sion $\pi/2$, puis une seconde. Quand nous mesurons alors l'état de cet électron, on trouve qu'il est dans l'état 1, et cela dans 100 pour cent des mesures *(voir l'encadré page 52)*. Au lieu d'être « floue », l'observable a été rendue précise.

Pour comprendre l'importance d'une telle manipulation, envisageons la porte logique la plus élémentaire d'un ordinateur, la porte NON. Avec cet élément de base des circuits logiques, le signal d'entrée, 0 ou 1, est transformé en son contraire, c'est-à-dire en 1 ou 0. Supposons maintenant que l'on se pose le problème suivant : construire la « racine carrée » de NON, c'est-à-dire une porte logique qui, agissant deux fois de suite sur une entrée, produit sa négation. À partir des portes logiques classiques, ce problème est sans solution, alors qu'une impulsion $\pi/2$ résout le problème pour un bit quantique atomique, puisque la succession de deux impulsions $\pi/2$ inverse 0 en 1, ou 1 en 0. Des expérimentateurs ont obtenu des portes « racines carrées » et d'autres portes logiques impossibles en contexte classique à l'aide de bits quantiques constitués de photons, d'ions piégés, d'atomes ou encore de spins. Tous ces composants nouveaux constituent les éléments de base d'un ordinateur quantique.

Des algorithmes bien plus puissants

Lancé dans une tâche, un ordinateur, classique ou quantique, accomplit une séquence précise d'instructions – un algorithme. Or, on quantifie l'efficacité d'un algorithme en évaluant l'augmentation de son temps d'exécution quand l'importance (en quantité, en taille,…) des entrées augmente. Le temps nécessaire à la multiplication de deux nombres à N chiffres par l'algorithme habituel (celui que nous avons appris à l'école) augmente par exemple comme N^2. En revanche, le temps de calcul nécessaire pour accomplir, par la méthode la plus rapide que nous connaissions, l'opération inverse, c'est-à-dire la factorisation d'un nombre en ses facteurs premiers, augmente plus vite que toute puissance de N. L'algorithme de factorisation est donc considéré comme inefficace.

Toutefois, en permettant de construire de nouvelles portes logiques, la mécanique quantique rend de nouveaux algorithmes possibles. L'un des exemples les plus frappants est la factorisation d'un nombre. En 1994, Peter Shor, aux Laboratoires *Bell*,

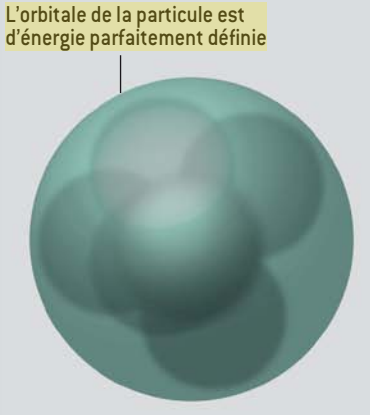
COMMENT DÉPASSER LES LIMITES DU CALCUL QUANTIQUE

Le monde microscopique est régi par des lois quantiques, et cela passe pour un obstacle infranchissable pour la miniaturisation en électronique. Toutefois, les physiciens ont appris à contourner les obstacles qui les inquiétaient tant. Et l'on peut s'attendre à ce que les ordinateurs atteignent leur plein potentiel au niveau quantique. Ils dépasseront alors de loin les machines actuelles.

Principe d'incertitude de Heisenberg

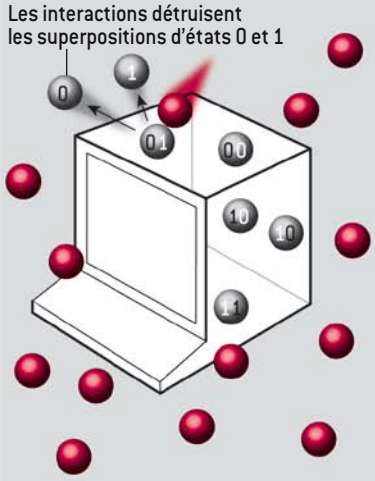
PROBLÈME : Ce principe quantique fondamental limite la précision de certaines mesures. Ainsi, si l'on détermine exactement la position d'une particule, elle aura tout un éventail de vitesses simultanées ; si, au contraire, c'est sa vitesse que l'on mesure exactement, sa position s'étalera de manière inéluctable. C'est pourquoi l'utilisation de la position et de la vitesse est inappropriée au stockage et au traitement de l'information.

SOLUTION : Dans des situations où la vitesse et la position ne peuvent qu'être incertaines, d'autres grandeurs observables peuvent au contraire être bien définies. C'est souvent le cas de l'énergie, mais dans les situations où l'énergie est incertaine, d'autres grandeurs observables conviennent.

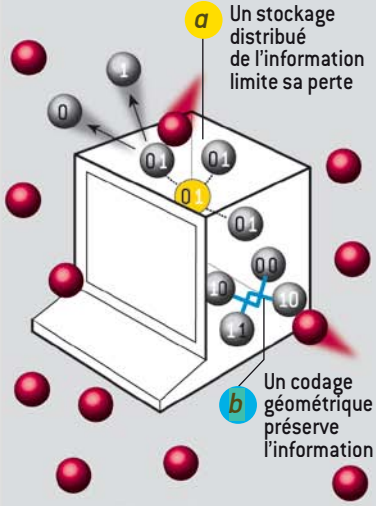


La décohérence des états de superposition

PROBLÈME : Les particules dont est formé un ordinateur interagissent avec leur environnement, ce qui fait perdre l'information stockée et fausse les calculs quantiques.



SOLUTION : Des techniques de correction d'erreurs peuvent compenser les effets de la décohérence assez longtemps pour que le calcul quantique s'achève. On peut par exemple répartir l'information quantique sur de multiples particules *(a)* ou la coder sous une forme géométrique, qui sera résistante par nature aux perturbations *(b)*.



Jen Christiansen

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.

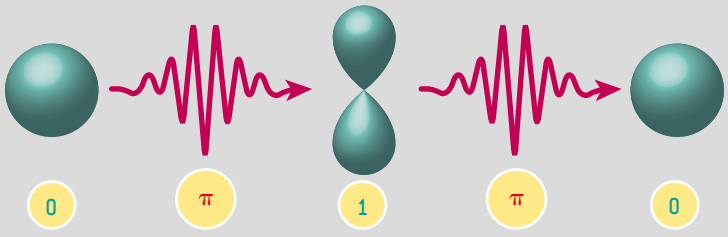
Pour toutes ces raisons, les premières applications pratiques des ordinateurs quantiques ne seront sans doute pas la factorisation, mais la simulation d'autres systèmes quantiques, tâche dont la durée dans les ordinateurs classiques augmente exponentiellement avec la taille des données. De telles simulations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

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.

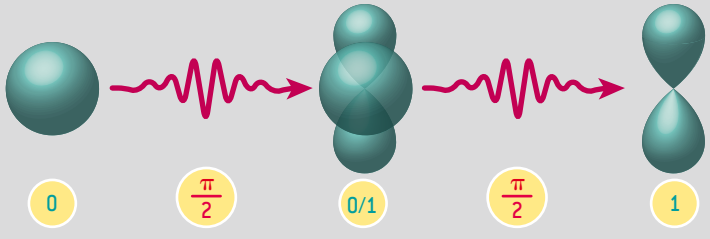
La fonction logique NON ordinaire

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.



Jen Christiansen

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