ORDINATEUR QUANTIQUE, POUR DEMAIN ?

Informatique en quête de quantique

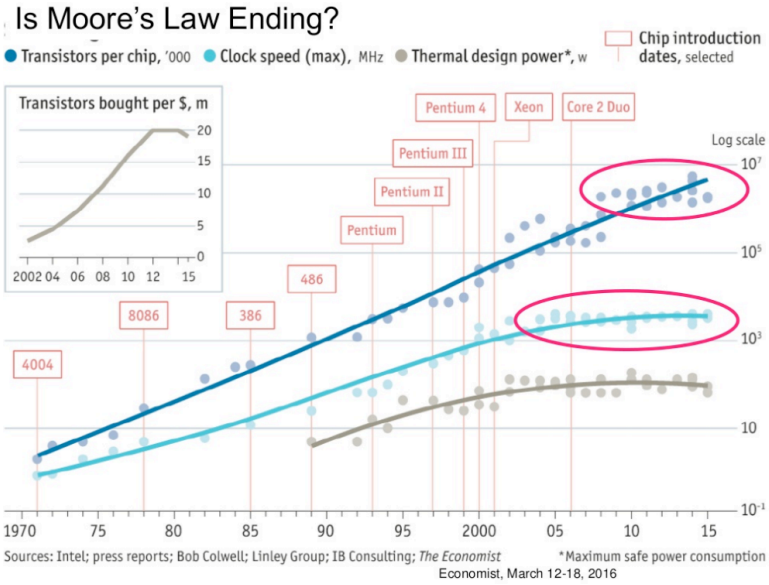
Jacques BAUDRON - jacques.baudron@ixtel.fr

Mai 2017

.

Table des matières

Depuis le début des années 1960 la loi de Moore appuie sa régulière ascension sur des gravures de plus en plus ténues dans le silicium. Las, que faire quand les gravures les plus fines s'essoufflent en se frottant aux confins de la physique ? La vingtaine de nanomètres aujourd'hui courante et les cinq visés pour demain nous rapprochent des défis pour la physique classique. Signe des temps : la première décennie de ce vingt-et-unième siècle a vu fleurir les machines multicœurs et la puissance continue à croître. La loi de Moore est en quête d'un saut technologique pour se perpétuer. L'Intelligence Artificielle forte en a fait un pré-requis.



Avec ses perspectives de calcul massivement parallèle, l'informatique quantique s'affiche en prétendant de choix. En a-t-elle les moyens ? Saura-t-elle répondre présent ? Penchons-nous d'abord sur l'étrange mécanique quantique puis regardons comment exploiter ce monde pour calculer.

QUANTIQUE : UN AUTRE MONDE

HORRIPILANTE PHYSIQUE QUANTIQUE

D'un côté *Elle* est indéniable. En faisant abstraction de la gravitation, *Elle* explique tout. Ce qui nous entoure, la chimie, l'électronique, la stabilité des éléments elle-même … Impossible de *La* récuser. Pire encore, la précision de *Ses* prévisions dépasse l'entendement : la mesure du moment magnétique de l'électron et le calcul théorique sont en accord avec treize chiffres significatifs. Pas le choix, il faut faire avec. On est tenu de *L*'accepter.

D'un autre côté *Elle* nous oblige à avaler des couleuvres : une particule n'existe que quand on la regarde, deux particules ayant été en contact peuvent rester liées quel que soit leur éloignement. Elles sont non-séparables. Très très déstabilisant. Il nous faut oublier toute représen-

tation mentale d'une particule, oublier toute notion de trajectoire, ne pas suivre nos intuitions et laisser notre bon sens loin de chez nous. Seules les mathématiques ont le droit de cité.

La mécanique quantique décrit la physique du tout petit à l'échelle de l'électron et en dessous. Le pas suivant sera l'unification des théories quantiques et gravitationnelles. Théorie des cordes ou gravitation quantique à boucles ? Les deux théories sont aujourd'hui en lice.

La mécanique quantique est tellement déconcertante que les efforts pour l'interpréter ont enfanté des théories où des univers se dédoublent, d'autres où la conscience de l'expérimentateur influe sur la mesure. Nous nous plaçons dans la suite de ce papier dans l'interprétation dite de Copenhague qui fait autorité de nos jours. Petit rappel (de mémoire) de l'avertissement de Richard Feynman : « Ce que je vais vous dire va vous paraître absurde, mais c'est la nature qui est absurde ».

Pénétrons l'absurde avant de préciser trois aspects structurants pour l'informatique quantique : la superposition, la décohérence et l'intrication.

MÉCANIQUE QUANTIQUE

Albert Einstein a voyagé d'un bout à l'autre de l'échelle des tailles : relativité générale dont on perçoit les effets au niveau cosmologique et mécanique quantique qui s'adresse aux particules en deçà de l'atome.

La lumière est un des premiers théâtres du quantique.

Le tout en moins de trente ans

1900	Planck	Introduction des quantas
1905	Einstein	Effet photo-électrique
1913	Bohr	Modèle atome
1924	De Broglie	Fonction d'onde
1925	Heisenberg, Schrödinger, Dirac	Formalisation de la mécanique quantique
1927	Born	Carré de la fonction d'onde = probabilité de trouver la particule

ONDE OU PARTICULE ?

Alors, la lumière, onde ou particule ?

Onde c'est une évidence, les figures d'interférences ne laissent aucune place au doute. Mais, particule c'est une certitude, comment la lumière traverserait-elle le vide ?

Pour expliquer le transport d'une onde lumineuse dans le vide, on a bien tenté « l'éther luminifère », matière étrange aux propriétés contradictoires qui vibrerait avec la lumière à la manière de l'air transportant le son. Hélas, ni l'expérimentation ni la théorie n'ont pu conforter l'hypothèse qui sera laminée par Einstein.

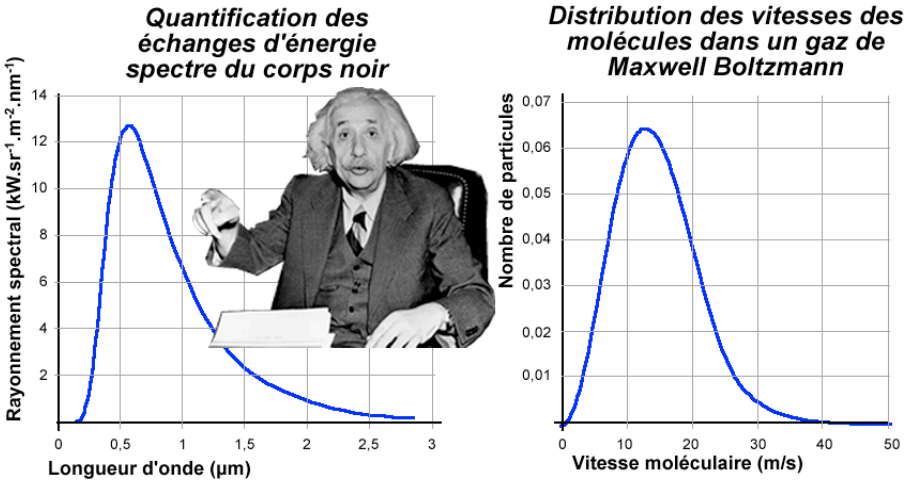
Au XVII^{ème} siècle, duel entre Isaac Newton, particule, et Christiaan Huygens, onde : Newton vainqueur. La notoriété du génie anglais qui avait dominé les planètes et leurs trajectoires eut raison du génie néerlandais. La particule ne souffrira nulle contestation durant le siècle des lumières.

