20/09/2005 - Par
Thierry Lombry, Informaticien

L'ordinateur quantique

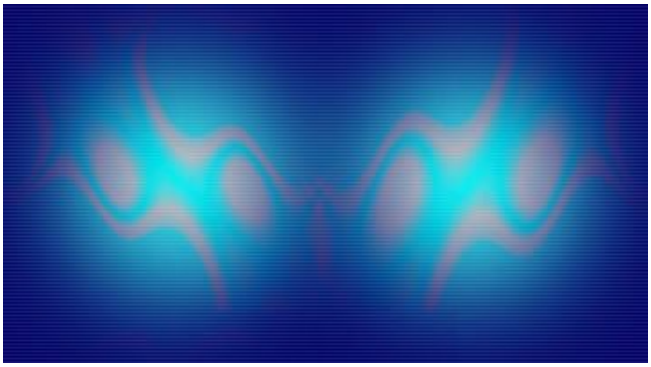
Le concept d'ordinateur quantique concerne à la fois la théorique classique de l'information, l'informatique et la physique quantique. Nous allons tenter de résumer en quelques pages non seulement le concept d'ordinateur quantique mais également le sujet plus complexe de la théorique quantique de l'information, un passionnant voyage dans la technologie de l'avenir.

Page 1/10 - L'ordinateur quantique

Depuis l'invention du premier circuit intégré monolithique par Jack Kilby de Texas Instruments en 1958, l'intégration des composants électroniques n'a cessé d'être améliorée au point que nous parvenons aujourd'hui à faire fonctionner des centaines de milliers de composants sur une puce (chip) mesurant à peine 1 cm^2, c'est la technologie ULSI (Ultra Large Scale Integration) qui détrône aujourd'hui le VLSI. A cette échelle les circuits mesurent une fraction de micron !

Le coeur de l'ordinateur : le microprocesseur

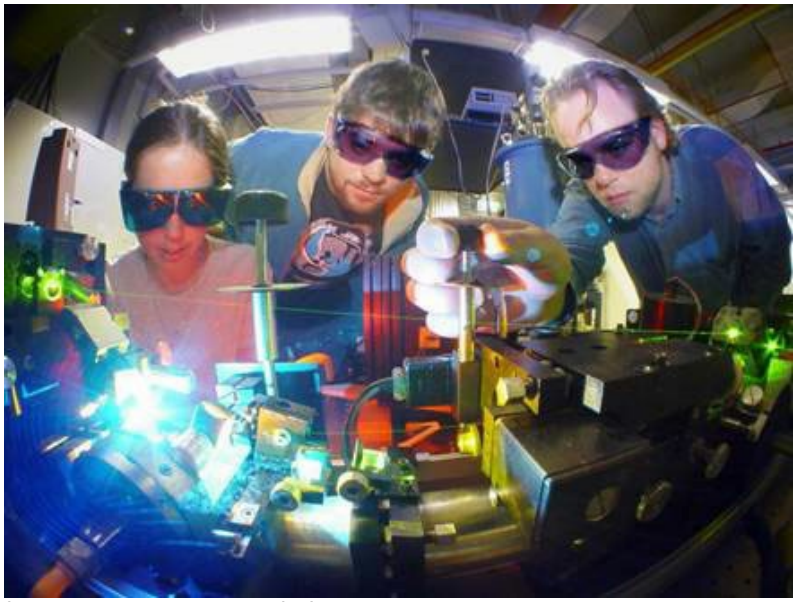
Mais à cette échelle la difficulté de fabrication devient digne d'une mission impossible. Non seulement les effets quantiques deviennent apparents mais en cours de fonctionnement les composants dissipent beaucoup de chaleur, réduisant d'autant leur durée de vie. A terme la solution des circuits intégrés présente donc des limitations mécaniques dont on ne peut pas s'affranchir.



Représentation artistique des fameux bits quantiques ou qubits. © U.Melbourne/Marc Coe.

