Le problème à N corps qui se cache derrière l'ordinateur quantique

Xavier Waintal (xavier.waintal@cea.fr)
Laboratoire Photonique, Électronique et Ingénierie Quantiques (PHELIQS)
Département de Nanophysique, IRIG, CEA Grenoble, 38054 Grenoble Cedex 9

Le concept d'ordinateur quantique recouvre deux réalités très différentes. Il y a d'une part de très belles expériences de physique qui se basent sur des systèmes appartenant à la nanoélectronique quantique (supraconducteurs, semi-conducteurs), l'optique quantique ou la physique atomique. D'autre part, il y a une promesse, celle que ces systèmes puissent être décrits avec grande précision par un modèle mathématique très épuré. Ce modèle est une instance d'un problème plus général, le problème quantique à N corps, que les physiciens étudient depuis des dizaines d'années.

Dans cet article, nous verrons qu'envisager l'ordinateur quantique sous l'angle du problème quantique à N corps donne un éclairage utile pour comprendre à quoi il pourrait servir ou les difficultés liées à son élaboration.

L'ordinateur quantique : le point de vue des informaticiens *versus* la réalité

L'ordinateur quantique, tel qu'il nous est présenté dans la presse grand public ou dans le « plan quantique national » donne en général le point de vue des théoriciens de l'informatique quantique. Ce point de vue utilise une mécanique quantique très simplifiée, dans laquelle on ne s'intéresse ni à l'espace, ni au temps, ni à l'énergie, ni aux statistiques quantiques (bosons ou fermions). Dans ce cadre théorique, on peut trouver un petit nombre d'applications où l'ordinateur quantique permettrait des accélérations exponentielles par rapport à ses homologues classiques.

L'application la plus connue est l'algorithme de Shor qui permet de factoriser rapidement un très grand nombre en produit de nombres premiers. Une autre application possible serait le calcul de l'énergie de l'état fondamental d'une molécule.

Les ordinateurs quantiques existants sont encore vraiment très loin de ce modèle simplifié et sont connus sous l'acronyme NISQ ("Noisy Intermediate Scale Quantum"), où le N qui vient de "noisy" souligne le fait qu'ils sont encore très imparfaits. Par exemple, aucun ordinateur quantique existant n'est capable de multiplier 3 par 5.

Il existe plusieurs technologies concurrentes. La plus avancée actuellement, développée par Google, utilise des puces supraconductrices à base d'aluminium et est fondée sur des techniques de fabrication très proches de celles de la microélectronique. La puce est alors plongée à très basse température (autour de 10 mK) grâce à un cryostat à dilution, et reliée à des générateurs de micro-ondes (1 à 10 GHz) qui envoient des séquences de *pulses* visant à manipuler l'état quantique (de façon très proche de ce qui se fait en résonance magnétique nucléaire).

Ce qui se joue aujourd'hui, c'est de savoir si le modèle simplifié de l'informatique quantique théorique peut représenter le réel avec suffisamment de précision pour que ses applications soient envisageables en pratique.

Article disponible sur le site https://www.refletsdelaphysique.fr ou https://doi.org/10.1051/refdp/202170018

1. Machines digitales (a) et analogiques (b) : ne pas confondre.

L'ordinateur quantique, une machine analogique

Les ordinateurs que nous connaissons sont des machines digitales. L'ordinateur digital est régi par des *bits* qui ne peuvent prendre que deux valeurs : 0 ou 1. Son état interne est essentiellement donné par le contenu de sa mémoire vive, quelques dizaines de milliards de *bits* pour un ordinateur de bureau. Par contraste, une machine analogique possède un état interne pouvant varier continument (fig. 1).

Ces machines analogiques ont une longue histoire [1], qui recouvre les règles à calcul que nos grands-parents utilisaient en lieu des calculatrices ; les circuits intégrateurs, dérivateurs ou additionneurs de l'électronique ; et un grand nombre d'autres dispositifs ingénieux (voir [2] pour l'exemple des ordinateurs basés sur les écoulements fluides). Elles sont beaucoup moins précises que les machines digitales et se limitent à des fonctions relativement simples.

