quantique analogique. Ces systèmes n'ont pas pour vocation d'être universels comme les ordinateurs mais restent suffisamment configurables pour simuler une variété d'évolutions quantiques apparaissant dans la nature. C'est notamment l'option explorée par Pasqal, une start-up issue de l'institut d'Optique, à Palaiseau. Leur dispositif utilise un ensemble d'atomes neutres piégés dont on peut régler les couplages pour mimer le système physique à simuler.

Plus inattendu, les ordinateurs quantiques sont aussi efficaces pour résoudre certains problèmes qui ne sont pas quantiques par essence, comme la décomposition en facteurs premiers de nombres très grands grâce à l'algorithme proposé en 1994 par le mathématicien Peter Shor du MIT (institut de technologie du Massachusetts).

Les promesses et les attentes sont donc grandes. À quel stade de développement sont les ordinateurs quantiques ?

En 2018, le spécialiste de l'informatique quantique John Preskill qualifiait la période actuelle d'« ère des NISQ » (*noisy intermediate-scale quantum era*), c'est-à-dire l'ère des processeurs dotés de cinquante à quelques centaines de qubits, soumis à pas mal d'erreurs non corrigées, on parle aussi de « bruit ».

Dans un ordinateur classique, on peut avoir des erreurs quand un bit change de valeur (*bit flip* en anglais) : un « 0 » peut accidentellement se transformer en « 1 » et inversement. Les qubits aussi sont susceptibles d'avoir des erreurs. Il existe deux types d'erreurs fondamentales : l'inversion de bit, qui correspond à l'erreur classique, et l'inversion de phase (*phase flip* en anglais), qui est purement quantique.

Ces erreurs proviennent d'interactions avec l'environnement et elles sont beaucoup plus fréquentes dans les systèmes quantiques. Il faut donc protéger le mieux possible les qubits de leur environnement. Mais il est impossible d'isoler totalement un système. Les erreurs se produisent ainsi de façon inéluctable.

Le fait de réaliser un calcul induit-il des erreurs ?

Dans un processeur, classique ou quantique, on veut traiter l'information pour faire des calculs. Pour cela, on utilise des portes logiques qui consistent à inverser la valeur d'un bit, additionner la valeur de deux bits, etc. Ces portes sont réalisées avec des transistors.

Dans l'ordinateur quantique, les portes logiques effectuent aussi des rotations dans l'espace des états du qubit (par exemple l'état initial « 0 » devient une combinaison de « 0 » et « 1 »), ou couplent plusieurs qubits voisins.

Les portes logiques ne sont jamais parfaites et introduisent aussi des erreurs, ne serait-ce que parce que le qubit peut être perturbé par son environnement durant l'opération. Une bonne mesure de la qualité du système est la profondeur atteignable, c'est-à-dire le nombre de portes ou opérations que l'on peut faire sur un qubit avant que le calcul ne contienne presque sûrement une erreur.

Que peut-on faire contre ces erreurs ?

Dans le cas classique, le code correcteur le plus simple repose sur la redondance : encoder un bit logique dans plusieurs bits physiques. Le bit « 0 » est dupliqué en « 000 » et 1 en « 111 ». Ainsi si on mesure plus tard « 010 » et qu'on suppose que les erreurs sont rares, on en déduit que la bonne valeur est 0 avec un « vote de majorité », et on peut rectifier le 1 du milieu en 0. Dans un processeur d'ordinateur classique, les codes correcteurs ne sont pas implémentés car les erreurs sont rarissimes. Ils sont en revanche très utiles quand on fait de la transmission d'information, pour communiquer avec un satellite par exemple.

