Les promesses de l'informatique quantique

Catégorie : **Mundus Numericus**
Tags : **algorithme, cyberpolitique, futur, physique, technique**
Personnages : **Richard Feynman, Peter Shor**

21 juillet 2019

Google, IBM, Microsoft... annonceront bientôt la « suprématie quantique ». Quels sont les enjeux de ce nouveau paradigme informatique ?

> Les faits scientifiquement démontrés restent immuables mais leur explication varie avec les progrès de la connaissance. Les théories de Darwin et de Pasteur sont déjà dépassées. L'atome, jadis miracle de simplicité, est devenu miracle de complexité.
>
> *Gustave Le Bon – Les incertitudes de l'heure présente*

Aujourd'hui…

Google et d'autres ne seraient plus très loin de pouvoir démontrer la « *suprématie quantique* »[1]. Ce terme désigne une configuration technique fondée sur les propriétés « quantiques » de la matière à l'échelle atomique et permettant de réaliser des calculs qu'aucun ordinateur classique ne pourrait matériellement finir avant l'extinction de l'univers.

[1] Kevin Hartnett pour Quanta Magazine – 18 juillet 2019 – *Quantum Supremacy Is Coming: Here's What You Should Know*

Il reste à obtenir cette configuration qui est en ce moment-même l'objet d'une lutte acharnée. Il restera ensuite à lui faire faire des calculs « intéressants » c'est-à-dire économiquement rentables ou stratégiquement nécessaires. L'un des calculs possibles par une telle machine est effectivement intéressant mais nous allons voir qu'il pose problème…

Informatique classique

Le milieu digital émerge (Émergence du milieu naturel digital) et libère des puissances économiques, sociales, politiques… dont nous, citoyens et consommateurs comblés, peinons encore à prendre la mesure. Nous sommes malgré tout conscients que nous traversons depuis le milieu des années 1990 une extraordinaire période de transition déterminée, en grande partie, par les technologies de l'information (les autres facteurs principaux – écologie et démographie – sont évidemment fondamentaux mais ne concernent pas directement nos réflexions).

L'informatique dite « classique », née au milieu du XXème siècle, résulte de la convergence de travaux théoriques dans de nombreux domaines : mathématiques, physique, chimie, ergonomie, psychologie cognitive… L'informatique, faisant désormais office d'environnement social et de milieu naturel, intéresse donc également la médecine, la morale, le légal, l'éducation… et façonne désormais notre culture. Il a ainsi fallu près de 80 ans de progrès technique et d'évolution transdisciplinaire pour en arriver à ce point : l'informatique est une technologie mature, quasi transparente, totalement intégrée à nos modèles socio-économiques et politiques. Plus encore : elle les façonne.

Dès lors, nous devenons ce qu'elle nous propose.

Réductionnisme

L'un des aspects les plus fascinants de ce mouvement historique rapide est qu'il est devenu impossible d'envisager le rapport (causal) entre les manifestations sans bornes du milieu digital dans nos vies quotidiennes et la « physique de base » de l'informatique fondée sur la notion mathématique de « bit ». Rappelons qu'un bit est la plus petite quantité d'information possible en informatique classique : il « vaut » 0 ou 1, il est « allumé » ou « éteint ».

Il y a désormais le même genre de « distance conceptuelle » entre l'un des bits qui animent, par exemple, le logiciel de notre jeu vidéo favori, et l'un des atomes qui constituent notre glace à la fraise (heureusement, nous n'avons pas plus à connaître la physique atomique pour apprécier une glace que de connaître la logique booléenne pour jouer à *Crash Team Racing Nitro-Fueled*).

Il y a cependant une différence majeure entre le bit et l'atome : le premier est artificiel. Donc, tout ce qui advient à l'échelle des ordres de grandeur successifs, depuis le bit jusqu'aux manifestations les plus générales du numérique (comme un virus informatique et ses effets mondiaux ou, mieux encore, le phénomène du remplacement de l'homme par ses robots) est techniquement défini par l'homme. C'est cette remontée d'ordres de grandeur successifs qui mène à la perte progressive du lien causal et explicatif avec les bits.