Un ordinateur quantique est également une machine analogique. Son état interne, noté $|\Psi\rangle$, est décrit par un très grand nombre de variables continues. Considérons une machine quantique dotée de N *bits* quantiques (que nous appellerons *qubits* par la suite). Pour N = 1, la machine peut se trouver dans n'importe quelle superposition $|\Psi\rangle = \Psi_0|0\rangle + \Psi_1|1\rangle$ des deux états $|0\rangle$ et $|1\rangle$ du *qubit*. L'état de la machine est alors donné par les deux nombres complexes Ψ_0 et Ψ_1. Pour N = 2, la machine peut se trouver dans une superposition
$|\Psi\rangle = \Psi_{00}|00\rangle + \Psi_{01}|01\rangle + \Psi_{10}|10\rangle + \Psi_{11}|11\rangle$
des quatre états possibles formés par les deux *qubits*. De façon générale, l'état d'une machine à N *qubits* est donné par :

$$|\Psi\rangle = \sum_{i_1 i_2 i_3 \cdots i_N} \Psi_{i_1 i_2 i_3 \cdots i_N} |i_1 i_2 i_3 \ldots i_N\rangle \quad (1),$$

où la somme s'entend sur tous les états possibles du premier *qubit* $i_1 = 0, 1$, du second *qubit* $i_2 = 0, 1$, etc. L'état d'une telle machine est donné par un nombre gigantesque 2^N de variables **continues**, la « fonction d'onde » $\Psi_{i_1 i_2 i_3 \cdots i_N}$. La puissance de calcul que va pouvoir atteindre un ordinateur quantique dépendra de façon cruciale de la précision avec laquelle on contrôlera les 2^N variables de la fonction d'onde. Une variable continue (comme le bouton rond à droite de la figure 1) ne peut être connue qu'avec une précision finie [3] (par exemple +/- 0,01 degré pour le bouton). Chaque opération (par exemple, un quart de tour du bouton vers la droite) est associée à une certaine précision avec laquelle elle est effectuée. Une difficulté supplémentaire vient de ce que l'on travaille « en aveugle » jusqu'à la fin du calcul. En effet, on ne peut pas vérifier quelle est la position du bouton de la figure 1 car, en mécanique quantique, regarder c'est modifier et on obtiendrait un résultat faux. La précision du système quantique se détériore donc à chaque opération (aussi appelée « porte »), mais également en l'absence d'opération : on parle alors de « décohérence ». Notons qu'à la fin du calcul, lorsqu'on mesure les *qubits*, on détruit l'état quantique, et on obtient une unique configuration $i_1 i_2 i_3 \ldots i_N$ avec la probabilité $|\Psi_{i_1 i_2 i_3 \cdots i_N}|^2$.

L'information extraite de la fonction d'onde est donc digitale et représente une infime partie de l'information analogique contenue dans la fonction d'onde.

Les physiciens ont l'habitude de décrire l'évolution d'un système quantique par son hamiltonien H. Si à un moment précis t_n l'hamiltonien est donné par H_n, l'évolution du système est alors décrite par son opérateur d'évolution U_n :

$$U_n = \exp(-iH_n t_n) \quad (2).$$

Les mathématiciens de l'informatique quantique ne s'intéressent pas à la dynamique quantique. Ils définissent un certain nombre de portes quantiques U_n qui agissent sur un ou deux *qubits* et supposent que les physiciens ont ou vont trouver une façon de contrôler H_n, de manière à obtenir la porte escomptée. Si l'on prépare tous les *qubits* initialement dans l'état $|0\rangle$, on obtient après n portes quantiques l'état suivant :

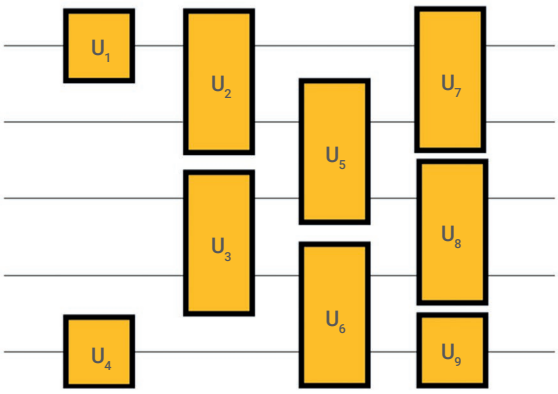
$$|\Psi\rangle = U_n U_{n-1} \ldots U_3 U_2 U_1 |000\ldots0\rangle \quad (3).$$

