Il existe un principe en physique quantique qui stipule que tout ce qui n'est pas interdit doit se produire (mais peut-être avec une probabilité ridiculement petite). Les erreurs sont donc une fatalité dans tous les domaines. On en retrouve dans le langage, la cuisine, la communication, le traitement des images et, bien sûr, le calcul. Pour que la société fonctionne correctement malgré ces erreurs, il est par conséquent indispensable de les contrôler et de les corriger. De nombreuses méthodes ont été développées, et ainsi un DVD rayé reste lisible, un QR code chiffonné est toujours déchiffrable ; les sondes spatiales transmettent des clichés de planètes lointaines sur des centaines de millions de kilomètres et le signal n'en demeure pas moins net. La correction des erreurs est l'un des outils les plus essentiels des technologies de l'information. Les erreurs sont peut-être inéluctables, mais elles sont aussi réparables.

Actuellement, les meilleures machines commettent une erreur toutes les 1000 portes

Cette loi de l'inévitabilité touche également les ordinateurs quantiques. Ces machines exploitent les règles fondamentales de la physique pour résoudre des problèmes que les ordinateurs classiques ne parviennent pas à résoudre de façon efficace. Ces dispositifs ont connu un intense développement ces dernières années et auront certainement un impact très fort sur la science et l'industrie de demain. Mais cette grande puissance s'accompagne d'une grande vulnérabilité. Les ordinateurs quantiques souffrent en effet d'erreurs que les techniques de correction standard ne sont pas en mesure de traiter.

Au début de ma carrière, en tant que physicienne théoricienne de la matière condensée, je me suis intéressée à certains comportements quantiques dans les matériaux. J'ai notamment étudié la supraconductivité, un phénomène associé à certains matériaux refroidis à une température proche du zéro absolu dans lesquels la résistance électrique devient nulle. À l'époque, mes préoccupations étaient bien éloignées de celles des ordinateurs quantiques.

Ces derniers en étaient alors encore à leurs balbutiements. Paul Benioff, du laboratoire américain Argonne, en avait proposé le principe en 1980, mais les premiers prototypes ont été construits près de vingt ans plus tard. En 2007, une découverte a eu un rôle clé dans le développement du domaine. Robert Schoelkopf, Michel Devoret et leurs collègues de l'université Yale ont mis au point une technique reposant sur la supraconductivité pour concevoir des ordinateurs quantiques. De nombreuses entreprises (IBM, Google, etc.) ont vite adopté cette approche pour créer leurs propres ordinateurs quantiques. Forte de mon expérience en matière de supraconductivité, j'ai rejoint IBM où je me suis consacrée à l'amélioration des opérations entre plusieurs qubits reliés entre eux et à l'étude des moyens de corriger les erreurs.

Le qubit est la version quantique du bit d'information classique qui prend la valeur « 0 » ou « 1 ». Le qubit exploite un phénomène quantique, la superposition des états : il est une combinaison de l'état « 0 » et de l'état « 1 ». En associant des qubits grâce à l'intrication quantique (*voir l'encadré page 33*), nous pouvons manipuler collectivement de plus grandes quantités d'information qu'un nombre équivalent de bits classiques. À cause de leur nature quantique, les qubits se comportent comme des ondes, qui interfèrent à la manière des ondes lumineuses. Ces interférences conduisent à des capacités de calcul bien plus riches que les simples inversions de bits classiques. Pour ces raisons, les spécialistes pensent que l'ordinateur quantique devrait effectuer certaines tâches bien plus efficacement qu'un ordinateur classique. Entre autres, la simulation de systèmes quantiques réels, la conception et l'analyse de nouveaux matériaux, la découverte de motifs cachés dans de vastes bases de données pour améliorer l'apprentissage automatique, ou la recherche de catalyseurs plus performants sur le plan énergétique pour les processus chimiques industriels.

DIMINUER LE NOMBRE DES ERREURS

Le souci est que de nombreuses propositions visant à résoudre des problèmes utiles exigent que les ordinateurs quantiques effectuent des milliards d'opérations logiques (mises en œuvre électroniquement par ce qu'on nomme des « portes logiques ») sur des centaines ou des milliers de qubits. Pour réaliser une telle prouesse, cela exige du système qu'il fasse au maximum une seule erreur par milliard de portes. Or, actuellement, les meilleures machines commettent une erreur toutes les 1000 portes. Face à l'écart considérable

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.

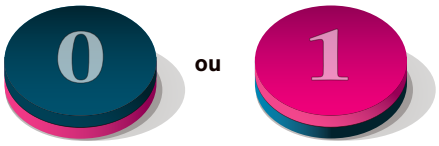
Pour comprendre pourquoi les travaux de Peter Shor et d'Andrew Steane ont constitué une telle avancée, il faut d'abord examiner comment fonctionne généralement la correction d'erreurs ordinaire. Un code correcteur d'erreurs simple effectue des copies de l'information, par exemple en représentant le 0 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

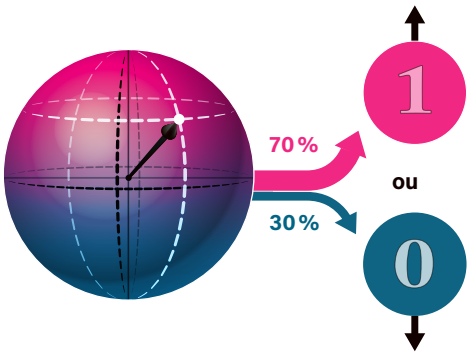
DES BITS AUX QUBITS

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.