Ordres de grandeur

Un smartphone contient de l'ordre de 10^{11} bits (1 suivi de 11 zéros). Nous créons chaque seconde dans le monde de l'ordre de 10^{15} bits (1 million de milliards), soit 10^{22} bits chaque année. C'est énorme mais une glace à la fraise contient 10^{27} atomes, chaque atome étant infiniment plus « complexe » qu'un bit. Malgré l'extraordinaire inflation mondiale de bits qui gouvernent nos sociétés et la débauche d'énergie électrique pour les animer (L'illusion d'un monde numérique « vert »), ils s'ébrouent dans un ordre de grandeur dérisoire : le substrat « atomique » du monde numérique est ridiculement petit et simple. Comparé au monde physique, il n'est qu'une infime écume.

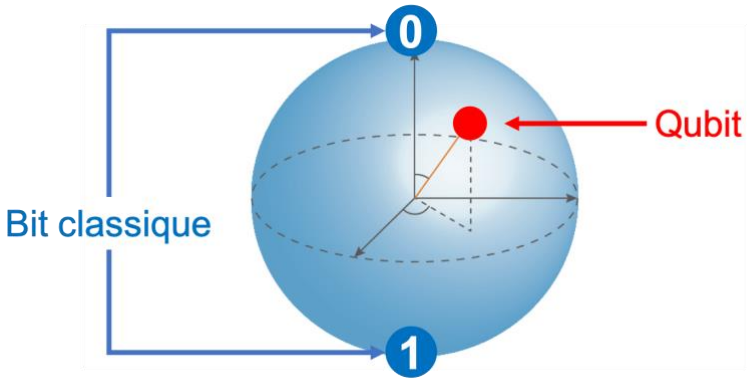
La nature des problèmes que nous pouvons pratiquement résoudre est en conséquence, et quoique nous puissions en penser (intelligence artificielle, etc.), extrêmement limitée. Les méthodes de protection informatique que nous utilisons sont d'ailleurs liées à ces limites intrinsèques : un bon cryptage nous garantit qu'il faudrait bien plus d'atomes que dans une glace à la fraise pour être décodé.

L'informatique dite « *quantique* » promet justement de changer radicalement d'ordre de grandeur et de déchaîner autre chose. Expliquons brièvement de quoi il s'agit.

Qubit

Le bit (0 ou 1, allumé ou éteint) est l'atome de base de l'informatique classique. L'informatique quantique utilise un autre atome de base : le « *qubit* » (quantum bit), qui peut occuper une infinité d'états intermédiaires entre 0 et 1. Il suffit donc déjà de comprendre ceci : le qubit est extraordinairement plus « subtil » que le bit.

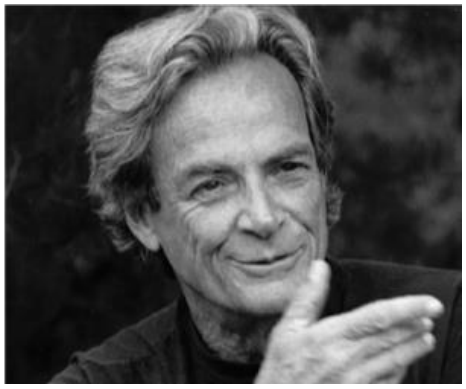
La représentation la plus simple et la plus fidèle de l'état (la « valeur ») d'un qubit est celle d'un point géographique sur une sphère. Au pôle nord la valeur classique 0, au pôle sud la valeur classique 1. Un bit classique ne peut donc occuper que ces deux positions. Mais le qubit peut se « placer » à n'importe quel autre endroit de la sphère :



Il n'est ni vraiment allumé, ni vraiment éteint (comme le célèbre chat de Schrödinger ne serait ni vraiment vivant, ni vraiment mort).

D'où vient cette idée étrange qu'un qubit serait utile à nos calculs ? Non pas des mathématiques, comme le bit classique, mais de la physique atomique. Il s'agit en quelque sorte de profiter des lois de la nature.