Début XIX^{ème}, Thomas Young et Augustin Fresnel réhabilitent Huygens en faisant interférer des ondes lumineuses. Hors de portée de l'emprise de Newton parce qu'autodidacte, le britannique Michael Faraday innove en introduisant le concept nouveau mais riche de champ. Son

compatriote James Maxwell enfonce le clou au cours de ce même siècle avec un jeu d'équations de propagation des ondes électromagnétiques. L'onde est là.

Puis en quelques années tout est bouleversé, ponctué par une avalanche de prix Nobel.

Nouveau génie, nouveau revirement tout début XX^{ème}. Le grand Albert est intrigué par la similitude entre le spectre des corps noirs et la distribution des vitesses des molécules dans un gaz : « *on est conduit à se demander si les lois de la production et de la transformation de la lumière n'ont pas également la même structure que si la lumière était constituée de quanta d'énergie de ce type* ».



Prémonition géniale : la lumière est particule. Il explique ainsi l'effet photo électrique en s'appuyant sur la toute nouvelle constante « h » issue des calculs menés par Max Planck sur le rayonnement du corps noir. Einstein cite en outre dans son article de 1905 (« *Un point de vue heuristique concernant la production et la transformation de la lumière* ») l'expérimentateur Philipp von Lenard qui avait constaté dès 1880 que la quantité de charges expulsées par un rayon lumineux dépend de sa couleur (sa fréquence, donc) et qu'une fréquence minimum est nécessaire. Après un début cordial, les relations entre Einstein et von Lenard se dégradent, le nationalisme de von Lenard s'accordant mal avec le pacifisme d'Einstein.

Oui mais … comment expliquer les si belles figures d'interférence indissociables des ondes ?

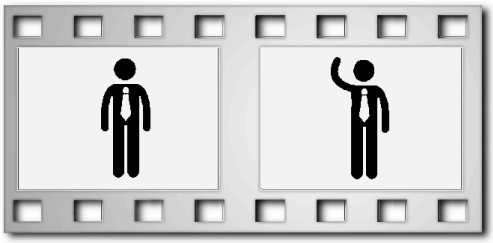
1924 : après une licence d'histoire, le français Louis de Broglie (prononçons « de Breuil ») obtient sa thèse de doctorat en sciences en étendant l'einsteinien concept de dualité onde corpuscule de la lumière à tout corpuscule, ce que Davisson et Germer confirmeront trois ans plus tard lors des expériences de diffraction de l'électron par des cristaux. Après les électrons, les neutrons, les atomes et même les molécules offrent le spectacle de la diffraction.

Les ondes de Louis de Broglie sont mises non pas en musique mais en mathématique par deux approches indépendantes. Werner Heisenberg et Erwin Schrödinger partent de deux modèles différents dont le formalisme sera consolidé par Paul Dirac. Le pas est franchi, les mathématiques deviennent l'unique approche de la mécanique quantique.

Max Born ouvre alors une voie pour l'interprétation de la mécanique quantique en reliant la fonction d'onde avec la probabilité de présence : le carré de la fonction d'onde indique une densité de probabilité de présence en chaque point. Richard Feynman développera les outils pour exploiter ces fonctions.

Peut-être est-ce le poids grandissant des mathématiques dans la physique qui troublait Einstein : « *ce qui est incompréhensible, c'est que le monde soit compréhensible* ».

On constate qu'entre deux interactions, la position d'une particule n'est pas déterminée. L'indétermination structure l'état quantique de la matière. On ne sait pas où elle est physiquement car seule une représentation mathématique rend effectivement compte de son comportement. La dualité vient de particules dont la probabilité de présence est ondulatoire.



S'il est un domaine où il faut se méfier des images et des analogies, c'est bien celui de la mécanique quantique. Cela dit, une question stupide me revient régulièrement à l'esprit : si l'image d'un film me montre un personnage bras baissé puis la suivante le bras levé je vois quelqu'un qui lève la main. Et pourtant, qui me prouve qu'entre ces deux images le personnage ne s'est pas gratté la joue ou frotté les yeux ? Pourquoi n'aurait-il pas chassé une mouche ? Questions sans réponse et là aussi c'est indéterminé.

Impossible donc de statuer : onde ou corpuscule ? Les deux ? De quoi la matière est-elle le nom ?

- ONDULATOIRE pendant la phase quantique. Isolées, les particules sont sous le régime de l'indétermination et toutes les possibilités sont superposées. Mathématiquement une fonction dite fonction d'onde donne accès à leur probabilité d'occurrence. Cette fonction est ondulatoire.
- CORPUSCULAIRE lors de la phase classique. Les interactions avec d'autres particules réduisent l'éventail des possibilités pour aboutir à une certitude. La matière devient matière.

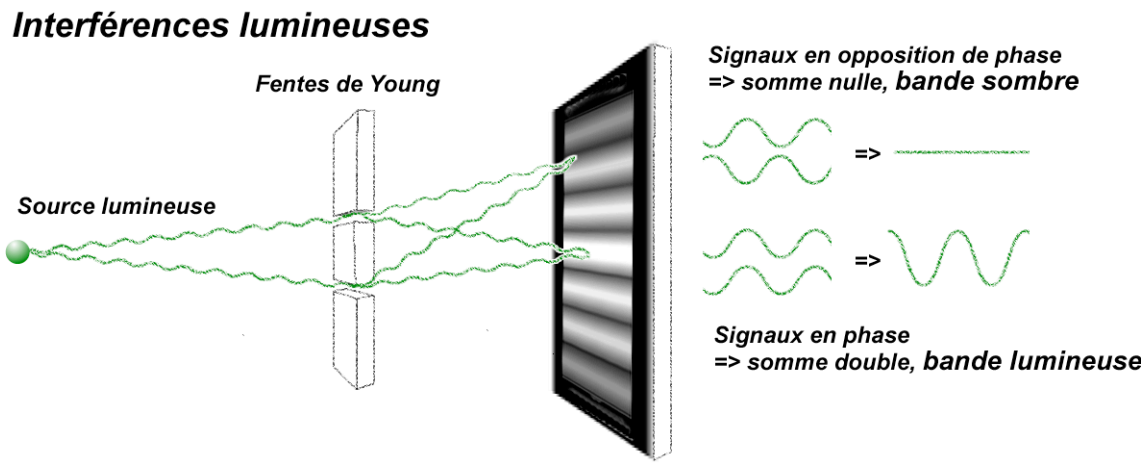
Les particules n'ont la forme que l'on perçoit au niveau macroscopique que lorsqu'elles sont observées, ou plus globalement qu'après interaction avec d'autres particules. En raccourci provocateur : une particule n'existe que quand on la regarde.

Examinons la dualité onde particule sous l'éclairage des expériences d'interférences.

INTERFERENCES

Cette expérience, réalisée en 1801 par Thomas Young met en évidence la nature ondulatoire de la lumière en faisant interférer deux rayons lumineux. Mais fait troublant, on obtiendra près de deux siècles plus tard le même résultat en envoyant non pas des ondes mais des particules une par une. Les particules interfèrent avec elles-mêmes.

