Les ordinateurs quantiques : un enthousiasme justifié

Giuseppe Di Molfetta [1]

Church, Feynman et la suprématie quantique

L'un des débats les plus intéressants de l'histoire de l'informatique moderne s'est développé autour de la thèse de Church-Turing, qui est devenue l'un des piliers de la théorie de la calculabilité. Dans sa version physique, elle stipule que toute fonction qui peut être calculée par un système physique peut être calculée par une machine de Turing. Il ne s'agit pas d'un théorème mathématique, mais plutôt d'une proposition sur le monde « réel », sur les limites précises entre la physique et ce qui est calculable. Depuis quatre-vingts ans que Church a proposé sa thèse, personne n'a découvert de contre-exemple. Si cette thèse est communément tenue pour vraie, sa version « forte » (ou efficace) ne l'est pas [4] :

> « *Just as the theory of computability has its foundations in the Church-Turing thesis, computational complexity theory rests upon a modern strengthening of this thesis, which asserts that any "reasonable" model of computation can be efficiently simulated on a probabilistic Turing machine (an efficient simulation is one whose running time is bounded by some polynomial in the running time of the simulated machine). Here, we take reasonable to mean in principle physically realizable.* »

1. Maitre de conférences, université Aix-Marseille.

DOI:10.48556/SIF.1024.18.35 **1024** – Bulletin de la SiF, numéro 18, Novembre 2021, pp. 35–42

Au début des années 1980, lorsque la théorie quantique était suffisamment avancée, il est devenu évident que cette histoire devait être révisée car, pour citer Richard Feynamn (*« Nature isn't classical, dammit ! »*). Simuler efficacement un système régi par les lois de la mécanique quantique sur une machine de Turing classique est un problème difficile, et très probablement impossible sans une baisse exponentielle de ses performances. Le mot « probablement » est obligatoire, car il n'existe, à ce jour, aucune preuve rigoureuse de l'existence d'une séparation entre la classe *bounded-error quantum polynomial* (BQP) et la classe *bounded-error probabilistic polynomial* (BPP), les classes de complexité des problèmes efficacement résolubles sur des ordinateurs quantiques et classiques respectivement. Ce que nous savons jusqu'à présent, c'est qu'il existe des exemples dans lesquels une machine quantique garantit « seulement » une amélioration polynomiale (et c'est le cas de l'algorithme de recherche quantique introduit par Grover) et d'autres cas pour lesquels un temps de calcul polynomial est garanti là où une machine classique prendrait un temps exponentiel (par exemple dans les problèmes de factorisation ou les problèmes HSP).

Face à l'absence de preuve rigoureuse, John Preskill a inventé le terme de suprématie quantique (*quantum supremacy*) en 2012 [11], faisant écho à une brillante intuition du scientifique soviétique Yuri Manin en 1980 [10]. Ce terme indique généralement la preuve de l'existence d'un seuil au-delà duquel aucun super-ordinateur classique n'est capable de gérer la croissance exponentielle de la mémoire et de la bande passante nécessaire pour simuler son équivalent quantique. Si le terme de suprématie quantique reste aujourd'hui encore difficile à appréhender, avec des contours flous et une définition qui ne fait pas l'unanimité, cela n'a pas empêché une série de résultats importants et des avancées technologiques ces dernières années.

The experimenter's nightmare et l'optimisme de la volonté

Pour comprendre l'ampleur du défi, il faut se rappeler que la manipulation d'un seul système quantique implique des problèmes très difficiles d'un point de vue technique, dont les solutions ont posé des défis sans précédent aux scientifiques. L'idée que l'information puisse être stockée dans des états quantiques microscopiques a ouvert la perspective d'utiliser la matière quantique elle-même pour effectuer des calculs. Malheureusement, la cohérence quantique qui permettrait, par exemple, aux algorithmes quantiques les plus récents de fonctionner est très fragile. Le scepticisme omniprésent n'a pas attendu pour se faire sentir, et ce sont les extraordinaires Serge Haroche et Jean-Michel Raimond qui ont émis les premiers doutes sur la faisabilité des ordinateurs quantiques [9] ; c'était en 1996, il y a vingt-cinq ans :

