Traduction de l'intervention d'Alain Connes à la World Tech Conference (24-27 juin 2026, Milan, Italie), "A glimpse of the quantum world" (un aperçu du monde quantique) [1]

Le maître de cérémonie : Alain Connes, je vous en prie, rejoignez-moi sur scène. Merci. Bienvenue. Vous montez. Pardon, je vous laisse la scène. Merci.

Alain Connes : Très bien. Eh bien, ma tâche consistera à essayer de vous donner un aperçu du monde quantique. Je ferai un voyage, pour ainsi dire, à partir de Heisenberg.

Comme Ugo [2] l'a mentionné, il fut, en quelque sorte, le premier à entrevoir pleinement le monde quantique. Je vais vous guider pas à pas et, pour finir, j'essaierai de vous expliquer le fonctionnement de l'ordinateur quantique.

Revenons donc 101 ans en arrière. Un jeune physicien de 23 ans travaillait alors à Göttingen.

Il souffrait d'une terrible crise de rhume des foins. À l'époque, le remède consistait à envoyer les patients dans un lieu exempt de pollen. Il existait une île non loin de là, Heligoland - essentiellement un rocher nu, sans pollen.

Heisenberg y fut envoyé. Il fut hébergé par une dame âgée dans une petite maison et il était déchargé de toute obligation d'enseigner. Il disposait de tout son temps. Il tentait d'établir les relations algébriques régissant l'atome, guidé par une idée forte : il ne devait utiliser que des grandeurs observables. C'est ainsi qu'il a élaboré son système. Un soir, il s'efforçait de vérifier l'une des lois fondamentales de la physique : la conservation de l'énergie.

Il enchaînait les calculs, commettait des erreurs algébriques élémentaires, et ainsi de suite, jusqu'à trois heures du matin. C'est alors que tout s'est mis en place.

Il a eu la certitude de tenir la vérité. Impossible de dormir, bien sûr. Il s'est alors rendu à l'est de l'île pour entreprendre une ascension.

C'était un alpiniste. Il a grimpé au sommet d'un rocher, quelque part. Il s'y trouvait une paroi rocheuse très abrupte.

Assis au sommet de ce rocher, il attendait le lever du soleil. Dans ses mémoires, il a décrit comment un paysage intellectuel magnifique s'est alors offert à son regard : celui de la mécanique quantique. Ce qu'il venait de découvrir, c'est ce que l'on a appelé plus tard la mécanique matricielle.

Il en ignorait alors le nom mathématique, mais il avait mis au jour quelque chose de véritablement extraordinaire. Ce qu'il a découvert, c'est que lorsqu'on traite un système atomique microscopique, on ne peut plus opérer comme nous avons l'habitude de le faire avec les nombres.

1. Transcription en LaTeX : Denise Vella-Chemla assistée d'outils logiciels divers, juillet 2026.
2. Ugo Moschella, Professeur de physique théorique, Université de l'Insubrie, Côme, et chercheur associé au CERN, Genève.

Voyez-vous, avec les nombres, 3 fois 5 est égal à 5 fois 3 ; l'ordre des termes n'a aucune importance. Or, Heisenberg a découvert que cette règle ne s'applique plus aux grandeurs physiques propres à un système atomique. On pourrait croire qu'il s'agit là d'une complication majeure ou d'une nouveauté absolue.

Pourtant, nous y sommes parfaitement habitués. Prenons l'exemple du jeu du scrabble : imaginez deux mots [3] : UNITED [4] et UNTIED [5].

Si l'on considère ces deux mots dans un monde commutatif, que fait-on ? On prend l'ensemble des lettres qui les composent. Ces ensembles sont identiques, car on passe du premier mot au second en intervertissant simplement deux lettres : le "i" et le "t". En réalité, ce que Heisenberg a compris en profondeur, c'est que dans le monde quantique, l'ordre des lettres ne peut être ignoré. Or, la nuance entre ces deux mots correspond précisément à la différence de sens qu'ils véhiculent.

Après tout, "united" (uni) et "untied" (détaché) ont des significations essentiellement opposées. Réfléchissez un instant : que se passe-t-il si je prends le mot "nuclear" (nucléaire) et que j'échange le "n" et le "u" ? Eh bien, si vous y pensez un peu, vous obtiendrez "unclear" (peu clair).

