Calculs quantiques

Peter Shor

Les ordinateurs quantiques sont d'hypothétiques machines qui effectuent des calculs en utilisant les principes de la mécanique quantique. Pour quelques problèmes de calcul difficiles, notamment ceux, importants en cryptographie, de la décomposition en facteurs premiers et de la recherche de logarithmes discrets, les meilleurs algorithmes connus pour les ordinateurs classiques sont exponentiellement plus lents que ceux que l'on a obtenus pour les ordinateurs quantiques. Bien qu'on n'en ait encore jamais construit, les ordinateurs quantiques semblent ne violer aucun des principes fondamentaux de la physique. J'expliquerai comment la mécanique quantique apporte cette puissance de calcul supplémentaire, et je décrirai sommairement l'algorithme de factorisation. L'une des principales difficultés pour la construction d'ordinateurs quantiques est de manipuler des états quantiques cohérents sans introduction d'erreurs et sans perte de cohérence. Ce problème peut être atténué grâce à l'utilisation de codes correcteurs d'erreurs quantiques ; si un ordinateur quantique ne peut être construit qu'avec un matériel modérément fiable, sa fiabilité peut être grandement accrue grâce à l'utilisation de logiciels appropriés. J'aborderai brièvement ces aspects de la question.

Address: AT&T Labs, Florham Park, USA
E-mail: shor@research.att.com