La figure 2 montre un exemple de circuit quantique. Parvenir à fabriquer un ordinateur quantique, c'est développer un système qui soit décrit aussi parfaitement que possible par les équations (1) et (3).

Où le problème quantique à N corps fait son apparition

Les équations (1), (2) et (3) forment une instance particulière de ce que l'on nomme le problème quantique à N corps, un problème central de la physique théorique. Si on interprète l'état $|0\rangle$ du *qubit* comme celui d'un *spin* pointant vers le bas et l'état $|1\rangle$

>>>



2. Un exemple de circuit quantique, à lire de gauche à droite, un peu comme une partition de musique. Chaque ligne correspond à un *qubit* et chaque porte U_n opère sur un ou deux *qubits* différents.

>>>

comme celui du *spin* pointant vers le haut, alors la fonction d'onde à N *qubits* peut être vue comme celle d'un système de N *spins* quantiques, et on aboutit à des problèmes de magnétisme (ferromagnétisme, antiferromagnétisme, liquides de *spin*, etc.). Si on généralise un peu le problème et qu'on étend l'espace à d'autres états $|2\rangle$, $|3\rangle$..., alors on peut interpréter ces différents états comme, par exemple, les niveaux d'énergie d'une molécule. La fonction d'onde à N corps correspond alors à la configuration électronique de la molécule. Si on étend les états $|0\rangle$, $|1\rangle$, $|2\rangle$, $|3\rangle$ ... à une base continue $|x\rangle$, on obtient le problème général de N particules en interaction, avec lequel on peut décrire, entre autres, toute la matière condensée. Enfin, si l'on passe également à la limite thermodynamique $N \to \infty$, alors on définit les théories quantiques des champs (comme l'électrodynamique quantique ou la chromodynamique quantique) qui sont les théories les plus fondamentales de la physique.

Le problème à N corps joue alors un double rôle vis-à-vis de l'ordinateur quantique : d'un côté il permet de relier le modèle simplifié de l'informatique théorique au réel, et en particulier de comprendre l'origine des imperfections et le caractère fondamental du phénomène de décohérence (l'intrication de l'état avec les degrés de liberté que l'on ne contrôle pas). De l'autre côté, on comprend pourquoi, parmi les applications pressenties pour l'ordinateur quantique, celles qui servent à résoudre le problème quantique à N corps (comme des problèmes de réactions chimiques) figurent en première place : un ordinateur quantique est essentiellement un problème à N corps bien contrôlé.

Une hiérarchie d'ordinateurs quantiques et leurs applications

Le même mot « ordinateur quantique » fait référence à une hiérarchie d'objets très différents, certains existants, d'autres très hypothétiques. Ils sont résumés dans le tableau 1.

#1. Les ordinateurs analogiques sans portes sont des expériences effectuées sur des systèmes modèles dont on cherche à contrôler l'hamiltonien H avec un maximum de précision. Au fur et à mesure que l'on obtient des accords de plus en plus quantitatifs entre les expériences d'une part et les prédictions théoriques du problème à N corps d'autre part, on envisage d'utiliser les résultats expérimentaux dans des régimes où l'on n'est plus capable de résoudre le problème à N corps théoriquement. C'est la **simulation quantique**. Elle pourrait donner des renseignements précieux sur des problèmes à N corps importants, comme ceux reliés à la supraconductivité à haute température critique. Aujourd'hui, de nombreuses expériences montrent des accords quantitatifs dans des régimes intéressants, mais on s'écarte encore très peu des régimes accessibles théoriquement (voir [4] pour un bel exemple).