Page 2/10 - Une révolution technologique

La question de l'existence éventuelle des ordinateurs quantiques émergea naturellement de la miniaturisation grandissante des composants électroniques. Dès les années 1970, il avait été compris que si elle continuait telle quelle, cette évolution allait mener à des composants de tailles atomiques, lesquels seraient entièrement sujets aux lois de la physique quantique. En 1982, le prix Nobel de physique Richard Feynman dynamisa cette réflexion restée auparavant assez abstraite et peu approfondie lorsqu'il imagina un modèle théorique illustrant comment un système quantique pourrait être utilisé pour faire des calculs. Rapidement, en 1985, David Deutsch de l'Université de Oxford, montra que de manière plus générale, les idées de Feynman pouvaient mener à un **ordinateur quantique,** un ordinateur qui effectuerait n'importe quelle tâche, mais serait capable de tirer avantage des propriétés quantiques de la matière, principalement du **principe de superposition des états.** Plus important pour la recherche en physique, Deutsch démontra qu'en principe un ordinateur quantique serait capable de **modéliser parfaitement n'importe quel processus physique, ce qui est impossible avec un ordinateur usuel** reposant sur la physique classique. Dans un premier temps les gens commencèrent donc à se mettre en quête de problèmes simples mais que seul un ordinateur quantique pourrait résoudre.



Chercheurs australiens développant la nouvelle génération d'ordinateur quantique. Imbrication quantique et qubit font à présent partie de leur nouveau langage informatique.
© ANU/RSPhysSE - Tous droits de reproduction interdit

Cette recherche s'avéra plus difficile que prévu, et il fallut attendre le milieu des années 90 pour qu'un chercheur des

laboratoires Bell – l'institut qui rassemble le plus de prix Nobel au mètre carré –, Peter Shor, invente des opérations mathématiques élémentaires propres aux ordinateurs quantiques et les applique pour créer un algorithme quantique de factorisation.

Exemple de factorisation : 120 = 5x4x3x2.

Quel est le rapport entre la factorisation et l'ordinateur quantique, demanderez-vous ? La cryptographie ! Grâce à cet algorithme, un ordinateur quantique est en mesure de casser les codes d'encryption les plus complexes en quelques secondes !

Rappelons brièvement l'utilité des clés dans le processus de cryptage/décryptage. Généralement un message secret est envoyé sous forme codée, une clé de conversion permettant de traduire le message codé en clair. Cette clé évite de devoir chiffrer et déchiffrer le message car l'émetteur et le destinataire disposent chacun d'une clé générant son propre système d'encryptage. Cette protection empêche même les concepteurs du programme d'encryptage de déchiffrer le message codé.

La sécurité d'un message codé dépend du nombre de clés. Un système à clé unique par exemple permet de "casser" un système, mais en général il va essayer systématiquement toutes les clés possibles sur le message à déchiffer jusqu'à pouvoir le lire.

Certains systèmes telle la substitution monoalphabétique simple, dispose d'un nombre de clés gigantesque : 26! permutations possibles des lettres de l'alphabet, soit environ $4x10^{26}$ possibilités. Le succès est donc loin d'être garanti dans un temps relativement court. Pour remédier à ce problème on peut utiliser des variations de fréquence des lettres dans les différentes langues naturelles, ce qui permet d'aboutir à des systèmes de cryptage disposant d'un nombre de clés réduit mais qui s'avèrent souvent beaucoup plus sûrs.

Devant ce défi qui intéresse autant les majors de l'informatique que les services d'espionnage ou l'armée, des centaines de chercheurs aux quatre coins du monde se sont donnés pour objectif de construire le premier ordinateur quantique d'ici quelques années.

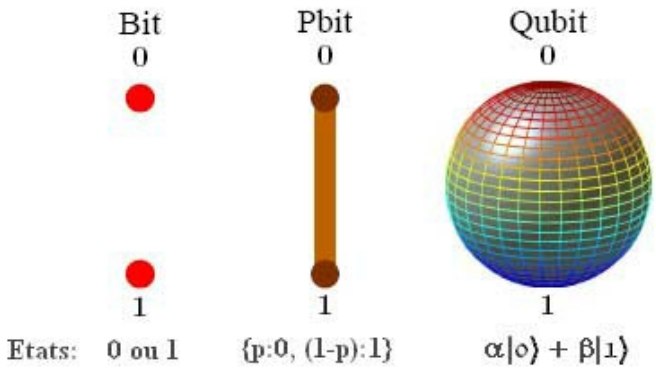
Certains très optimistes avancèrent même la date de 2008 voire 2020. Il est toutefois peu probable que nous verrons des ordinateurs quantiques au quotidien avant plusieurs décennies... Quoiqu'il en soit, la compétition est ouverte, avis aux chercheurs !