> *« . . . we think it fair to say that, unless some unforeseen new physics is discovered, the implementation of error correcting codes will become exceedingly difficult as soon as one has to deal with more than a few gates. In this sense*

the large-scale quantum machine, though it may be the computer scientist's dream, is the experimenter's nightmare. »

Aujourd'hui, le prix Nobel Serge Haroche est l'un des protagonistes de la deuxième révolution quantique, même s'il reste prudent. Mais avant que les scientifiques puissent accepter une telle révolution, un certain nombre d'étapes — d'une importance fondamentale pour le développement d'un processeur quantique — ont dû être franchies dans le monde de la physique atomique. Les premiers pas dans cette direction ont été faits par le physicien Hans Dehmelt (prix Nobel en 1989) [6] qui a réussi à isoler un seul ion dans une chambre à vide et à le suspendre dans le vide à un point prédéterminé et contrôlable. Puis Juan Zoller et Peter Cirac ont réalisé qu'un seul ion pouvait agir comme une porte quantique [5], en construisant le premier registre quantique avec deux types distincts d'informations stockées en fonction des caractéristiques physiques de l'ion. Le premier bit quantique était né !

Deux ans après les propos de Haroche et Raimond, l'algorithme de recherche quantique, proposé par Lev Grover aux Bell Labs, a été mis en œuvre sur le premier ordinateur quantique de 3 bits (*3-qubit NMR computer*) [13]. Depuis lors, la course au développement de machines de calcul quantique de plus en plus contrôlables et programmables n'a jamais cessé, ouvrant la voie au développement de technologies considérées comme irréalisables dix ans plus tôt seulement : communications quantiques par satellite, premiers prototypes d'architectures quantiques distribuées, simulateurs quantiques programmables à 256 qubits pour étudier de nouveaux états de la matière, pour ne citer que trois des nouveaux résultats expérimentaux de cette année. Les organismes publics nationaux et internationaux et les grandes entreprises internationales telles qu'IBM et Google ont trouvé leur place dans cette histoire, et sont devenus des acteurs incontournables du futur proche des technologies quantiques.

La suprématie quantique ?

En 2019, il revient en effet à Google AI Quantum de rouvrir le débat controversé sur la suprématie quantique [2]. Après de nombreuses recherches théoriques et technologiques, les ingénieurs quantiques de Google ont construit un ordinateur quantique programmable appelé Sycamore, doté de 53 qubits et de portes quantiques avec deux qubits pour chaque paire. L'expérience informatique, très simple en soi, consistait à effectuer une mesure de tous les qubits après seulement 20 passages du circuit (problème *Random Circuit Sampling*, RCS), à répéter l'expérience quelques millions de fois pour obtenir une statistique décente, et enfin à comparer le résultat expérimental avec le résultat théorique attendu. Le même calcul, qui prenait un peu plus de deux minutes sur Sycamore, était exponentiellement plus lent sur le plus puissant ordinateur classique disponible, par exemple le Summit. Pour vous donner une idée, considérez que le Summit occupe l'espace de deux courts de tennis entiers et consomme des mégawatts d'énergie électrique, alors que Sycamore est une simple

puce dans un refroidisseur avancé. Chaque fois que nous ajoutons un seul qubit à Sycamore, Summit doit doubler de taille pour suivre. Si Sycamore avait, disons, 70 qubits, Summit occuperait l'espace d'une ville entière pour effectuer le même calcul ! Le résultat de Google n'est ni le premier ni le dernier à étonner la communauté scientifique et le grand public. Quelques mois plus tard, les chinois ont révélé leur Jiuzhang, basé sur les photons, qui a atteint une puissance de traitement de 76 qubits, estimée à des milliards de fois plus rapide que Sycamore. Le test de Google présente sans aucun doute de nombreuses limites, à commencer par les niveaux d'erreur élevés, et une preuve définitive de la suprématie quantique n'est pas claire, mais nous sommes ici confrontés au fait que, pour la première fois, un dispositif de 53 qubits a été véritablement capable de traiter 9 milliards (10^{15}) d'amplitudes de probabilités complexes, avec un avantage temporel sur n'importe quel superordinateur classique de la planète : un résultat objectivement surprenant. Il est difficile d'imaginer que ce sera la dernière, et selon les mots de l'enthousiaste Scott Aaranson [1] :

