Séance publique du 5 janvier 2026

Ordinateur quantique : to be and not to be

Jean-Pierre NOUGIER, Michel CHEIN, Michel ROBERT
Académie des Sciences et Lettres de Montpellier

MOTS-CLÉS :
Physique quantique, qubit, superposition, intrication, algorithmes quantiques, calcul quantique

RÉSUMÉ :
Cette conférence explore les fondements de l'informatique quantique, depuis les principes physiques qui sous-tendent son fonctionnement jusqu'aux défis technologiques actuels. Elle aborde d'abord les concepts clés de la physique quantique qui distinguent cette technologie des ordinateurs classiques : le qubit, la superposition, l'intrication et la décohérence. Les spécificités des algorithmes quantiques sont ensuite décrites : complexité, portes et circuits quantiques, gestion des erreurs, ainsi que des exemples emblématiques comme l'algorithme de Shor, illustrant le potentiel de cette approche. Enfin, un état de l'art des technologies de réalisation est proposé, couvrant les principales plateformes expérimentales développées à ce jour : ions piégés, supraconducteurs, spins électroniques (silicium ou nanotubes), atomes froids et photons. Les défis du calcul intensif, des fondements théoriques aux réalisations concrètes, sont mis en perspective avec les supercalculateurs actuels, soulignant les enjeux et les opportunités de cette transition technologique.

1. Les fondements physiques de l'ordinateur quantique

La mécanique classique décrit le mouvement des objets « à l'échelle du visible », qui va des petits objets jusqu'aux planètes, aux étoiles et aux galaxies. Les lois en sont étudiées depuis des temps immémoriaux, ont été formalisées en particulier par Newton au XVII^{e} siècle, elles sont maintenant bien connues, et nous sommes tous familiers de l'attraction universelle ou de l'électromagnétisme. Elles ont été complétées au début du XX^{e} siècle par les théories de la relativité restreinte et de la relativité générale d'Einstein.

Les objets microscopiques (particules élémentaires, atomes, molécules) n'obéissent pas aux lois de la mécanique classique, mais aux lois de la mécanique quantique, découvertes au début du XX^{e} siècle par Planck, Einstein, Schrödinger, Bohr, Heisenberg, de Broglie, Fermi, Feynman, etc. Cette théorie a débouché sur la "première révolution quantique", une multitude d'applications dont bénéficie notre environnement quotidien : lasers, photopiles solaires, LEDs (diodes électroluminescentes), et tous les semiconducteurs grâce auxquels fonctionne toute l'électronique moderne qui commande nos appareils ménagers, smartphones, téléviseurs, ordinateurs, automobiles, etc. Nous baignons ainsi dans un monde quantique dont nous utilisons chaque jour sans le savoir les étranges propriétés.

Dans les années 1950 déjà, Richard Feynman (Prix Nobel de Physique 1965) avait proposé de simuler la physique quantique avec des ordinateurs quantiques. En 1982, Alain Aspect (prix Nobel de physique 2022) démontre expérimentalement l'existence de l'intrication quantique et des *i*négalités de Bell, fondements de la communication et du calcul quantique. Débute alors, selon sa propre expression, la "seconde révolution quantique" où l'on tente d'utiliser des conséquences de la théorie quantique pour mettre en œuvre de nouvelles applications, dont l'ordinateur quantique est un exemple type.

Le fonctionnement de l'ordinateur quantique se fonde essentiellement sur trois propriétés spécifiques à la mécanique quantique que nous avons bien du mal à appréhender, même sur le plan conceptuel : le qubit, l'intrication et la décohérence.

1.1. Le qubit

L'ordinateur classique utilise un langage binaire, constitué de "bits" pouvant prendre soit la valeur 0, soit la valeur 1. Ces bits ont mis en œuvre par des transistors pouvant soit laisser passer un courant électrique (valeur 1), soit bloquer le courant (valeur 0). Ainsi, à la première scène de l'acte III du drame "Hamlet" de William Shakespeare, le prince Hamlet pose d'emblée la question existentielle « to be or not to be, that is the question ».

L'ordinateur quantique lui aussi utilise des bits, appelés "qubits" (pour "quantum bits"), qui contrairement aux bits classiques peuvent se trouver à la fois dans les états 0 et 1, notés $|0\rangle$ et $|1\rangle$ (se lit "ket 0 et ket 1"). En effet, la mécanique quantique nous enseigne qu'un système qui possède deux états de base $|0\rangle$ et $|1\rangle$ peut se trouver non seulement dans l'un des deux états $|0\rangle$ ou $|1\rangle$, mais aussi dans n'importe quelle combinaison $\alpha|0\rangle + \beta|1\rangle$, où α et β sont des nombres qui peuvent être réels ou complexes. Le système est alors en proportion $|\alpha|^2$ dans l'état $|0\rangle$ et $|\beta|^2$ dans l'état $|1\rangle$, il est donc *à la fois* dans les états $|0\rangle$ et $|1\rangle$. Il répond donc à la question « to be and not to be, that is the question » !

Pour comprendre une telle situation, considérons un faisceau lumineux, qui d'après la mécanique quantique est constituée par un flux de particules appelées photons, qui se déplacent à la vitesse de la lumière. On sait que la lumière peut être polarisée. Cette propriété et utilisée par les photographes, qui savent que la lumière du ciel est partiellement polarisée : en faisant tourner un filtre spécial appelé "polariseur", ils assombrissent plus ou moins la lumière du ciel car une partie plus ou moins grande de la lumière (c'est-à-dire un nombre plus ou moins grand de photons) traverse le filtre. La lumière qui a traversé le filtre est polarisée dans la direction de polarisation du filtre. Chaque photon est un qubit dans l'état que nous désignerons par exemple par $|1\rangle$ si sa polarisation est verticale, $|0\rangle$ si elle est horizontale.

Faisons l'expérience suivante (figure 1) : une source de lumière envoie un faisceau lumineux sur un polariseur suivi par un second polariseur (appelé "analyseur") et éclaire un écran qui intercepte le faisceau émergent de l'analyseur. Supposons que la polarisation de l'analyseur soit verticale, ce qui est représenté figure 1 par la flèche verticale blanche dans l'analyseur. Envisageons alors trois cas particuliers :

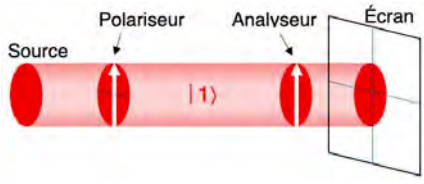


Figure 1 : Polariseur vertical

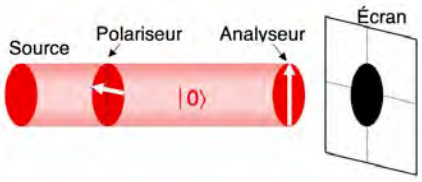


Figure 2 : Polariseur horizontal

- 1er cas. Le polariseur est lui aussi polarisé verticalement (figure 1) : la lumière sortant du polariseur est alors polarisée verticalement, elle est dans l'état que nous désignerons par $|1\rangle$. L'analyseur étant lui aussi vertical, toute la lumière le traverse et éclaire l'écran.
- 2e cas. Le polariseur est polarisé horizontalement (figure 2) : la lumière sortant du polariseur est alors polarisée horizontalement, elle est dans l'état que nous désignerons par $|0\rangle$. L'analyseur étant vertical, aucune lumière ne traverse l'analyseur et donc aucune lumière n'atteint l'écran.
- 3e cas. C'est le plus intéressant. Le polariseur est polarisé à 45° (figure 3) : la lumière qui en ressort est alors polarisée à 45°, elle est dans l'état $(1/\sqrt{2})\,|0\rangle + (1/\sqrt{2})\,|1\rangle$, c'est à dire à moitié [car $(1/\sqrt{2})^2 = 1/2$] dans l'état $|0\rangle$ et à moitié dans l'état $|1\rangle$. L'analyseur est alors à 45° du polariseur, on constate que la moitié de la lumière traverse l'analyseur. En d'autres termes, un photon sur deux traverse l'analyseur. Que se passe-t-il si, au lieu d'envoyer un flux lumineux, qui contient des milliards de photons, on envoie les photons un par un (on sait le faire depuis une quarantaine d'années) ? On remarque que, statistiquement, un photon sur deux traverse l'analyseur. C'est à dire qu'un photon, parfois passe, parfois ne passe pas : il a une chance sur deux de passer, et il nous est impossible de prévoir si un photon émis va passer ou ne pas passer. Il s'agit là d'une indétermination structurelle, contre laquelle nous ne pouvons rien. Elle n'est pas due à un défaut de compréhension de notre part, c'est un phénomène inhérent aux "lois de la nature".

