INFORMATIQUE

L'ordinateur quantique : un domaine de recherche en pleine expansion

En 2011, l'entreprise américaine D-Wave annonçait la commercialisation du premier ordinateur quantique. Cette irruption d'une entreprise privée dans un secteur dominé par la recherche fondamentale publique faisait l'effet d'une petite bombe. Aucun chercheur ne croyait atteindre cet objectif si rapidement. Nous discutons ici des perspectives ouvertes par le calcul quantique, avant de revenir sur le cas D-Wave.

PAR MANUEL HOUZET*

L'industrie des ordinateurs actuels s'est développée en utilisant deux découvertes majeures : le transistor en silicium (John Bardeen, Walter Brattain et William Shockley, 1947) et la théorie de l'information (Claude Shannon, 1948)[1]. La première découverte a permis de concevoir des transistors de tailles de plus en plus réduites. En assemblant un nombre croissant de transistors sur une surface de plus en plus petite, les microprocesseurs sont devenus de plus en plus puissants. Dans les années 1990, la miniaturisation a fait passer l'industrie informatique des microtechnologies aux nanotechnologies – les tailles typiques passant du micron au nanomètre[2]. La seconde découverte a indiqué comment transmettre l'information de la façon la plus fiable et la moins coûteuse en temps et en énergie. Cette information est codée en langage binaire, c'est-à-dire en séquence de 0 et de 1 aussi appelée bit[3]. Les transistors permettent de réaliser des portes logiques effectuant des opérations : la valeur des bits en sortie d'une porte est entièrement déterminée par leur valeur en entrée. Ces opérations forment la base du calcul informatique que la théorie de Shannon a permis d'optimiser.

La loi de Moore rend compte du doublement de la densité de transistors dans les microprocesseurs tous les 18 mois. Il existe pourtant une limitation fondamentale à la miniaturisation : l'échelle quantique.

DE PLUS EN PLUS PETIT

La miniaturisation se poursuivant, on assiste depuis plusieurs années à l'apparition d'applications toujours plus performantes. Une loi empirique formulée par G. Moore en 1965 continue de rendre compte du doublement de la densité de transistors dans les microprocesseurs tous les 18 mois. Il existe pourtant une limitation fondamentale à la miniaturisation : l'échelle quantique ! En effet, les dimensions des transistors des ordinateurs ou smartphones commencent à s'approcher de quelques nanomètres, alors que les atomes dont ils sont constitués sont de l'ordre d'une fraction de nanomètre. Lorsque le canal d'un transistor n'est plus défini par un nombre suffisant d'atomes, les performances de ce dernier se dégradent. La mécanique quantique qui détermine les propriétés des électrons en est la cause. En effet, le courant électronique qui s'écoule à travers un transistor classique implique un grand nombre d'électrons, dont les propriétés moyennes peuvent être décrites semi-classiquement comme celles d'un fluide[4]. Lorsque leur taille diminue, le comportement quantique de chaque électron entraîne des déviations significatives par rapport au comportement classique moyen. La taille des atomes induit donc une limitation fondamentale à la miniaturisation… Les technologies actuelles se rapprochent inéluctablement du régime où la physique quantique ne garantira plus un fonctionnement fiable des circuits électroniques ! Loin de n'être qu'une nuisance, les effets quantiques pourraient au contraire s'avérer très utiles.

LE TEMPS DE CALCUL

Une autre limitation de nos ordinateurs classiques est qu'ils ne sont pas adaptés pour résoudre certains problèmes dans un temps raisonnable. Ainsi un voyageur voulant visiter Paris, Londres, Madrid et Rome dans un ordre quelconque, mais en parcourant une distance minimale, devra examiner toutes les possibilités pour trouver le choix optimal. Ou encore, pour factoriser un nombre entier en produit de facteurs premiers[5], nous apprenons à l'école que l'on peut examiner s'il est divisible par les nombres premiers connus (2, 3, 5, 7…). Dans ces exemples, le temps mis par les ordinateurs classiques pour résoudre le problème devient dramatiquement grand si le nombre de villes à parcourir ou la taille du nombre augmentent[6]. En particulier, l'impossibilité de factoriser les très grands nombres est utilisée en cryptographie pour garantir la sécurité des informations échangées sur un réseau de télécommunication. Pour envisager une alternative à l'informatique classique, une piste qui semble prometteuse consiste à utiliser les états dits enchevêtrés, propres à la mécanique quantique. Considérons un système quantique à 2 niveaux pouvant se trouver dans l'état 0, correspondant à l'occupation de l'un des états, ou dans l'état 1, correspondant à l'autre état. En outre, à la différence des systèmes classiques, le système quantique peut se trouver dans n'importe quelle superposition de ces deux états. Le bit quantique, ou qubit, ainsi réalisé permet de coder infiniment plus d'information que le bit classique. Soient deux qubits a et b placés dans une superposition des états 0a et 1b d'une part, et des états 1a et 0b d'autre part. Les états 0a1b et 1a0b sont enchevêtrés : si on mesure le qubit a dans un état particulier (0 ou 1), alors on sait que le qubit b se trouve automatiquement dans l'autre état (1 ou 0). Pour autant, aucune des deux possibilités n'était prédéterminée dans l'état quantique initial.