> « *The computer revolution was enabled, in large part, by a single invention : the transistor. Before transistors, we were stuck with failure-prone vacuum tubes. Yet vacuum tubes kind of, sort of worked : they translated abstract Boolean logic into electrical signals reliably enough to be useful. We don't yet have the quantum computing version of the transistor — that would be quantum error correction. Getting there will surely require immense engineering, and probably further insights as well. In the meantime, though, the significance of Google's quantum supremacy demonstration is this : after a quarter century of effort, we are now, finally, in the early vacuum tube era of quantum computing.* »

En effet, je pense qu'il est difficile de nier, même pour les plus sceptiques, que les avancées de ces dernières années suggèrent combien et quelles étapes importantes ont été franchies dans la direction d'un hardware quantique fonctionnant dans un régime difficile à atteindre pour un ordinateur classique. Mais le scepticisme n'est pas seulement du côté des physiciens expérimentaux. De nombreux informaticiens le sont, et c'est compréhensible. D'une part, parce que les ordinateurs quantiques actuels ne permettent pas d'effectuer des calculs très complexes, en raison de l'absence de codes permettant de corriger les erreurs induites par l'environnement. En fait, de tels codes nécessiteraient des milliers de qubits physiques, un objectif qui, dans les prévisions les plus optimistes, ne sera pas atteint avant les dix prochaines années. Un autre élément qui dérange une bonne partie de la communauté informatique est le manque d'indépendance vis-à-vis du matériel physique et la mesure dans laquelle cela conditionne entièrement les modèles et les algorithmes de l'informatique quantique. Alors que l'informatique classique est rapidement parvenue à être indépendante de la machine physique, cela semble difficile, voire impossible, pour

l'informatique quantique. Une collaboration étroite entre les communautés des informaticiens et des physiciens est désormais nécessaire. En effet, si avec l'avènement des ordinateurs modernes, nous avons assisté à une séparation progressive entre les premiers et les seconds, l'informatique quantique soulève de nouvelles questions qui se situent intimement à la frontière entre la physique et l'informatique théorique. C'est dans cette zone frontière de plus en plus vaste que de nombreux étudiants ont fait leurs premiers pas dans la recherche, une dynamique qui, à terme, risque inévitablement de pénaliser le système d'enseignement et de recherche français, encore peu interdisciplinaire.

Le calcul quantique : une nouvelle grammaire

L'enthousiasme croissant suscité par ces questions n'est pas seulement lié au développement des premiers ordinateurs quantiques, qui suscite en soi l'intérêt d'un vaste réseau d'acteurs privés et publics. Cet enthousiasme a des racines plus profondes : aujourd'hui, les modèles informatiques conçus par les informaticiens deviennent la nouvelle grammaire pour l'étude des processus naturels. Après avoir conquis la mécanique quantique et la thermodynamique, l'information et son traitement sont devenus centraux, par exemple, dans l'étude de la gravité ou de la biologie. Dans cette révolution, informaticiens et physiciens travaillent et travailleront ensemble, pour développer un langage commun, trente ans après les mots de Feynman.

De la simulation de la nature…

L'un des domaines dans lesquels cette symbiose semble être la plus forte est la simulation quantique, l'une des principales applications à court terme des ordinateurs quantiques. L'idée d'un simulateur quantique trouve son origine dans les premiers travaux de David Deutsch et de sa machine de Turing quantique universelle [7] qui représente dans la théorie de la calculabilité quantique exactement ce que la machine de Turing universelle représente pour la calculabilité classique. L'idée d'une machine quantique universelle a ensuite conduit Seth Lloyd, en 1996, à démontrer qu'une telle machine agit effectivement comme un simulateur quantique universel. Pouvoir simuler un phénomène physique dont la théorie est connue est d'un intérêt extraordinaire, car cela nous donne accès à l'étude d'états exotiques de la matière auxquels nous n'aurions pas accès autrement, et inspirera probablement de nouvelles générations d'ordinateurs quantiques. Mais il est encore plus intéressant de comprendre dans quelle mesure un simulateur quantique peut réellement capturer la réalité qui nous entoure. Cette question soulève des interrogations profondes sur la version quantique de la thèse de Church-Turing, et peut en même temps suggérer de nouveaux problèmes dans la compréhension de la nature.