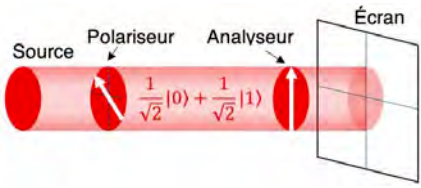


Figure 3 : Polariseur à 45°

Cette expérience nous montre plusieurs choses :

1. La polarisation de la lumière, qui est un qubit, peut se trouver non seulement dans les états $|0\rangle$ ou $|1\rangle$, mais aussi dans n'importe quelle combinaison de ces états : à chaque direction de polarisation du polariseur correspond un état de la lumière qui en émerge, qui est une combinaison des états de bas $|0\rangle$ et $|1\rangle$. *Il est donc possible de préparer un qubit (ici un photon) dans l'état qu'on souhaite.* Un qubit se trouve donc en général partiellement dans l'état $|0\rangle$ et partiellement dans l'état $|1\rangle$. Il est à la fois dans les états $|0\rangle$ et $|1\rangle$. *C'est cette propriété du qubit de se trouver à la fois dans les états $|0\rangle$ et $|1\rangle$ qui fait la puissance des ordinateurs quantiques* : pour rechercher un livre dans une bibliothèque, l'ordinateur classique va comparer successivement (je schématise) le titre de chaque livre au titre recherché ; l'ordinateur quantique va pouvoir examiner plusieurs livres à la fois, d'où un gain de temps qui peut être considérable.

2. Toute mesure effectuée sur le qubit modifie son état : l'analyseur qui mesure la polarisation du photon, détruit sa polarisation : le photon qui avant d'atteindre l'analyseur était dans l'état $\alpha|0\rangle + \beta|1\rangle$, combinaison des états $|0\rangle$ et $|1\rangle$, se trouve après mesure par l'analyseur :
   - soit dans l'état $|0\rangle$ avec la probabilité $|\alpha|^2$,
   - soit dans l'état $|1\rangle$ avec la probabilité $|\beta|^2$.

Une mesure transforme donc un qubit en bit classique. Ceci a en particulier deux conséquences :

- En cryptographie : l'individu A veut transmettre un message à B. Ce message est intercepté par l'espion E qui en fait une copie et le redirige vers B. Si le message est classique, B ne s'aperçoit pas que son message a été intercepté. Si le message est quantique, la lecture du message par E modifie les qubits, donc modifie le message, donc B peut savoir que le message a été intercepté. La cryptographie quantique est ainsi beaucoup plus sûre que la cryptographie classique. Notons de plus qu'un ordinateur quantique peut décoder un message encodé de manière classique, ce qu'un ordinateur classique ne peut pas faire.
- Lorsqu'un ordinateur exécute un programme, il est parfois utile d'en contrôler des étapes intermédiaires, donc de lire des résultats intermédiaires. Ceci est possible avec un ordinateur classique, mais pas avec un ordinateur quantique car la lecture d'un qubit modifie le qubit donc fausse la suite des opérations. Un tel contrôle ne peut se faire que sur des circuits redondants qui exécuteraient en parallèle le même programme que le circuit principal.

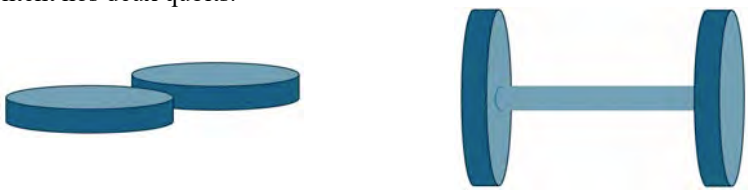
3. L'émergence d'un photon de l'analyseur est un phénomène totalement imprévisible car structurellement aléatoire. Il en résulte que *le résultat donné par un ordinateur quantique revêt un caractère probabiliste* alors qu'un ordinateur classique donne un résultat certain.

1.2. L'intrication

Un ordinateur est un appareil qui permet de stocker des données et d'exécuter un programme. Dans un ordinateur classique, les bits d'entrée sont transformés par le programme pour donner des bits de sortie. De même, l'ordinateur quantique devra transformer des qubits, c'est à dire relier des qubits les uns aux autres. Il est possible de relier des qubits au moyen d'une opération qui s'appelle l'intrication. Lorsque deux qubits sont intriqués, ils ne constituent plus deux systèmes indépendants, ils constituent un système unique, qui possède deux propriétés :

- toute action sur l'un des deux qubits modifie l'autre qubit.
- cette modification est instantanée, quelle que soit la distance qui sépare les deux qubits.

Pour essayer de comprendre comment cela fonctionne (je dis bien : "essayer" : je n'y arriverai pas !), imaginons que nous disposions de deux disques (figure 4a), qui représentent nos deux qubits.



(a) (b)

Figure 4 : Représentation schématique de deux qubits avant (a) et après (b) intrication

L'intrication consiste à lier ces deux qubits, par exemple en les reliant par une barre (figure 4b). Au départ (figure 4a) nous avons un système constitué par deux disques (deux qubits), que nous pouvons manipuler séparément. Une fois reliés par une barre (c'est à dire une fois les qubits intriqués, figure 4b) ces deux disques constituent un seul système, un haltère : si nous faisons tourner l'un des deux disques, l'autre tourne

instantanément du même angle, quelle que soit la longueur de la barre qui les relie, c'est à dire quelle que soit la distance qui les sépare. Il en est de même pour des qubits intriqués, mais :

- D'une part la "force" qui maintient les qubits liés est invisible, c'est comme le disait Einstein « une force fantôme ».
- D'autre part, lorsqu'on agit sur une des deux particules, l'autre réagit *instantanément*. Bien qu'il fût l'un des initiateurs de la mécanique quantique, dès les années 1920 Einstein s'est opposé à l'idée qu'une action à distance puisse se dérouler instantanément, c'est à dire que la réaction puisse se faire dans un temps inférieur au temps de propagation de la lumière. Sans remettre en cause les principes fondamentaux de la mécanique quantique, Einstein a émis l'hypothèse que la description quantique n'était pas complète, qu'il y avait des variables cachées dont on n'avait pas tenu compte. Cette question a été soulevée à partir de 1935 par un fameux article d'Einstein, Podolsky et Rosen[1] sur les propriétés surprenantes des états intriqués (appelés aussi pour cette raison états EPR). Einstein s'opposait ainsi à Niels Bohr[2] sur l'interprétation à donner à la théorie quantique. Ce débat a duré jusqu'à la fin de leurs vies. Il a été tranché par les expériences réalisées en 1982 par Alain Aspect ([3] et [4]) qui pour cela a obtenu le prix Nobel de Physique en 2022. Alain Aspect a réussi à éloigner deux qubits intriqués à une distance de 12 mètres l'un de l'autre, et a pu démontrer que lorsqu'on agissait sur un qubit, l'autre réagissait en un temps inférieur au temps de propagation de la lumière entre les deux qubits. Depuis lors, des expériences de téléportation quantique ont permis de séparer des qubits intriqués sur des distances d'une centaine de kilomètres[5] et même plus[6], et de confirmer l'instantanéité des réactions. Dans ce débat entre Einstein et Bohr, c'est Bohr qui avait raison. Chose plus extraordinaire encore, en 2012, des cristaux à base d'ytterbium et de néodyme, de dimension visible à l'œil nu, gros comme des morceaux de sucre, ont pu être intriqués par l'équipe suisse de Nicolas Gisin de l'Université de Genève ; plus exactement, un milliard d'atomes d'un cristal a pu être intriqué avec un milliard d'atomes de l'autre cristal. On est encore loin de pouvoir intriquer des morceaux entiers : à titre d'exemple, un gramme de fer contient 10 000 milliards de fois plus d'atomes que ceux intriqués par l'équipe suisse.