Richard Feynman



Richard Feynman (1918-1988) était l'un des physiciens les plus géniaux et influents de sa génération. En 1965, il obtient le prix Nobel de physique pour ses travaux en électrodynamique quantique (QED en anglais). Cette théorie permet de décrire le comportement de particules élémentaires (électrons, photons…) avec une extraordinaire précision. A cette toute petite échelle (le milliardième de mètre tout au plus), les règles physiques n'ont rien à voir avec celles que nous connaissons par notre expérience sensible. Il nous faut une « traduction » mathématique et une interprétation (une façon de parler) qui permettent à notre intuition de jouer son rôle imaginatif et créatif. Ce n'est pas gagné (nous soulignons)[2] :

> Plusieurs années après [le prix Nobel], au cours d'une conférence, [Richard Feynman] dit qu'il ne s'attendait pas à ce que l'audience comprenne la QED parce que lui-même ne la comprenait pas. Les lois sont assez tordues [screwy] et il trouvait particulièrement agaçant que la théorie repose sur des probabilités plutôt que sur la certitude.

Retenons ceci : la physique quantique est « tordue », difficile à comprendre (elle traite de phénomène pour lesquels nous n'avons aucun sens) et parle de probabilités…

Les ordinateurs (classiques) commençaient à se développer à l'époque de Feynman et les physiciens les utilisaient pour calculer des trajectoires, simuler l'évolution de petits systèmes, etc. Mais ces ordinateurs se révélèrent incapables de simuler des systèmes quantiques, trop « complexes ». Alors en 1982, l'inventeur Richard Feynman publiera un article intitulé « *Simulating Physics with Computers* », où il explique que pour simuler des systèmes quantiques (des électrons, des photons… à l'échelle atomique et subatomique), il faut des ordinateurs… quantiques ! Des ordinateurs qui fonctionnent comme les objets qu'ils cherchent à simuler. . C'est un peu comme si nous cherchions à simuler le cerveau avec de vrais neurones plutôt qu'avec des simulacres mathématiques...

C'est donc bien un *physicien* qui a eu l'inspiration, il y presque 40 ans, de l'informatique quantique. C'est assez extraordinaire : jamais un mathématicien comme Alan Turing, l'un des principaux théoriciens de l'informatique classique (Le corps de Turing), n'aurait pu l'imaginer.

[2] Dick Selwood pour Electronic Engineering Journal – 24 mai 2018 – *Richard Feynman and Quantum Computing*

Étrangetés quantiques

L'atome de l'informatique quantique est donc le qubit. Il obéit aux lois de la physique quantique et se comporte donc « comme » une particule élémentaire. Ces lois sont vraiment très étranges, difficiles à expliquer et à se représenter. Elles ont été déduites par les physiciens au fur et à mesure de leurs observations.

Voici l'un de ces principes (qui n'est pas le plus déterminant pour l'informatique quantique mais qui suffit à comprendre la différence radicale de nature entre un bit et un qubit – pour quelques précisions supplémentaires, voir la fin de l'article).

L'état du qubit (l'emplacement sur la sphère) est gouverné par des équations mathématiques. Il ne se trouve pas n'importe où et ne se « déplace » pas n'importe comment. Mais *nous ne pourrons jamais l'observer ailleurs qu'au pôle nord ou au pôle sud*, dans l'état 1 ou l'état 0, comme un bit classique !

Autrement dit, isolé du monde extérieur, « en catimini », le qubit s'anime sur la sphère : il balance entre le 0 et le 1 selon les lois de la physique quantique. Mais si l'on veut savoir dans quel état il se trouve, il faut l'observer, donc échanger avec lui de l'énergie. Mais cet échange le fige alors dans l'état 0 ou l'état 1. Les lois de la physique quantique ne nous donnent que la probabilité à chaque instant de l'observer dans l'un des deux états classiques.

