

deux qubits logiques (A et B), de la même façon, vous menez l'opération entre les qubits physiques correspondants des qubits logiques A et B: le qubit 1 de A avec le qubit 1 de B, le qubit 2 de A avec le qubit 2 de B, etc. Comme cette porte limite les interactions entre les qubits physiques, les erreurs se propagent peu et restent sous contrôle.

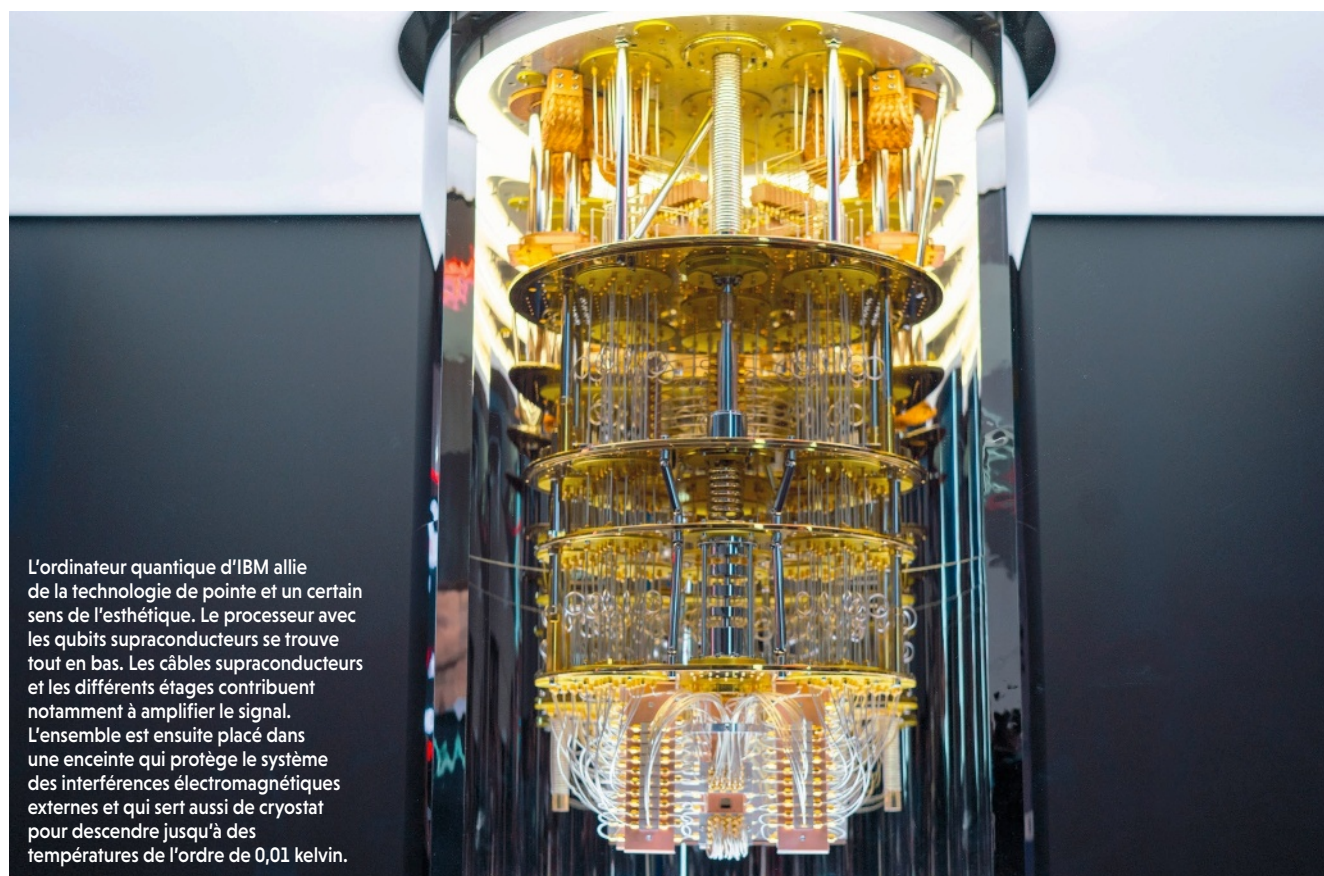
Si toutes les portes nécessaires pour construire un jeu universel de portes étaient transverses, la vie serait simple. Mais, en 2008, Bryan Eastin et Emanuel Knill, de l'institut américain des standards et des technologies, ont montré dans un théorème fondamental qu'aucun code quantique ne peut effectuer un calcul universel en utilisant uniquement des portes transverses.