Page 3/10 - Comment fonctionne un ordinateur quantique ?

Nous savons qu'un ordinateur classique traite des informations élémentaires, **des bits**, qui ne peuvent présenter **qu'un état parmi deux possibles** : 0 ou 1. **C'est le langage binaire.** La révolution que propose l'informatique quantique est de remplacer ces bits par des **bits quantiques, ou q(u)bits en abrégé,** pouvant prendre un ensemble de valeurs beaucoup plus large. En effet, la physique quantique, **avec son principe de superposition**, permet à un état d'être un "mélange" d'autres états. Ainsi, un qbit peut prendre les valeurs 0 ou 1, mais aussi un état constitue de 10% de 0 et 90% de 1, ou toute autre combinaison. Ceci signifie que quand on mesure la valeur du qbit, on a 10% de chances de trouver 0 et 90% de trouver 1. **En gros, le qbit peut être à la fois dans l'état 0 et l'état 1** (c'est une facon un peu cavalière d'exprimer un résultat mathématique precis et il ne faut pas mettre trop de poids dans cette interprétation). **La richesse offerte par ce principe se paie cependant par l'introduction d'une incertitude dans la mesure du qbit**.

Un peu plus concrétement, avec 4 bits, un ordinateur classique peut traiter un état parmi 2^4 soit 16 états différents :

0000, 0001, 0010, 0011, etc. Dans un ordinateur quantique, les quatre qbits pourraient être dans une supersposition de tous ces états. Dans cette situation, **l'avantage de l'ordinateur quantique est de pouvoir traiter simultanément les 16 états.**



A gauche un bit ordinaire est caractérisé par deux états, 0 ou 1. Au centre un pbit ou "bit probabiliste". Il représente la distribution des probabilités d'un bit. L'expression indiquée signifie que le pbit a une probabilité p d'être dans l'état 0 et 1-p d'être dans l'état 1. C'est l'exemple typique de la pièce de monnaie que l'on jete en l'air : elle a 1 chance sur 2 de tomber sur pile, 1 chance sur 2 de tomber sur face. A droite, le qubit opère dans un univers multidimensionnel, ses états propres correspondant à la surface d'une sphère dite de Bloch tandis que ses états logiques correspondent aux pôles de cette sphère.
© W.H.Zurek et al - Tous droits de reproduction interdit

Des ordinateurs quantiques équipés de processeurs de N qubits permettent donc de gérer 2^N informations différentes simultanément ! Ils calculent donc N fois plus vite qu'un ordinateur classique puisqu'ils sont capables d'effectuer ces calculs en parallèle ! Le nombre de qubits augmente donc de manière exponentielle la puissance du travail en parallèle. Il est ainsi facile de calculer qu'un ordinateur quantique de 300 qbits pourraient gérer environ 10^{90} informations, soit **plus que le nombre d'atomes dans l'Univers observable.**

Aujourd'hui nous sommes cependant encore loin de pouvoir gérer autant d'états et les prototypes d'ordinateurs quantiques les plus puissants travaillent au mieux avec 7 qubits, l'équivalent d'un processeur de 7 bits mais massivement parallèle.

Gérer la décohérence

Lorsqu'un système quantique est dans un état quantique qui est une superposition de plusieurs états classiques, on parle d'état cohérent, et le phénomène est désigné sous les noms "emmêlement ou imbrication quantique". **Mais l'une des raisons pour lesquelles il est très difficile de produire aux échelles macroscopiques des états intriqués est qu'aussitôt qu'un système quantique interagit avec son environnement, il “décohère” et tombe dans l'un des états classiques.**

La puissance potentielle des ordinateurs quantiques dépend des propriétés de parallélisme présentes dans l'état d'imbrication quantique. Le phénomène de décohérence représente donc un obstacle majeur pour la fabrication de tels ordinateurs car il signifie un retour vers des états classiques, mais aussi une perte d'information et un grand risque d'erreurs dans les calculs."

