

entre la théorie et la pratique, les physiciens ont d'abord pensé que l'informatique quantique ne resterait qu'une curiosité scientifique.

La donne a changé en 1995, lorsque Peter Shor, des laboratoires Bell, aux États-Unis, et, indépendamment, Andrew Steane, de l'université d'Oxford, au Royaume-Uni, ont mis au point la correction quantique des erreurs. Ils ont montré comment les chercheurs peuvent répartir la valeur d'un seul qubit d'information sur plusieurs qubits physiques, afin de construire des ordinateurs quantiques fiables à partir de composants peu fiables. Tant que les qubits physiques sont d'une qualité suffisante pour que leur taux d'erreur soit inférieur

à un certain seuil, il est possible de corriger les erreurs plus vite qu'elles ne s'accumulent.

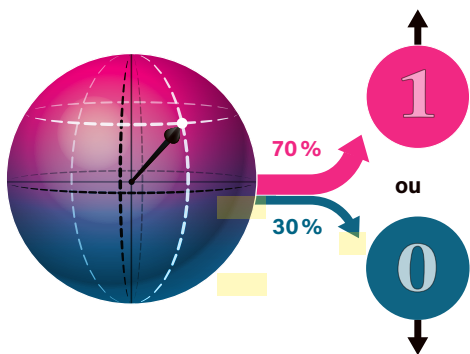
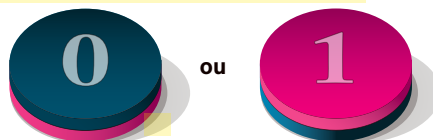
Pour comprendre pourquoi les travaux de Peter Shor et d'Andrew Steane ont constitué une telle avancée, il faut d'abord examiner comment fonctionne généralement la correction d'erreurs ordinaire. Un code correcteur d'erreurs simple effectue des copies de l'information, par exemple en représentant le 0 par 000 et le 1 par 111. Grâce à cette redondance, si votre ordinateur lit un 010, il conclut que la valeur originale était probablement 0. Un tel code reste robuste tant que le taux d'erreur est assez faible pour qu'au plus une copie du bit soit erronée. La stratégie générale consiste à

DES BITS AUX QUBITS

L'ordinateur quantique exploite les règles de la mécanique quantique pour dépasser les capacités des machines classiques. Les qubits, l'unité d'information de ces systèmes, peuvent être dans une « superposition » de différents états. Un phénomène quantique, l'intrication, permet aux propriétés des qubits d'être fortement corrélées – si vous avez deux qubits intriqués et que vous mesurez individuellement leurs propriétés, vous obtenez des résultats aléatoires, mais si vous les regardez ensemble, vous constatez que l'état d'un qubit est lié à l'état de l'autre qubit. Des qubits intriqués contiennent davantage d'information que deux qubits séparés.

Des bits...

Un bit classique prend une des deux valeurs : 0 ou 1, à l'image des côtés d'une pièce.

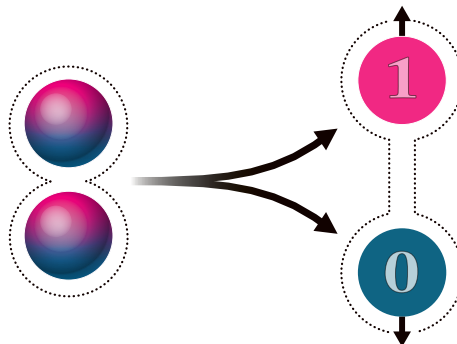


... aux qubits...

Un qubit, lui, a bien plus d'états possibles. On les représente comme tous les points à la surface d'une sphère de rayon unité. Le pôle nord serait ici l'état 1, tandis que le pôle sud serait l'état 0. Pour tous les autres points de la sphère, le qubit est dans une superposition de ces deux états. Les coordonnées d'un point de la sphère indiquent le « poids » que représentent les états 0 et 1 dans le qubit. Elles sont aussi liées à la probabilité de mesurer l'état 0 ou l'état 1 quand on observe le qubit. En effet, lors d'une mesure, la superposition s'effondre. Le qubit prend alors la valeur 0 ou 1, comme un bit classique. Pour exploiter les capacités de l'ordinateur quantique, il faut préserver l'état de superposition pendant tout le calcul.

... aux qubits intriqués

Si deux qubits sont intriqués, leurs états ne sont plus indépendants ; ils sont fortement liés. Quand on mesure l'état d'un qubit intriqué, on sait instantanément dans quel état se trouve l'autre qubit sans même avoir à le mesurer. Cet effet persiste peu importe la distance qui sépare les deux qubits.