#2. Dans un ordinateur analogique à portes, on fait en sorte que la dynamique quantique soit décrite par des portes U_n. La machine la plus aboutie actuellement est celle de Google [5], à base de circuits supraconducteurs. Elle compte N = 53 *qubits*. Ces machines

Difficulté	Type d'ordinateur quantique	Exemples d'applications
#1	Ordinateur analogique sans portes	Simulations quantiques
#2	Ordinateur analogique à portes, basse fidélité	Validation du système. « Suprématie quantique »
#3	Ordinateur analogique à portes, haute fidélité	Calculs variationnels de chimie quantique
#4	Ordinateur digitalisé sans mémoire quantique (calculs quasi déterministes)	Factorisation de nombres premiers Calculs exacts de chimie quantique
#5	Ordinateur digitalisé avec mémoire quantique	Intelligence artificielle, algèbre linéaire

Tableau 1. Différents types d'ordinateurs quantiques et les applications qui peuvent être envisagées.

servent essentiellement à valider le fait que le modèle mathématique donné par les équations (1) et (3) représente correctement le système. Dans l'expérience [5], les auteurs ont comparé le résultat d'une expérience avec celui d'un calcul exact de la fonction d'onde (calcul effectué sur un ordinateur classique). On définit ainsi une fidélité F qui vaudrait 1 pour une machine parfaite et tend vers 0 au fur et à mesure que l'état de la machine quantique perd en précision. Cette fidélité décroît exponentiellement avec le nombre n de portes :

$$F = f^n \qquad (4).$$

Google est parvenu d'une part à valider l'équation (4) et d'autre part à conserver une fidélité effective par porte autour de f = 99 %. Ceci est en soi un résultat remarquable, car cette fidélité n'est que légèrement inférieure aux meilleures fidélités obtenues avec cette technologie. En revanche, l'état de la machine après seulement une vingtaine d'opérations par *qubit* n'a plus qu'un lointain lien (F = 0,1 %) avec ce que serait un état parfait.

> “Le même mot *ordinateur quantique* fait référence à une hiérarchie d'objets très différents.”

Google qualifie le résultat [5] de « suprématie quantique » [6] en argumentant que l'état obtenu est impossible à simuler, *« même en 10 000 ans sur le plus gros ordinateur du monde »*. L'expression est discutable. D'une part, tous les problèmes à N corps sont exponentiellement difficiles à simuler, et en particulier tous les simulateurs de type #1. D'autre part, et c'est plus intéressant, parce que la difficulté supposée est celle de la simulation d'un état parfait, très loin de l'état dégradé à F = 0,1% démontré par Google. Les techniques à N corps de « compression d'états quantiques » donnent ici un nouvel éclairage [6] : la compression d'états quantiques, un peu comme la compression d'image, permet de calculer des états quantiques qui, en échange d'une perte de fidélité, sont exponentiellement plus faciles à calculer. Dans certaines situations, on constate que des fidélités aussi élevées que celles obtenues par Google sont retrouvées avec des ressources de calcul classiques très limitées [7].

#3. Calculs stochastiques à haute fidélité. On voudrait pouvoir utiliser ces ordinateurs analogiques à portes pour des applications utiles. Une des applications qui semble la plus accessible est le calcul variationnel en chimie quantique. On se sert ici des portes quantiques pour préparer une fonction d'onde censée représenter l'état fondamental d'une molécule. En répétant l'expérience un grand nombre M de fois, on échantillonne la fonction d'onde et construit une estimation de l'énergie associée avec une précision $1/M^{1/2}$. On optimise ensuite les paramètres qui définissent les portes pour minimiser cette énergie et obtenir une approximation de l'énergie de la molécule. La précision atteinte dépend crucialement des erreurs introduites à chaque porte quantique.

Cette approche est très similaire à une technique importante du problème à N corps : le calcul Monte-Carlo quantique variationnel (VQMC), où l'on échantillonne et optimise également une fonction d'onde. Les deux approches ont une complexité algorithmique (vitesse de calcul) similaire.