De plus, **la mesure de la valeur contenue dans les qbits brise la superposition**, et on se retrouve dans la même situation que dans le cas classique : chaque qbit contient la valeur 0 ou 1 après la mesure ! On semble donc perdre d'un coup tous les avantages offerts par les propriétés quantiques. **Une des grandes difficultés de ce domaine est ainsi de trouver des algorithmes propres aux ordinateurs quantiques et qui permettent de ne pas perdre le résultat du calcul quand on le lit..."**

- **Trouver le résultat**

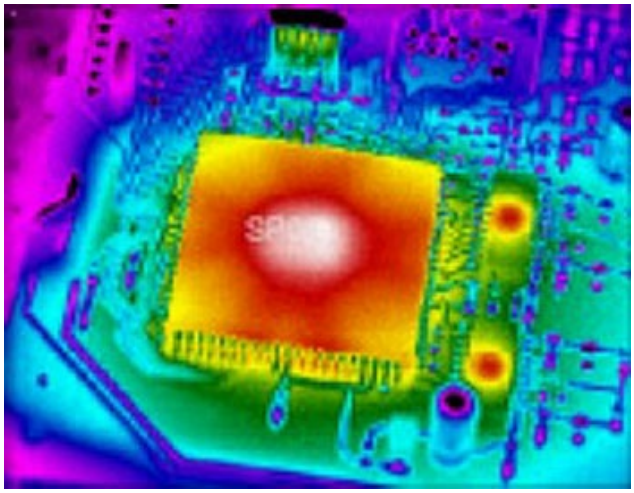
Mais ce n'est pas le seul problème auquel les physiciens doivent faire face. L'ordinateur quantique travaillant dans un univers mathématique multidimensionnel, les résultats d'un calcul effectué en parallèle sont distribués dans autant d'univers parallèles ou différents.

Quelle est la conséquence pratique de ce phénomène ?

L'utilisation d'états imbriqués pour une série de calculs donnée signifie que la solution finale du calcul se trouve délocalisée dans l'ensemble des interférences créées par les différentes étapes classiques. En pratique, cela signifie que si vous regardez un calcul particulier, l'équivalent d'un état intermédiaire, vous prenez le risque de perturder les autres calculs et de faire disparaître les interférences, ce qui provoquera en quelques sortes le “plantage” du calcul quantique.

Page 4/10 - Eviter de perdre l'information

Aujourd'hui l'un des problèmes majeurs de l'informatique, outre les effets quantiques qui deviennent sensibles, c'est la dissipation de chaleur par les composants. De nos jours la température de la majorité des CPU Intel ou Motorola les plus rapides dépasse allègrement les 80°C ! Pour éviter qu'ils ne surchauffent ils doivent être refroidis (ventilés ou par circulation d'un bain d'huile) sous peine de "planter" l'ordinateur.

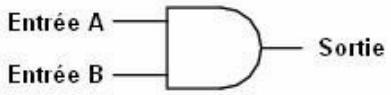


Emission thermique d'un processeur rapide conçu par Sierra Pacific Corp. Evitez de le toucher lorsque l'ordinateur fonctionne car sa température peut dépasser 80°C !
© SPC - Tous droits de reproduction interdit

L'ordinateur quantique présente un problème similaire bien que son origine soit différente. **En effet, même si les ordinateurs quantiques ne présentent pas réellement de limites en vitesse de calcul ou en capacité mémoire, en revanche, un autre problème surgit : celui de la perte d'information en cours de calcul par décohérence.**

En effet, les physiciens considèrent que pour fonctionner le plus rapidement possible, les opérations effectuées par un ordinateur quantique doivent être réversibles : les données entrées doivent par exemple être déductibles des résultats. **Un calcul irréversible signifie une perte d'information que l'on peut assimiler à une dissipation de chaleur dont l'effet limitera les performances de l'ordinateur.**

Porte AND à 2 entrées 1 sortie

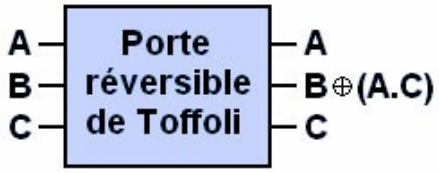


A	B	Sortie
0	0	0
0	1	0
1	0	0
1	1	1

En 1976, Charles H. Bennett d'IBM démontra qu'il était possible de fabriquer un ordinateur universel, la fameuse machine de Turing, en utilisant uniquement des portes réversibles. En exprimant un programme en terme d'opérations sur des primitives réversibles il prouva que le traitement n'était pas significativement plus lent.