La manipulation nécessite deux sources de lumière parfaitement similaires que l'on construit à partir d'une source lumineuse monochrome envoyée sur deux fentes.

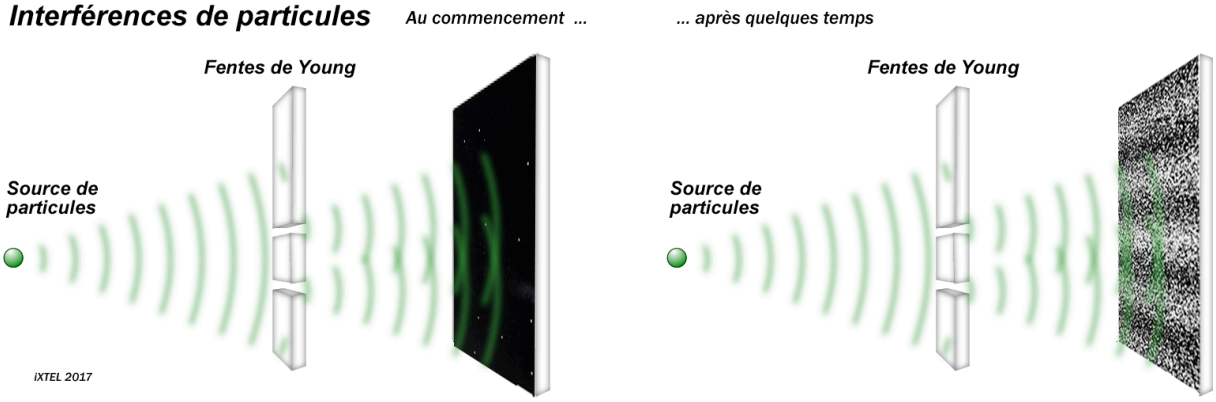


Les deux faisceaux lumineux se combinent sur un écran disposé derrière ces fentes.

- Les longueurs des trajets et donc les temps mis par chacun des faisceaux diffèrent suivant le point d'impact sur l'écran, la position symétrique de la source faisant figure d'exception avec deux trajets de longueurs identiques.
- La somme des faisceaux en chacun des points dépend de la position relative des deux signaux. En phase ils vont doubler d'amplitude, en opposition ils vont s'annuler. Le résultat est une alternance de bandes claires et sombres.

Si on ferme l'une ou l'autre des fentes, les figures disparaissent. Nous avons là la signature d'une onde.

La situation devient totalement déstabilisante dès que l'on remplace le faisceau lumineux par des jets de particules envoyées les unes après les autres.



Notons qu'envoyer les photons un par un a longtemps relevé de l'expérience de pensée et que ce n'est que dans les années 1980 que le physicien français Philippe Grangier y est parvenu à Orsay.

De prime abord, la tentation est forte d'assimiler l'envoi de photons et celui de balles de tennis. On s'attend à voir deux fortes concentrations d'impacts au regard des fentes. Sauf que peu

à peu les intrigantes figures d'interférence se dessinent, avec des bandes quasi vierges de tout impact et d'autres à forte concentration. Les figures disparaissent si on occulte une fente. Tout comme avec les faisceaux lumineux de Young en 1801. Bizarre, non ? Une particule (photon, électron, molécule) « sait » si il y a une ou deux fentes. Par abus, on entend souvent que la particule emprunte simultanément les deux chemins. L'image est à éviter car elle fait référence à la notion de trajectoire qui n'a pas de signification en physique quantique, indétermination oblige. Entre la source et l'écran il y a superposition des deux routes possibles.

Attardons-nous sur cette superposition qui nous sera tant utile pour les ordinateurs quantiques.

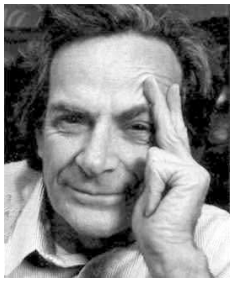
SUPERPOSITION

La superposition décrit cet état défiant l'intuition entre deux mesures, observations ou plus largement interactions. On est alors dans l'incapacité de préciser les paramètres (spin, position, quantité de mouvement etc.) d'une particule. La cause n'est pas à chercher dans quelque faiblesse voire incertitude de nos méthodes d'observation : la particule n'est alors plus physiquement définie. Son état est indéterminé.

Abandonnons toute représentation physique de la particule pendant la superposition. Le plus « raisonnable » est de considérer que la particule n'a plus d'existence physique durant cette période et qu'il lui faut laisser la place à une représentation mathématique : un vecteur décrivant un champ dans un espace mathématique, l'espace de Hilbert. Chaque vecteur est lui-même somme de vecteurs représentant chacun les différentes possibilités des valeurs que peuvent prendre les paramètres (spin, position, quantité de mouvement etc.). Il permet de calculer les probabilités d'occurrence de chacun des états. Cette fonction mathématique est une onde qui s'étale dans tout l'espace, la fonction d'onde de Schrödinger. L'état d'un système quantique est mathématiquement décrit par une somme infinie de vecteurs dont le physicien Richard Feynman à l'origine de l'électrodynamique quantique a édifié les règles de calcul.

Lors de la superposition, toutes les possibilités sont empilées, mais attention : pas mélangées. Ce ne sont pas deux liquides qui se fondent en un seul. Si les valeurs « 7 » et « 9 » sont envisagées, ce n'est nullement pour prendre « 8 » comme résultat. On a une certaine probabilité d'obtenir « 7 », une autre d'obtenir « 9 ».

Au cours de cette phase de superposition les expressions telles « un photon passe par les deux fentes » ou « le chat est à la fois mort et vivant » n'ont de fait pas de signification puisque trajectoires comme états sont indéterminés. Il est d'ailleurs préférable de parler d'indétermination plutôt que d'incertitude, ce dernier terme pouvant évoquer à tort un problème de méthode de mesure. Heisenberg a utilisé « incertitude » dans un tout premier temps puis s'est ravisé avec « indétermination ». Trop tard : les traductions françaises avaient déjà gravé l'incertitude dans le marbre. Mais rassurez-vous, après moult débats les plus grands physiciens n'ont pas réellement convergé une terminologie unique.



La méthode de calcul du génial professeur Feynman permet de déterminer la probabilité d'avoir un impact en chaque point sur l'écran en fonction des deux routes possibles. La valeur de cette probabilité suit une courbe sinusoïdale qui est précisément celle de l'onde observée par

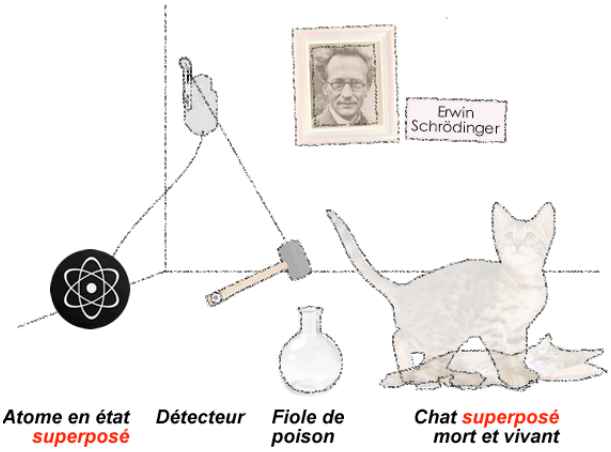
Thomas Young. Voilà une forme de réponse à la question onde ou particule : la lumière est une particule dont la probabilité de présence épouse une onde.