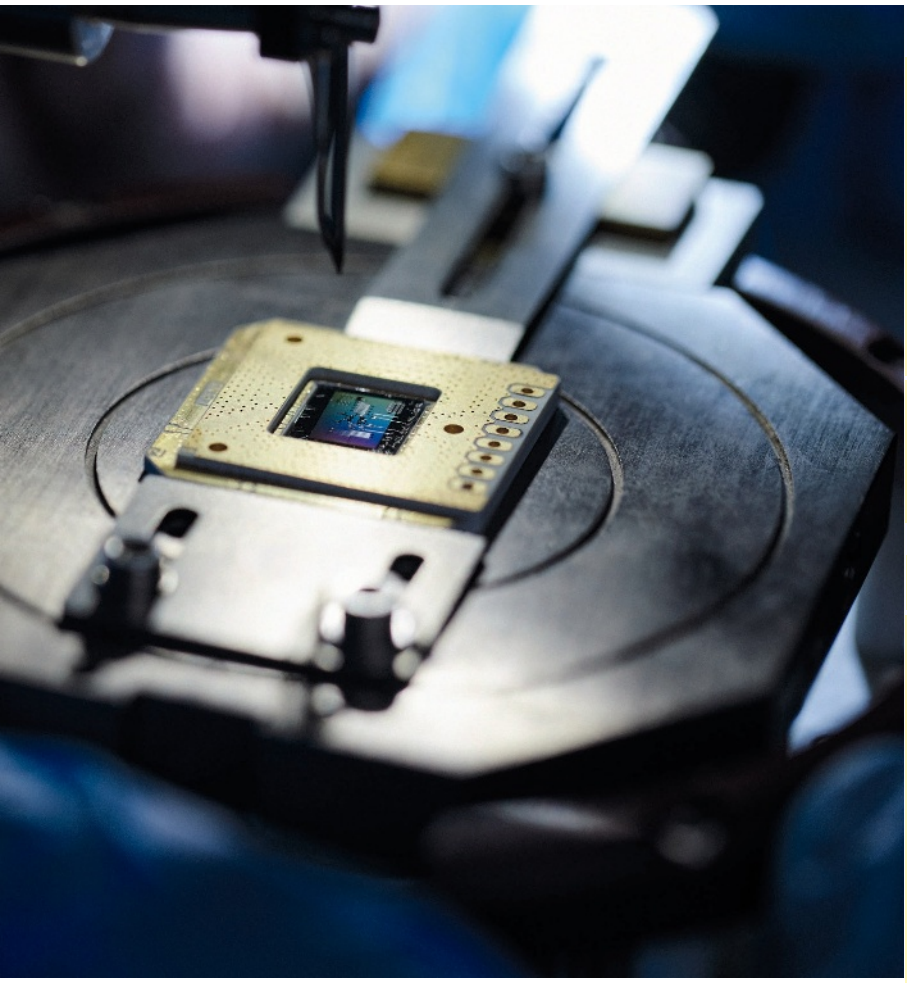
La correction des erreurs de qubits est bien plus difficile à cause de leur nature quantique et du problème de la mesure. Quand on mesure la valeur d'un qubit dans une superposition d'états, on provoque l'effondrement de cette superposition et on n'observe qu'un seul des états possibles. La moindre fuite d'information (comme l'émission d'un photon) qui nous renseignerait sur le système conduit à la destruction de la superposition. Or il faut préserver la superposition des états des qubits tout au long du calcul pour que celui-ci aboutisse. On ne peut ainsi pas simplement mesurer les qubits physiques pour savoir si une erreur s'est produite et la rectifier.

Quelle est alors la solution ?

La solution consiste toujours à encoder l'information d'un qubit dit « logique » de manière redondante dans un plus grand nombre de qubits physiques. L'idée est ensuite de faire d'astucieuses mesures globales qui nous disent si le système contient une erreur (on parle de « syndromes d'erreurs ») et comment la corriger. Ces syndromes sont conçus intelligemment pour ne pas faire fuir d'information sur l'état de superposition du qubit lui-même lorsqu'ils sont mesurés. Pour l'implémentation de ces approches, on fait appel à des codes correcteurs quantiques dont il existe différents types (*voir* Calculer plus vite… et sans erreur ? *page 31*). Un point essentiel est qu'un code correcteur demande toujours une redondance, on utilise plusieurs qubits physiques pour une unité d'information quantique (le qubit logique). Plus on veut réduire les erreurs, plus le rapport du nombre de qubits physiques sur le nombre de qubits logiques (en anglais l'*overhead*) augmente.

