

a mis au point un algorithme quantique accomplissant la factorisation de nombres à N chiffres en une série d'étapes augmentant non pas exponentiellement, mais comme N^2 . Dans le cas d'autres types de problèmes, telle la recherche au sein d'une longue liste, les ordinateurs quantiques offrent des avantages moins marquants, mais ils seront tout de même notablement plus avantageux que les ordinateurs classiques. Certes, tous les algorithmes quantiques ne sont pas aussi efficaces que l'algorithme de

Shor, et nombre d'entre eux ne sont pas plus rapides que leurs équivalents classiques.

Pour toutes ces raisons, les premières applications pratiques des ordinateurs quantiques ne seront sans doute pas la factorisation, mais la simulation d'autres systèmes quantiques, tâche dont la durée dans les ordinateurs classiques augmente exponentiellement avec la taille des données. De telles simulations pourraient avoir un énorme impact en pharmacie ou dans le développement de nouveaux matériaux.

Pour autant, les ordinateurs quantiques n'existent pas encore. Ceux qui ne croient pas à la possibilité d'en réaliser mettent en avant le problème de l'enchaînement d'opérations logiques successives. En effet, outre les difficultés techniques liées à la manipulation d'atomes ou de photons uniques, il faut empêcher – et c'est le principal problème – que le calcul quantique ne soit perturbé par les interactions du système quantique, qui stocke et traite l'information, avec son environnement. Ce processus, que l'on nomme la décohérence, est souvent présenté comme une limite fondamentale au calcul quantique.

En fait, ce n'est pas le cas. La théorie quantique fournit des moyens de corriger les erreurs dues à la décohérence. En effet, si les sources d'erreurs satisfont certaines conditions – par exemple si les erreurs aléatoires se produisent indépendamment sur chacun des bits quantiques et si les portes logiques fonctionnent de façon assez précise –, alors il est possible de faire fonctionner les calculateurs quantiques de façon stable et aussi longtemps que l'on voudra.

Repousser les limites des mathématiques

Le cas des nouvelles fonctions logiques illustre le fait que les progrès de la connaissance du monde physique entraînent aussi des progrès en logique et en calcul. Bien que les vérités mathématiques soient indépendantes de la physique, nous en acquérons souvent la connaissance en exploitant des phénomènes physiques. Une démonstration mathématique est une suite d'opérations logiques. Donc, ce qui est démontrable ou non dépend des fonctions logiques (telle la fonction NON) que les lois physiques permettent de réaliser.

Ces fonctions doivent être assez simples sur le plan physique pour que nous ne puissions douter de leur fonctionnement, et notre confiance sur ce point est enracinée dans notre connaissance du monde physique. Puisqu'elle ajoute au répertoire des opérateurs logiques disponibles de nouvelles fonctions, telles que la « racine carrée » de NON, la physique quantique permettra aux mathématiciens de franchir des barrières que l'on supposait exister dans le monde des abstractions pures.

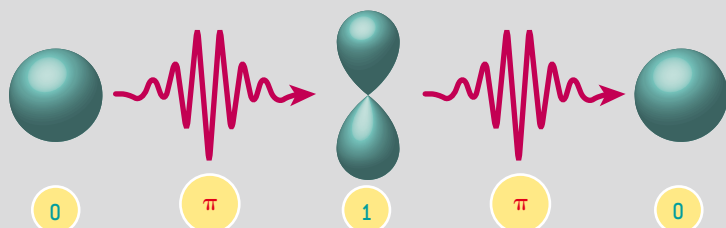
Supposons par exemple que la résolution d'un problème mathématique dépende de

IMPOSSIBLE? MAIS NON !

Les ordinateurs quantiques seront non seulement capables de faire tout ce que font aujourd'hui les ordinateurs classiques, mais ils pourront aussi accomplir de nouvelles fonctions logiques. Dans l'exemple ci-dessous, deux états électroniques d'un atome représentent les deux valeurs possibles d'un bit. Dans un état ou l'autre d'un tel bit atomique, l'électron n'a ni position ni vitesse définies : il s'étale sur des régions sphériques ou ovales nommées orbitales (en vert), et sa vitesse a toute une plage de valeurs différentes simultanées. Néanmoins, les deux états ont une énergie bien définie, qui détermine la valeur du bit.

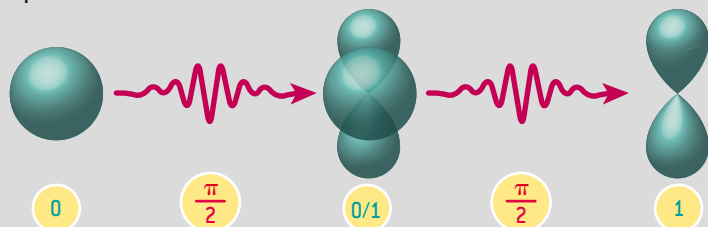
La fonction logique NON ordinaire

Pour effectuer l'opération logique la plus élémentaire, celle que l'on nomme NON et qui consiste à inverser la valeur d'un bit, on procède en envoyant des impulsions lumineuses de fréquence, durée et intensité adéquates (on les nomme des impulsions π). Si l'électron est initialement dans l'état 0, il se retrouve alors dans l'état 1, et vice-versa.



