# Peut-on parler de suprématie quantique ?

Michel Le Bellac (Michel.Le_bellac@inln.cnrs.fr)
Professeur émérite, Université Côte d'Azur

En octobre 2019, Google annonçait qu'une de ses équipes avait « démontré la suprématie quantique ». Un article de Arute et al. suivait, publié dans Nature 574 (2019) 505-510, décrivant la réalisation expérimentale d'un ordinateur programmable de 53 qubits. Dans ce contexte, établir la suprématie quantique consiste à démontrer qu'un calcul peut être effectué en quelques heures par un dispositif fonctionnant selon les règles quantiques, alors que les plus puissants des ordinateurs classiques ne pourraient pas obtenir le résultat en un temps raisonnable. Cet énoncé est délibérément vague (« raisonnable ») et arbitraire (« quelques heures ») et sera précisé, autant que faire se peut, dans la suite de cet article. Avant d'aborder le cœur du sujet, je commencerai par un bref rappel sur les briques de base de l'ordinateur quantique : le «qubit », le principe de superposition et l'intrication. Pour plus de détails sur ces sujets, je renvoie à l'encadré « Superposition, cohérence, qubits et intrication » de l'article de Michèle Leduc et Sébastien Tanzilli [1]. J'examinerai ensuite les algorithmes quantiques, le problème dif cile de la correction des erreurs et en n la suprématie quantique.

## Principes de l'ordinateur quantique

De façon très schématique, un algorithme classique mis en œuvre sur un ordinateur standard effectue des opérations bien dé nies sur des données exprimées sous forme de « bits », des entités qui peuvent prendre exclusivement les valeurs 0 ou 1, et dont les supports physiques sont des objets classiques : aimants, condensateurs, impulsions laser, etc. Ces bits peuvent être enregistrés au départ du calcul dans une mémoire sous forme d'une suite de 0 et de 1 : c'est le registre de données.

Un bit quantique, ou en abrégé « qubit », peut exister non seulement dans l'un des deux états de base où sa valeur est 0 ou 1, mais aussi dans une superposition linéaire de ces deux états. Un qubit est en fait ce que l'on appelle en physique quantique un système à deux niveaux, en général deux niveaux d'énergie $E_0$ et $E_1$, correspondant à des états quantiques de base $|0\rangle$ et $|1\rangle$, avec les notations habituelles. L'exemple paradigmatique de qubit est le spin 1/2, où les deux états quantiques sont les deux états d'énergie différente du spin 1/2 dans un champ magnétique. On peut aussi citer les deux états d'énergie d'un atome ou d'un ion à deux niveaux, ou encore les deux états de polarisation orthogonaux d'un photon. Les deux états de base sous-tendent un espace vectoriel complexe à deux dimensions, et l'état le plus général est représenté par un vecteur $|\psi\rangle$ de cet espace, une superposition linéaire des deux états de base avec deux coef cients a et b qui sont des nombres complexes : $|\psi\rangle = a|0\rangle+b|1\rangle$, $|a|^2+|b|^2 = 1$.