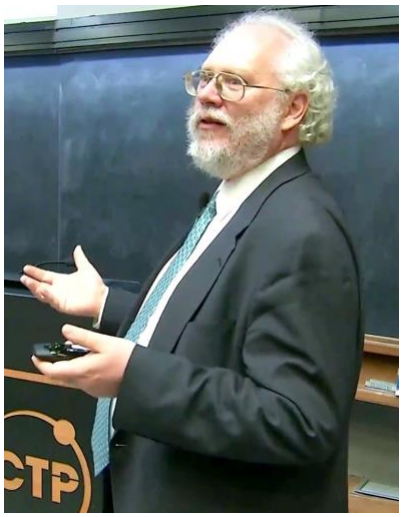
Le qubit est comme une pièce de monnaie lancée en l'air. Dans son parcours aérien, la pièce obéit aux lois précises de la mécanique classique newtonienne. Elle décrit en l'air, selon ces lois, une trajectoire parabolique et tourne sur elle-même. Mais compte tenu de l'imprécision de nos connaissances sur l'ensemble de l'expérience (vitesse de départ, état du sol au point d'impact, etc.) elle a autant de chances de retomber sur le côté pile que sur le côté face. Ce n'est qu'une fois à terre que nous connaîtrons la face d'arrivée.

Ce n'est qu'une fois observé qu'un qubit se révèle… un bit. C'est d'ailleurs la raison pour laquelle il est encore possible de parler d'informatique puisque la solution d'un problème, le résultat d'un algorithme quantique qui a animé les qubits durant leur « vol » est bien en définitive de nature binaire, c'est-à-dire classique.

Risques quantiques

Depuis l'article de Feynman, les chercheurs essayent de fabriquer un ordinateur quantique (avec *quoi* donc faire un vrai qubit ?). Cela s'avère extrêmement difficile et demande des moyens considérables que seules les plus grandes agences gouvernementales ou les plus riches acteurs numériques (Google, IBM, Microsoft…) peuvent mobiliser. Mais quel intérêt de dépenser des milliards s'il ne s'agit que de simuler des systèmes quantiques ? En quoi tout ceci nous concerne-t-il ?

Parallèlement, d'autres chercheurs ont mené des travaux en algorithmique quantique. Étant donné un système de qubits et les lois quantiques qui les animent, peut-on utiliser ce système pour faire des calculs intéressants ?



Ce n'est qu'en 1994 que le mathématicien américain Peter Shor fait grand bruit en inventant un algorithme quantique intéressant, basé sur un système de qubits, qui permet de réaliser ce qu'aucun algorithme classique ne peut faire dans un temps raisonnable : trouver les facteurs premiers d'un nombre entier assez grand. Par exemple étant donné le nombre 576460752303423487, trouver que :

$$576460752303423487 = 179951 \times 3203431780337$$

On imagine qu'il faut en principe essayer toutes les combinaisons possibles jusqu'à trouver la bonne, ce qui devient rapidement impraticable pour des nombres beaucoup plus grands. La difficulté de réaliser cette décomposition est à la base de tous nos systèmes de cryptographie et donc de protection des informations transitant notamment sur internet. Et sans système cryptographique inviolable, pas de commerce électronique par exemple.

Donc, si un ordinateur quantique faisant tourner l'algorithme de Shor voyait le jour, c'est tout le milieu numérique mondial qui deviendrait instantanément inutilisable. Or, un tel ordinateur est probablement faisable. Il n'y a donc pas le choix : il faut le faire. Aucun État ne peut attendre qu'une autre puissance développe avant lui de cette arme atomique numérique.

Mais de combien de temps dispose-t-on ?

17 ans

Un rapport américain publié début 2019[3] dresse sur 272 pages un état des lieux complet, sérieux et très documenté, de la recherche en informatique quantique à partir des informations publiques disponibles (les éventuels travaux de telle ou telle entreprise ou de tel ou tel État peuvent être tenus secrets). Voici l'une des conclusions du rapport :

> Le temps nécessaire pour créer un grand ordinateur quantique […] capable de faire tourner l'algorithme de Shor […] ou d'autres applications utiles est probablement de plus d'une décennie.