La difficulté principale de cette approche réside, de nouveau, dans la précision. Plus on va vouloir utiliser un grand nombre de portes ou un grand nombre de *qubits*, plus la fidélité de la fonction d'onde va se détériorer. Or, l'expérience qui nous vient du VQMC est que des variations minuscules d'énergie peuvent être associées à des changements physiques importants. Par exemple, la différence d'énergie entre l'aluminium supraconducteur et l'aluminium dans son état normal correspond à une variation relative d'énergie qui n'est que de 10^{-8}, bien que les deux états soient drastiquement différents. En ce qui concerne la chimie, on cherche des précisions de quelques meV pour pouvoir résoudre des trajectoires réactionnelles, soit des précisions relatives de 10^{-4} environ. L'équation (4) semble indiquer que nous sommes très loin de pouvoir envisager cette application dans des cas utiles (des démonstrations sur des petites molécules facilement accessibles au calcul classique ayant déjà été faites).

#4. L'étoile du Berger : l'ordinateur quantique digitalisé. On en vient maintenant aux applications imaginées de l'ordinateur quantique les plus spectaculaires, celles qui donneraient à la fois un résultat **déterministe** et **une accélération exponentielle**. Ce sont sur elles que portent les plus gros espoirs et elles guident les plus gros investissements. En général, lorsqu'on mesure chaque *qubit* d'une machine, on obtient une configuration $i_1 i_2 i_3 ... i_N$ avec la probabilité $|\Psi_{i_1 i_2 i_3 ... i_N}|^2$, *i.e.* le résultat d'un calcul est aléatoire. On peut chercher à effectuer des moyennes en répétant l'expérience un grand nombre de fois comme en **#3**, mais pour pouvoir véritablement parler de calcul, il faudrait obtenir un résultat $i_1 i_2 i_3 ... i_N$ de manière déterministe. Pour cela, un outil théorique a été inventé par le mathématicien Peter Shor, la transformée de Fourier quantique (TFQ). Il s'agit d'un circuit quantique qui effectue des interférences destructives pour toutes les configurations sauf une, celle qui correspond au résultat escompté. La TFQ a permis de formuler des algorithmes quantiques qui pourraient être exponentiellement plus rapides que leurs homologues classiques. Parmi eux, le plus célèbre est l'algorithme de Shor pour la factorisation de grands nombres premiers. Il pourrait, hypothétiquement, permettre de décoder des communications cryptées de type https.

Ici encore, c'est la précision qui vient rendre ces applications très compliquées. Pour tenter d'estimer la difficulté, supposons un instant qu'un algorithme de Shor a été réalisé de manière parfaite et qu'une seule étape du calcul, la toute dernière, a été faite de façon bruitée. Considérons le cas d'une clé de 2000 *bits* (taille typique d'une clé utilisée aujourd'hui) que l'on cherche à factoriser, soit 4000 *qubits* et un taux d'erreur de 10^{-3} (l'état de l'art). La probabilité d'obtenir le bon résultat est de $(1\text{-}10^{-3})^{4000}$, soit seulement 2%. Or, l'algorithme de Shor ne nécessite pas une mais des millions d'étapes, chacune d'entre elles étant bruitée. Même avec des *qubits* de qualité très supérieure à ceux d'aujourd'hui, de tels algorithmes sont impossibles.

>>>

>>>

La correction d'erreur quantique et les portes résistantes aux erreurs. C'est encore Shor qui propose une solution théorique au problème précédent, en inventant ce qui a été très improprement appelé la **correction d'erreur quantique** (CEQ). La CEQ consiste à encoder des *qubits* « logiques » sur plusieurs *qubits* physiques, pour obtenir des *qubits* logiques plus résistants aux erreurs que les *qubits* physiques originaux. La CEQ pourrait hypothétiquement permettre de fabriquer des *qubits* logiques de précision arbitraire. L'idée ici est de digitaliser les valeurs possibles de la fonction d'onde et de n'effectuer que des portes quantiques qui respectent cette digitalisation. Cette dernière a un cout : l'essentiel des *qubits* présents et des portes effectuées servent à garantir l'intégrité et la précision des *qubits* logiques. Une étude [7], pas particulièrement pessimiste, chiffre ce cout pour une machine à 100 *qubits* logiques : il faut compter plusieurs *milliards* de *qubits* et jours continus de calculs pour obtenir un résultat, si l'on suppose une fidélité initiale f = 99,9999 %.