Par exemple, nous savons maintenant que les physiciens utilisent ce qu'ils appellent la théorie des champs quantiques pour décrire les particules élémentaires. Or, formellement, une telle théorie nécessite un nombre infini de degrés de liberté par unité de volume. Prétendre simuler exactement une telle théorie à l'aide d'une machine à états finis est tout simplement impossible. Par définition, un simulateur quantique nécessite une description discrète du phénomène à simuler, où discret signifie un système constitué de composants disjoints, par exemple des qubits. La question de savoir si un circuit quantique peut saisir toute la réalité d'un phénomène physique à une telle échelle reste ouverte et continuera sans aucun doute à faire l'objet d'études dans les années à venir. Autre exemple, le problème de la combinaison d'un phénomène quantique discret avec le concept d'espace-temps continu est l'énigme la plus fascinante dans la communauté des physiciens depuis des décennies. La formulation d'un modèle de gravité quantique a soulevé des questions fondamentales sur la causalité, la localité, l'unitarité, et l'osmose entre la physique et l'informatique a rendu possible des descriptions alternatives, de nouveaux langages. Le bagage théorique des informaticiens pourrait jeter un nouvel éclairage sur ce grand défi, en faisant entrer des concepts tels que l'universalité, la classification et la complexité dans une zone frontalière toujours plus riche, ouvrant de nouvelles perspectives à la recherche de réponses et, en définitive, au progrès scientifique. Mais il existe bien d'autres domaines dans lesquels ces simulateurs quantiques de quelques dizaines de qubits jouent un rôle novateur, de l'étude des différentes phases quantiques de la matière, cruciale pour la conception de nouveaux matériaux, aux premières simulations de réactions chimiques, comme la dernière réalisée sur Sycamore il y a tout juste un an. Dans cette nouvelle expérience, l'équipe AI Quantum a concentré ses efforts sur la simulation d'un processus chimique simple — l'approximation Hartree-Fock d'un système chimique réel — dans ce cas particulier, une molécule de diazène réagissant avec des atomes d'hydrogène [3]. Bien sûr, une telle simulation ne dit encore rien de la supériorité des ordinateurs quantiques, puisque la même simulation peut être réalisée efficacement sur un ordinateur classique. Mais elle confirme la validité méthodologique, la preuve de principe, des éléments de base de ce qui, dans dix ans, conduira à des simulations chimiques d'un ou deux ordres de grandeur plus importants [14].

L'intérêt de ces récents résultats, pour revenir au cauchemar des expérimentateurs, est que nous n'avons pas eu besoin d'attendre des ordinateurs quantiques parfaits et tolérants aux pannes. L'avènement de machines telles que Sycamore et Jiuzhang, communément appelées NISQ (*noisy intermediate-scale quantum*), sont déjà capables d'innover dans des régimes qui seront bientôt difficiles à atteindre pour les ordinateurs classiques actuels, en simulant un large éventail de systèmes quantiques existant dans la nature, bien qu'en utilisant un nombre limité de ressources.