C'est en réalité assez court. En effet, c'est à peu près le temps nécessaire pour déployer à l'échelle mondiale, sur tous les systèmes informatiques, de nouveaux protocoles cryptographiques classiques résistants à l'algorithme de Shor (« *migration time* »). Mais de plus, une fois ces protocoles déployés, il faut leur laisser le temps de crypter

[3] National Academies of Sciences, Engineering, and Medicine – 2019 – *Quantum Computing: Progress and Prospects (2019)*

suffisamment d'informations pour que l'essentiel du volume de données mondiales sensibles repose en paix dans les datacenters (« *security shelf life* ») avant l'arrivée d'un grand ordinateur quantique. On estime ce temps à 7 ans en moyenne.

Nous n'avons donc que 17 ans de protection devant nous à partir du moment où nous disposons d'un algorithme *classique* de cryptage post-quantique (il existe aujourd'hui plusieurs pistes sérieuses mais rien de définitif). Si un tel algorithme est proposé, disons, en 2020, il ne faudrait pas qu'un grand ordinateur quantique soit opérationnel à grande échelle avant 2037. Sinon, c'est toute la sécurité du milieu digital, sur lequel repose notre économie, qui serait compromise.

Un grand ordinateur quantique est-il possible ?

Ce ne sera pas simple...

L'une des principales difficultés est que les qubits doivent être totalement isolés de leur environnement pour effectuer un vol « libre » (en catimini), un déplacement purement quantique sur leur sphère d'état. Au moindre échange d'énergie (chaleur, radiation…), leur comportement quantique cesse ou est entaché d'erreurs. C'est un peu comme si nous lancions une pièce de monnaie en l'air, nos équations prêtes, et que soudain le vent se levait et perturbait la trajectoire théorique en modifiant la probabilité finale de « pile » et de « face ».

Mais il est impossible d'isoler totalement un système du reste de l'univers (il y toujours « un peu de vent »). Plus il y a de qubits et plus les « calculs » durent longtemps, plus les petites perturbations s'accumulent malgré le vide, l'obscurité et le froid quasi absolu qui règnent au sein des machines quantiques. Il existe des solutions partielles à ce problème mais elles restent difficiles à mettre en œuvre. Certains chercheurs émettent d'ailleurs de gros doutes quant à la possibilité d'une machine quantique utile[4].

Mais les moyens déployés sont considérables...

Suprématie quantique

Les fantastiques progrès de l'informatique (la fameuse « loi de Moore », qui s'épuise aujourd'hui dans sa version classique) sont bien sûr le résultat de formidables avancées techniques. Mais surtout, ces progrès étaient absorbés au fur et à mesure par le système économique, transformés en revenus gigantesques, et donc largement financés. L'informatique quantique devra de la même façon prouver rapidement son utilité pratique (économique) pour sortir des sphères militaires et de la recherche et accéder ainsi aux financements nécessaires à son déploiement à grande échelle sur des décennies.

La première étape consiste à fabriquer un ordinateur capable de démontrer sans ambiguïté la « *suprématie quantique* », c'est-à-dire capable d'exécuter un calcul qu'aucun ordinateur classique à base de bits ne pourra jamais effectuer (dans un temps raisonnable). Ce jour-là, l'annonce sera largement connue du grand public et on conçoit

[4] Katia Moskvitch pour Quanta Magazine – 7 février 2018 – *The Argument Against Quantum Computers*

l'énorme enjeu d'image pour la première équipe ou la première société commerciale à y parvenir. Tant que cette suprématie quantique n'est pas démontrée, les organismes de recherche investissent sur des fonds publics ou privés (souvent dans le plus grand secret).

IBM, Intel, Microsoft, Google… La Chine y consacrent ainsi des milliards de dollars. S'agissant d'une technologie de grande rupture, qui conditionne la sécurité des États, L'Europe tente de rester dans la course[5] :

> Lancé par la Commission Européenne le 29 octobre [2018] à Vienne, le programme Quantum Technologies Flagship est réparti dans quatre domaines : le calcul quantique, la simulation quantique, la communication quantique et la métrologie quantique. Cette répartition est assez habituelle. On la retrouve dans les plans de pays comme les USA ou la Chine.

Ce programme est financé à hauteur de 1 milliard d'euros sur 10 ans. Une paille... Comme d'habitude, l'Europe reste terriblement sous-investie et divisée.