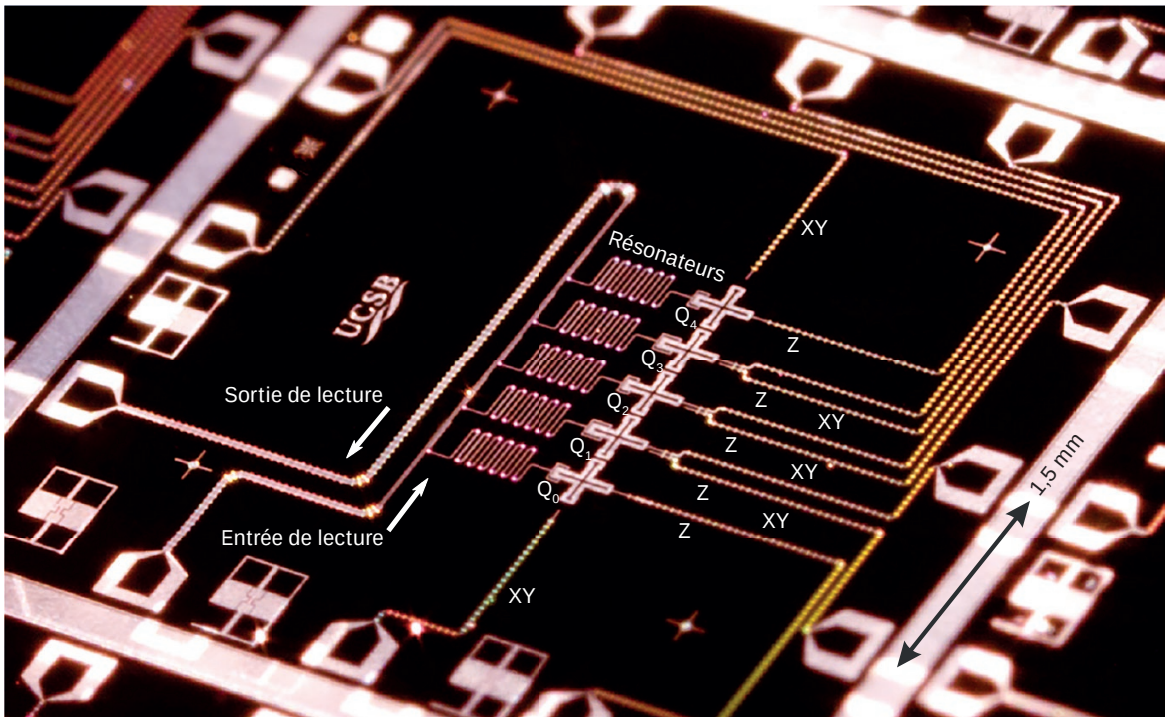
La physique quantique conduit à réviser de fond en comble la notion habituelle d'information, celle qui est portée par des objets classiques. L'information portée par des objets quantiques comme les qubits possède des propriétés radicalement nouvelles. Par exemple :

1. On ne peut pas dupliquer un état quantique inconnu[(a)] : c'est le théorème de non-clonage quantique.
2. Il est impossible en général de distinguer avec 100% de succès deux états quantiques différents.
3. L'information portée par un état intriqué[(b)] de deux qubits est distribuée sur ceux-ci, et elle est délocalisée si les deux qubits sont séparés spatialement.

Alors que dans un ordinateur classique l'état d'un calcul est dé ni par les



Article disponible sur le site https://www.refletsdelaphysique.fr ou https://doi.org/10.1051/refdp/202067004




1. Image optique d'un processeur intégré avec cinq qubits supraconducteurs. Les cinq qubits ($Q_0$ à $Q_4$, au centre de la figure) sont en forme de croix et disposés suivant un réseau linéaire. À leur gauche on trouve cinq résonateurs formés de guides d'ondes résonants utilisés pour la mesure des qubits individuels. Le câblage dédié au contrôle et à la manipulation des qubits est situé à droite. Afin de minimiser la décohérence, l'énergie thermique doit être largement inférieure à la différence $\delta E = E_1 - E_0$ entre les deux niveaux d'énergie $E_0$ et $E_1$ du qubit, et le processeur est maintenu à une température $T = 20$ mK grâce à un réfrigérateur à dilution, de sorte que $k_B T \ll \delta E$. Source : R. Barends et al., Nature, 508 (2014) 500.