Allons plus loin sur ce parcours quantique vertigineux : le calcul est d'autant plus précis que la fonction d'onde incorpore l'intégralité des chemins possibles. Pour trouver les treize chiffres significatifs du moment magnétique de l'électron, il a fallu envisager des chemins … qui remontent le temps ! Tous ces mécanismes sont décrits avec humour et clarté dans « Lumière et matière » de Richard Feynman. Si vous ne voulez lire qu'un seul livre sur la mécanique quantique, c'est lui qu'il faut choisir.

La phase quantique est cet état d'indétermination où toutes les possibilités sont superposées. Les calculateurs quantiques s'appuient sur la superposition pour manier en un seul calcul toutes les valeurs que peut prendre une variable.

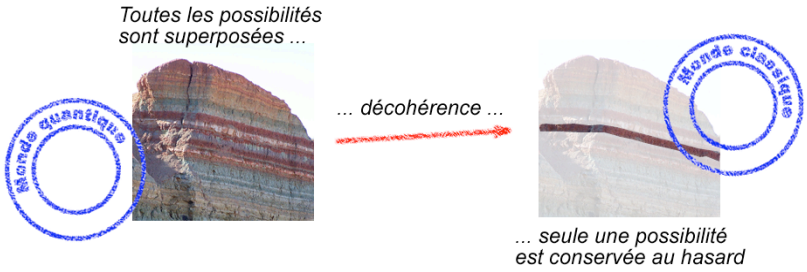
DÉCOHÉRENCE

Le passage de la superposition à l'état macroscopique relève du même registre un peu fou. Dès qu'il y a interaction, typiquement lors d'une mesure, la particule rejoint notre monde classique et prend aléatoirement une valeur parmi celles proposées dans la fonction d'onde. L'histoire de la particule auparavant est alors totalement perdue. La situation est la suivante : une particule « n'existe » que quand on la mesure, ou plus largement quand il y a interaction. Vertigineux.

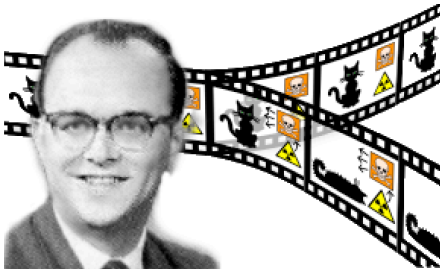


Pour souligner avec humour l'absurdité de la chose, Erwin Schrödinger a mis en scène un chat dans sa fameuse expérience de pensée. Le but est d'appliquer le comportement d'une particule superposée à un être macroscopique pour tenter de montrer la non complétude de la mécanique quantique. Le sort du chat (mort ou vivant) dépend d'une particule en superposition de deux états dont l'un déclenche un mécanisme fatal pour le chat car constitué d'un marteau qui brise une fiole de gaz mortel. Schrödinger expose une situation burlesque où la superposition en deux états indéterminés s'applique au chat pour une superposition mort / vivant.

Le message de Schrödinger est là pour souligner qu'à son sens la mécanique quantique n'est pas complète et ne représente pas totalement la réalité, point de vue soutenu également par Einstein. Mais son trait d'humour est depuis des décennies traité avec sérieux et gravité. « *Quand j'entends 'Chat de Schrödinger', je sors mon revolver* » nous prévient Stephen Hawking dans son approche positiviste pour qui il est vain de tenter de décrire la réalité depuis les équations quantiques, leur seul but étant la prédiction des résultats. La fonction d'onde décrit non pas la réalité mais la connaissance que nous en avons. L'état mort/vivant du chat n'a pas de réalité et ne peut être l'objet de discussion.



La théorie de la décohérence nie également la possibilité de poursuivre la superposition à l'état macroscopique. La superposition d'états ne peut exister puisque les interactions inéluctables avec les particules d'un objet macroscopique nous conduisent immédiatement à un état classique. La théorie, soutenue par des personnalités comme le prix Nobel Murray Gell-Mann est considérée comme la plus complète à ce jour pour expliquer la transition quantique / classique. Serge Haroche a reçu son prix Nobel en 2012 pour les mesures réalisées sur les temps de décohérence.



Pour Hugh Everett, il se crée autant d'univers qu'il y a d'états superposés. Pour Eugène Wigner c'est la conscience qui dicte l'état dans lequel se stabilise la particule. D'autres interprétations existent mais les physiciens pragmatiques tiennent le choc en considérant que la mécanique quantique ne concerne que les particules prises individuellement et ignore les chats macroscopiques.

Notons qu'à mon sens le calcul tel qu'il est appliqué par Richard Feynman donne une réponse immédiate à la question du passage de l'état de superposition à l'état classique (réduction du paquet d'onde) : le calcul nous donne une probabilité de présence en fonction de tous les chemins possibles. Lorsque le nombre de chemins possibles diminue, la probabilité d'occurrence de chacun augmente. Quand enfin les interactions sont si nombreuses qu'elles ne laissent qu'un seul chemin possible la probabilité devient une certitude. Le monde classique n'est autre que le monde quantique avec une probabilité de « 1 ». C'est le cas avec les objets macroscopiques et nous retrouvons là la théorie de la décohérence. Là encore, bravo Monsieur Feynman.

Le vocabulaire consacre l'expression « réduction du paquet d'onde » quand on ne considère qu'une particule et l'expression « décohérence » quand on s'adresse à un objet macroscopique. La décohérence est la difficulté majeure des ordinateurs quantiques.

Pour faire court

- *La décohérence est la transition entre le monde de l'indétermination et le monde classique macroscopique due aux multiples interactions entre les multiples particules.*
- *Seule une valeur de paramètre (spin, position, quantité de mouvement etc.) est retenue au hasard parmi celles superposées dans la fonction d'onde.*

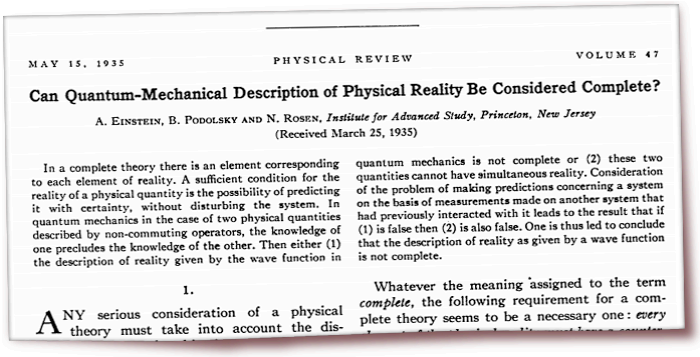
Accrochez-vous, nous ne sommes pas au bout de l'absurde et plongeons dans l'intrication en introduisant une deuxième particule dans nos considérations.