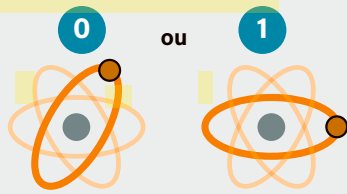
CIRCUITS QUANTIQUES

Les circuits quantiques sont des représentations abstraites de l'informatique quantique, analogues aux circuits de l'informatique théorique classique. Avec ces diagrammes, on met de côté les aspects physiques du système (peu importe ici que les qubits soient portés par des circuits supraconducteurs ou autre) et on se concentre sur les opérations de manipulation des qubits.

Un ordinateur quantique peut être réalisé de différentes façons, le qubit est alors représenté par diverses propriétés du système. Trois exemples d'approches.

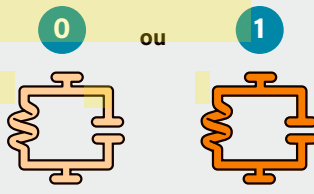
Ion

L'orbite électronique définit le qubit



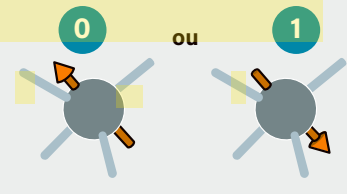
Supraconducteur

La superposition de différents états de charge du circuit définit le qubit



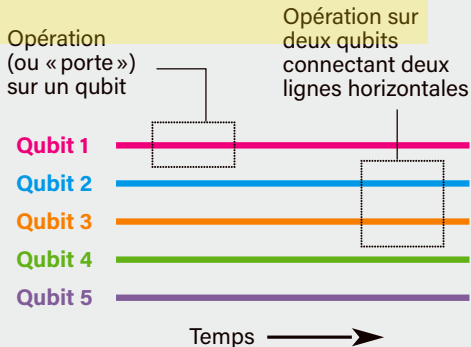
Spin dans la matière

Le spin d'un atome dans un réseau définit l'état quantique



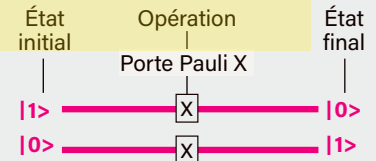
Peu importe la réalisation physique, les opérations peuvent toujours être représentées par le même type de diagrammes, les circuits quantiques.

Ils ressemblent à des partitions musicales. Chaque ligne horizontale représente un qubit. Les « notes » représentent les opérations, on parle de « portes logiques ». Comme pour la musique, la progression dans le diagramme est temporelle. Elle montre la séquence des opérations que l'on applique aux différents qubits.

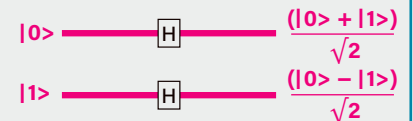


Différentes opérations sont représentées par différents symboles pour les portes.

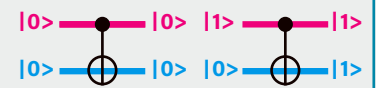
Un *bit flip* (nommée la porte « Pauli-X », et notée [X]) inverse un qubit. Il transforme un 1 en 0, et inversement.



Une porte de Hadamard [H] place un qubit dans une superposition.



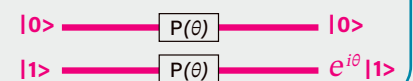
Si deux qubits sont connectés par une ligne verticale, l'inversion du second est conditionnée par la valeur du premier. La porte est dite « contrôlée ».



Une porte d'inversion contrôlée qui implique trois qubits est nommée « porte de Toffoli ».



Une porte peut également modifier la phase du qubit d'un angle arbitraire $[P(\theta)]$.



Chaque porte présente un taux d'erreur – la probabilité que le système physique qui réalise la porte donne une mauvaise valeur, de la même façon qu'un musicien risque de jouer une fausse note. En l'absence d'un système de correction des erreurs, un circuit livre un mauvais résultat avec une probabilité proportionnelle au taux d'erreur des portes : le nombre de fausses notes devient alors si grand qu'on ne reconnaît plus le morceau de musique. Grâce à des qubits auxiliaires, il est possible de détecter la présence d'erreurs et de les corriger. Ci-contre, un exemple simple de circuit corrigeant les erreurs. Pour un qubit d'information, il nécessite trois qubits. Le circuit compare des paires de qubits. Une paire indique qu'une erreur s'est produite, deux paires indiquent où elle s'est produite, et la porte de Toffoli applique la correction. Avec cette stratégie, on extrait l'information sur l'erreur sans révéler l'information quantique du qubit.