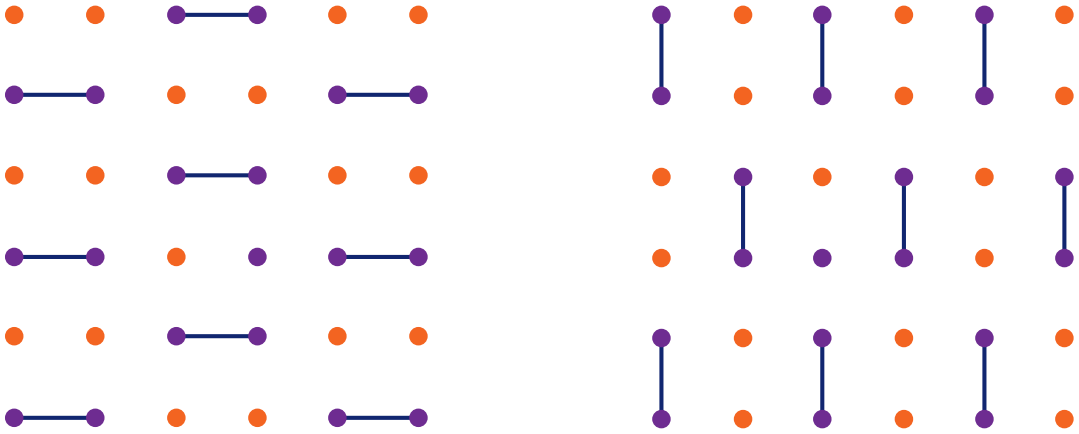
valeurs individuelles des bits à un certain instant, dans un ordinateur quantique l'information est distribuée sur l'ensemble des qubits via leurs corrélations, lesquelles ne peuvent pas être décrites par une distribution de probabilité classique.

Le phénomène de décohérence est intimement lié à l'intrication : si un qubit interagit quantiquement avec un environnement externe, alors l'évolution quantique se passe dans un espace plus grand que celui du qubit et on risque de détruire les superpositions linéaires, ou superpositions cohérentes, avec comme conséquence la perte du fil du calcul.

L'exécution d'un algorithme par un ordinateur quantique suit le schéma d'une expérience type de physique quantique, telle qu'on l'enseigne dans un cours de licence. L'expérience débute par une phase de préparation, où l'on fabrique un registre de données avec n qubits. Par exemple, si n = 5, le registre de données pourra se trouver dans un état $|\psi\rangle = |01101\rangle$, où le premier qubit est dans l'état $|0\rangle$, le second dans l'état $|1\rangle$, etc. On applique ensuite une évolution unitaire U sur le registre de données, $|\psi\rangle_A \to U|\psi\rangle$, au moyen de **portes logiques quantiques** : les qubits sont manipulés par des champs classiques, en général électromagnétiques, en utilisant le phénomène des oscillations de Rabi[c]. Les portes quantiques sont soit des portes individuelles agissant sur l'état d'un seul qubit, soit des portes dites « à deux qubits », agissant sur l'état global des deux qubits. Enfin, on effectue une mesure des qubits une fois terminée l'évolution unitaire nécessaire pour exécuter l'algorithme. En raison de la linéarité de la mécanique quantique, si l'on connaît l'action de la transformation U sur les états $|01101\rangle$ et $|10010\rangle$ par exemple, alors on la connaît aussi sur toute superposition $a|01101\rangle + b|10010\rangle$. Cette aptitude de l'ordinateur quantique à agir non seulement sur certains états précis mais aussi sur toute combinaison linéaire de ces états, est parfois appelée « parallélisme quantique ». On pourrait (abusivement[d]) en déduire qu'un algorithme quantique est susceptible d'explorer simultanément toutes les branches d'un calcul, mais la mesure finale des qubits ne laisse subsister qu'une seule de ces branches : c'est la fameuse « réduction du paquet d'ondes ». L'ordinateur quantique va devoir utiliser toute la puissance des superpositions, interférences et intrications, pour faire émerger le résultat recherché de la mesure finale des qubits, et cela avec une certaine probabilité. C'est pourquoi la cohérence des qubits doit être soigneusement préservée tout au long du calcul, et c'est là le défi principal du calcul quantique.

La décohérence est donc l'ennemi public numéro un de l'ordinateur quantique. En effet, cette dernière, due au couplage des qubits avec leur environnement, détruit les délicates superpositions linéaires, et toute possibilité de calcul quantique s'effondre. Il faut d'une part isoler les qubits de leur environnement autant que faire se peut (fig. 1). Mais d'autre part le fonctionnement des portes quantiques, ainsi que les mesures, exigent des interactions des qubits avec des champs extérieurs. Les champs classiques ne s'intriquent pas avec les qubits et n'entraînent pas de décohérence. Néanmoins, isoler les qubits de leur environnement et agir efficacement sur eux sont deux exigences qui peuvent a priori être difficiles à concilier.