INTRICATION

Les particules partagent des paramètres communs dès qu'elles interagissent. C'est l'intrication. Le spin par exemple peut prendre deux valeurs complémentaires, +1 et -1. Quand deux particules interagissent elles vont partager ces deux valeurs. Elles sont unies sous le régime de la non-séparabilité. L'indétermination s'applique au couple intriqué et avant mesure la valeur de chacun n'est pas décidée. Les deux états sont superposés. L'affectation des valeurs +1 et -1 pour chacune des deux particules se fera au hasard lors d'une mesure de l'une des deux. L'autre prendra immédiatement la valeur complémentaire, et ce quelle que soit la distance les séparant. Notons que ces deux propriétés, aléa et non-séparabilité, siéent pleinement à la cryptographie symétrique.

Cette couleuvre a fait déborder le vase du Grand Albert, le pilier des deux révolutions – relativité et mécanique quantique - du vingtième siècle. Il n'a jamais pu admettre que le hasard se mêlât de la physique. Lancer une pièce à pile ou face donne un résultat aléatoire, mais si les conditions initiales sont connues avec précision alors le résultat devient prédictible. Pour Einstein, la mécanique quantique ne peut déroger à la règle, au rebours des affirmations du physicien Niels Bohr. Un spin ne se décide pas au hasard. Il existe quelque part des variables cachées car « Dieu ne joue pas aux dés ». Notons qu'Einstein ne remettait absolument pas en cause la mécanique quantique. Il en était un pilier majeur. Le seul point qui le dérangeait était cette intrusion du hasard. Les particules sont de connivence grâce à des variables cachées. Pour de Broglie, Bohm ou Bell la position de la particule serait un bon candidat pour ce type de variable.

Albert Einstein, Boris Podolsky et Nathan Rosen imaginent en 1935 une expérience de pensée, le paradoxe EPR. Peut-on considérer que la physique quantique est complète sans les variables cachées ? Ce court papier, quatre pages, est un de ceux qui est le plus souvent cité en référence alors que curieusement il n'en contenait pas lui-même. Pour montrer que le hasard ne peut décider d'un paramètre, EPR considère deux particules intriquées. L'une aura un spin +1 et l'autre -1. Si hasard il y a, la mesure de l'une devra immédiatement se répercuter sur l'autre. L'éloignement des deux particules intriquées étant arbitraire, on peut aboutir à une vitesse de transport de l'information qui outrepasserait la vitesse de la lumière. Einstein est le mieux placé pour affirmer que ça ne se fait pas. Les deux particules doivent s'être mises d'accord au préalable à l'aide de variables aujourd'hui cachées. Face à la clarté de l'argumentation EPR, la réponse de Bohr apparait beaucoup plus délicate à appréhender.



MAY 15, 1935 PHYSICAL REVIEW VOLUME 47

Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?

A. EINSTEIN, B. PODOLSKY AND N. ROSEN, *Institute for Advanced Study, Princeton, New Jersey*
(Received March 25, 1935)

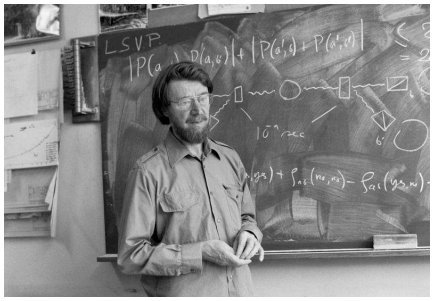
In a complete theory there is an element corresponding to each element of reality. A sufficient condition for the reality of a physical quantity is the possibility of predicting it with certainty, without disturbing the system. In quantum mechanics in the case of two physical quantities described by non-commuting operators, the knowledge of one precludes the knowledge of the other. Then either (1) the description of reality given by the wave function in quantum mechanics is not complete or (2) these two quantities cannot have simultaneous reality. Consideration of the problem of making predictions concerning a system on the basis of measurements made on another system that had previously interacted with it leads to the result that if (1) is false then (2) is also false. One is thus led to conclude that the description of reality as given by a wave function is not complete.

1.

ANY serious consideration of a physical theory must take into account the dis-

Whatever the meaning assigned to the term *complete*, the following requirement for a complete theory seems to be a necessary one: *every*

La suite infirmera EPR, l'expérience de pensée sera contredite par l'expérience réelle.



En 1964, le physicien irlandais John Stewart Bell traduit à partir de la théorie des ensembles l'expérience de pensée d'EPR en une inégalité mathématique. Si cette inégalité est violée alors il y a action instantanée à distance quelle que soit la distance. Pour Bell, c'était le moyen pour prouver qu'Einstein avait raison, qu'il n'y avait pas d'action à distance et qu'il fallait continuer les recherches pour débusquer des variables (position ?) cachées. L'inéquation a ouvert la porte aux expérimentations pour statuer sur la question fondamentale : est-ce que la valeur d'un paramètre (spin, position, quantité de mouvement etc.) est choisie au hasard lors de la mesure ou préexiste ? Quand un radar vous indique que vous roulez à 132 km/h on peut raisonnablement penser que vous étiez déjà à cette même vitesse l'instant d'avant. Une particule mesurée à 1000 km/s était-elle à cette vitesse juste avant la mesure ou cette vitesse était-elle non déterminée ?

On doit au français Alain Aspect la fructueuse mise en œuvre pratique de ces expériences en 1982 dans les laboratoires d'optique d'Orsay. La conclusion est implacable : Einstein, Podolsky et Rosen se sont trompés. Il n'y a pas de variables cachées. Ou alors elles sont globales. C'est bel et bien lors de la mesure que se détermine la valeur des paramètres. Dieu joue aux dés, et la mécanique quantique se joue de l'espace.

Désarçonné, Bell en bon disciple d'Einstein a entamé des recherches sur la base d'une sorte d'ether avec un temps absolu. Hélas ce génie est parti trop tôt pour aboutir à un résultat. Trop tôt également pour recevoir le prix Nobel. Ne tardons pas trop pour l'attribuer au toujours jeune Alain Aspect : il a quand même trouvé la réponse à la question soulevée par Einstein !

Notons qu'en 2006 d'autres expériences conduites elles aussi en France laissent à penser que la mécanique quantique se joue également du temps. Dans quel monde ne vivons-nous pas …

Cela dit et à mon sens, les notions d'intrication ou de non-séparabilité ne sont pas si choquantes dans une théorie bâtie sur des champs, tels que l'union entre la mécanique quantique et la relativité restreinte nous l'impose.

Résumons l'intrication.

- *Deux particules sont intriquées lorsqu'après avoir interagi elles partagent un (ou plus) paramètre commun. Il y a non-séparabilité.*
- *Ce paramètre est indéterminé jusqu'à ce qu'il y ait « mesure » sur une des deux particules et ce quelle que soit la distance entre les deux particules.*
- *Transmission à **distance** et valeurs **aléatoires** sont des atouts pour la cryptologie.*

Munis de ces éléments nous pouvons aborder l'informatique quantique.

INFORMATIQUE QUANTIQUE

L'ordinateur quantique est annoncé comme une technologie à même d'assurer la continuité de la loi de Moore, avec l'Intelligence Artificielle en ligne de mire. On annonce de grandes avancées pour cette année 2017. Depuis plus de dix ans les circuits silicium des ordinateurs classiques se frottent aux frontières du trop petit et les puces multi-cœurs pallient l'impossible poursuite de la miniaturisation des gravures. Le quantique sera-t-il le relai ?