Cela aboutit à la porte de Toffoli dont les entrées sont entièrement déductibles des sorties.

Notons que le signe $\oplus$ représente une addition modulo 2 (par ex.: $1 \oplus 1 = 0$)



Page 5/10 - Le problème de la conscience

L'informatique quantique présente d'intéressantes implications dans le monde de l'intelligence artificielle.

Si nous regardons des créatures artificielles telles que les robonautes de la NASA, P3, COG ou le chien AIBO, il est parfois difficile de faire la part des choses, de savoir ce qui est programmé de ce qui est acquis, où est le réflexe et la conscience... simulée ?

Un robonaute qui sera bientôt au service des astronautes de l'ISS © Nasa

Tout le monde s'est un jour demandé si finalement ces robots n'avaient pas quelque peu conscience d'eux-mêmes. Leur créateur en tout cas aimerait y croire. Certaines personnes considèrent toutefois que l'esprit humain est capable de réaliser des actions impossibles à réaliser par une machine de Turing. Le débat est loin d'être clôturé.

Le robot P3 de Honda.
© Honda - Tous droits de reproduction interdit

Selon la thèse de Church-Turing il existe, ou il est possible de fabriquer un ordinateur quantique universel programmable, afin de réaliser toutes les tâches informatiques pouvant être réalisées par n'importe quel objet physique. Cette thèse implique que tout objet, de la pierre à l'univers considéré dans son ensemble peut être considéré comme un ordinateur quantique et chacun des processus physiques identifiables, peut être considéré comme le résultat d'un calcul.

Dans ce contexte, la thèse de Church-Turing nous permet d'avancer une idée très hardie : puisque tous les ordinateurs sont fonctionnellement équivalents et que tout ordinateur donné peut en simuler un autre, il doit être possible de simuler la pensée rationnelle consciente en utilisant un ordinateur quantique. **Reste à le démontrer et ce sera peut-être l'histoire de toute une vie de chercheur.**

COG s'interrogeant sur son état de conscience.
© MIT/Rodney Brooks - Tous droits de reproduction interdit

Si les ingénieurs du MIT ou de Qubit pensent qu'il est possible de résoudre le problème de l'intelligence artificielle, certains physiciens tel Roger Penrose de l'Université d'Oxford pense que la conscience est tellement complexe qu'elle requiert une physique beaucoup plus exotique et encore inconnue.

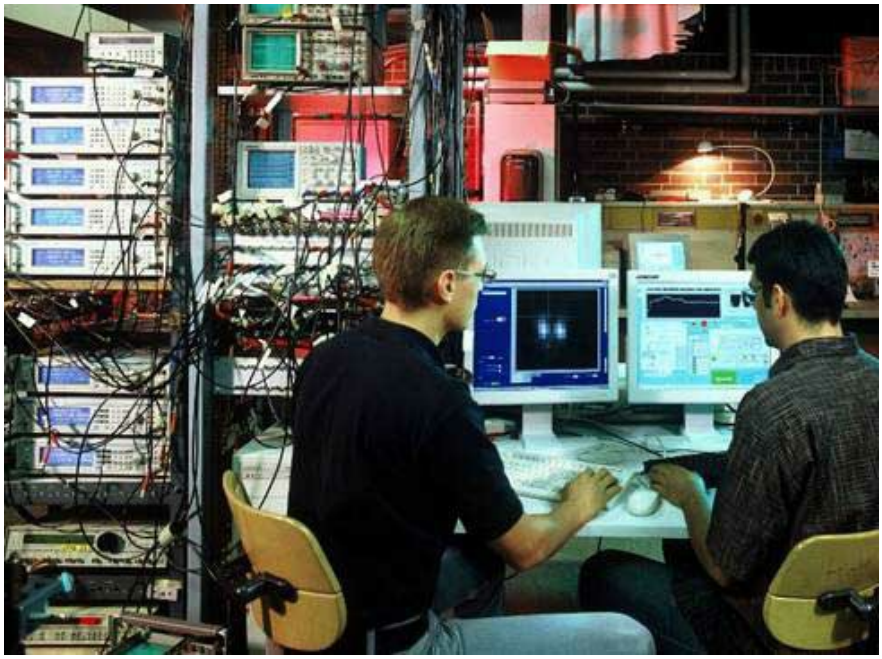
Page 6/10 - Fabrication d'un ordinateur quantique