>>>



2. Version très schématique de l'architecture du processeur de Google.
Les qubits sont disposés suivant un réseau bidimensionnel 6 x 6 et peuvent interagir avec leurs plus proches voisins (portes à deux qubits). La figure décrit deux cycles successifs du calcul. À chaque cycle, les qubits représentés par des points rouges sont soumis à l'action de portes individuelles, tandis que les qubits représentés par des points bleus, reliés par un trait, sont soumis à l'action de portes à deux qubits. À l'intérieur d'un cycle, les portes peuvent être exécutées dans un ordre arbitraire car les opérations quantiques correspondantes commutent.

>>>

## Algorithmes et erreurs quantiques

Il existe un nombre très limité (autour de cinq selon la manière dont l'on compte) d'algorithmes quantiques qui surpassent les classiques. Le plus connu est l'algorithme de Shor, qui permettrait de casser le chiffrement RSA, universellement utilisé pour crypter des données. En effet, dans ce chiffrement, on se donne un nombre entier N très grand, produit de deux nombres premiers p et q : N = pq. Le nombre N est public, mais p et q sont gardés secrets. L'algorithme de Shor permet, étant donné N, de trouver les facteurs p et q et de casser le chiffrement RSA. La taille du problème est donnée par le nombre n de bits nécessaires dans le registre de données, qui dans ce cas est tout simplement déduit de $n = 2N$.
La procédure de chiffrement utilise un cas particulier de fonction dite à sens unique, une fonction facile à calculer mais dif cile à inverser : il est immédiat de faire le produit de deux entiers, mais long en temps de calcul, étant donné N, de trouver p et q.
Le meilleur algorithme classique connu nécessite un temps proportionnel à $\exp(n^{1/3})$, alors que l'algorithme de Shor se contente de $n^3$. On passe d'un temps exponentiel (dans la taille des données) à un temps polynomial – c'est-à-dire un temps proportionnel à une puissance de n – et on observe donc un gain exponentiel. Ce gain exponentiel est la signature de la suprématie quantique.

Cependant, il convient de faire trois mises en garde.
1. L'exemple de l'algorithme de Shor est pour le moment purement théorique et la dé nition de la complexité du calcul, polynomiale ou exponentielle, n'est valable qu'asymptotiquement, pour n.
2. Il n'est pas prouvé mathématiquement qu'aucun algorithme classique ne puisse faire mieux que $\exp(n^{1/3})$. Les experts estiment peu probable que l'on trouve un jour un algorithme polynomial pour la factorisation, mais ce n'est pas rigoureusement exclu.
3. On est très loin de pouvoir fabriquer un ordinateur quantique capable de factoriser un nombre de 2048 = 11 2 bits (617 chiffres), ce qui signerait l'acte de décès de tous les chiffrements RSA actuels. On estime qu'il faudrait de l'ordre de $10^8$ à $10^9$ qubits physiques pour un tel calcul alors que, nous allons le voir, nous sommes aujourd'hui limités à une centaine de qubits.

Un des handicaps majeurs du calcul quantique est la nécessité de corriger les erreurs. Les portes quantiques ne fonctionnent jamais correctement à cent pour cent, bien que des progrès considérables aient été faits ces dix dernières années sur leurs taux d'erreurs. Il en existe d'autres sources : décohérence due à des interactions avec le milieu extérieur, erreurs de mesure, dans la transmission des qubits, etc. Les codes correcteurs d'erreurs classiques fondés sur la redondance ne peuvent pas se transposer directement au cas quantique en raison du théorème de non clonage, qui interdit de dupliquer les qubits pendant la phase de calcul.
Cependant, on a mis au point théoriquement des codes correcteurs d'erreurs quantiques, qui permettent de remplacer des opérations sur des qubits physiques par des opérations sur des qubits logiques formés avec des groupements de qubits physiques, et où les erreurs sont corrigées. Un code correcteur standard est celui de Steane, qui utilise un qubit logique et sept qubits physiques, auxquels ils faut ajouter tout un cortège de qubits auxiliaires destinés à détecter et corriger les erreurs tout au long du calcul. Avec le taux d'erreur actuel des portes quantiques, une estimation optimiste est qu'il faudrait aux alentours de $10^4$ qubits physiques pour construire un qubit logique.