Cela nous dit quelque chose d'important sur les ordinateurs quantiques. Si vous entendez quelqu'un dire que la particularité de l'informatique quantique réside dans la superposition et l'intrication, méfiez-vous ! Tous les états de superposition et d'intrication ne sont pas spéciaux. Certains sont mis en œuvre par un groupe de portes transverses que nous appelons le «groupe de Clifford». Un ordinateur classique peut simuler efficacement des calculs quantiques qui n'utilisent que des portes de Clifford (porte de Hadamard, porte

d'inversion contrôlée ou porte de changement de phase, voir l'encadré pages 34-35). En revanche avec des portes qui n'appartiennent pas au groupe de Clifford, la simulation classique sera très difficile. Mais ces portes ont tendance à ne pas être transverses et donc à avoir une mauvaise fidélité (c'est-à-dire qu'elles ont une probabilité élevée d'introduire des erreurs).

COMMENT FAIRE SANS LES PORTES NON-CLIFFORD ?

La meilleure astuce dont nous disposons pour mettre en œuvre des portes non-Clifford protégées du bruit se nomme la distillation d'états magiques. Cette technique a été proposée en 2004 par Emanuel Knill puis par Andrei Kitaev et Sergey Bravyi. Vous pouvez implémenter des portes non-Clifford en utilisant uniquement des portes Clifford si vous avez accès à des états quantiques dits «magiques» (correspondant à une superposition particulière des états «0» et «1»). Ces états magiques doivent toutefois être très purs, c'est-à-dire comporter très peu d'erreurs. Andrei Kitaev et Sergey Bravyi ont montré que, dans certains cas, il est possible de partir d'une collection d'états magiques bruités et de les distiller, en employant exclusivement des portes de



L'ordinateur quantique d'IBM allie de la technologie de pointe et un certain sens de l'esthétique. Le processeur avec les qubits supraconducteurs se trouve tout en bas. Les câbles supraconducteurs et les différents étages contribuent notamment à amplifier le signal. L'ensemble est ensuite placé dans une enceinte qui protège le système des interférences électromagnétiques externes et qui sert aussi de cryostat pour descendre jusqu'à des températures de l'ordre de 0,01 kelvin.

Clifford parfaites (on suppose ici que les portes de Clifford sont déjà protégées contre les erreurs). On aboutit à des états magiques moins nombreux, mais plus purs. En répétant plusieurs fois la procédure de distillation, on extrait un état magique pur à partir de nombreux états bruités.

Lorsque vous obtenez un état magique pur, vous pouvez le faire interagir avec le qubit contenant l'information. Pour cela, on utilise un processus de « téléportation quantique » : l'état du qubit d'information est transféré dans un autre état. Ce dernier correspond exactement à l'opération d'une porte non-Clifford. L'état magique est sacrifié dans le processus.

Aussi astucieuse que soit cette approche, elle est aussi extrêmement coûteuse. Pour un code de surface standard, la distillation des états magiques consomme 99% du calcul global. Il est clair que nous avons besoin de méthodes pour améliorer ou contourner cette distillation. En attendant, il est possible de continuer à travailler avec des ordinateurs quantiques bruités en utilisant la technique d'atténuation des erreurs. Au lieu d'essayer de concevoir un circuit quantique (voir l'encadré pages 34-35) pour corriger les erreurs de calcul en temps réel (ce qui nécessite des qubits supplémentaires), l'atténuation des erreurs fait appel à un ordinateur classique qui apprend à estimer la contribution du bruit et à l'annuler. Vous n'avez pas besoin de qubits supplémentaires, mais vous le payez en exécutant davantage de circuits quantiques (pour apprendre l'impact du bruit) et en introduisant plus de traitement classique.