Les forces qui agissent à notre échelle entre deux corps (gravitation, forces électromagnétiques, etc.) sont locales, c'est à dire que leur effet diminue au fur et à

---

[1] EINSTEIN A., PODOLSKY B., ROSEN N., « Can Quantum Mechanical description of physical reality be considered complete ? », *Phys. Rev.*, **47,** 777 (1935)

[2] BOHR N., « Can Quantum Mechanical description of physical reality be considered complete ? », *Phys. Rev.*, **48**, 696 (1935)

[3] ASPECT A., GRANGIER P. et ROGER G., *Phys. Rev. Lett.,* Vol. **49**, Iss. 2, pp. 91–94 (1982)

[4] ASPECT A., DALIBARD J. et ROGER G., *Phys. Rev. Lett*., Vol. **49**, Iss. 25, pp. 1804–1807 (1982)

[5] YIN Juan, REN Ji-Gang, LU He, CAO Yuan, YONG Hai-Lin, WU Yu-Ping, LIU Chang, LIAO Sheng-Kai, ZHOU Fei, JIANG Yan, CAI Xin-Dong, XU Ping, PAN Ge-Sheng, JIA Jian-Jun, HUANG Yong-Mei, YIN Hao, WANG Jian-Yu, CHEN Yu-Ao, PENG Cheng-Zhi & PAN Jian-Wei, « Quantum teleportation and entanglement distribution over 100-kilometre free-space channels », *Nature* **488**, p. 185–188 (2012).

[6] MA Xiao-song, HERBST Thomas, SCHEIDL Thomas, WANG Daqing, KROPATSCHEK Sebastian, NAYLOR William, MECH Alexandra, WITTMANN Bernhard, KOFLER Johannes, ANISIMOVA Elena, MAKAROV Vadim, JENNEWEIN Thomas, URSIN Rupert, ZEILINGER Anton, « Quantum teleportation using active feed-forward between two Canary islands », *Nature* 489, p. 269 (2012).

mesure que la distance entre les corps augmente. Au contraire, l'intrication quantique est non locale, le système où elle s'exerce ne dépend pas de la distance entre les particules qui interagissent[7]. Ainsi, différents éléments d'un système peuvent ne pas être indépendants même s'ils sont très éloignés l'un de l'autre.

Ces expériences ouvrent des perspectives considérables, telles la cryptographie quantique, la téléportation quantique, les ordinateurs quantiques. D'où le nom de « Seconde révolution quantique » donné par Alain Aspect aux différentes applications possibles mettant en œuvre l'intrication de qubits.

1.3. La décohérence

La décohérence est un processus selon lequel des particules ou des systèmes quantiques peuvent évoluer ou se modifier de façon incontrôlée. Nous avons vu que toute mesure effectuée sur un qubit modifie son état. Ainsi, un qubit qui avant une mesure était dans une combinaison d'états, par exemple dans l'état $\alpha|0\rangle + \beta|1\rangle$, se retrouve, après une mesure effectuée sur lui, soit dans l'état $|0\rangle$ soit dans l'état $|1\rangle$, c'est à dire devient un bit classique. Nous avons vu aussi que, si deux qubits sont intriqués, toute action sur l'un modifie l'autre. Les éléments perturbateurs sont multiples. Toute interaction avec l'extérieur est susceptible de créer ce type de perturbation, donc des erreurs : vibration, ondes acoustiques, champ électro-magnétique, perte d'un photon dans une fibre, et surtout agitation thermique due à une élévation de température ou à un contact thermique avec l'extérieur.

Pour qu'un ordinateur quantique fonctionne, il faut que les qubits conservent leurs propriétés quantiques tout le temps du calcul, or la moindre interaction avec l'environnement détruit les propriétés quantiques du système. Et cela est d'autant plus vrai que le nombre de qubits augmente.

2. Algorithmique quantique

2.1. Problème, Algorithme, Programme

Un *problème* susceptible d'être traité par l'informatique est généralement exprimé par un mélange de langue (naturelle) et de mathématiques qui, dans tous les cas, doit être représentable par des notions mathématiques.

Faire une multiplication de deux nombres entiers positifs, représenter un entier par le produit de ses diviseurs premiers $312 = 2.2.2.3.13 = 2^3.3.13$ – qui s'appelle factoriser un nombre entier – sont des exemples de problèmes concernant des nombres. Il existe de nombreux problèmes usuels ne concernant pas des nombres comme : trier par ordre alphabétique les noms des habitants d'une ville, trouver le nombre d'occurrences du mot « je » dans le discours d'un homme politique, colorier la carte des départements sans que deux départements contigus aient la même couleur, parcourir un ensemble de villes sans passer deux fois par la même ville (voyageur de commerce) etc.

Les caractéristiques essentielles de la notion intuitive d'un *algorithme* sont les suivantes : c'est une *séquence finie d'instructions* simples et *précises* (pour la multiplication apprise à l'école primaire en France de deux nombres entiers en représentation décimale : multiplication de deux chiffres qui permet la multiplication

[7] Nous ne comprenons pas pourquoi cette « force fantôme » peut ainsi agir à distance. Mais comprenons-nous pourquoi deux charges électriques s'attirent ou se repoussent à distance ? Nous l'observons seulement…

d'un nombre par un chiffre si on sait faire des reports, puis addition de deux chiffres, décalage d'un nombre, addition de deux nombres …), qui dit comment produire à partir d'une *entrée* (des données transmises à l'algorithme avant qu'il commence) en *sortie* le résultat (une fonction des entrées) en un *nombre fini d'étapes*.

Il existe généralement plusieurs algorithmes pour résoudre un problème donné (c'est le cas de tous les exemples donnés précédemment.) Par exemple, de nombreuses références d'algorithmes de multiplication de deux entiers sont données dans Wikipedia[8].

Pour être exécuté par un ordinateur, les instructions d'un algorithme et leur enchainement doivent pouvoir être transformées en des instructions de l'ordinateur, c'est-à-dire en un programme. Un *programme* est une représentation particulière d'un algorithme – écrite dans un certain langage formel (un langage de programmation, il y en a beaucoup) – exécutable par un ordinateur. Les relations entre un algorithme et un programme censé faire pareil ne sont pas simples : un programme fait-il ce qu'on voudrait qu'il fasse (la preuve de programme) est un problème difficile.

2.2. Complexité d'un algorithme, d'un problème, d'un programme

Avant de programmer un algorithme résolvant un problème, il peut être utile de savoir si le résultat sera obtenu en un temps raisonnable et si on dispose de suffisamment de place. Le critère essentiel est, généralement, le temps de calcul. Comme le temps de calcul est très contextuel – il dépend du système, du langage de programmation, du programmeur, du réseau etc. – on remplace ce temps par un majorant du nombre d'instructions fonction de la taille n des données, dans les plus mauvais cas et lorsque n est grand, que l'on note $O(f(n))$.

Dans l'exemple de la multiplication, la taille des données, n, est le nombre de chiffres du plus grand des deux nombres. Par exemple, multiplions 367 par 879, n=3. On doit multiplier 7 par 9, puis 6 par 9 et ajouter un éventuel report (faire une addition), puis 3 par 9 etc. donc faire n^2 multiplications de chiffres, des reports puis des additions qui sont moins coûteuses que les multiplications. Une expression précise du nombre d'instructions est un polynôme du second degré en n, la taille du problème qui croit comme n^2. Cette première analyse, certes grossière mais nécessaire, s'exprime en disant que la complexité de l'algorithme de multiplication de l'école primaire est en $O(n^2)$.