En somme, Heisenberg a mis en évidence un phénomène d'une extrême subtilité. Il s'avère que les relations algébriques - la manière dont on manipule les grandeurs physiques - sont plus subtiles en physique quantique. L'une des conséquences en est la suivante.

On ne peut pas attribuer une valeur simultanée à deux grandeurs qui ne commutent pas, c'est-à-dire qui ne satisfont pas à cette règle de commutation. C'est là le célèbre principe d'incertitude de Heisenberg, qui a joué un rôle fondamental en physique, et plus particulièrement en physique quantique.

Voilà où nous en sommes. Or, il se trouve qu'à Göttingen, où l'on comptait de nombreux mathématiciens, von Neumann a en quelque sorte compris la nature des mathématiques sous-tendant la découverte de Heisenberg.

D'une certaine manière, comme nous le verrons, cette découverte fondamentale de Heisenberg a eu - pour les raisons que je vais expliquer - des conséquences considérables, tant pour les mathématiques que pour la physique. Un autre fait remarquable qui en découle est, par exemple, l'impossibilité d'intervertir deux grandeurs physiques - comme c'est le cas, bien entendu, pour l'exemple classique de la position et de l'impulsion, etc., mais il existe une alternative à cela. Il existe un moyen d'intervertir deux grandeurs physiques lorsqu'on évalue leur produit dans un état thermique.

J'espère ne pas avoir à définir ici ce qu'est un état thermique. Disons simplement qu'un état thermique est un état sur lequel on peut évaluer des grandeurs physiques. Il s'avère qu'une loi permet, dans un tel état, d'intervertir A et B - ou, si vous préférez, de placer B devant A.

3. La conférence est donnée en anglais.
4. adjectif : "unis".
5. adjectif : "détachés".

Mais cela a un prix, un prix lié au temps. C'est un fait absolument fondamental que je vais utiliser à maintes reprises : on peut intervertir A et B dans un état thermique (c'est-à-dire un état défini à une certaine température).

Quel est donc ce prix à payer ? Il faut laisser l'opérateur B, que l'on a placé devant A, évoluer dans le temps. Mais de quelle manière ? Il doit évoluer selon un temps qui n'est pas le temps réel, mais qui fait intervenir un nombre introduit au XVIe siècle par un mathématicien italien nommé Bombelli. Bombelli a eu le génie d'inventer un nombre alors jugé totalement impossible par les mathématiciens de l'époque ; il l'a appelé "più di meno", ce qui constitue, en soi, une idée extraordinaire.

Il y a "più" (plus) et "meno" (moins) ; Bombelli a eu l'idée d'inventer un nombre intermédiaire. Pour les mathématiciens, ce nombre est bien connu : il s'agit du nombre i, la racine carrée de moins un. La loi remarquable que j'ai inscrite ici stipule que, pour intervertir A et B, il faut laisser B évoluer, mais en temps imaginaire.

La durée correspondant à ce nombre de Bombelli est extrêmement courte. À température ambiante, elle est de l'ordre de 25 femtosecondes. Qu'est-ce qu'une femtoseconde ? Il s'agit d'une durée si brève que la trajectoire de la lumière sur ce laps de temps ne serait que de quelques microns.

Eh bien, cette loi - qui a impliqué de nombreuses personnes - est connue sous le nom de condition de Kubo-Martin-Schwinger. Elle a été formulée par Haag, Hugenholtz et Winnick, et deux mathématiciens, Tomita et Takesaki, y ont également travaillé. C'est là, toutefois, que j'ai apporté l'une de mes contributions majeures à la science.

Qu'ai-je découvert il y a 54 ans ? J'ai découvert que l'évolution temporelle associée à l'état thermique - lorsque l'on considère l'une de ces algèbres, cette structure fondamentale définie pour encoder la mécanique quantique - ne change pas (à une symétrie interne près de l'algèbre) lorsque l'on modifie l'état. Ces symétries internes sont, pour ainsi dire, celles qui découlent de la non-commutativité. Cette découverte a eu un impact considérable, car elle a révélé que ces algèbres possèdent une sorte d'évolution temporelle "intrinsèque" (ou "donnée par la nature"). Elles génèrent leur propre temps, simplement en vertu de leur non-commutativité.