#5. Les mémoires quantiques. Il existe encore une classe d'applications qui pourrait étendre grandement les applications possibles de l'ordinateur quantique. En particulier, l'algorithme HHL résoudrait des problèmes d'algèbre linéaire avec de nombreuses applications possibles à l'intelligence artificielle. Pour résoudre un problème linéaire de type $A\Psi = \Phi$ (où A est une matrice et Ψ et Φ des vecteurs de très grandes dimensions), l'idée est de construire le problème quantique correspondant, $A|\Psi\rangle = |\Phi\rangle$, et l'algorithme HHL produirait l'état $|\Psi\rangle$ qui résoudrait cette équation. Au-delà des difficultés pratiques, les applications de type **#5** souffrent de difficultés conceptuelles : tout d'abord, il faut être capable d'encoder l'état $|\Phi\rangle$, *i.e.* créer de façon contrôlée un état paramétré par un nombre astronomique 2^N de nombres complexes. On ne sait pas aujourd'hui comment on pourrait réaliser ces « mémoires quantiques » qui, de toute façon, seraient limitées par le temps utilisé pour les initialiser. De plus, si on admet avoir réussi à produire l'état $|\Psi\rangle$, seule une minuscule fraction de l'information contenue dans $|\Psi\rangle$ pourra être extraite (*i.e.* une seule configuration $i_1i_2i_3...i_N$ par expérience).

Terminons avec six idées reçues sur l'ordinateur quantique

A - Il pourra remplacer l'ordinateur classique. Si l'ordinateur quantique est capable en théorie de faire de la logique classique, il ne saurait remplacer nos ordinateurs de bureau. Pour s'en rendre compte, il suffit de reprendre l'exemple [8] d'un ordinateur de type **#4** : il faudrait plusieurs jours pour produire une configuration de 50 *bits* $i_1i_2i_3...i_N$. En termes de flux d'information, on parle ici de micro-octets par seconde, quand nos ordinateurs de bureaux traitent des milliards d'octets par seconde. **L'ordinateur quantique pourrait donc être destiné à fournir peu d'informations de haute qualité** (comme l'énergie d'activation d'une réaction chimique), **mais en aucun cas une grande quantité d'informations**. Il faut donc faire très attention aux propositions autour de l'intelligence artificielle, qui correspondent souvent implicitement à de grandes quantités de données.

B - Une fois obtenue la fidélité des qubits *au-dessus du seuil, il ne reste plus qu'à passer à l'échelle.* Cette idée fort répandue fait allusion aux seuils des théorèmes des codes CEQ. Ces derniers prédisent en effet que pour pouvoir construire un *qubit* logique, les *qubits* physiques doivent posséder une fidélité au-dessus d'un certain seuil (autour de 99% pour les codes les plus tolérants). Une fois ce seuil dépassé, on peut augmenter arbitrairement la fidélité des *qubits* logiques en utilisant davantage de *qubits* physiques. **Les codes CEQ ne peuvent cependant protéger que des erreurs pour lesquelles ils ont été conçus,** et les systèmes quantiques ne seront, par construction, jamais protégés contre certaines erreurs. Il n'y a pas aujourd'hui d'implémentation convaincante de ces codes. Si on parvient à développer des *qubits* logiques, la CEQ permettra d'améliorer la précision jusqu'au point où les erreurs non corrigées deviendront dominantes (voir [9] pour une discussion détaillée). Notons enfin que pour passer à l'échelle, **chaque *qubit*** ou presque doit être parfait, ce qui nécessite un contrôle de la fabrication du système à un niveau inédit. Il faut également être capable de traiter en temps réel des *térabits* (10^{12} *bits*) par seconde d'information classique pour assurer le contrôle du CEQ.

C - La fabrication de l'ordinateur quantique est aujourd'hui devenue un problème d'ingénierie. Faire un ordinateur quantique, c'est garantir que la machine est bien décrite par un modèle mathématique fort sophistiqué. Cela ne saurait être fait sans une compréhension fine de son fonctionnement. Nous n'avons jamais testé la mécanique quantique de façon aussi fine que ce que l'on s'apprête à faire avec ces ordinateurs quantiques.