Donnons tout de suite la réponse, c'est non. La technologie n'est pas au rendez-vous. Non que la faisabilité soit en cause : la physique l'autorise, ça devrait le faire tôt ou tard. Mais le savoir-faire technologique dans ce monde étrange ne fait que balbutier et la perspective de la maîtrise des algorithmes les plus complexes (problème NP-complets) n'est pas encore acquise. Il y a du boulot tant sur les aspects matériel qu'algorithmique.

Sémantiquement, l'appellation « ordinateur quantique » elle-même porte à discussion. Faire tourner un programme spécifique sur une machine générique est l'essence même des ordinateurs classiques ; les ordinateurs quantiques d'aujourd'hui sont des calculateurs spécifiques nantis de portes logiques pour intégrer un algorithme dédié. La programmation n'est pas à l'ordre du jour et le terme calculateur quantique est plus approprié que celui d'ordinateur quantique. Cela dit, nous utiliserons indifféremment les deux termes dans la suite de ce papier.

Quant aux performances alléchantes, elles sont attendues mais un avantage clair face aux ordinateurs classiques reste à confirmer. Les affirmations parues dans la presse sur la suprématie quantique faussent un peu la question en requérant des ordinateurs classiques une démarche identique à celle des calculateurs quantiques. Ainsi, demander à un ordinateur classique de multiplier n x p en pratiquant p additions du nombre n comme en mécanique quantique n'a pas grande signification. Les victoires annoncées aujourd'hui de la mécanique quantique portent sur des problèmes que l'informatique classique résout plus rapidement avec ses méthodes.

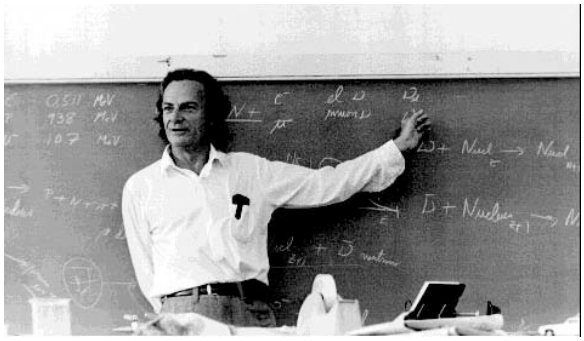
La cryptanalyse est doublement intéressée par le monde quantique : d'une part les calculateurs pourraient venir à bout des factorisations et d'autre part la superposition alliée à intrication offrent à la fois vrai aléatoire et transmission confidentielle de clef pour le chiffrement symétrique. Ce dernier point ne relève pas des ordinateurs quantiques mais de l'utilisation des caractéristiques du monde quantique.

En parallélisant massivement les calculs, le modèle théorique des ordinateurs quantiques rend linéaires des problèmes qui étaient exponentiels dans l'informatique classique. Le gain en puissance promet d'être substantiel. Mais quel est calendrier pour le passage à la pratique ? Arriverons-nous à étendre les lois du microscopique à un monde bien proche du macroscopique ?

Penchons-nous pour commencer sur la mécanique de ces calculateurs.

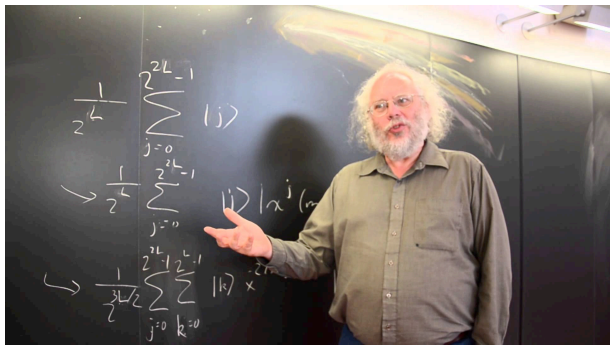
CALCULONS QUANTIQUE

Les travaux du physicien Paul Benioff de l'*Argonne National Labs* en 1981 mettent le pied sur le terrain de l'ordinateur quantique en imaginant un ordinateur classique qui exploiterait certains phénomènes quantiques.



Le grand physicien Richard Feynman, père de l'électrodynamique quantique se heurtait en 1982 à la résolution d'équations de fonctions d'onde des particules pour laquelle l'intégrale des chemins possibles pour aller d'un point à l'autre doit être analysée. La complexité n'a pas de limite : il faut tenir compte des trajectoires remontant le temps pour gagner quelques décimales ! L'ordinateur est incontournable dans ces recherches mais avec des limites trop tôt atteintes. Fin connaisseur du principe de superposition de la mécanique quantique, Richard Feynman a bien vite saisi le parti à en tirer pour bénéficier d'un parallélisme massif. « *Au lieu de nous plaindre que la simulation des phénomènes quantiques demande des puissances énormes à nos ordinateurs actuels, utilisons la puissance de calcul des phénomènes quantiques pour faire plus puissant que nos ordinateurs actuels* ». C'est pour des besoins en simulation de physique quantique qu'a émergé le concept d'ordinateur quantique.

Avancée notable, David Deutsch de l'Université d'Oxford publie en 1984 un papier sur l'architecture d'un ordinateur ne reposant que sur les règles de la mécanique quantique. Les bases sont jetées, l'ordinateur quantique est possible.



L'engouement décisif – comprendre l'intérêt et les moyens financiers - sera lancé par le mathématicien Peter Shor en 1994 avec un algorithme pour ordinateur quantique capable de s'attaquer à la factorisation de grands nombres. Menace de poids pour la cryptographie ! Depuis industrie, universités, grands laboratoires et autres Gafam's parcourent à grand pas décidés l'univers de l'indétermination. Ça tâtonne : les résultats sont là et ne sont pas là, comme un hommage au chat mort et vivant.

Bon cela étant posé, il y a de quoi être intrigué (intriqué ?) : comment peut-on prétendre construire un ordinateur à partir d'un processus dont les réponses sont le fruit du hasard ? Plongeons dans cette informatique qui impose des raisonnements qui n'ont rien à voir avec ceux auxquels on est familier, bannissons nos intuitions. Disruptons.

QUANTIQUE ET ORDINATEUR

Le principe de superposition sur lequel est construite la mécanique quantique précise qu'entre deux interactions une particule quitte son statut « classique » pour entrer dans le domaine quantique des ondes de probabilité. Elle ne retrouve le statut « classique » que lors d'une nou-

velle interaction. En quelque sorte, une particule « n'existe » que quand on l'observe. En prenant l'exemple du déplacement d'un photon, on peut préciser le lieu de départ, celui de l'arrivée mais point de trajectoire entre les deux.

Toutes les routes imaginables sont prises en compte dans une fonction mathématique nommée fonction d'onde. Cette fonction ondulatoire permet de déterminer la probabilité de présence en tout point. Mais attention : on ne fait pas la moyenne de ces possibilités comme on pourrait mélanger des liquides mais on superpose toutes les possibilités. Au moment de la lecture une seule possibilité est retenue parmi toutes. Au hasard. Les autres sont oubliées. Le résultat qui nous intéresse est noyé parmi tous les résultats. Superposés. Avec de nouveau le hasard pour la lecture. Donc … que faire d'un résultat aléatoire ?