Du fait qu'un ordinateur quantique manipule des qubits, sa fabrication n'a plus rien à voir avec celle d'un ordinateur conventionnel ; son processeur ne contient plus de transistor ou de diode par exemple.

Il faut élaborer une nouvelle et très haute technologie capable de faire exister des qubits en superpositions d'états 0 et 1. La méthode pour y parvenir... n'existe pas ; nous en sommes encore au stade expérimental avec tous les échecs et les quelques succès que cette étape sous-entend.

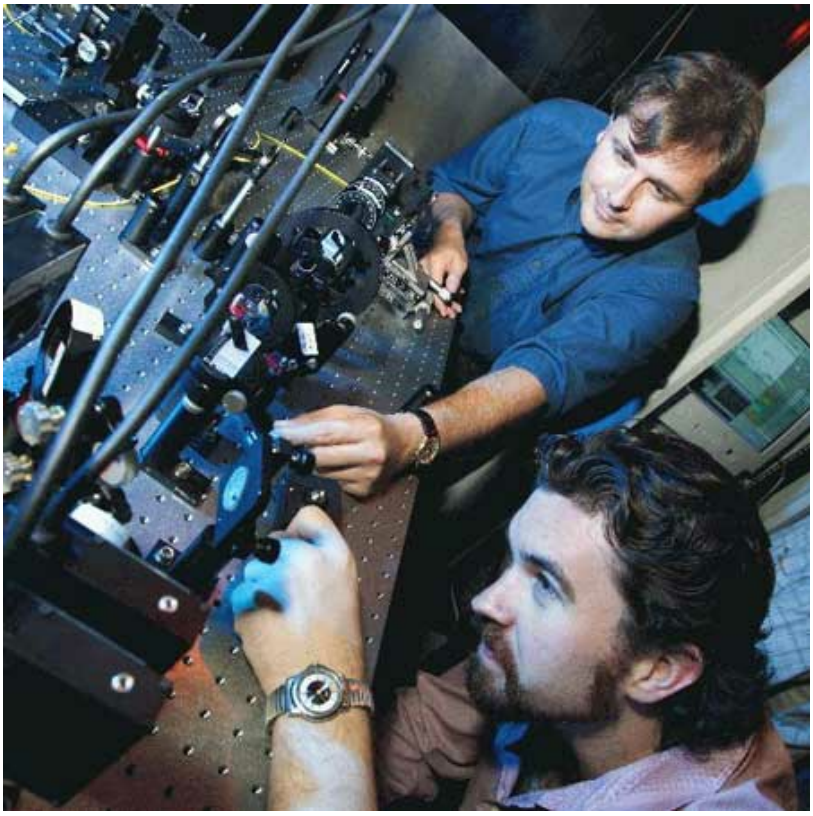
- **A - Laser et point quantique**

L'une des solutions pour créer un qubit consiste à élaborer un “point quantique” qui est fondamentalement un électron piégé dans une cage d'atomes, performance technique qui est aujourd'hui accessible aux laboratoires de Bell ou d'IBM par exemple qui peuvent manipuler des atomes individuellement.