La complexité d'un *problème* est la complexité du « meilleur » (au sens ci-dessus) algorithme le résolvant. La complexité de l'algorithme de Schönhage et Strassen pour multiplier deux nombres entiers est $O(n\times\log(n)\times\log(\log(n)))$ et on conjecture – de nombreux informaticiens pensent – qu'il n'y a pas de meilleur algorithme que $O(n\times\log n)$. En 2019, Harvey et van der Hoeven on construit un algorithme en $O(n\times\log(n))$, ils n'ont pas prouvé que l'on ne pouvait faire mieux donc la conjecture est toujours ouverte. De plus ce n'est qu'un résultat théorique car le régime asymptotique n'est atteint que (section 5 de[9]) pour des nombres d'une taille supérieure à 2^a avec $a = 1729^{12}$, il ne faut donc pas se précipiter pour programmer ce dernier algorithme !

La plupart du temps on ne connaît qu'un nombre minimum d'instructions qu'il faut exécuter pour résoudre un problème, et sa complexité est ainsi comprise entre un tel nombre et la complexité du meilleur algorithme connu pour le résoudre.

Tous les problèmes (mathématiques) n'ont pas de solution algorithmique. Il existe des problèmes, au sens donné ci-dessus, n'ayant pas d'algorithme de résolution et ce quelle que soit sa complexité, il existe des problèmes incalculables. Par exemple, on peut

[8] https://fr.wikipedia.org/wiki/Algorithme_de_multiplication_d%27entiers

[9] HARVEY D., van der HOEVEN J., *Integer multiplication in time O(n log n)*, Annals of Mathematics, 2021, 10.4007/annals.2021.193.2.4. hal-02070778v2

démontrer qu'il n'existe pas d'algorithme pour le « problème de l'arrêt », qui est celui de déterminer si étant donné un programme quelconque et une donnée quelconque le programme s'arrête pour cette donnée. Il existe aussi des nombres réels incalculables, un nombre réel calculable étant un nombre pour lequel il existe un algorithme construisant la suite de ses chiffres (éventuellement infinie.)

La thèse de Church-Turing dit que : « Aucun progrès technologique ne remettra en cause le modèle mathématique de calcul défini par Church et Turing en 1936. » Depuis, les centaines de modèles formels de calcul construits (machine de Turing, fonction récursive, RAM (Random Access Machine, ordinateurs classiques), PRAM (Parallel RAM), machine de Turing non déterministe, Machine de Turing quantique, …) calculent tous les mêmes fonctions. Tous ces modèles mathématiques formalisent correctement la notion de méthode effective de calcul qu'aucun progrès technologique ne remettra en cause y compris les algorithmes quantiques, car tout algorithme quantique peut être simulé par un algorithme classique (en nécessitant éventuellement un temps beaucoup plus long) !

Si les ordinateurs quantiques ne permettent pas de calculer plus de fonctions que les ordinateurs classiques pourquoi tant de bruit ?

2.3. Pourquoi des ordinateurs quantiques ?

Parce que savoir si une fonction est calculable est nécessaire mais pas suffisant pour pouvoir la calculer *réellement* c'est-à-dire sur une machine physique en un temps raisonnable. S'il faut un millier d'années pour calculer le résultat qu'on souhaite ce n'est pas très raisonnable.

Or, toujours plus de problèmes nécessitent des calculs gigantesques ceci pour diverses raisons. Parce que le nombre de données (la taille du problème) est gigantesque, c'est notamment le cas avec l'IA actuelle, ou parce que la complexité du meilleur algorithme classique connu nécessite des calculs très longs, c'est la cas avec l'algorithme de chiffrement RSA (Rivest, Shamir, Adelman 1977) le plus utilisé pour échanger des données confidentielles sur internet, soit parce que c'est l'un des nombreux problèmes pour lesquels il n'existe pas d'autre solution qu'exponentielle sur un ordinateur classique (comme celui du voyageur de commerce.)

Le quantique est une étape (peut-être la dernière ?) dans la course à la rapidité : algorithme optimal, algorithme approché, probabiliste, parallèle, quantique. En effet, si un algorithme est en $O(2^n)$, n étant la taille des données du problème, sur un ordinateur classique, ce problème est bien calculable théoriquement mais incalculable pratiquement dès que n est grand alors qu'on peut essayer de construire un algorithme en O(n) sur un ordinateur quantique.

Richard Feynman, prix Nobel de physique en 1965 pour ses travaux en électrodynamique quantique, avait introduit et posé les premières questions concernant le calcul quantique en 1982[10]. Il suggérait qu'un ordinateur manipulant l'information en suivant les règles de la mécanique quantique pourrait résoudre des problèmes inaccessibles par des ordinateurs classiques. C'était vraiment le début de l'aventure du calcul quantique. Dès 1985, David Deutsch introduisit la machine Turing quantique et montra la magie du quantique en construisant un algorithme quantique faisant appel une seule fois à un oracle *(une fonction de {0,1} dans {0,1}, question f(0) = f(1) ?)* alors que sans le quantique il fallait 2 appels.

Ensuite, tout alla très vite, machine de Turing quantique universelle, preuve qu'un ordinateur quantique pouvait être exponentiellement plus rapide qu'un ordinateur classique, etc. Tout alla très vite, du moins, sur le plan théorique.

[10] FEYNMAN R., Intern. Journal of Theoretical Physics, vol.21, 1982

Ce qui est nouveau et fondamental par rapport à l'informatique classique où l'unité d'information est le bit représenté soit par 0, soit par 1 est que l'on peut *superposer* les deux états quantiques de base $|0\rangle$ et $|1\rangle$.

Un ***1-qubit*** correspond à l'état d'une particule qui peut osciller entre un état au repos et un état excité, « c'est un peu comme une pièce de monnaie lancée en l'air. Tant que la pièce tourne dans l'air, pile et face ont les mêmes chances de se produire. Ce n'est que lorsque la pièce est retombée que l'on peut lire le résultat (c'est la partie "mesure") et ensuite le résultat est définitivement figé à pile ou bien à face »[11]. Formellement, un 1-qubit est un état quantique obtenu par combinaison linéaire des deux états quantiques de base :

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

α et β étant des nombres complexes. ($|0\rangle$ peut être représenté par le vecteur (1 0), et $|1\rangle$ par le vecteur (0 1). $|\psi\rangle$ est donc le vecteur (α β) que l'on peut représenter plus fidèlement comme un point sur une sphère (la sphère de Bloch) en représentant un nombre complexe par sa notation trigonométrique
$z = a + i.b = r.\cos(\theta) + i.r.\sin(\theta)$ avec $r = \sqrt{(a^2 + b^2)}$ et θ angle de l'axe des x avec le vecteur (a,b).)

La *mesure* d'un état quantique normé $|\psi\rangle$ (dans ce cas : $|\alpha|^2 + |\beta|^2 = 1$) va renvoyer le bit 0 avec la probabilité $|\alpha|^2$ ou le bit 1 avec la probabilité $|\beta|^2$. Si $\alpha = \beta = 1/\sqrt{2}$ alors 0 et 1 ont la même probabilité 1/2. La mesure d'un état quantique $|\psi\rangle$ le perturbe de façon irrémédiable. C'est un élément fondamental d'un circuit quantique. C'est le seul moment où l'on peut obtenir une information sur un état quantique $|\psi\rangle$, mais c'est aussi la fin du qubit, car la mesure ne renvoie que 0 ou 1 et perturbe irrémédiablement l'état quantique.

Un ***2-qubit*** est défini par la superposition de 4 états quantiques

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$$

(où le vecteur de $|00\rangle$ est le produit tensoriel $|0\rangle \otimes |0\rangle$ soit (1000), $|01\rangle$ a pour vecteur le produit tensoriel $|0\rangle \otimes |1\rangle$ soit (0100), $|10\rangle$ est le produit tensoriel $|1\rangle \otimes |0\rangle$ soit (0010) et $|11\rangle$ est le produit tensoriel $|1\rangle \otimes |1\rangle$ soit (0001).)
La mesure d'un 2-qubit est un mot binaire de longueur 2 :
00 avec la probabilité $|\alpha|^2$, 01 avec la probabilité $|\beta|^2$, 10 avec la probabilité $|\gamma|^2$, 11 avec la probabilité $|\delta|^2$

Avec un 2-qubit, c'est comme si on avait en même temps les 4 mots binaires de longueur 2, c'est la version quantique de l'union de deux bits.