Ce sont donc des objets dynamiques. Il n'est pas nécessaire de choisir un état particulier, comme un état thermique. Toutes ces évolutions temporelles sont uniques, à une symétrie interne près.

Cela m'a permis, en juin - il y a 54 ans, alors que je séjournais en Norvège -, de ramener le cas dit "de type III" (qui semblait auparavant insoluble) à celui des automorphismes de type II. Voilà pour l'aspect mathématique. Si je devais faire graver quelque chose sur ma pierre tombale, ce serait précisément ce fait simple : le changement d'état n'altère pas l'évolution temporelle.

Il existe donc cette évolution temporelle intrinsèque. Mais cela implique quelque chose de bien plus profond encore ; car, comme l'a expliqué Ugo, nous avons pris l'habitude, depuis Galilée et Newton, d'attribuer toute la variabilité du monde à l'écoulement du temps. Mais, d'une certaine manière, cela montre qu'en fait, le temps devrait émerger du monde quantique et que, dans ce domaine

quantique, il devrait y avoir une agitation, une variabilité, plus fondamentales que l'écoulement du temps.

Si je le pense, c'est notamment grâce à un échange que j'ai eu avec Nicolas Gisin, un physicien suisse ; il m'a remis une petite puce que l'on peut fixer sur un iPhone. Qu'est-ce que cette petite puce ? C'est, pour ainsi dire, le plus petit générateur quantique de nombres aléatoires au monde. Il s'agit d'un dispositif fondé sur le principe d'incertitude et sur la non-commutativité, qui produit - qui vous fournit - un nombre aléatoire absolument impossible à reproduire.

En d'autres termes, même si vous connaissiez la disposition de tous les atomes du dispositif, vous seriez incapable de le reproduire. Pourquoi ? Parce que ce nombre n'existe pas avant que l'effervescence quantique ne se soit produite. C'est un point fondamental, notamment pour des raisons de sécurité, car bon nombre des dispositifs que nous utilisons à des fins de sécurité reposent sur des nombres aléatoires.

Mais si vous tentez de générer des nombres aléatoires avec un ordinateur ou un système ordinaire, personne ne vous garantit que l'opération est sûre. En réalité, elle ne l'est pas. Pour conclure mon exposé, je souhaite vous expliquer pourquoi l'ordinateur quantique suscite la crainte de ceux qui utilisent des dispositifs classiques à des fins de sécurité.

Prenons le cas du système classique le plus répandu, appelé `RSA` [6] : en tant que mathématicien, vous partez de deux nombres premiers très, très grands - je suppose que vous connaissez le principe - et vous en calculez le produit. Pour transmettre des informations, c'est ce produit des deux nombres premiers qui est rendu public. Or, l'enjeu de sécurité réside dans l'impossibilité, pour un tiers, de retrouver les deux nombres premiers à l'origine de ce produit.

Il s'avère qu'avec des ordinateurs ordinaires, cette opération est effectivement impossible. En substance, le nombre d'opérations à effectuer est comparable au nombre d'atomes dans l'univers ; cela dépasse largement les capacités de tout ordinateur classique. Pourquoi, alors, cela devient-il possible avec un ordinateur quantique ? Il s'agit d'un algorithme conçu par Peter Shor, et je tiens à vous expliquer le rôle clé que joue ici le quantique.

Pourquoi cela fonctionne-t-il ? Tout d'abord, quelle est la démarche ? Quelle est l'idée sous-jacente ? Elle remonte essentiellement à Gauss. L'idée, relevant de la théorie des nombres, est très simple : il s'agit de travailler dans l'algèbre des entiers modulo l'entier connu que l'on souhaite factoriser.

Le fait que ce nombre ne soit pas premier implique que, dans cette algèbre, on doit pouvoir trouver deux nombres dont le produit est nul, sans que ces nombres le soient eux-mêmes. C'est ce que l'on cherche à faire. Pour y parvenir, on choisit un nombre au hasard parmi ces entiers, par exemple 3. D'ailleurs, Gauss utilisait le nombre 3 lorsqu'il construisait le polygone à 17 côtés.