. . . à la nature du calcul

Les simulateurs quantiques ont joué un rôle fondamental pour repenser certains phénomènes physiques. Nous en avons déjà parlé à plusieurs reprises. Ce dont nous n'avons pas suffisamment parlé, c'est de la mesure dans laquelle un phénomène naturel peut inspirer de nouveaux modèles ou algorithmes de calcul. De nombreux modèles classiques non conventionnels de calcul sont inspirés par des phénomènes naturels, par exemple en biologie, on peut citer les membranes cellulaires ou le système immunitaire. Certains de ces phénomènes ont inspiré de nouvelles familles d'algorithmes, comme dans le cas des fourmis : des insectes sociaux hautement coopératifs qui recherchent de la nourriture en grands groupes et communiquent indirectement à l'aide d'une substance chimique appelée phéromone. Fait remarquable, chaque fourmi explore l'espace de solution d'un problème et communique avec ses congénères par le biais d'une variable partagée, à savoir la phéromone. Ce comportement a permis le développement d'une nouvelle famille d'algorithmes d'optimisation et de recherche (*Ant Colony Optimization* [8]). Parfois, certains de ces phénomènes ont le mérite d'être facilement accessibles en nature, plus rarement programmables et bénéficient certainement de millions d'années d'adaptation en avance sur l'informatique à peine plus qu'adolescente. Non seulement la biologie, mais les particules élémentaires pourraient mettre en œuvre certains algorithmes que nous connaissons d'une manière différente et peut-être en suggérer de nouveaux. Récemment, des chercheurs français [12] ont montré que les défauts topologiques dans les matériaux cristallins pourraient se comporter comme des oracles dans un algorithme de recherche, et que les électrons qui s'y propagent « chercheraient » ces défauts avec la même complexité que le célèbre algorithme introduit par Grover. Mais qu'est-ce que cela a à voir avec la course actuelle aux technologies quantiques ? En première approximation, pas beaucoup, et de telles preuves pourraient inspirer, dans le meilleur des cas, de nouvelles familles d'algorithmes non conventionnels, comme l'algorithme de nos chères fourmis. Le fait est que les algorithmes quantiques, tels que nous les connaissons, nécessitent des ordinateurs quantiques suffisamment tolérants aux erreurs, et un tel horizon est encore loin des possibilités techniques actuelles. Que certains algorithmes quantiques se réalisent spontanément dans la nature dans des conditions environnementales défavorables pourrait constituer un raccourci fascinant pour une nouvelle génération d'ordinateurs quantiques (analogiques) « naturels ». Et malgré la prudence qui s'impose à l'égard de ce type de résultats et de leur impact potentiel, il reste tout à fait d'actualité de comprendre dans quelle mesure les progrès de la simulation quantique de phénomènes physiques jusqu'alors difficiles d'accès peuvent non seulement nous aider à appréhender la nouvelle physique, mais aussi avoir des retombées intéressantes et inattendues dans le développement de nouvelles technologies.

Références

[1] Scott Aaranson, NYT, 2019.

[2] Arute, Frank, et al. *Quantum supremacy using a programmable superconducting processor*, Nature, 574.7779, 2019.

[3] Arute, Frank, et al. *Hartree-Fock on a superconducting qubit quantum computer*, Science, 369.6507, 2020.

[4] Bernstein, E. et Vazirani, *U. Quantum complexity theory*, SIAM Journal on Computing, 26, 5 octobre 1997.

[5] Cirac, Juan I., et Peter Zoller. *Quantum computations with cold trapped ions*, Physical review letters, 1995.

[6] Dehmelt, Hans. *A single atomic particle forever floating at rest in free space : New value for electron radius*, Physica Scripta, T22, 1988.

[7] Deutsch, David. *Quantum theory, the Church–Turing principle and the universal quantum computer*, proceedings of the Royal Society of London, A. Mathematical and Physical Sciences, 400.1818, 1985.

[8] M. Dorigo & T. Stützle, Ant Colony Optimization, MIT Press, 2004.

[9] Serge Haroche et Jean-Michel Raimond, *Physics Today*, 1996.

[10] Manin, Yuri, *Computable and uncomputable* (in russian), Sovetskoye Radio, Moscow, 1980.

[11] Preskill, John. *Quantum computing in the NISQ era and beyond*, Quantum, 2018.

[12] Roget, Mathieu, et al. *Grover search as a naturally occurring phenomenon*, Physical Review Letters, 124.18, 2020.

[13] Vandersypen, Lieven MK, et al. *First implementation of a three quantum bit search algorithm*. No. quant-ph/9910075, 1999.

[14] Yuan, Xiao. *A quantum-computing advantage for chemistry*, Science, 369.6507, 2020.