Plus généralement, un ***n-qubit***, $n \geq 1$, est la superposition de 2^n états cubiques :

$$|\psi\rangle = \alpha_1|00\ldots0\rangle + \alpha_2|00\ldots1\rangle + \gamma|10\rangle + \delta|11\rangle + \alpha_2{}^n|11\ldots1\rangle.$$

Ainsi un n-qubit permet de considérer en même temps les 2^n mots binaires de longueur n.
Travailler avec un n-qubit correspond à travailler sur tous les 2^n n-bits classiques
0.0 . . . 0.0, 0.0 . . . 0.1, . . ., 1.1 . . . 1.1
en même temps, alors que l'informatique classique ne s'occupe que d'un seul n-bit à la fois.

2.4. Portes et circuits quantiques[12]

De même qu'un calcul sur un ordinateur classique revient à transformer des bits en des bits en utilisant des portes logiques, un calcul sur un ordinateur quantique, revient à transformer des qubits en des qubits en utilisant des portes quantiques.

La *porte* X est la transformation linéaire qui échange les états $|0\rangle$ et $|1\rangle$ (elle correspond à la porte NOT en informatique classique) :

$X(|0\rangle) = |1\rangle$ et $X(|1\rangle) = |0\rangle$, ainsi $X(\alpha|0\rangle + \beta|1\rangle) = \alpha X(|0\rangle) + \beta X(|1\rangle) = \alpha|1\rangle + \beta|0\rangle = \beta|0\rangle + \alpha|1\rangle$.

[11] BODIN A., « QUANTUM, Un peu de mathématiques pour l'informatique quantique », http://exo7.emath.fr/cours/livre-quantum.pdf
[12] BODIN A., *ibidem*

La *porte de Hadamard* H est la transformation linéaire définie par :
H ($|0\rangle$)= $\frac{1}{\sqrt{2}} \times (|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}} \times |0\rangle + \frac{1}{\sqrt{2}} \times |1\rangle$ et H ($|1\rangle$)= $\frac{1}{\sqrt{2}} \times (|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}} \times |0\rangle - \frac{1}{\sqrt{2}} \times |1\rangle$
en mesurant H ($|0\rangle$) ou H ($|1\rangle$ on obtient les bits 0 ou 1 avec la probabilité 1/2.
H *(|0⟩) et* H *(|1⟩) sont deux qubits différents qui ont la même mesure.* Une porte de Hadamard réalise une superposition uniforme des deux états de base.

En mettant en série deux portes de Hadamard si l'entrée est $|0\rangle$ la sortie est $|0\rangle$, si l'entrée est $|1\rangle$ la sortie est $|1\rangle$. Il en est donc de même pour un circuit composé d'un nombre pair de portes H. Par contre, un circuit composé d'une unique porte H réalise une superposition uniforme de $|0\rangle$ et de $|1\rangle$. Il en est de même pour un circuit composé d'un nombre impair de portes H. Ainsi, avec des portes H on peut construire une *vraie* suite aléatoire de bits, ce qui est important, en particulier, dans les méthodes de Monte Carlo (pour la simulation en physique des particules, l'optimisation, l'intégration etc.)

La porte CNOT est définie par :

CNOT ($|00\rangle$) = $|00\rangle$), CNOT ($|01\rangle$) = $|01\rangle$), CNOT ($|10\rangle$) = $|11\rangle$), CNOT ($|11\rangle$) = $|10\rangle$)

En utilisant une porte H et une porte CNOT (cf. la figure 5) on peut construire le 2-qubit

$$|\psi\rangle = \frac{1}{\sqrt{2}} \times |00\rangle + \frac{1}{\sqrt{2}} \times |11\rangle.$$

La probabilité de mesurer 00 est 1/2, celle de 11 aussi, et les mots binaires 01 et 10 ont une probabilité de 0. Les états quantiques des deux 1-qubits sont dits *intriqués*. Dans l'analogie avec le lancer en l'air de pièces de monnaie, les deux pièces sont liées entre elles le résultat est le même sur les deux pièces : on obtient soit pile et pile, soit face et face.

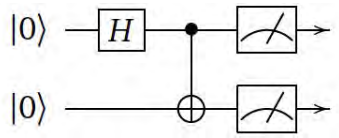


Figure 5 : Réseau quantique intriquant $|00\rangle$ et $|11\rangle$

Dans ce schéma H représente une porte de Hadamard, ⊕ une porte CNOT et le cadran d'un compteur la mesure d'un 1-qubit.

2.5. Erreurs

Les résultats d'un algorithme quantique sont des résultats probabilistes. Les probabilités sont inhérentes aux calculs réalisés avec des qubits. Ce ne sont pas des « erreurs » et en répétant un nombre suffisant de fois le calcul on s'approche de la solution exacte.

L'une des difficultés de l'informatique quantique est la nécessité à la fois d'isoler au mieux les qubits de leur environnement (pour éviter la décohérence), tout en cherchant à les contrôler pour faire des opérations dessus. La solution consiste à améliorer le matériel pour mieux isoler l'information des perturbations, et créer des codes de correction d'erreur quantique (QEC, pour Quantum Error Corrections).

L'idée de base de la QEC est de créer des qubits pour effectuer des opérations redondantes, et d'appliquer des codes de correction d'erreurs. On utilise donc un groupe de plusieurs qubits dits « physiques » pour coder l'information d'un seul qubit dit « logique ». En déterminant l'état des qubits physiques, on sait alors, du fait de l'intrication, si le qubit logique est ou non dans l'état prévu. S'il ne l'est pas, on le corrige immédiatement. En pratique, toutefois, la mise en place des QEC est plus compliquée : on estime qu'il faudrait environ 1 000 qubits physiques pour chaque qubit logique utilisable pour les calculs. L'ordinateur quantique idéal devrait donc comporter, pour

quelques milliers de qubits logiques, quelques millions de qubits : nous sommes actuellement loin de pouvoir manipuler et contrôler autant de qubits. On essaie donc d'améliorer à la fois la technologie de fabrication des qubits et les algorithmes de correction d'erreur. Dans le quantique aussi, les choses évoluent très rapidement : les deux types d'erreurs principaux sont le "*bit flip*" qui fait basculer l'état du qubit de $|0\rangle$ à $|1\rangle$ ou de $|1\rangle$ à $|0\rangle$ et le "*phase flip*" qui fait basculer l'état du qubit de $|0\rangle + |1\rangle$ à $|0\rangle - |1\rangle$. Des chercheurs INRIA, en collaboration avec la startup Alice & Bob qui utilise des qubits supraconducteurs, annoncent[13] avoir mis au point des qubits dits "qubits de chat" qui par nature ne sont pas sujets aux erreurs *bit flip,* et un logiciel efficace de correction d'erreur des *phase flips* permettant de ramener de 1 000 à 30 le nombre de qubits physiques pour un qubit logique.

2.6. La rupture : l'algorithme de Shor

En 1995 Shor publia un algorithme quantique[14] (ayant un grand nombre de qubits) pour factoriser un entier n en $O(\log(n)^3)$ et en espace $O(\log(n))$. Aujourd'hui, il n'existe pas d'algorithme classique en temps $O(\log(n)^k)$ pour n'importe quel k. Les algorithmes classiques deviennent donc rapidement impraticables quand n est grand, alors que l'algorithme de Shor peut casser le RSA en temps plus court. Il a été aussi étendu pour attaquer beaucoup d'autres cryptosystèmes à clé publique. (Comme tous les algorithmes quantiques, l'algorithme de Shor est probabiliste : il donne la réponse correcte avec une grande probabilité et la probabilité d'échec peut être diminuée en répétant l'algorithme.) *La découverte de Shor a été l'une des motivations principales pour la construction un ordinateur quantique.*

Pour comprendre l'algorithme de Shor il faut connaitre des mathématiques (nombres complexes, algèbre linéaire, l'algorithme de chiffrement RSA, donc de l'arithmétique et la transformée de Fourier, des probabilités …).

Ainsi, si la *thèse qualitative* de Church-Turing n'est pas remise en cause par le quantique la *thèse quantitative* disant que tout modèle de calcul « raisonnable » peut être simulé efficacement par une Machine de Turing probabiliste est, elle, remise en cause.

