

3

TOUS LES CHIFFRES IMPORTENT

En physique classique, on utilise des nombres réels pour représenter les variables physiques. On considérera par exemple la fonction continue f vérifiant $f(x) = 2x$ si x est compris entre 0 et $1/2$, et $f(x) = 2(1 - x)$ si x est compris entre $1/2$ et 1, pour représenter l'évolution de la coordonnée longitudinale d'un point quand on applique la transformation du boulanger à une pâte qui est allongée puis repliée en deux sur elle-même de manière répétée (on itère l'application de la fonction f à la coordonnée initiale).

L'étude de cette transformation déterministe illustre l'importance de tous les chiffres du nombre réel x donnant la coordonnée d'un point initial quand on suit sa position lors de la manipulation répétée du boulanger. On observe le phénomène de la « montée des chiffres » : les chiffres les plus loin dans le développement en base 2 de x prennent progressivement de plus en plus d'importance en s'approchant de la virgule. Prenons par exemple pour coordonnée initiale le nombre x_0 , écrit en base 2, est :

$x_0 = 0,0100100010000100000100000010000001...$
La suite des nombres $x_n = f(x_{n-1})$ donnant sa position quand on applique successivement la transformation du boulanger est représentée ci-dessous.

$x_0 = 0,0100100010000100000100000010000001...$
 $x_1 = 0,100100010000100000100000010000001...$
 $x_2 = 0,11011101111011111011111101111110...$
 $x_3 = 0,01000100001000001000000100000001...$
 $x_4 = 0,1000100001000001000000100000001...$
 $x_5 = 0,1110111101111101111101111110111110...$
 $x_6 = 0,00100001000001000000100000001...$
 $x_7 = 0,0100001000001000000100000001...$
 $x_8 = 0,100001000001000000100000001...$

est indéterministe. Pour Nicolas Gisin, il s'agit là d'une illusion, et elle est due à l'usage des nombres réels pris trop au sérieux et de la confusion déjà évoquée entre modèle et réalité.

Pour Nicolas Gisin, « la physique classique n'est déterministe que si l'on attribue à l'outil que sont les nombres réels une signification physique. Dès que l'on réalise que les nombres réels mathématiques ne sont "pas vraiment réels", c'est-à-dire qu'ils n'ont aucune signification physique, il s'ensuit que la physique classique n'est pas déterministe. »

En effet, quand on considère l'évolution d'un système physique, par exemple quelques particules ponctuelles à partir d'une situation initiale donnée, elle n'est effectivement déterminée de manière unique et calculable instant après instant qu'à la condition que les données initiales (les positions et vitesses des particules) soient connues avec une précision infinie. Cela revient à prendre au sérieux que les variables physiques sont bien équivalentes à des nombres réels comportant une infinité de décimales.

UNE MÉCANIQUE QUI NE SUPPOSE PAS D'INFORMATIONS INACCESSIBLES

Nicolas Gisin a imaginé une théorie équivalente à la mécanique classique dans laquelle on considère que le système initial dont on étudie l'évolution n'est connu qu'avec une précision limitée, et que ce n'est qu'une fois que le système physique évolue et lorsque c'est nécessaire que les décimales non connues au départ sont fixées, cela de manière différée et aléatoire. Il défend que « cette alternative à la mécanique classique est plus naturelle, car elle ne suppose pas d'informations inaccessibleles. »

Tout ce qu'est capable de prévoir la mécanique classique est prévu de la même façon par la mécanique alternative de Gisin, et nous avons autant de raisons de croire en cette mécanique non déterministe que nous en avons de croire en la mécanique classique déterministe.

Nicolas Gisin en déduit que la question : « La physique classique est-elle déterministe ? » n'est pas une question scientifique.

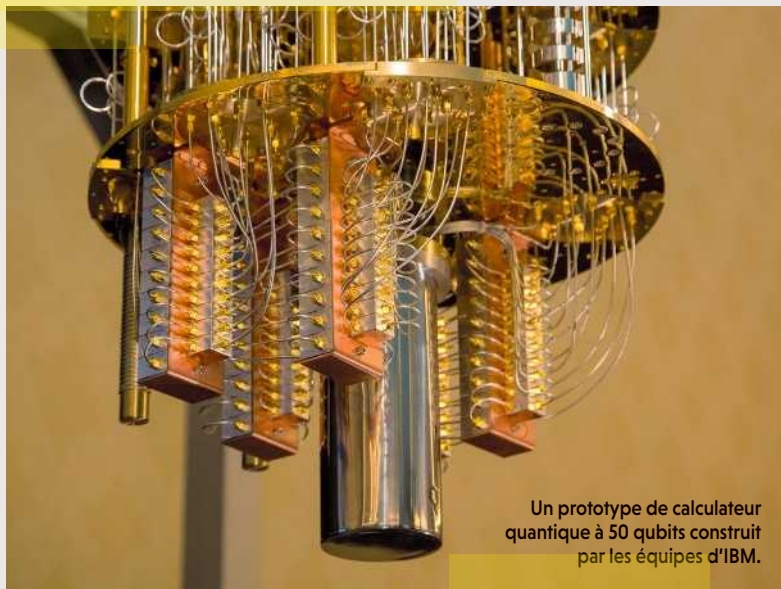
Pour compléter sa démonstration, il revient sur la théorie de De Broglie-Bohm de la mécanique quantique qui, en utilisant l'idée qu'existeraient des variables cachées, propose une version déterministe de la mécanique quantique. Bien que cette théorie ait peu de défenseurs, elle n'a pas été réfutée et on peut donc affirmer que, pas plus que la mécanique classique ne décrit vraiment un monde déterministe, la mécanique quantique n'en décrit un vraiment indéterministe.

La mécanique classique et la mécanique quantique sont chacune, au choix, déterministe ou non déterministe et il n'existe pas de moyen empirique pour départager les options. Hervé Zwirn est d'accord avec Nicolas Gisin sur ce point de vue : « La question de savoir si la nature est déterministe ou pas est une fausse question épistémologique qui n'a pas de solution. Elle semble grammaticalement poser une question qui concerne la nature elle-même alors qu'en fait, elle concerne nos moyens de description. »

Une autre raison doit nous rendre méfiants vis-à-vis des nombres réels utilisés en physique. Elle est liée à l'existence des principes de finitude : de même qu'il existe un principe physique fondamental stipulant qu'aucun objet réel et qu'aucune information ne peut voyager

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