Notons que toutes les possibilités « listées » dans la fonction d'onde ne bénéficient pas de la même fortune. Le calcul quantique joue sur des pondérations pour favoriser les « bons » résultats par une probabilité plus élevée.

D'une manière générale on n'a pas le choix, il faut faire avec l'aléatoire. Dieu joue aux dés. Dans la recherche des facteurs premiers d'un grand nombre par exemple, on n'est pas sûr que la valeur obtenue soit correcte. C'est probable mais le résultat n'est validé qu'après avoir été effectivement vérifié avec ledit grand nombre sur une machine classique. Si ce n'est pas le cas on réitère le calcul jusqu'au tirage du bon résultat. On n'a en effet pas de deuxième chance en piochant de nouveau dans les états superposés car ils ont été détruits par la lecture, effondrement de la fonction d'onde oblige.

Les chemins du calcul quantique sont fidèles à l'étrangeté du monde quantique et tellement en opposition avec nos approches familières en informatique classique.

QUBIT

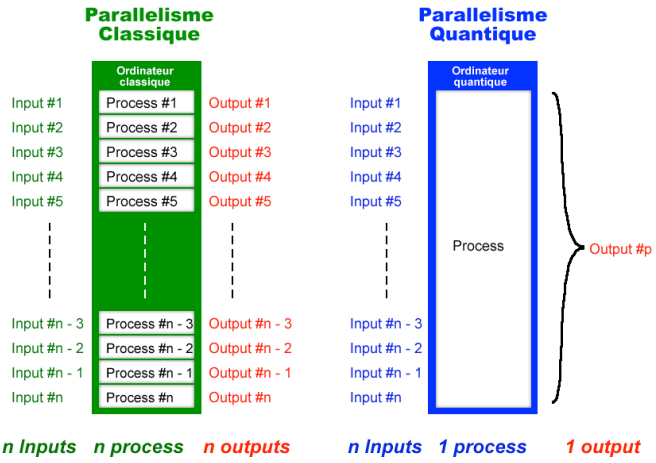
La coutume a légué à nos civilisation la base dix, héritage du dénombrement sur le bout de nos doigts. L'ordinateur classique utilise la base deux, le courant passe ou pas. Le bit informatique prend les valeurs « 0 » ou « 1 », et en juxtaposant quatre bits dans un registre on peut représenter un nombre compris entre zéro et quinze.

Dans le monde quantique, on utilise également un système à deux états grâce à des propriétés physiques comme le spin par exemple, tout comme dans un ordinateur classique. Sauf que le monde quantique vient avec sa part d'étrangeté : le qubit, ainsi nomme-t-on le bit quantique, peut prendre **à la fois** les valeurs zéro et un. C'est la magie du principe de superposition.

Un exemple classique illustre le bénéfice de la superposition par la mise en scène un joueur indélicat au jeu de pile ou face : il utilise des pièces truquées avec la même figure des deux côtés.

En mécanique classique, il faut faire deux lectures pour s'assurer que la pièce est non truquée, alors que la superposition quantique nous renseigne en une passe unique. Le gain est de deux. Avec quatre qubits, on obtient tout comme en informatique classique seize valeurs sauf qu'ici on manipule simultanément tous les nombres compris entre zéro et quinze. Bizarre, non ? Mais surtout très puissant car avec cent qubits on peut faire un calcul sur deux puissance cent valeurs en une seule passe. C'est massivement parallèle.

Tempérons néanmoins notre enthousiasme : le parallélisme utilisé n'est pas celui de l'informatique classique où le travail est découpé et réparti judicieusement entre des machines qui exécutent chacune une tâche spécifique et délivrent chacune un résultat dédié. Les calculateurs quantiques n'appliquent qu'un seul et même traitement à toutes les variables et n'obtiennent qu'un résultat unique pour tous.



Les calculs massivement parallèles, aujourd'hui identifiés comme domaine de prédilection de l'informatique quantique, font appel à un mode de fonctionnement sans grand rapport avec notre monde classique. Performances comme domaines d'application restent à être évalués.

QU'EST DEVENU LE « COPIER/COLLER » ?

Notons une conséquence majeure du principe de lecture : l'adieu à la fonction « Copier ». En 1982, Wootters, Zurek, et Dieks énoncent le théorème de non-clonage quantique.

Une variable quantique est un état de superposition de toutes les valeurs possibles. À la moindre lecture, seule une valeur est retenue, les autres sont oubliées. Ce qui réduit à néant tout espoir de faire un « Copier » d'une variable. Il n'y a pas de clonage possible. On ne peut pas affecter à la variable « b » la valeur de la variable « a ». La variable « a » serait immédiatement réduite à une valeur unique piochée au hasard dans toutes celles proposées par la superposition. De nouveau, le calcul quantique est aussi déroutant que la mécanique du même nom, là encore les algorithmes quantiques sont spécifiques. On ne peut pas « porter » une application classique. Excel pour QuanticOS n'est pas encore d'actualité. Ah oui, il y a encore du boulot.

Cela dit, si le quantique exclut le « copier » il autorise une variante de « coller » sous la forme d'une reconstruction du même état du qubit à distance. C'est la téléportation aux riches applications en perspective, à commencer par la régénération d'un signal.

DÉCOHÉRENCE

Nous touchons là *le* grand défi de l'ordinateur quantique qui est de maîtriser le passage intempestif de l'état quantique à l'état classique.

Dans le monde quantique, on fait des sauts de puce entre les mesures, lectures ou plus globalement entre les interactions. Entre deux interactions on est dans cet état magique de superposition où le calculateur calcule. A chaque interaction on efface la superposition pour ne garder qu'une valeur. Le passage de la superposition quantique à la structure classique est la décohérence.

L'opération est volontaire lors de la lecture ou accidentelle lorsqu'elle est provoquée par des perturbations comme des vibrations ou de la lumière. Le physicien français Serge Haroche a reçu le prix Nobel 2012 pour ses travaux sur la décohérence du photon grâce à des pièges à photons construits avec des miroirs. La décohérence survient en un temps inversement proportionnel au nombre de particules.

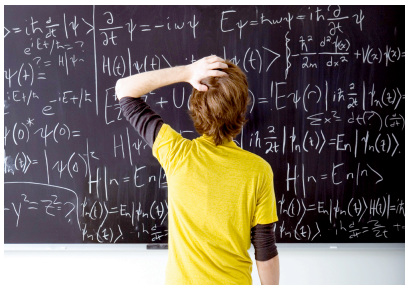
L'enjeu est de rester quantique un temps suffisamment long pour avoir le temps de calculer. Les particules doivent être à l'abri de toute perturbation, d'où des températures de fonctionnement très très basses. Pas loin du zéro absolu, cet état où tout mouvement est arrêté. Isolation maximum certes, mais il faut quand même cohabiter avec d'autres qubits et franchir des portes logiques. Le « passage à l'échelle » est particulièrement délicat. On sait de nos jours manipuler des registres d'une (grosse ?) dizaine de qubits, mais guère plus.