Un autre algorithme quantique qui a suscité un grand intérêt est celui de Grover[15] qui trouve un élément donné dans un ensemble non ordonné de n éléments en $O(\sqrt{n})$ au lieu de $O(n)$.

Depuis, de très nombreux algorithmes quantiques ont été écrits pour des problèmes « difficiles » – problèmes pour lesquels il n'existe pas d'algorithme polynomial sur des ordinateurs classiques – dans de nombreux domaines (recherche opérationnelle, optimisation, simulation, apprentissage automatique, …)[16].

Et se pose alors la question : sera-t-il possible de programmer ces algorithmes, c'est-à-dire sera-t-il possible de construire des ordinateurs quantiques ayant suffisamment de qubits ?

---

[13] 2504-FR_Transcript_Cat-qubits-and-LDPC-Codes-a-New-Step-Towards-Quantum-Error-Correction_Alice-and-Bob, d'après : https://www.inria.fr/fr/ordinateur-quantique-architecture-inedite#:~:text=Une%20architecture%20très%20peu%20consommatrice%20de%20qubits&text=Nos%20premiers%20tests%20montrent%20qu,de%20correction%20d'erreurs.%20»

[14] SHOR P.W., Polynomial Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, https://arxiv.org/abs/quant-ph/9508027

[15] GROVER L.K., *A fast quantum mechanical algorithm for database search*, Proceedings, 28th Annual ACM Symposium on the Theory of Computing, (May 1996) p. 212

[16] BOURREAU E., FERRY G., LACOMME P., *Introduction à l'informatique quantique*, Eyrolles

3. Des supercalculateurs aux ordinateurs quantiques

Examinons les défis du calcul haute performance, entre la progression spectaculaire des supercalculateurs industriels et l'émergence des prototypes d'ordinateurs quantiques les plus avancés.

3.1. Les défis du calcul intensif : des fondements théoriques aux réalités technologiques

Il y a un siècle, l'effervescence scientifique, de la relativité à la physique quantique, a suscité de nombreuses contributions, par exemple d'Alan Turing sur les notions de calculabilité en 1936. Sa machine est au départ une expérience de pensée, qui ne pouvait être concrétisées qu'à travers le prisme des technologies de l'époque : les relais électromécaniques, suivis par les tubes électroniques jusqu'à la réalisation du premier ordinateur électronique, l'ENIAC en 1946 d'une capacité de 5000 additions par seconde pour 150 kilowatts, soit de l'ordre de 30 Watts pour une simple addition. Le développement de l'électronique puis de la micro et nano électronique s'est axé sur des développements de procédés de fabrication physiques et chimiques dans les semiconducteurs, du transistor au circuit intégré, amplifié par la suite par la convergence avec d'autres disciplines comme l'informatique ou le traitement du signal et de l'information, pour nous amener à l'internet des objets nomades communicants et aux smartphones actuels. Ces progrès technologiques ont permis de porter les capacités de calcul à quelques millions d'instructions par seconde au début des années 80, jusqu'aux machines exaflopiques actuelles, d'une capacité de deux milliards de milliards d'instructions par seconde pour une puissance de 30 MW[17]. Les supercalculateurs actuels s'appuient sur la seule technologie dominante depuis un demi-siècle, la technologie CMOS poussée aujourd'hui à ses limites (échelle du nanomètre) par des acteurs industriels qui se sont succédé (Fairchild, Motorola, Texas Instruments, IBM, Intel, STmicroelectronics, … jusqu'à TSMC (Taiwan Semiconductor Manufacturing Company). Cette technologie permet ainsi de réaliser des systèmes intégrés composés de processeurs de calcul d'une complexité d'intégration pouvant dépasser une centaine de milliards de transistors. Elle est identique pour toutes les applications numériques, des smartphones aux supercalculateurs, ce qui a permis de rentabiliser les investissements massifs nécessaires pour atteindre les échelles d'intégration nanométriques (2 nm pour la longueur de canal d'un transistor). Les développements actuels d'applications et de services d'intelligence artificielle générative conduisent à concentrer ces moyens de calcul dans des centres mutualisés de calculs et de données (data centers) qui mettent en évidence les limites énergétiques de ces infrastructures de calcul et de stockage des données, de l'ordre de 1 GW pour les plus gros data centers.

3.2. Quelles technologies pour réaliser les qubits du calcul quantique ?

Les approches qui permettront de réaliser un ordinateur quantique c'est à dire d'appliquer des lois physiques pour contrôler des objets quantiques individuels conduisent à plusieurs technologies développées en parallèle par des acteurs industriels utilisant les ions piégés, les supraconducteurs, les spins des électrons dans le silicium ou des nanotubes, les atomes froids, les photons.

[17] 2025 edition of the TOP500 list of the world's most powerful supercomputers https://top500.org/lists/top500/2025/11/

- **Ions piégés**[18]
  Des ions sont des atomes auxquels on a arraché un ou plusieurs électrons. Ils se retrouvent donc électriquement chargés positivement. Ils sont suspendus dans le vide, confinés et manipulés avec précision par des champs électromagnétiques et/ou des lasers. On peut encoder les états électroniques internes de chaque ion, donc créer un qubit, au moyen d'impulsions laser ou d'impulsions microondes. Ces qubits peuvent être intriqués en localisant deux ou plusieurs ions dans le même piège par les forces électrostatiques s'exerçant entre eux. Développés depuis le début des années 1990, avec des prototypes actuels tels que ceux développés par la société IonQ, ils ont des temps de cohérence très élevés pouvant atteindre plusieurs minutes. En contrepartie, ils sont lents à manipuler, ce qui a pour conséquence de ralentir les calculs. Les techniques de piégeage sont compliquées à mettre en œuvre et limite le nombre de qubits.
- **Supraconductivité**[19]
  Les circuits supraconducteurs apparus à la fin des années 1990, sont des circuits électriques de taille micrométrique comportant des électrodes métalliques qui deviennent supraconductrices, c'est-à-dire qui conduisent l'électricité sans résistance donc sans échauffement, à très basse température. Ces circuits se comportent comme des atomes artificiels dont il est possible de manipuler l'état quantique. Les qubits supraconducteurs ont des temps de cohérence moins longs que les ions piégés mais ils sont en revanche plus rapides à manipuler, et leur technique de fabrication est plus simple, ce qui permet d'envisager leur intégration en grand nombre sur une puce, donc susceptibles d'un développement industriel. C'est la raison pour laquelle IBM, Google ou Microsoft ont choisi cette technologie. Le plus grand ordinateur quantique au monde, en 2025, est construit par IBM[20], qui a développé le processeur quantique Condor de 1121 qubits, avec pour objectif de développer un supercalculateur quantique de 100 000 qubits d'ici 2033. Cette "puce" quantique fonctionnant avec des qubits supraconducteurs, IBM a pour cela développé un réfrigérateur destiné à accueillir plusieurs processeurs quantiques du type Condor à une température de quelques dizaines de millikelvins, proche du zéro absolu (- 273,15 degrés Celsius). Des recherches sont parallèlement menées pour réduire autant que possible la température afin d'une part de positionner au démarrage les qubits dans l'état $|0\rangle$, d'autre part augmenter le temps de cohérence. Par exemple, des chercheurs des universités du Maryland aux USA et de Chalmers en Suède ont démontré la possibilité d'atteindre une température de 22 millikelvins[21].
- **Spin électronique**[22]
  Il s'agit d'isoler des électrons dans une matrice de silicium et d'utiliser leur spin, sorte de rotation de la particule sur elle-même, comme bit quantique d'information. Développés récemment par exemple en France par a société Quobly, ces qubits sont encore relativement « fragiles ». Mais de l'avis général, ils devraient parvenir bientôt aux mêmes niveaux de performance que les autres dispositifs. Leur fabrication utilise les mêmes techniques que la microélectronique, de sorte que l'intégration à grande

[18] https://lejournal.cnrs.fr/articles/ordinateur-les-promesses-de-laube-quantique ; https://www.ionq.com
[19] https://lejournal.cnrs.fr/articles/ordinateur-les-promesses-de-laube-quantique
[20] https://www-spinquanta-com.translate.goog/news-detail/discover-the-worlds-largest-quantum-computerin20250106092507?_x_tr_sl=en&_x_tr_tl=fr&_x_tr_hl=fr&_x_tr_pto=rq&_x_tr_hist=true
[21] Ali Aamir M. et al., « Thermally driven quantum refrigerator autonomously resets a superconducting qubit », *Nature Physics*, vol. 21, p. 318-323 (2025)
[22] https://lejournal.cnrs.fr/articles/ordinateur-les-promesses-de-laube-quantique

échelle est tout à fait envisageable. La start-up française “C12 quantum electronics” quant à elle piège des électrons non pas dans le silicium, mais dans des nanotubes de carbone, ce qui pourrait, en théorie, améliorer l’isolation et le temps de cohérence des qubits, tout en maintenant un couplage fort pour une manipulation rapide des qubits.