La racine carrée de NON

Cette procédure peut être modifiée afin de créer une opération qui n'existe pas en électronique conventionnelle : la « racine carrée de NON ». Pour ce faire, une impulsion dite $\pi/2$, d'amplitude plus faible et de durée plus courte que l'impulsion π , transforme l'état électronique 0 ou 1 en une superposition de ces deux états ; une seconde impulsion $\pi/2$ fait alors passer l'électron soit dans l'état 1 (s'il était au départ dans l'état 0), soit dans l'état 0 (s'il était au départ dans l'état 1). De telles nouvelles fonctions logiques confèrent aux ordinateurs quantiques une puissance énorme.



la détermination des facteurs premiers d'un énorme entier N . Supposons que N soit si énorme que, même si toute la matière de l'Univers avait été utilisée pour construire un ordinateur classique qui calculerait depuis que l'Univers existe, cette machine ne serait toujours pas capable de factoriser N . Or un ordinateur quantique pourra fournir les facteurs premiers rapidement, clef sans laquelle le problème mathématique resterait sans solution. Autrement dit, la physique quantique permettrait aux mathématicques de repousser leurs limites.

Puisque de nouveaux types de calculs sont possibles grâce aux phénomènes quantiques, pourquoi les physiciens ont-ils craint que la théorie quantique limite le progrès scientifique ? La réponse remonte à l'époque où cette théorie est née sous le nom de mécanique quantique. Erwin Schrödinger (1887-1961), l'un de ses pères, puisqu'il est l'auteur de son équation fondamentale, prévint un jour son auditoire qu'il allait dire quelque chose qui pouvait être considéré comme insensé : il déclara alors que son équation décrit toutes les évolutions possibles d'une particule, lesquelles ne sont « pas des alternatives, mais se produisent vraiment toutes simultanément ». Ce lauréat du prix Nobel de physique de 1933 ne faisait en fait qu'affirmer que son équation décrit la réalité ! Pour autant, Schrödinger éprouvait par avance le besoin de se défendre du risque qu'on le prenne pour un fou.

Une philosophie qui s'est égarée

Pourquoi en était-il ainsi ? Parce qu'au début du XX^e siècle, la plupart des physiciens étaient sous l'influence de doctrines philosophiques entravant l'acquisition de nouveaux savoirs. La physique fondamentale est en fait si intimement liée à la philosophie qu'au début du XX^e siècle, l'influence de cette dernière a pu avoir des effets nocifs sur des parties entières de la physique. Ces doctrines problématiques sont l'empirisme logique (« Si ce n'est pas vérifiable par l'expérience, cela n'a pas de sens. »), l'instrumentalisme (« L'essentiel est que les prédictions marchent, inutile de se préoccuper de ce qui les amène. ») et le relativisme philosophique (« Les affirmations ne sont pas objectivement vraies ou fausses, elles ne sont que légitimes ou illégitimes dans une culture particulière. »).

Tous ces courants ont en commun de s'opposer au réalisme philosophique, à savoir à l'idée pleine de bon sens que le monde physique existe et que la méthode scientifique permet d'accumuler des connaissances sur lui.

C'est dans cette atmosphère philosophique que le physicien Niels Bohr a développé son influente interprétation de la théorie quantique, qui nie la possibilité de parler de phénomènes comme s'ils existaient objectivement. On n'y est pas autorisé à se demander quelles valeurs prennent les grandeurs physiques tant qu'on ne les mesure pas. Les physiciens, qui, par vocation, ne peuvent s'empêcher de se poser de telles questions, ont essayé de ne plus le faire, et la plupart d'entre eux ont formé leurs étudiants à ne pas le faire. La théorie à la pointe du domaine scientifique le plus fondamental semblait contredire l'existence même d'une réalité physique connaissable objectivement.

Certains philosophes, tels Bertrand Russell et Karl Popper, n'ont pas abandonné le réalisme. Tous les physiciens non plus : Einstein (1879-1955) et David Bohm (1917-1992) se sont opposés au courant dominant, puis Hugh Everett (1930-1982) a proposé que les quantités physiques prennent réellement plus d'une valeur à la fois (ce qui est notre vision des choses). Toutefois, dans l'ensemble, les philosophes ne se sont pas intéressés vraiment à la réalité, et même si les physiciens ont continué à se servir de la théorie quantique dans un grand nombre de leurs domaines, la recherche sur la nature exacte des phénomènes physiques s'est égarée.

La situation s'améliore depuis deux ou trois décennies, et l'on peut dire que c'est la physique qui a remis la philosophie sur les rails. Les gens veulent de toute façon comprendre la réalité, et nous dépassons enfin les limites assignées par des points de vue philosophiques néfastes.

Et si la théorie quantique finit par être réfutée, de sorte que des barrières plus fondamentales empêchent la construction d'ordinateurs quantiques ? Ce serait stimulant, car cela nous permettra non seulement de faire évoluer la physique fondamentale, mais aussi sans doute d'envisager des techniques de calcul encore plus fascinantes. La théorie de « ce qui met la théorie quantique en défaut » ne peut qu'être prometteuse, de sorte que, d'une façon ou d'une autre, il n'y aura pas de limite au savoir et au progrès. ■



LA GRAVURE DE FLAMMARION, qui date du XIX^e siècle, soulève la question des limites à la connaissance et de la possibilité de les franchir.

■ BIBLIOGRAPHIE

D. Deutsch, *The Beginning of Infinity : Explanations That Transform the World*, Penguin, 2011.

Le monde quantique, *Dossier Pour la Science* n° 68, juillet-septembre 2010.

C. Monroe et D. Wineland, *Calcul quantique avec des ions*, *Pour la Science*, n° 374, décembre 2008.

S. Aaronson, *Les limites du calcul quantique*, *Pour la Science*, n° 367, mai 2008.

J. Horgan, *L'ordinateur en mathématiques*, *Pour la Science*, n° 194, décembre 1993.