

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.

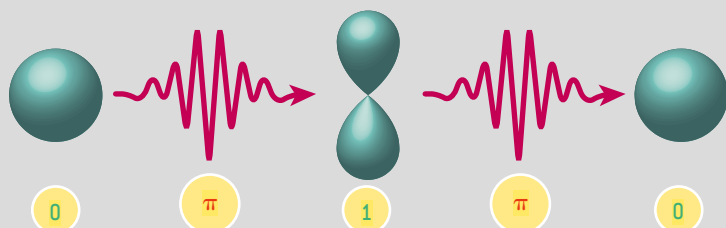
Supposons par exemple que la résolution d'un problème mathématique dépende de

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.