## L'ère du NISQ et *Sycamore*

Compte tenu de l'état de l'art aujourd'hui, il est prudent de ne pas prendre pour argent comptant les ambitions af chées du calcul quantique, a n de ne pas susciter de faux espoirs infondés. Que peut-on raisonnablement af rmer, étant donné que l'on sait aujourd'hui fabriquer un ordinateur quantique comportant une cinquantaine de qubits physiques ? En 2018, John Preskill, transfuge de la physique des particules et

auteur de contributions très importantes sur le calcul quantique, a proposé le concept de NISQ : Noisy Intermediate Scale Quantum technologies (« technologies quantiques bruitées d'échelle intermédiaire ») pour caractériser la situation actuelle du calcul quantique. Dans cette ère du NISQ, on dispose de processeurs quantiques comportant de 50 à 100 qubits (échelle « intermédiaire »), mais sans code de correction d'erreurs, d'où le qualificatif « bruité ».

Dans ces conditions, existe-t-il des problèmes où l'on peut prouver qu'un ordinateur quantique est « infiniment » plus rapide qu'un ordinateur classique, autrement dit peut-on déjà prouver la suprématie quantique ? Arute *et al.* ont mis au point un processeur de 53 qubits, construits avec des circuits supraconducteurs comprenant des jonctions Josephson, qui permettent de fabriquer des atomes artificiels à deux niveaux (fig. 1), et ils ont exploré une des pistes possibles, celle de « l'échantillonnage de circuits quantiques aléatoires ».

Dans le processeur de Google, baptisé Sycamore, les qubits sont disposés suivant un réseau à deux dimensions (fig. 2) et chaque qubit est susceptible de se coupler à l'un de ses plus proches voisins grâce à une porte à deux qubits. De plus, chaque qubit peut être soumis individuellement à l'action d'une porte quantique choisie de façon aléatoire parmi trois portes possibles, ce qui fabrique un circuit quantique aléatoire. Quelques données numériques : les qubits sont au nombre de $n = 53$, disposés suivant un réseau 2D et la dimension de l'espace de Hilbert des qubits est $2^n \simeq 10^{16}$. Dans une simulation complète, le nombre maximum de portes à un qubit est de ¾ 1100, celui de portes à deux qubits de ¾ 400. Le calcul procède par cycles successifs (fig. 2) et le nombre de cycles est au maximum $m = 20$. Les portes à un qubit sont contrôlées par des impulsions électromagnétiques d'une durée de l'ordre de 25 ns, tandis que les portes à deux qubits ont une durée d'activation d'environ 12 ns. On peut donc réaliser une simulation complète en un temps de l'ordre de la microseconde, et en pratique $10^6$ simulations sont effectuées en 200 s, ce qui permet un excellent échantillonnage de la distribution de probabilité des qubits mesurés.

Pour effectuer une simulation, on part d'un état initial $|\ >$ des n qubits, on applique une transformation aléatoire unitaire $U$ réalisée physiquement par la configuration des portes quantiques choisie pour cette simulation particulière, et les qubits dans la configuration $U|\ >$ sont mesurés dans la base $\{|0>, |1>\}$. Le résultat de la simulation numéro i est une chaine de bits $x_i = \{y_1, y_2, \ldots, y_n\} \in \{0, 1\}^*$, où $\{0, 1\}^*$ désigne l'ensemble des chaines de bits. Une propriété des circuits aléatoires est que certaines chaines de bits sont beaucoup plus probables que d'autres dans une simulation donnée, au lieu d'être distribuées uniformément. En effet, ces circuits fabriquent des états hautement intriqués, et on observe des phénomènes d'interférences qui rappellent celui de « tavelures » (speckles) que l'on peut voir en éclairant une surface rugueuse avec un laser. La déviation par rapport à la distribution uniforme est mesurée par l'entropie croisée :