La société Alice&Bob explore la piste de qubits de chats, des qubits supraconducteurs dans lesquels il est possible d'éliminer un type d'erreurs. Ici, la puce est intégrée dans le dispositif, qui permet de la connecter et de la refroidir, afin d'en mesurer les caractéristiques.

© Further Studio/Nil Hoppenot



En théorie, on est capable d'améliorer la résistance à toutes les erreurs quantiques à partir de 5 qubits physiques d'assez bonne qualité par qubit logique. En pratique, on ne veut pas juste réduire la probabilité d'erreur, mais rendre les erreurs presque impossibles alors même qu'elles sont encore trop fréquentes au niveau physique. Cela demande des *overheads* beaucoup plus importants, typiquement de l'ordre de 1000 à 10000 qubits physiques bruités par qubit logique. Cette valeur est énorme, car il faut ensuite plusieurs milliers de qubits logiques pour faire tourner des algorithmes intéressants comme celui de Shor.

Y a-t-il des moyens de diminuer le nombre de qubits ?

Avec les machines actuelles, dans l'ère du NISQ, on ne fait simplement pas de correction d'erreur, pour garder un nombre raisonnable de qubits utiles. On se contente d'une profondeur faible où la probabilité d'erreur globale reste acceptable.

Une des grandes questions théoriques est de savoir s'il est possible de faire des calculs utiles avec ces machines NISQ à profondeur limitée. On est raisonnablement confiant sur le fait que les calculs effectués par ces machines sont difficiles ou impossibles pour les ordinateurs classiques (ou en tout cas le seront bientôt) et donc que ces machines sont, en un certain sens, puissantes. Mais on ne sait rien faire d'utile avec. Ça n'enlève rien à l'exploit technologique que représentent les processeurs américains et chinois. Mais il est fort probable que nous ayons atteint les limites de cette approche.

Pour aller plus loin et arriver à des ordinateurs universels capables de mener des calculs utiles, il va falloir réduire les erreurs d'un facteur au moins 1 milliard. Les codes correcteurs d'erreurs deviennent alors indispensables.

Mais comment ne pas faire exploser l'« overhead » ?

Il existe différentes stratégies. On peut d'abord essayer de perfectionner davantage les codes correcteurs, mais il est peu probable qu'il y ait encore beaucoup à gagner sur ce front. La stratégie qui me semble la plus pertinente sur le long terme consiste à améliorer les supports physiques des qubits. L'idée est de produire des qubits le plus « propres » possible, les plus résistants à certaines formes de bruit grâce à des stratégies de correction passives. Cela n'éliminera jamais totalement les erreurs. Il faudra toujours utiliser des codes quantiques, mais de façon moins massive, et donc avec un *overhead* limité.

Quels sont les différents supports physiques de qubits à l'étude actuellement ?

Pour l'implémentation des qubits physiques, les qubits supraconducteurs sont probablement la technologie la plus mature. De nombreuses équipes ont contribué à leur développement, mais on peut signaler en particulier les travaux précurseurs dans les années 1990 et 2000 de Yasunobu Nakamura, à l'université de Tokyo, et des Français Daniel Esteve et Michel Devoret du CEA-Saclay, ce dernier étant désormais à la tête d'une des toutes meilleures équipes du domaine à l'université Yale.

Pour concevoir un qubit, l'idée la plus simple est de prendre un degré de liberté auquel on peut associer les valeurs « 0 » ou « 1 » et qui est déjà élémentaire, par exemple le spin d'une particule. Au contraire, dans les supraconducteurs, on associe les valeurs « 0 » ou « 1 » à un grand nombre de degrés de liberté microscopiques, correspondant à des paires d'électrons qui circulent dans une boucle supraconductrice dotée d'une jonction Josephson (un élément isolant séparant deux supraconducteurs est traversé par un courant électrique par effet tunnel, c'est l'effet Josephson). Le courant dans le système supraconducteur peut se trouver dans différents