ATTÉNUER LE BRUIT

Par exemple, si vous pouvez caractériser le bruit dans le processeur quantique ou l'analyser à partir d'un ensemble d'expériences sur des circuits bruités qui peuvent être simulés efficacement dans un ordinateur classique, vous pouvez utiliser ces connaissances pour faire une bonne estimation de la sortie du circuit quantique idéal (sans bruit). Ce circuit peut être considéré comme la somme de circuits bruités, chacun pondéré en fonction des informations des simulations. Ou alors, exécutez votre circuit quantique plusieurs fois en modifiant le bruit à chaque fois. À partir des différents résultats, vous pouvez ensuite extrapoler le signal attendu si le système fonctionnait sans erreur.

Ces techniques ont des limites. Elles ne s'appliquent pas à tous les algorithmes, et même lorsqu'elles s'appliquent, leur efficacité reste réduite. Mais une bonne stratégie consiste à combiner l'atténuation des erreurs et la correction des erreurs. Notre équipe théorique a récemment montré qu'en utilisant la correction d'erreur pour les portes de Clifford et

l'atténuation d'erreur pour les portes non-Clifford, il est possible de simuler des circuits quantiques universels sans avoir besoin de distillation d'états magiques. De cette façon, il serait possible de surpasser les capacités d'ordinateurs classiques avec des ordinateurs quantiques plus petits. L'équipe a estimé que la combinaison particulière d'atténuation et

La distillation d'états magiques est la meilleure astuce à notre disposition

de correction des erreurs permet de simuler des circuits comportant jusqu'à 40 fois plus de portes non-Clifford que ce qu'un ordinateur classique peut gérer.

Pour continuer à progresser et imaginer des moyens plus efficaces de traiter les erreurs dans les ordinateurs quantiques, la stratégie idéale consiste en une boucle de rétroaction optimale entre les ingénieurs et les théoriciens. Grâce à ce dialogue constant, les théoriciens adaptent les circuits quantiques et les codes correcteurs d'erreurs aux contraintes techniques des machines tandis que les ingénieurs conçoivent des systèmes qui répondent aux spécificités des codes correcteurs d'erreurs. Le succès des ordinateurs quantiques dépend de la capacité à trouver des compromis entre ces deux approches.

Je suis fier d'avoir contribué à faire passer l'informatique quantique du monde des démonstrateurs de laboratoire à un ou deux qubits au stade où certaines sociétés ouvrent la possibilité à des utilisateurs d'accéder à des systèmes quantiques comportant des dizaines de qubits *via* le *cloud*. Mais la partie est loin d'être gagnée. Pour tirer parti des possibilités tant vantées de l'informatique quantique, il faudra développer des systèmes qui fonctionnent en dessous du seuil d'erreur, des codes quantiques capables de corriger les erreurs restantes avec le moins de qubits et de portes supplémentaires possible, et de meilleurs moyens de combiner la correction et l'atténuation des erreurs. Nous écrivons progressivement l'histoire des ordinateurs de demain, mais la route reste longue et semée d'embûches. ■

BIBLIOGRAPHIE

C. R. Monroe et al., **L'ordinateur quantique en kit**, Dossier Pour la Science, n° 93, octobre 2016.

S. Aaronson, **Les limites du calcul quantique**, Pour la Science, n° 367, mai 2008.

S. B. Bravyi et A. Y. Kitaev, **Universal quantum computation with ideal Clifford gates and noisy ancillas**, Physical Review A, 2005.

S. B. Bravyi et A. Y. Kitaev, **Quantum codes on a lattice with boundary**, arXiv:quant-ph/9811052, 1998.