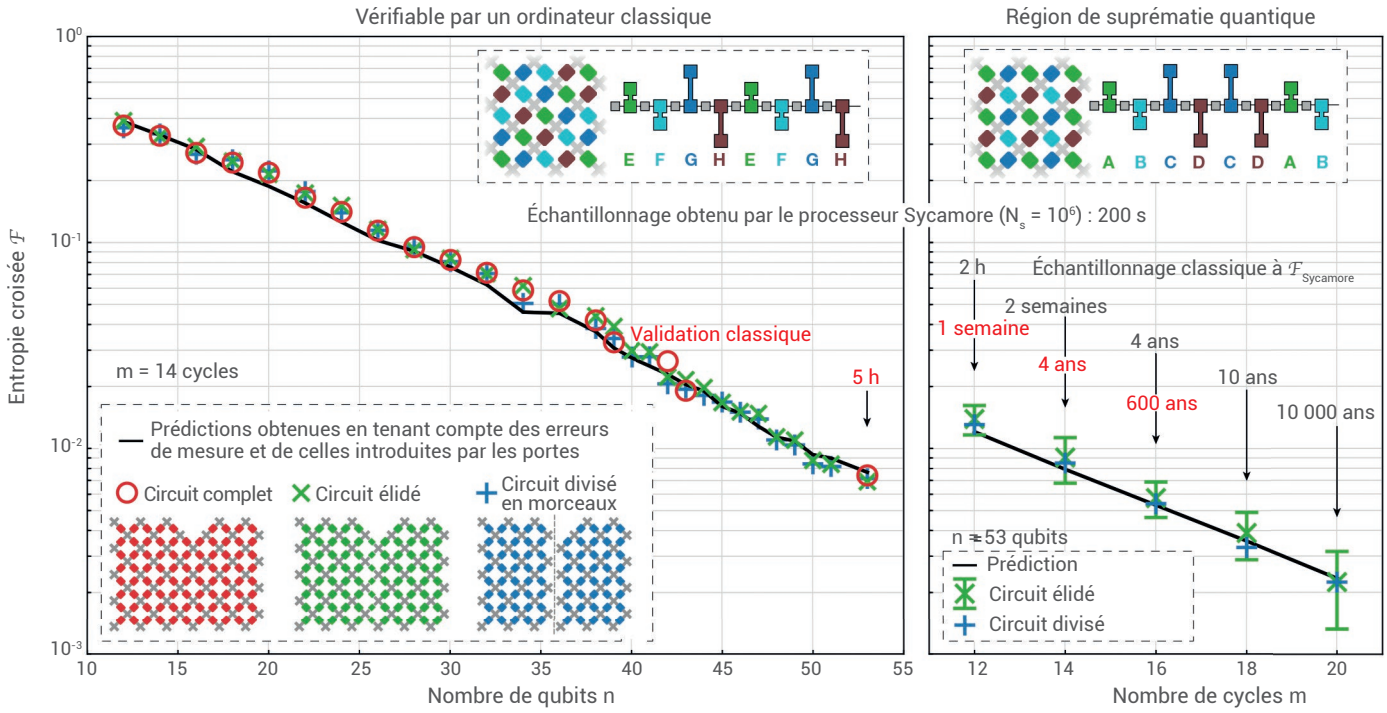
$$\mathcal{F} = 2^n \langle p(x_i) \rangle_i \quad 1 \ ,$$

où $p(x_i)$ est la probabilité de la chaine $x_i$ et la moyenne est prise sur l'ensemble des chaines. Dans le cas d'une distribution uniforme $p(x_i) = 2^{-n}$, soit $\mathcal{F} = 0$. Dans le cas d'un circuit aléatoire idéal fonctionnant sans erreurs, on montre que la distribution suit exponentielle et on en déduit $\mathcal{F} = 1$. Cependant, en raison du fonctionnement imparfait des portes et des erreurs de mesure, on s'attend à une valeur expérimentale $\mathcal{F} < 1$ : les erreurs détruisent partiellement la cohérence et le résultat tend vers la distribution uniforme[a]. L'objectif est d'atteindre, en présence d'erreurs, une valeur de $\mathcal{F}$ suffisamment élevée pour qu'elle ne soit pas calculable en un temps polynomial (temps variant comme un polynôme du nombre d'entrées) sur un ordinateur classique. Autrement dit, une simulation du circuit quantique par un ordinateur classique ne pourrait en aucun cas produire en un temps polynomial le degré d'intrication nécessaire pour obtenir une valeur suffisamment élevée de $\mathcal{F}$.

