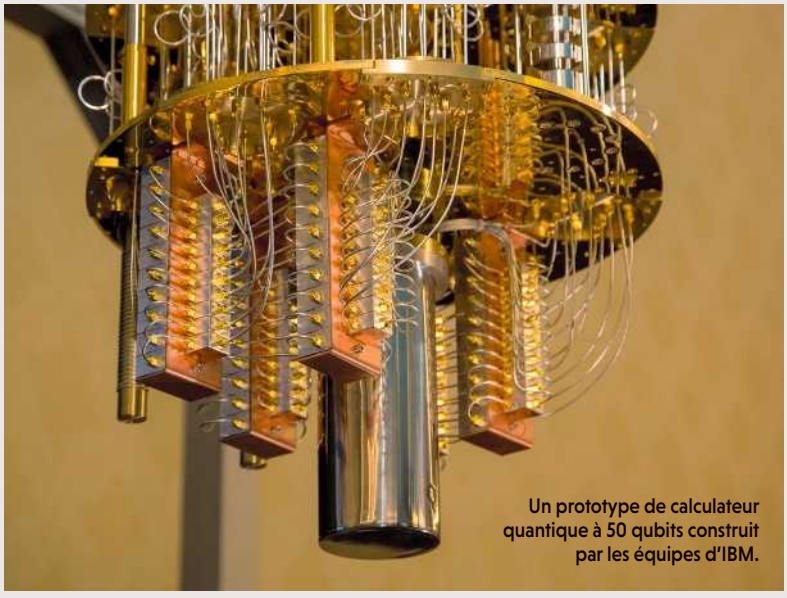
4

LES CALCULATEURS QUANTIQUES



Un prototype de calculateur quantique à 50 qubits construit par les équipes d'IBM.

Depuis vingt-cinq ans, on mène des travaux sur les systèmes de calcul quantique. Ceux-ci, en théorie, seraient capables de calculer plus rapidement que les ordinateurs classiques. Ils utilisent des bits quantiques, ou qubits, au lieu de bits. L'idée repose sur la possibilité de mener, grâce à la superposition quantique, des calculs parallèles en grand nombre et revient à considérer qu'il n'y a pas de limite à l'exactitude de la théorie quantique, même quand elle contredit le principe de densité finie de l'information, lui-même lié à la méfiance que les nombres réels doivent nous inspirer.

L'objectif de la « suprématie quantique » est de mener avec un ordinateur quantique un calcul infaisable avec un ordinateur classique. Il aurait récemment été atteint par Google, mais l'exploit est contesté par les chercheurs d'IBM. Même si l'objectif est atteint, des chercheurs font remarquer que les méthodes envisagées ne produiront rien d'utile, car elles concernent des calculs spécialisés de densités de probabilité qui n'ont pas d'intérêt pratique. Nul n'a prouvé que les recherches concernant les ordinateurs quantiques n'aboutiront pas, mais divers spécialistes, dont Sabine Hossenfelder, physicienne théoricienne à l'institut d'études avancées de Francfort, expliquent qu'il faut rester prudent. Elle écrit : « Quand verrons-nous un ordinateur quantique avec des millions de qubits ? Personne ne sait. Le problème est qu'il est peu probable que les approches dominantes à l'heure actuelle puissent s'adapter pour changer d'échelle. [...] On ne sait pas comment dépasser quelques centaines de qubits. C'est à la fois un problème d'ingénierie et un problème de coût. Cela explique pourquoi, ces dernières années, on a beaucoup parlé des ordinateurs NISQ *(noisy intermediate scale quantum computers)*. Il s'agit en réalité d'un terme inventé pour faire croire aux investisseurs que l'informatique quantique aura des applications pratiques au cours des prochaines décennies. Même s'il est possible qu'on sache prochainement faire fonctionner des NISQ, personne ne sait en tirer quelque chose d'utile. Je ne suis pas très optimiste sur le fait que les ordinateurs quantiques auront bientôt des applications pratiques. Je crains que l'informatique quantique ressemble à la fusion nucléaire ; c'est-à-dire qu'elle reste toujours prometteuse, mais ne fonctionne jamais vraiment. »

> plus vite que la lumière, il semble que les physiciens soient prêts à reconnaître qu'un volume fini d'espace ne peut pas contenir une quantité infinie d'informations.

Les informaticiens Pablo Arrighi, de l'université d'Aix-Marseille et Gilles Dowek, de l'Inria et de l'ENS Paris-Saclay, défendent cette idée d'un principe de densité finie d'information et considèrent qu'il devrait être affirmé clairement, comme celui de la vitesse limitée.

