

un condensateur. Un bit quantique peut par exemple être obtenu à partir d'un atome, en utilisant deux états d'énergie d'un électron atomique : l'état de plus basse énergie, que l'on nomme l'état fondamental, peut jouer le rôle du 0, tandis que celui du 1 peut être joué par un état d'énergie supérieure.

Pour manipuler cette information, les physiciens envoient sur l'atome des impulsions lumineuses π , c'est-à-dire des impulsions ayant la fréquence, la durée et l'amplitude adéquates pour faire passer l'atome de 0 à l'état 1 et *vice-versa*. Les physiciens peuvent aussi ajuster la fréquence pour manipuler deux atomes qui interagissent, afin qu'un atome contrôle ce qui arrive à l'autre. Nous avons ainsi tous les ingrédients nécessaires à la construction des composants élémentaires des ordinateurs classiques que sont les portes logiques à un et à deux bits, et cela sans que le principe d'incertitude ne soit une entrave.

Précisons ce que le principe d'incertitude dit exactement et ce qu'il ne dit pas. Parmi les propriétés mesurables d'un atome ou d'un autre système physique, que l'on appelle « observables », certaines peuvent être déterminées, à un instant donné, de façon précise. Le principe d'incertitude n'exclut donc pas qu'une observable puisse être mesurée avec précision. Il affirme juste que toutes les observables d'un système physique ne sauraient être mesurées avec précision en même temps.

Dans le cas d'un électron atomique, l'observable mesurée précisément est son énergie et, de fait, dans l'état 0 comme dans l'état 1, la particule électrique a une énergie parfaitement définie. Cela implique que d'autres observables, telles la position et la vitesse, ne peuvent être déterminées avec précision. On dit que l'électron est délocalisé (il n'a pas de position bien définie) et, de même, sa vitesse prend simultanément toute une plage de valeurs. Si nous essayions de stocker de l'information au moyen de la position et de la vitesse de particules, nous nous heurterions effectivement à une limite quantique. La solution consiste donc à choisir judicieusement les observables qui vont servir de bits quantiques pour le codage de l'information.

Cette situation rappelle le numéro comique où un patient dit à son docteur « Ça me fait mal quand je fais ceci. », ce à quoi le docteur répond : « Alors ne le faites pas. » Si telle ou telle propriété physique d'une particule se révèle difficile à déterminer de

façon précise, le mieux est de contourner le problème en se servant d'autres observables pour stocker de l'information.

Si notre seul but est de construire des ordinateurs classiques en employant des atomes plutôt que des transistors, alors tout ce dont nous avons besoin, ce sont des observables que l'on peut mesurer précisément. Toutefois, la physique quantique offre bien plus, puisqu'elle nous donne aussi la possibilité d'exploiter des observables qui, dans certaines situations, ne peuvent être mesurées que de façon imprécise : les observables « floues ». Le fait que les observables puissent prendre simultanément de multiples valeurs augmente beaucoup leur intérêt pratique.

Une racine carrée de NON

L'énergie, par exemple, est souvent d'une valeur précise, mais un système physique peut être dans plusieurs états d'énergie à la fois. Par exemple, en plus d'être dans l'état fondamental 0 ou dans l'état excité 1, un électron atomique peut aussi être dans une superposition des deux états, c'est-à-dire à la fois dans l'état 0 et dans l'état 1.

Tout système physique est susceptible de se trouver dans un état superposé. Quand on sait préparer un tel état, le mesurer et le manipuler de façon fiable, il peut servir de bit quantique. Dans le cas d'un bit quantique atomique, l'usage d'impulsions lumineuses adéquates permettra de commuter l'énergie d'un électron d'une valeur précise à une autre, ou encore d'une valeur précise à une valeur indéterminée (état superposé), et *vice-versa*. Ainsi, une impulsion π échange les états 0 et 1, tandis qu'une impulsion $\pi/2$ (de même fréquence mais de durée ou d'amplitude moitié) place l'électron dans une superposition des états 0 et 1.

Si nous mesurons l'énergie de l'électron dans une telle superposition, nous trouverions soit l'énergie de l'état fondamental 0, soit l'énergie de l'état excité 1, les mesures donnant l'un ou l'autre résultat avec des probabilités égales (50 pour cent). Les prophètes de malheur en concluent que nous sommes limités par l'aléa quantique.

En fait, il n'en est rien, car on peut facilement contourner cet obstacle apparent et, ce faisant, créer une fonction nouvelle. Au lieu de mesurer l'électron, laissons-le dans cet état de superposition. Considérons par exemple un électron dans l'état 0, et appliquons-lui une première impul-

■ LES AUTEURS



David DEUTSCH est professeur de physique à l'Université d'Oxford, en Grande-Bretagne. Artur EKERT dirige le Centre des technologies quantiques de Singapour ; il est aussi professeur à l'Institut de mathématiques d'Oxford.



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 connaissons, 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.

Position déterminée avec précision

Vitesse floue, imprécisément définie



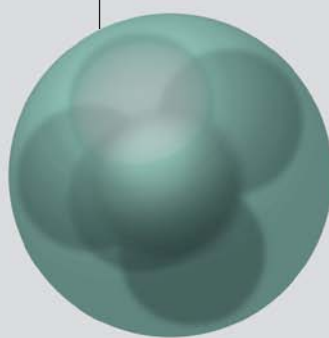
Position floue, imprécise

Vitesse déterminée avec précision



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.

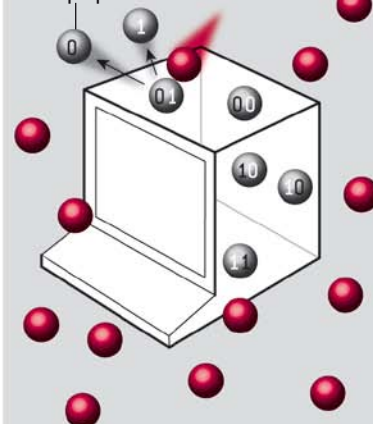
L'orbitale de la particule est d'énergie parfaitement définie



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.

Les interactions détruisent les superpositions d'états 0 et 1



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].