D - Il va permettre d'inventer de nouveaux médicaments, de révolutionner l'intelligence artificielle et de réduire drastiquement

1• https://fr.wikipedia.org/wiki/Calculateur_analogique

2• A. Adamatzky, "The dry history of liquid computers", https://arxiv.org/abs/1811.09989

3• M.I. Dyakonov, "State of the Art and Prospects for Quantum Computing", dans *Future Trends in Microelectronics: Frontiers and Innovations*, eds. S. Luryi, J. Xu et A. Zaflavsky (2013), pp. 266-285, Wiley. https://arxiv.org/pdf/1212.3562.pdf

4• Z. Iftikhar *et al.* , "Two-channel Kondo effect and renormalization flow with macroscopic quantum charge states", *Nature* **526** (2015) 233-236. https://arxiv.org/abs/1602.02056

5• F. Arute *et al.*, "Quantum supremacy using a programmable superconducting processor", *Nature* **574** (2019) 505-510. www.nature.com/articles/s41586-019-1666-5

6• Pour une introduction au problème, voir M. Le Bellac, « Peut-on parler de suprématie quantique ? », *Reflets de la Physique*, **67** (2020) 4-8. https://doi.org/10.1051/refdp/202067004

7• Y. Zhou *et al.*, "What limits the simulation of quantum computers?", *Phys. Rev. X* **10** (2020) 041038. https://arxiv.org/abs/2002.07730

8• M. Reiher *et al.*, "Elucidating reaction mechanisms on quantum computers", *PNAS* **114** (2017) 7555. https://arxiv.org/abs/1605.03590

9• X. Waintal, "What determines the ultimate precision of a quantum computer", *Phys. Rev. A* **99** (2019) 042318. https://arxiv.org/abs/1702.07688

10• Voir le "quantum bullshit detector" pour une longue série d'exemples : https://twitter.com/BullshitQuantum

notre consommation d'électricité grâce à des nouvelles réactions chimiques optimisées. Toutes ces applications relèvent pour l'instant de la liste au père Noël [10]. En revanche, elles mettent l'accent sur l'importance du problème quantique à N corps. Les techniques classiques pour ce dernier ont fait des progrès conceptuels et pratiques importants et pourraient bien amener toutes ou une partie de ces applications.

E - Les codes de correction quantique corrigent les erreurs. La CEQ est fondamentalement différente de la correction d'erreur classique : à aucun moment on ne peut accéder à l'information cachée dans la fonction d'onde, sous peine de la perdre. On ne peut donc pas corriger la perte de précision (*i.e.* on ne peut pas regarder dans quelle position se trouve le bouton de la figure 1), mais seulement ralentir la décohérence (première étape) ou améliorer la précision des portes (deuxième étape dite « tolérance aux fautes », beaucoup plus difficile).

F - Les ordinateurs quantiques existent déjà, on peut les acheter ou les utiliser sur Internet. Il existe en effet des plateformes expérimentales dans de nombreux laboratoires, mais aucune pour l'instant n'est vraiment utile. La plupart ont entre 10 et 20 *qubits* avec une fidélité $f < 99\ \%$. Une entreprise canadienne propose plusieurs centaines de *qubits* de très faible fidélité, dont l'utilité est très fortement débattue.

Conclusion

L'ordinateur quantique est une belle aventure mais, on le comprend, il est difficile de prédire à quoi va aboutir cet effort inédit pour créer et utiliser des états quantiques macroscopiques. L'auteur peine à envisager que l'on puisse parvenir à l'ordinateur quantique de type **#4** sans des ruptures conceptuelles majeures avec les approches suivies actuellement. L'ordinateur quantique souffre par ailleurs d'une différence importante avec les débuts d'autres technologies, comme l'électronique ou l'intelligence artificielle : elle réside dans l'absence d'applications précoces qui pourraient venir amorcer le chemin vers d'autres plus ambitieuses. ▮