Prenons par exemple le nombre 3 et élevons-le à différentes puissances. En fait, on le met au carré, encore et encore. Une fois qu'on a effectué suffisamment d'élévations au carré - ce qui ne demande

6. Inventé en 1977 par Ron Rivest, Adi Shamir et Leonard Adleman du Massachusetts Institute of Technology, l'algorithme `RSA` tire son nom de leurs initiales.

finalement que peu d'opérations, donc c'est tout à fait faisable -, on sait alors calculer n'importe quelle puissance de ce nombre.

Pourquoi ? Parce que pour calculer une puissance n, il suffit d'écrire n en base 2, puis d'effectuer le produit correspondant. C'est donc simple ; cela ne présente aucune difficulté.

Le problème, c'est qu'on se retrouve avec une fonction qui dépend de la puissance choisie ; pour factoriser le nombre de départ, il faut comprendre les périodes de cette fonction. Cette fonction est périodique ; elle possède certaines périodes.

Il faut donc cerner ces périodes. Si l'on tente l'opération sur un ordinateur classique, le simple fait de stocker cette fonction est impossible, car elle comporte trop de valeurs.

Par ailleurs, connaître une ou deux valeurs de cette fonction ne permet pas d'en déterminer la période. Quelle est donc l'idée maîtresse de l'algorithme de Shor ? L'idée clé est que, pour trouver une période, il faut "écouter". Et pour écouter, il faut appliquer ce que l'on appelle la transformée de Fourier.

Or, la transformée de Fourier exploite une propriété quantique fondamentale et inédite. Quelle est cette propriété ? Elle nous ramène, là encore, à Bombelli. Elle tient au fait que, si le monde classique manipule des amplitudes de probabilité - qui sont des nombres positifs -, le monde quantique utilise des amplitudes complexes, analogues à des racines carrées de ces amplitudes de probabilité.

Ces amplitudes complexes s'additionnent linéairement, ce qui permet d'appliquer la transformée de Fourier. Cette dernière possède une propriété remarquable : lorsqu'on la mesure, on obtient automatiquement la période. Pourquoi ? Parce qu'en dehors de la période, les différentes phases s'annulent mutuellement, alors qu'au niveau de la période, elles s'additionnent pour produire une valeur très élevée.

Voici donc ce qui se passe : il existe une méthode pour réaliser cette opération à l'aide d'un ordinateur quantique. Vous construisez donc un état à partir de ces diverses mesures, puis vous souhaitez lui appliquer la transformée de Fourier.

La beauté, le cœur même de cet algorithme, réside dans la possibilité de décomposer la transformée de Fourier en un très petit nombre d'opérations élémentaires réalisables sur l'état quantique. Ensuite, vous mesurez la transformée de Fourier et vous déterminez une période. Or, l'obstacle majeur auquel se heurte actuellement l'ordinateur quantique est ce que l'on appelle la décohérence.

Il s'agit, en somme, du fait que lorsque vous créez cet état quantique, vous ouvrez une petite fenêtre sur le monde quantique. Mais cette fenêtre se referme presque aussitôt. Pourquoi ? Parce que tout tend à devenir classique, et que l'intrication que vous avez créée est un phénomène totalement instable.

Ainsi, tout l'enjeu de l'ordinateur quantique est de nous ouvrir une fenêtre sur ce monde quantique merveilleux - un univers qui, pour ainsi dire, évoque le monde merveilleux d'*Alice au pays des mer-*

veilles. Le problème, toutefois, est que la fenêtre que nous parvenons à ouvrir actuellement demeure extrêmement instable ; nous cherchons donc à prolonger la durée d'ouverture de cette fenêtre sur le monde quantique.

Il s'agit donc, pour l'instant, d'un défi technologique. Je tiens toutefois à souligner que, lorsque vous vous renseignez sur cet algorithme, vous pouvez tomber sur des informations erronées. En réalité, l'essence même du système consiste à pouvoir décomposer la transformée de Fourier en termes très simples.

Pour conclure, qu'est-ce que l'ordinateur quantique ? C'est un dispositif philosophiquement merveilleux, car il nous donnera accès à un monde où la variabilité est plus fondamentale et où, pour ainsi dire, la nouveauté incessante du monde quantique constitue le véritable battement de l'horloge divine. Merci.