Demain…

L'ordinateur quantique existe déjà mais il lui manque encore d'être assez « grand » et fiable pour cocher la première case, celle de la suprématie quantique, c'est-à-dire pour faire mieux qu'un ordinateur classique. Quand ce sera le cas (demain, dans quelques mois, années ?), la bataille stratégique sera officiellement lancée et le compte à rebours du monde digital classique sera enclenché.

Il faudra ensuite des dizaines d'années pour qu'à partir de ce nouvel atome, le qubit, se déploient de nouveaux outils et paradigmes, ordre de grandeur après ordre de grandeur, jusqu'à transformer nos systèmes économiques, sociaux, politiques... et donc peut-être notre culture elle-même.

Aller plus loin…

Il existe de très nombreux articles d'introduction à l'informatique quantique mais nous n'en n'avons pas encore trouvé qui vulgarise correctement le sujet (y en a-t-il ?). Il faut toujours être un peu matheux, programmeur, physicien...

Cet article est lui-même délicat et c'est bien l'une des difficultés du thème : nous manquons du vocabulaire et des représentations pour le partager avec le plus grand nombre. Quelle aporie ! Voilà un milieu digital qui se développe à une vitesse extraordinaire, qui nous conditionne tous et dont les principes échappent à la plupart d'entre nous !

Mais si vous êtes un peu matheux, programmeur, physicien... ou simplement très curieux voici deux rapides compléments au sujet de l'informatique quantique.

---

[5] Olivier Ezratty pour Frenweb.fr – 12 novembre 2018 – *L'Europe et le quantique*

Premièrement, la puissance spécifique de l'ordinateur quantique, qui lui permet de résoudre des calculs « avant la fin de l'univers », est liée à un phénomène quantique appelé « *intrication* »[6]. Plusieurs qubits peuvent se trouver dans un état (position sur la sphère) lié, et ceci indépendamment de la distance entre eux. Cette codépendance instantanée permet à un système quantique d'occuper simultanément tous les états possibles d'un problème de dimension exponentielle. C'est pourquoi un ordinateur quantique peut être exponentiellement plus rapide qu'un ordinateur classique pour certains types de calcul. C'est par exemple le cas de la décomposition d'un nombre entier en facteurs premiers par l'algorithme de Shor.

Deuxièmement, nous avons expliqué que le moindre bruit, la moindre brise perturbe le qubit et déforme le calcul. En physique, cela veut dire que le qubit ne doit pas échanger d'énergie avec son environnement. Par exemple, il ne doit pas « chauffer ». Cette condition absolue explique pourquoi on ne peut pas faire n'importe quel calcul classique avec des qubits. Prenons la multiplication :

$$2 \times 12 = 24$$

Lorsque l'ordinateur classique a fini son calcul, les nombres 2 et 12 ont été « remplacés » par la solution : 24. De l'information a donc été perdue ! En effet, étant donné 24, il est impossible de savoir si c'est le résultat de 2 x 12, 3 x 8 ou 4 x 6... Or, lorsque de l'information est perdue, l'entropie thermodynamique augmente (De l'infosphère à une éthique gazeuse) et donc de la chaleur est produite : la multiplication classique chauffe !

La multiplication quantique doit donc procéder différemment. Elle doit être thermodynamiquement neutre donc *réversible* (« *adiabatique* »). Il faut pouvoir inverser le calcul. La solution intuitive est évidente. Il faut conserver au moins l'un des deux nombres proposés au calcul :

$$2 \times 12 = 24\ [2]$$

Ainsi de 24 [2] on peut remonter à 2 x 12. En informatique quantique, tous les algorithmes doivent ainsi être réversibles. C'est possible mais pas toujours simple.

Alors, l'informatique quantique ne dégage-t-elle vraiment aucune chaleur ? Permettrait-elle de contribuer au climat ? Malheureusement non : il faut beaucoup d'énergie pour isoler l'ordinateur du monde extérieur, le refroidir par exemple…

[6] Wikipédia – *Intrication quantique*