DES PARADOXES DE LA MÉCANIQUE QUANTIQUE

Cet enchevêtrement a fasciné les « inventeurs » de la mécanique quantique dès les années 1920. Il a donné lieu à la formulation de nombreux paradoxes qui ne peuvent pas être expliqués en physique classique. Ainsi, Albert Einstein, Boris Podolsky et Nathan Rosen (EPR) ont discuté en 1935 comment le résultat de la mesure de deux qubits a et b séparés spatialement pourrait signifier qu'une information a été échangée instantanément, en violation du principe de causalité de la théorie de la relativité (limitant la vitesse maximale de propagation d'une information par celle de la lumière)[7]. Un autre paradoxe célèbre est celui du chat de Schrödinger enfermé dans une boîte où se trouve un qubit (microscopique) capable, selon son état, de déclencher l'ouverture d'une fiole empoisonnée (macroscopique). La physique quantique prévoit que le chat se trouve dans une superposition quantique entre les états "mort" et "vivant". C'est seulement lorsqu'on ouvre la boîte qu'on projette classiquement le chat dans l'état "mort" ou "vivant" ! À l'origine, ces paradoxes étaient conçus comme des expériences de pensée montrant que la mécanique quantique aboutit à des conséquences défiant notre imagination. Alain Aspect a réussi à réaliser l'expérience EPR avec des photons (grains de lumière) se comportant comme des qubits (1980-82). Le domaine de l'optique quantique auquel la France a apporté des contributions importantes (prix Nobel de Claude Cohen-Tannoudji en 1997 et Serge Haroche en 2012) a longtemps été en pointe pour la réalisation de qubits avec des atomes piégés entre deux miroirs. Depuis, de nombreux systèmes ont été proposés pour réaliser des qubits plus facilement manipulables. Des atomes artificiels réalisés avec des circuits supraconducteurs ont permis d'obtenir des résultats similaires et des portes quantiques manipulant de tels qubits ont été construites. De nombreux paradoxes de la mécanique quantique ont alors pu être testés en laboratoire.

Au-delà de l'exploration des principes de base de la physique, le calcul quantique (…) pourrait permettre de résoudre des problèmes dont la solution n'est pas accessible en temps raisonnable sur un ordinateur séquentiel classique

DES PROBLÈMES DE CALCUL QUI DEVIENDRONT ACCESSIBLES

Au-delà de l'exploration des principes de base de la physique, l'intérêt du calcul quantique et d'un éventuel ordinateur quantique repose sur le fait que la manipulation d'un grand nombre de qubits massivement enchevêtrés pourrait permettre de résoudre des problèmes dont la solution n'est pas accessible en temps raisonnable sur un ordinateur séquentiel classique. En 1994, Peter Shor a proposé un algorithme quantique efficace pour le problème de factorisation. Il a été testé expérimentalement avec un nombre modeste mais croissant de qubits. On a ainsi factorisé 21 = 3 x 7 en 2012 ! L'ordinateur quantique de D-Wave évoqué précédemment a, lui, été conçu pour résoudre le problème du voyageur. Les chercheurs ont en fait testé ses performances et n'ont pas observé de gain de temps par rapport aux ordinateurs traditionnels. Cependant, les compétences acquises par D-Wave sont déjà impressionnantes et ont convaincu Google et la NASA de s'associer à la conception d'un prototype de deuxième génération. La réalisation d'un ordinateur quantique autrement plus performant pourrait rester une chimère. Il est cependant indéniable que ce domaine de recherche a beaucoup fait progresser notre compréhension de la mécanique quantique. Prédire quelles seront les véritables applications qui en résulteront est une tâche difficile. De ce point de vue, il est important que les financements attribués à ce type de recherche préservent l'esprit de curiosité comme moteur des progrès futurs. ■

Le super calculateur de la Nasa situé à Columbia (USA)

***MANUEL HOUZET est chercheur en physique (manuel.houzet@cea.fr)**

(1) Ces découvertes ont été faites au sein du même laboratoire de recherche fondamentale (Bell labs) hébergé par une entreprise privée du secteur des télécommunications (AT&T) aux Etats-Unis, au sein duquel les chercheurs (parmi lesquels 7 prix Nobel) disposaient d'une très grande autonomie thématique et financière, et qui a disparu au début des années 2000.
(2) Cf. Les nanosciences : enjeux scientifiques et sociétaux, A. Lopes et J.-N. Aqua, numéro 1 de Progressistes (préciser ?).
(3) « Bit » est l'acronyme de binary digit (chiffre binaire en anglais).
(4) En toute rigueur, la mécanique quantique est aussi nécessaire pour dériver les propriétés de ce fluide, dont le comportement est plutôt qualifié de semi-classique.
(5) Les nombres premiers sont des nombres entiers uniquement divisibles par 1 et par eux mêmes.
(6) En pratique, aucun ordinateur classique ne peut résoudre le problème du voyageur avec quelques centaines de milliers de villes ou factoriser des nombres écrits avec quelques centaines de chiffres.
(7) Un tel effet caractérise en fait la non-localité des lois de la mécanique quantique.