- **Atomes froids**

Des qubits peuvent être réalisés à partir d’atomes. Il faut pour cela que ces atomes puissent être manipulés, donc être immobilisés. Or des atomes isolés (atomes de gaz par exemple) sont en perpétuelle agitation, dite agitation thermique : plus la température est élevée, plus l’agitation des atomes est importante. Des atomes immobiles sont des atomes froids, et même ultra froids, leur température doit être de l’ordre du microkelvin (quelques millionièmes de degrés Celsius au-dessus du zéro absolu !) voire du nanokelvin. On peut pour cela par exemple les confiner en les bombardant, dans une enceinte à vide, avec des photons, c’est-à-dire des faisceaux laser (figure 6) ou par effet Sisyphe.

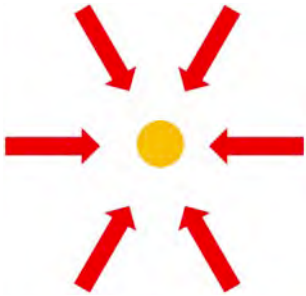


Figure 6 : Schéma d’immobilisation d’un milliard d’atomes de sodium ou de rubidium dans une enceinte à vide par confinement par des faisceaux laser

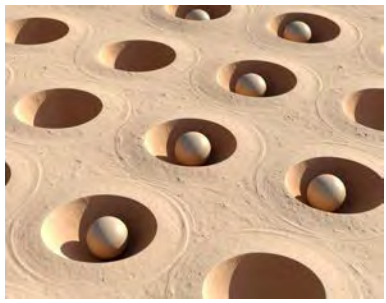


Figure 7: Représentation schématique d’atomes froids piégés dans un réseau

Ces atomes ultra-froids sont placés à l’intérieur d’un réseau régulièrement espacé constitué par une grille plane comportant des « micropièges » d’un micromètre de diamètre espacés de trois micromètres. Chaque micropiège constitue une sorte de puits où un atome peut se loger, comme des billes se logeant au fond de trous (figure 7). Ces atomes sont 10 000 fois plus petits que les qubits supraconducteurs. Chaque qubit d’atome froid doit être positionné de façon très précise. Des chercheurs chinois ont assemblé par intelligence artificielle dans une grille parfaite 2024 atomes froids en 60 millisecondes. Ils ont utilisé pour cela une version améliorée de “pinces optiques” utilisées en recherche médicale pour la manipulation de protéines. Les experts estiment que leur technique pourrait permettre de développer des processeurs comportant entre 1 000 et 10 000 qubits d’atomes ultra-froids. Les processeurs quantiques à atomes ultra-froids pourraient avoir des performances comparables à celles des meilleurs processeurs actuels à la fois en matière de nombre de qubits, de possibilités d’interconnexion et de cohérence. En France, cette technique est mise en œuvre par la société Pasqal qui s’appuie sur des technologies optique, mécanique et électronique pour contrôler des atomes à l’aide de pinces optiques qui sont des lasers permettant de refroidir les atomes pour les positionner dans une enceinte à vide. Cette méthode permet de déplacer les atomes et de reconfigurer l’architecture de calcul selon le problème à résoudre. L’intégration de ces dispositifs dans des baies de calcul d’ordinateurs quantiques permet de mettre en œuvre une centaine de qubits

physiques avec des consommations énergétiques de quelques kW très inférieures aux technologies exploitant les supraconducteurs.

- **Photons**
  Les photons peuvent être utilisés comme qubits. La filière photonique offre trois avantages : elle fonctionne à température ambiante, contrairement à la plupart des autres technologies quantiques qui requièrent un froid extrême, elle utilise des composants dérivés du silicium, matériau bien maitrisé dans la filière électronique, et elle utilise les mêmes fibres optiques qu'internet. En France, cette technique est mise en œuvre par la PME Quandela, qui dispose d'un savoir-faire dans la production de sources de lumière capables d'émettre des photons un par un, et qui commercialise des prototypes d'ordinateurs quantiques d'une dizaine de qubits physiques avec comme atouts un fonctionnement à température ambiante, et une consommation énergétique réduite d'un ordre de grandeur identique aux atomes froids.

3.3. Situation de la France

La France, reconnue pour son excellence en recherche fondamentale (voir Annexe) avec des organismes de recherche très impliqués comme Le CNRS, le CEA ou l'INRIA, mise sur une stratégie nationale et européenne combinant recherche publique, startups innovantes et partenariats industriels, pour se positionner comme un acteur clé du quantique en formant une nouvelle génération de talents. Les « Maisons du Quantique » rassemblent au sein d'écosystèmes locaux les différents acteurs du calcul quantique hybride pour fédérer un panel de talents industriels et académiques du domaine sur le territoire national. Cinq projets ont été sélectionnés en régions Grand Est, Auvergne-Rhône-Alpes, Nouvelle Aquitaine, Occitanie et Île-de-France. Les technologies alternatives développées par des startups comme Quandela (Qubits photoniques), Pasqal (atomes neutres, laser), Alice&Bob (circuits supraconducteurs robustes) ou Quobly et C12 (spin) pourraient offrir un avantage différenciant si elles atteignent la maturité industrielle avec un nombre de qubits suffisant.

Ces étapes s'inscrivent dans la feuille de route France 2030 doté d'un budget de près de 2 milliards d'euros pour créer un écosystème complet recherche, formation, industrialisation en développant des synergies public-privé pour accélérer l'innovation et faciliter l'accès aux prototypes de machines quantiques via le cloud (VeriQloudPlateforme d'accès au calcul quantique) et l'opérateur GENCI (Grand Équipement National de Calcul Intensif) soutenu par EuroHPC et le programme France 2030. GENCI a déployé en 2025 deux machines quantiques majeures en France : Lucy développé par Quandela ordinateur quantique photonique de 12 qubits, et Ruby de Pasqal ordinateur quantique à atomes neutres (atomes froids manipulés par laser) de 100 qubits. Ces 2 machines sont intégrées à des infrastructures HPC pour former des plateformes hybrides uniques en Europe. Elles sont installées en France au TGCC (Très Grand Centre de Calcul) du CEA à Bruyères-le-Châtel (Essonne) par GENCI (Grand Equipement National de Calcul Intensif, www.genci.fr). Ces installations s'inscrivent ainsi dans la stratégie française et européenne de développement d'une filière quantique souveraine, en s'appuyant sur des technologies développées par des startups françaises.

3.4. Sobriété énergétique

Compte tenu de l'état de l'art, les impacts énergétiques et environnementaux des ordinateurs quantiques se comparent difficilement à ceux des supercalculateurs classiques (HPC). Pour la plupart des tâches actuelles les machines quantiques sont moins efficaces que les HPC, si on se réfère en termes de consommation par opération

utile. Pour les supercalculateurs exaflopiques actuels la consommation électrique provient principalement des milliers de processeurs et accélérateurs GPU, des systèmes de refroidissement qui ont gagnés en efficacité (refroidissement liquide, récupération de chaleur), la consommation est élevée pour des calculs complexes. Pour un calcul équivalent, un ordinateur quantique peut être en principe moins énergivore si l'algorithme quantique est exponentiellement plus efficace (par exemple en simulation moléculaire). Pour les supraconducteurs le refroidissement cryogénique nécessite des températures proches du zéro absolu, ce qui consomme des centaines de kW selon le dimensionnement. Les systèmes Photonique (Quandela) ont l'avantage d'un fonctionnement à température ambiante avec néanmoins des besoins énergétiques (lasers).