Le problème est évidemment celui du contrôle des erreurs. Étant donné que le processeur fonctionne sans code de correction d'erreurs, il n'y a aucune garantie que le résultat du calcul soit fiable : dans l'ère du NISQ se pose en général la question de la fiabilité de tout calcul quantique mené sur un processeur qui ne corrige pas les erreurs. Autrement dit, comment peut-on vérifier le résultat du calcul, ou comment peut-on s'assurer que ce qui sort de l'ordinateur quantique a quelque chose à voir avec ce que l'on attend de la théorie ? Dans le cas de l'algorithme de Shor, la vérification est facile : si l'ordinateur quantique nous donne les facteurs premiers p et q de N, il suffit de faire la multiplication : est-ce que $pq = N$ ou non ? Mais un processeur d'une cinquantaine de qubits fonctionnant sans erreurs permettrait au mieux de factoriser un nombre de 25 bits, et on serait très loin de la suprématie quantique, car un tel nombre serait factorisé par un ordinateur classique en une fraction de seconde ! Dans le cas présent, est-ce que mesurer une valeur élevée de $\mathcal{F}$ reflète la réalité d'un véritable calcul quantique ou une accumulation d'erreurs sans signification ? Dans une étape préliminaire, il est indispensable d'étalonner les sources d'erreurs. De façon très schématique et pour fixer les ordres de grandeur, cet étalonnage donne une probabilité d'erreur $e_1 \simeq 0{,}15\%$ pour les portes à un qubit, $e_2 \simeq 0{,}6\%$ pour les portes à deux qubits et $e_3 \simeq 4\%$ pour les mesures[b]. Ceci permet de modéliser $\mathcal{F}$ comme produit des probabilités que les portes et les mesures fonctionnent sans erreur. Cette modélisation prenant en compte l'effet des erreurs est validée par des simulations classiques jusqu'à un nombre de cycles $m = 14$, avec une valeur de $\mathcal{F} \simeq 10^{-2}$, la durée maximale de la simulation classique étant de l'ordre de 5 heures (fig. 3). En augmentant le nombre de cycles jusqu'à $m = 20$, on obtient en 200 s la valeur $\mathcal{F} \simeq (2{,}2 \pm 0{,}2)\ 10^{-3}$, ce qui diffère significativement de la valeur zéro. Il faudrait 10 000 ans au superordinateur classique le plus performant disponible aujourd'hui pour obtenir cette valeur. En ce sens, on a atteint la suprématie quantique.

Il est donc plausible que la suprématie quantique ait été prouvée sur cet exemple, mais on doit néanmoins souligner que le calcul quantique correspondant n'a évidemment pas le moindre intérêt pratique ! De plus, on rencontre un problème analogue à celui signalé pour l'algorithme de Shor : est-on vraiment certain d'avoir utilisé le meilleur algorithme de calcul classique ? Une équipe d'IBM estime avoir développé un algorithme classique qui reproduirait le résultat de l'équipe de Google en deux jours et demi, et non 10 000 ans ! La question reste ouverte. Une autre objection est que simuler classiquement l'état réel obtenu par Arute *et al.*, incluant les erreurs, est bien moins exigeant en temps de calcul que simuler l'état exact, car l'espace de Hilbert des états réels est une fraction infime de l'espace de Hilbert total.