UNE DENSITÉ FINIE D'INFORMATION

Bien sûr, un tel principe empêcherait de croire que la position d'une particule et sa vitesse soient déterminées par des nombres réels dont l'infinité de décimales contient potentiellement une infinité d'informations. Pablo Arrighi et Gilles Dowek proposent une expérience de pensée : « Imaginons une quantité infinie d'informations exprimée sous la forme d'une suite illimitée de 0 et de 1 ; nous pouvons voir cette séquence comme les chiffres d'un nombre réel et écarter les mâchoires d'un pied à coulisse d'une distance correspondant à ce nombre. Cela placerait une quantité infinie d'informations dans un volume fini. Bien sûr, nous avons tous appris que cette idée est absurde et que la distance entre les mâchoires d'un pied à coulisse est fixée avec une précision finie de trois ou quatre chiffres. Il est surprenant que l'affirmation qu'une grandeur physique est toujours définie avec une précision finie n'ait jamais reçu le statut de principe en physique. »

L'idée de ce principe de densité finie d'information, si on savait le rendre précis, aurait une incidence sur les pronostics que l'on fait concernant les capacités futures des ordinateurs quantiques. Le mode de fonctionnement de ces ordinateurs sur lesquels des recherches se poursuivent depuis plus de vingt-cinq ans est la superposition quantique : on obtient dans un volume fini d'espace une grande puissance de calcul en superposant les états quantiques d'un système qu'on fait calculer et qui mène plusieurs calculs en parallèle. Cette possibilité de superposer les calculs est envisagée sans limite et conduirait en théorie à pouvoir dépasser les capacités de calcul des systèmes fondés sur la physique classique.

On sait ainsi comment s'y prendre pour tirer de la mécanique quantique un algorithme fonctionnant en temps polynomial (c'est-à-dire rapidement) pour factoriser les nombres entiers. Cet algorithme conçu par l'Américain Peter Shor en 1995 n'a pas d'équivalent classique connu. Certains systèmes cryptographiques, dont le système RSA notamment utilisé pour les cartes bancaires, s'appuient sur la difficulté de la factorisation. On craint donc que leur sécurité soit mise prochainement en danger.

Pourtant, dès 2003, le logicien Leonid Levin, professeur à l'université de Boston, a exprimé

des réserves sur ce que l'on peut attendre des ordinateurs quantiques. Pour lui, croire aux pouvoirs colossaux des ordinateurs quantiques, c'est croire à la possibilité de la manipulation physique de nombres comportant une très grande quantité de décimales, et c'est donc presque croire à l'existence physique des nombres réels et à la capacité de placer dans un espace fini une quantité illimitée d'informations.

À propos de la mise en œuvre de l'algorithme de Shor, Leonid Levin écrivait: «Le problème majeur réside dans l'idée que les équations quantiques de base restent valides avec plusieurs centaines, voire plusieurs millions, de décimales, car c'est là que résident les chiffres significatifs des amplitudes quantiques pertinentes. Or nous n'avons jamais vu de loi physique valable sur plus d'une dizaine de décimales et, en physique, la prise en compte de nouvelles décimales supplémentaires exige en général de repenser en profondeur les concepts de base d'une théorie.»

Pablo Arrighi insiste au sujet de la mécanique quantique sur la séparation en deux du principe de densité finie d'information: il y a d'un côté l'idée qu'il serait impossible que trop de qubits (bits quantiques) soient présents dans un même dispositif contenu dans un volume fini, et il y a de l'autre l'affirmation des limites aux nombres de décimales des nombres réels utilisés par nos théories (y compris la mécanique quantique).

Aujourd'hui, la réalisation d'ordinateurs quantiques progresse et on réussit avec eux à factoriser des entiers de 7 chiffres. Le nombre 56153 a ainsi été factorisé par un système quantique, avec pour résultat 233×241. Le record atteint en 2018 semble être 4088459 = 2017×2027. Reste que les ordinateurs classiques sont pour l'instant bien supérieurs aux ordinateurs quantiques; par exemple, ils factorisent assez facilement des entiers de 100 chiffres. Les lents progrès du côté quantique ne font guère craindre pour la cryptographie dans l'immédiat. Un rapport de l'Académie des sciences des États-Unis paru en 2019 (*voir la bibliographie*) décrit la situation des recherches en calcul quantique; il est venu refroidir l'enthousiasme excessif des médias en indiquant par exemple qu'il n'y a rien à craindre en cryptographie, au moins pour les dix années à venir.