3.5. Hybridation HPC/Quantique

Les ordinateurs quantiques ne fonctionneront pas seuls, mais en complémentarité étroite avec les supercalculateurs classiques péta et exaflopiques[23]. L'idée est d'utiliser le quantique uniquement pour les parties du calcul avec des algorithmes conduisant à un avantage quantique certain. Par exemple les deux machines installées au TGCC sont physiquement intégrés aux infrastructures HPC, via des interconnexions rapides. Les ordinateurs quantiques ne remplaceront pas les supercalculateurs, mais les compléteront pour des tâches spécifiques. L'hybridation HPC-quantique est actuellement la voie privilégiée avec néanmoins des défis comme la latence et la synchronisation dans le transfert de données entre HPC et quantique avec des temps de calcul différents pouvant conduire à des goulots d'étranglement.

En attendant la généralisation des ordinateurs quantiques, on peut utiliser des émulateurs quantiques : il s'agit d'ensembles de matériels et de logiciels classiques (telle la plateforme Atos Quantum Learning Machine) capables de simuler sur des ordinateurs classiques des algorithmes quantiques conçus pour fonctionner sur des ordinateurs quantiques. On simule au moyen d'un ordinateur classique puissant les interactions qui interviennent dans un vrai ordinateur quantique (superposition d'états, intrication, décohérence, etc.). Il existe des émulateurs qui simulent spécifiquement tel type de matériau utilisé en quantique, tel "exQalibur" de l'entreprise Quandela pour le photonique, ou "Pulser" de l'entreprise Pasqal pour les atomes neutres. La quasi-totalité des émulateurs proposent un mode de fonctionnement sans erreur (= mode logique) et un mode de fonctionnement avec simulation des erreurs quantiques évoquées ci-dessus (= mode physique).

Ces émulateurs permettent :

- d'apprendre à coder des algorithmes quantiques avec un matériel classique, voire même avec un ordinateur portable,
- de visualiser le déroulement interne d'un algorithme quantique (par exemple la progression des calculs), ce qui est très difficile à faire avec un ordinateur quantique à cause de la décohérence, ainsi qu'il est expliqué plus haut,
- de développer et tester à petite échelle (c'est à dire sur quelques qubits) de nouveaux algorithmes quantiques, ainsi que des codes de correction d'erreurs.

Malheureusement la durée d'exécution et la consommation de mémoire augmentent exponentiellement avec le nombre de qubits simulés. Par exemple, pour

[23] Xiaosi Xu, Simoon Benjamin, Jianxin Chen, Jinzhao Sun, Xiao Yuan, Pan Zhang, « A Herculean task : classical simulation of quantum computers », Science Bulletin 70 (23), p. 4104-4112, (2025), https://www.sciencedirect.com/science/article/pii/S2095927325010382#s0005

stocker le vecteur d'état d'un système quantique à N qubits, il faut 8×2^N octets de mémoire : c'est à dire pour 20 qubits 8×2^{20} = 8 MB (8 millions de bits) ; pour 40 qubits 8×2^{40} = 8 TB (= 8 téra bits, soit 8 millions de millions de bits).

3.6. Avantage quantique : quelles applications futures ?

Le calcul quantique ouvre des perspectives révolutionnaires pour résoudre des problèmes d'une complexité inégalée. Ses applications s'étendent à des domaines aussi variés que l'exploration de la Terre (modélisation climatique, optimisation des ressources), la chimie quantique (simulation des réactions moléculaires pour concevoir de nouveaux matériaux ou médicaments), la médecine personnalisée (accélération de la découverte de traitements). Autant de défis où la puissance quantique pourrait transformer notre approche de la science et de l'innovation :

- Optimisation industrielle par exemple en aéronautique pour optimiser les trajectoires de vol, réduire la consommation de carburant, concevoir de nouveaux matériaux, optimiser les réseaux électriques, la gestion des smart grids, la prospection pétrolière.
- Logistique : Simulation de chaînes d'approvisionnement complexes (ex : gestion des flux pour les grands ports ou les plateformes de e-commerce).
- Chimie et matériaux : Simulation moléculaire : Modélisation de réactions chimiques pour la découverte de nouveaux médicaments, la simulation de nouveaux matériaux pour les batteries du futur…
- Finance : modélisation de scénarios financiers complexes (stress tests, portefeuilles d'investissement).
- Intelligence Artificielle : Hybridation entre calcul quantique et IA classique pour l'apprentissage automatique sur des jeux de données massifs (ex : reconnaissance d'images).
- Cybersécurité et cryptographie post-quantique : migration des infrastructures critiques vers des algorithmes résistants aux attaques quantiques avec le rôle essentiel joué par l'ANSSI (Agence nationale de la sécurité des systèmes d'information). Ce sujet est bien évidemment stratégique en termes de souveraineté et de sécurité ce qui explique les investissements actuels en Chine, USA, et Europe.

4. Conclusion

On ne sait pas aujourd'hui si ce foisonnement aboutira à des ordinateurs spécifiques fiables, chacun dévolu à une tâche particulière, ou s'il sera possible de construire des ordinateurs "généralistes" susceptibles de résoudre une grande variété de problèmes, comme aujourd'hui les ordinateurs classiques. La question n'est plus de savoir s'il sera ou non possible de construire des ordinateurs quantiques, mais quand déboucheront sur le marché des machines performantes (cohérence, correction d'erreurs efficace, nombre de qubits significatifs). Il faudra alors être en mesure, pour profiter des avantages du quantique, de programmer ces ordinateurs, ce qui ne pourra se faire qu'au moyen d'algorithmes très différents de ceux utilisés avec les ordinateurs classiques. C'est à cet objectif que tentent de répondre les émulateurs développés actuellement. D'ici 2050, l'état de l'art en informatique quantique devrait connaître des avancées tant sur le plan technologique qu'applicatif, même si les prédictions restent toujours sujettes à des incertitudes scientifiques et économiques. Les feuilles de route des leaders actuels prévoient des ordinateurs quantiques tolérants aux fautes, avec des milliers de qubits logiques, intégrés aux infrastructures cloud et HPC. En parallèle les supercalculateurs actuels ont encore de beaux jours devant eux.

La “première révolution quantique”, qui a débuté à l’orée du XX^{e} siècle, a donné lieu à une multitude d’applications industrielles qui ont bouleversé notre vie quotidienne. La “seconde révolution quantique”, qui a débuté en 1982 avec la mise en évidence expérimentale de l’intrication, en est aujourd’hui à ses balbutiements, mais elle apportera peut-être dans les décennies à venir, notamment par l’alliance de l’ordinateur quantique et de l’intelligence artificielle, des bouleversements aussi importants aux générations futures.

Annexe

Il nous semble utile de montrer combien les chercheurs français sont pionniers dans ce domaine, comme le montre l’encadré ci-dessous.

Depuis la création du prix Nobel en 1901, 18 français ou françaises ont obtenu le prix Nobel de Physique, dont 7 dans le domaine de la mécanique quantique, parmi lesquels 4 sont impliqués dans les fondements de l’ordinateur quantique (les dates indiquées sont celles de l’obtention du prix Nobel, pas celles de leurs découvertes) :
– Robert Cohen-Tanoudji (1997) : Développement de techniques de refroidissement et de piégeage d’atomes par laser (utiles pour manipuler les qubits).
– Albert Fert (2007) : magnétorésistance géante.
– Serge Haroche (2012) : méthodes de mesure de systèmes quantiques individuels (essentielles pour les qubits)
– Alain Aspect (2022) : mise en évidence de l’intrication de photons (fondement du traitement de l’information quantique).
– Pierre Agostini et Anne L’Huillier (2023) : génération d’impulsions attoseconde pour l’étude de la dynamique des électrons dans la matière.
– Michel Devoret (2025) : découverte de l’effet tunnel quantique macroscopique (permettant à des milliards d’électrons de traverser une barrière infranchissable selon la physique classique, ouvrant ainsi la voie à des applications majeures en informatique quantique).