>>>




3. La suprématie quantique est-elle démontrée ? Encadrés du haut : organisation des portes. On remarque la différence de motif à droite et à gauche. Figure de gauche : évaluation de l'entropie croisée $\mathcal{F}$ pour deux circuits simplifiés ("élidé" et "divisé") qui diminuent le temps de simulation en fonction du nombre de qubits avec un nombre de cycles $m$ = 14. Les simplifications sont validées par une simulation numérique classique (cercles rouges). Les prédictions pour $\mathcal{F}$ (trait épais noir) sont calculées à partir des erreurs mesurées. Figure de droite : pour 14 ≤ $m$ ≤ 20 et 53 qubits, le temps de calcul de la simulation classique devient prohibitif. Chiffres rouges : simulation du circuit complet. Chiffres gris : simulation du circuit simplifié.
Source : F. Arute et al., Nature (2019) 505.

>>>

## Conclusion

En conclusion, l'ordinateur quantique continue à progresser, mais on est encore très loin d'ordinateurs capables de résoudre un problème spéci que pratique comme casser le chiffrement RSA. Pour reprendre une comparaison due à Scott Aaronson, si l'on fait une analogie avec les ordinateurs classiques, nous en sommes au stade des ordinateurs à lampe de 1945. En revanche, dans les dix prochaines années, on peut s'attendre à des ordinateurs quantiques dédiés (par opposition à programmables) capables de résoudre des problèmes limités de simulation d'intérêt pratique : mise au point de médicaments, simulation de systèmes physiques de la matière condensée, etc. On doit d'une part prendre avec prudence des annonces médiatiques souvent exagérées et, d'autre part, poursuivre la recherche fondamentale et appliquée sur les ordinateurs quantiques, car elle touche à des problèmes de physique de base sur les limites possibles de la mécanique quantique, et même des problèmes de science fondamentale : validité ou non de la thèse de Church-Turing étendue qui af rme que tout processus physique peut être simulé en temps polynomial sur une machine de Turing. En n, les retombées de ces recherches pourraient être tout autres que celles que nous pouvons imaginer aujourd'hui. ■


( Q VDYRL

1• M. Leduc et S. Tanzilli, Reflets de la Physique, 51 (2016) 28-33.

2• K. Hartnett, « Suprématie quantique : le guide pratique », Dossier Pour la Science (mai-juin 2020) 8690.

3• K. Hartnett, « Une suprématie contestée », Dossier Pour la Science (mai-juin 2020) 92-95.

4• M. Le Bellac, A Short Introduction to Quantum Information and Computation , Cambridge University Press (2007)

5• T. Meunier, « La course aux qubits », Dossier Pour la Science (mai-juin 2020) 78-84.


(a) Dans la version orthodoxe de la mécanique quantique, « état quantique inconnu » est un oxymore (une contradiction), car un état doit être connu de quelqu'un.

(b) Il est facile d'imaginer des états à deux qubits, par exemple |00> où les deux qubits sont dans l'état |0>, ou |11> où les deux qubits sont dans l'état |1>. Le principe de superposition nous dit que la superposition a|00> + b|11>, $|a|^2 + |b|^2 = 1$, représente aussi un état physique que l'on peut fabriquer au laboratoire : c'est un exemple d'état intriqué.

(c) Le couplage d'un qubit à un champ oscillant pendant une durée aléatoire permet de mettre le qubit dans l'état de superposition souhaité, par exemple de le faire passer de l'état |0> à l'état |1>.

(d) Dans une expérience de fentes d'Young avec des particules quantiques, on dit souvent que « la particule est passée par les deux fentes ». Mais il s'agit d'une image, d'une interprétation, la mécanique quantique stricto sensu ne dit rien de tel. Dans l'interprétation de de Broglie-Bohm, qui reproduit exactement toute la mécanique quantique non relativiste, la particule passe par une seule des deux fentes.

(e) On montre que l'entropie croisée est donnée par $\mathcal{F} \bullet (1 - e)^m$, où e est un taux d'erreur moyen de l'ordre de 1%.

(f) On obtient de meilleurs résultats en utilisant comme qubits des ions piégés, pour lesquels $e_1 \simeq 0{,}007\%$ et $e_2 \simeq 0{,}1\%$. Malheureusement, il est pour le moment impossible de rassembler plus d'une vingtaine de qubits de ce type dans un processeur.