Même si l'on ne peut pas statuer sur l'objection de Leonid Levin, peut-être faut-il s'interroger sur le principe de densité finie d'information: concerne-t-il la mécanique quantique et sous quelle forme précisément?

Puisque les nombres réels utilisés en physique sont dangereux et sources d'illusions, comment les éviter?

Du côté des mathématiques, plusieurs options se présentent. Plutôt que d'utiliser les nombres réels, on pourrait n'utiliser que les nombres rationnels (nombres quotients de deux entiers). Il serait gênant cependant de ne plus avoir le nombre $\sqrt{2}$!

On pourrait agrandir un peu cet ensemble de nombres en y ajoutant tous les nombres algébriques, qui sont les solutions d'équations polynomiales à coefficients entiers. Notre $\sqrt{2}$ serait alors un nombre acceptable… mais pas le nombre π qui est non algébrique (transcendant). On pourrait considérer tous les nombres calculables, c'est-à-dire définissables par algorithmes. Cette fois, π serait dans le corps de ces nombres calculables, qui est dénombrable: il a autant d'éléments qu'il y a de nombres entiers. Le corps des nombres calculables a d'assez bonnes propriétés et on a étudié sérieusement l'idée d'en faire une base pour la physique, par exemple dans le livre *Computability in Analysis and Physics*, de Marian Pour-El et Ian Richards (Cambridge University Press, 1989 et 2017).

Hélas, avec ces approches, il reste vrai qu'entre deux nombres, il y en a toujours une infinité d'autres. Il n'y a pas non plus de limite à la quantité d'informations contenue dans ces nombres. De plus, l'analyse mathématique que l'on construit avec eux est sensiblement plus compliquée que l'analyse classique. D'où un faible intérêt de la part des physiciens.

LIMITER L'USAGE DES NOMBRES RÉELS?

Du côté des physiciens, diverses approches qui limitent l'usage des nombres réels ont été tentées. La plus importante est sans doute la théorie de la gravitation quantique à boucles, dont Carlo Rovelli, à l'université de Marseille, est un promoteur (*voir* Pour la Science *de juin 2019*). La théorie résulte de la volonté de concilier la notion d'espace-temps de la relativité générale et la mécanique quantique. Elle propose avec sérieux l'idée d'un espace discret. Le formalisme mathématique des réseaux de spin, des graphes portant localement une information finie et dont les nœuds forment l'espace, évite en un sens les volumes finis ayant une densité infinie d'information. Il constitue donc un bon début de réponse aux problèmes évoqués, même si ce n'est pas le but principal de la théorie.

Une conséquence de cette conception de l'espace est qu'en se contractant, les trous noirs finiraient, à cause de la non-divisibilité infinie de l'espace, par rebondir et devenir des trous blancs (*voir* Pour la Science *d'août 2019*), que l'on tente aujourd'hui d'observer.

Disposerons-nous bientôt d'une théorie utilisable et efficace, proposant des outils mathématiques raisonnables pour modéliser la réalité physique et évitant les pièges des modèles à contenus excessifs d'informations? Nous l'ignorons, mais ce n'est pas impossible. Et dans ce cas, cela prouverait le bien-fondé des soucis que ressentent de nombreux physiciens et philosophes. ■

BIBLIOGRAPHIE

Quantum computing. Progress and prospects, *National Academies Press*, 2019 (https://doi.org/10.17226/25196)

N. Gisin, **Indeterminism in physics, classical chaos and Bohmian mechanics. Are real numbers really real ?**, *David Bohm Centennial Symposium, London, Oct. 2017*, 2019 (https://arxiv.org/pdf/1803.06824.pdf).

P. Arrighi et G. Dowek, **The principle of a finite density of information**, dans H. Zenil, *Irreducibility and Computational Equivalence*, Springer, pp. 127-134, 2015.

C. Rovelli et F. Vidotto, **Covariant loop quantum gravity : An elementary introduction to quantum gravity and spinfoam theory**, Cambridge University Press, 2014.

D. Ruelle, **Are real numbers the same for physicists and mathematicians ?**, 2012 (https://bit.ly/31rJ3SW).

L. Levin, **Polynomial time and extravagant models**, *Problems of Information Transmission*, vol. 39(1), pp. 92-103, 2003.

R. Penrose, **L'esprit, l'ordinateur et les lois de la physique**, Dunod, 1997.