Ingénieurs et savants ne sont pas restés les deux pieds dans le même qubit et ont élaboré un mécanisme de calcul d'erreur qui devrait repousser les limites. La décohérence se traduit par des erreurs de transmission. Les télécoms confrontées à ce même obstacle ont depuis longtemps su user des mathématiques pour maîtriser le haut-débit. Le savoir-faire en calcul et correction d'erreurs a été mis à profit ; les résultats sont spectaculaires. Le problème est que pour protéger un qubit, on a besoin de plusieurs qubits. Qu'il faut protéger, cela va de soit. La science est trop récente pour chiffrer de manière fiable ce surplus mais comptez dix à quinze qubits redondants par qubit utile dans le contexte de registres d'une dizaine de qubits utiles. Le point est d'autant plus critique que ces calculs d'erreurs ne peuvent aboutir que si au départ le taux d'erreur est suffisamment faible, condition s'accommodant mal de l'augmentation du nombre de qubits. La factorisation par exemple est d'une exigence redoutable sous peine d'une dérive rapide. Qu'en sera-t-il avec des mots d'une centaine de qubits ? Saura-t-on gérer des particules en état de superposition par milliers ? J'insiste, il y a du boulot.

ALGORITHME DE SHOR

Voici juste quelques considérations sur l'application phare qui fait trembler la cryptographie.

Peter Shor, spécialiste du calcul quantique est un mathématicien américain. Il s'est penché sur la factorisation de grands nombres, et en a tiré une méthode polynomial de calcul. Polynomial ? La complexité croît linéairement avec la taille du nombre alors qu'elle était exponentielle en informatique classique. La question représente un intérêt majeur pour le fonctionnement d'Internet : c'est sur la difficulté de factoriser que repose le secret des transactions.



Voyons les performances des calculateurs classiques. Le 12 décembre 2009, après deux ans de travaux une solide équipe de treize mathématiciens et cryptologues menée par Thorsten Kleinjung a extrait avec succès les facteurs premiers d'un nombre formé de deux cent trente deux chiffres après avoir fait tourner quatre-vingt processeurs classiques pendant six mois *(Factorization of a 768-bit RSA modulus, version 1.4, February 18, 2010).* Beaucoup de chiffres dans une simple phrase dont le seul but est d'illustrer l'énormité de la tâche. Les clefs RSA utilisées en cryptographie font au moins 1024 bits, la valeur 2048 bits étant recommandée par l'ANSSI pour demeurer à l'abri d'une factorisation par des ordinateurs classiques. En pratique, la complexité des meilleurs algorithmes à ce jour épouse une exponentielle fonction du nombre de bits, plus précisément deux à la puissance racine cubique du nombre de bits. Les secrets sont bien préservés sous la protection des nombres premiers.

Avec un calculateur quantique, les calculs sont plus légers car toutes les opérations sont menées simultanément. D'exponentielle, la complexité devient linéaire : elle croît avec le double du nombre de bits suivant l'algorithme de Shor, des optimisations par recyclage de qubits permettant encore de réduire ce nombre. En 2012, 21 a été factorisé avec huit qubits. La factorisation d'un nombre de 2048 bits ne prendrait qu'une petite centaine de secondes.

Cela étant posé, petit calcul : pour « casser » 2048 bits, il faut avec l'algorithme de Shor deux fois plus de qubits, soit 4096 qubits et probablement quelque cent millions de portes. Or le calcul d'erreurs pour pallier la décohérence est gourmand en qubits redondants, au minimum cinq ainsi que le mentionne le cours de Serge Haroche, mais apparemment le calculateur D-Wave 2X en demanderait un minimum de treize. Pour casser RSA ce sont plusieurs dizaines voire la centaine de milliers de qubits qu'il faut maîtriser. Ah oui quand même. Le chat de Schrödinger montre sa queue ! Ces valeurs sont (aujourd'hui …) d'autant plus inconcevables qu'il faut maintenir le tout en état de superposition suffisamment long (une centaine de secondes), alors que l'unité de temps de maintien de la superposition (aujourd'hui …) est plutôt la milliseconde. Il y a du boulot, vous dis-je. C'est sans appréhension que je continue à saisir mon code bancaire.

Relevons quand même le remarquable exploit de l'équipe de Nike Dattani de l'Université de Kyoto qui en novembre 2014 à partir de seulement quatre qubits a factorisé 56 153. Mais l'algorithme utilisé ne concerne que des séries de nombres spécifiques : 143, 56 153, 291 311, ce dernier sur six qubits étant attendu prochainement. Les succès pour quelques séries ne mettent pas en danger la factorisation utilisée en cryptologie.

RÉSUMONS-NOUS SUR QUELQUES POINTS …

– L'ordinateur quantique continuité de l'ordinateur classique ?

Non, l'ordinateur quantique ne se comporte pas comme un ordinateur classique. Les modes de traitement de l'information n'ont rien à voir avec nos logiciels. Seuls quelques domaines (simulation, optimisation, recherche de nombres premiers, base de données) sont aujourd'hui identifiés. La complémentarité des deux technologies dans des machines hybrides pourrait avoir un certain sens.

– L'ordinateur quantique pour demain ?

Non, et nous ne sommes pas près d'être prêts. Sur un plan matériel la décohérence se pose en obstacle majeur. Des pistes sérieuses de résolution existent, restent à les étendre à plusieurs centaines de qubits. Il reste par ailleurs à étoffer une panoplie des algorithmes aujourd'hui fort réduite.

- La décohérence est-elle insurmontable ?

Oui, à court terme. Physiquement la quantité d'interactions entre particules rend impensable l'utilisation de registres de taille suffisante pour construire une machine opérationnelle. Cela dit … la totalité des physiciens qui en 1920 élaboraient des expériences de pensée était persuadée que jamais on ne pourrait les réaliser.

Selon Schrödinger au début des années 1950 réussir à observer une particule unique relevait du fantasme et délivrerait des résultats absurdes. La suite lui a donné à moitié raison : de telles observations ont été réalisées et les résultats en ont confirmé l'absurdité. Alors, un jour peut-être ?

- Des concurrents pour l'ordinateur quantique ?

Oui, un certain nombre. Citons l'ordinateur à ADN qui s'appuie sur la biologie moléculaire en faisant travailler des enzymes ou l'ordinateur neuronal - sans aucun lien avec les réseaux neuronaux - construit autour de neurones biologiques. Mais nous ne disposons encore que de projets certes prometteurs mais non confirmés.

L'histoire n'est pas terminée, elle est en cours. Ce sera l'occasion de rééditer ce papier !

A PROPOS DE L'AUTEUR

Créateur de la société iXTEL société spécialisée en architecture de réseau et qualité de service auprès des opérateurs et de l'IUT-T, membre fondateur de Forum ATENA, intervenant dans diverses écoles d'ingénieurs dont le groupe Télécom, l'Université de Lille et l'Institut Léonard de Vinci, Jacques Baudron se penche sur l'impact des nouvelles plateformes reposant sur internet : blockchain, big data, Intelligence Artificielle, « bulles » des réseaux sociaux, informatique quantique … Il a organisé avec le Forum ATENA le colloque « La Blockchain a-t-elle les moyens de ses ambitions »

Autres publications et livres blancs :

- *WiMAX à l'usage des communications haut débit (collectif)*
- *La sécurité à l'usage des collectivités locales et territoriales (collectif)*
- *Mythes & Légendes des TIC (collectif)*
- *Intelligence Artificielle et innovation : possible ?*
- *Le transport de la synchronisation*
- *QoS*