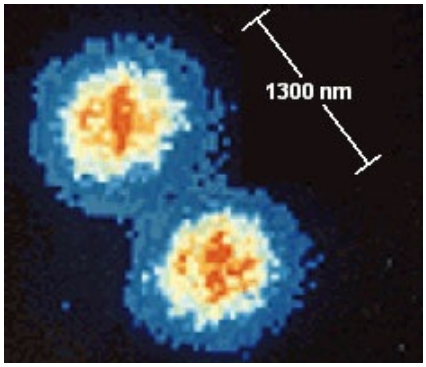
Les jeunes ordinateurs quantiques ont encore besoin de l'ancienne génération ! Ces deux étudiants de l'UIBK sont à la console d'ordinateurs conventionnels servant à piloter les lasers et les source radiofréquences d'un ordinateur quantique.
© UIBK/C.Lackner - Tous droits de reproduction interdit

Lorsque ce minuscule “point” est éclairé par une impulsion laser d'une longueur d'onde et d'une durée bien déterminée, l'électron passe dans un état excité. Une seconde impulsion laser provoque sa chute vers son état fondamental. Les états, fondamental et excité de l'électron représentent les états 0 et 1 d'un qubit, l'application du rayon laser représentant une fonction NOT provoquant le changement d'état, 0 vers 1 ou 1 vers 0 du qubit.



Les chercheurs Andrew G.White (arrière-plan) et Jeremy L. O'Brien de l'Université de Queensland réglant les portes NOT d'un ordinateur quantique
© IBM - Tous droits de reproduction interdit

Si l'impulsion laser est moitié moins longue que la durée nécessaire à la fonction NOT, l'électron passe dans une superposition d'états fondamentaux et excité simultanément; cela correspond à l'état d'imbrication quantique du qubit. Des fonctions logiques plus complexes peuvent être créées en utilisant des points quantiques arrangés par paires.



Deux ions de baryum au repos contenant chacun un seul qubit sont maintenus séparés par un rayon laser refroidit près du zéro absolu afin d'étudier la durée du phénomène de décohérence.
© A.White/J.O'Brien - Tous droits de reproduction interdit

Si ce principe fonctionne en théorie, la création d'un ordinaire quantique de cette manière présente certaines difficultés qui empêchent actuellement de progresser.

- **B - Les ordinateurs solides, liquides ou à gaz**

Les chercheurs du MIT, IBM ou du JPL ont experimenté d'autres solutions que le point quantique pour élaborer leur

ordinateur quantique. **Plusieurs techniques font appel à des molécules ou des atomes individuels ou encore à la polarisation d'une lumière laser comme support d'information. Une nouvelle fois le principal problème est la décohérence.**

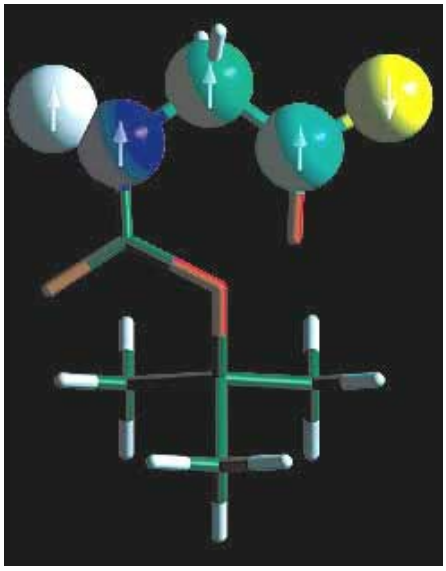
La solution la plus intéressante fait appel à la résonance magnétique nucléaire (RMN) qui permet, grâce à l'émission d'ondes radios spécifiques, de détecter les changements de spin.

Les Drs Isaac Chuang et Costantino Yannoni manipulant des éprouvettes contenant des molécules organiques. Aussi étonnant que cela soit, elles constituent le coeur de leur ordinateur quantique. A l'arrière-plan le cylindre métallisé est l'aimant à supra-conducteur du système RMN. © IBM - Tous droits de reproduction interdit

Comment fonctionne un système RMN ? A l'image des installations médicales, les équipements RMN utilisés en physique quantique sont constitués d'aimants supra-conducteurs capables de générer des champs magnétiques supérieurs à 2 Tesla. Cette intensité est nécessaire car la sensibilité du système augmente proportionnellement à l'intensité du champ magnétique. Pour étudier les structures atomiques et moléculaires, les champs radiofréquences sont de l'ordre de 500 à 750 MHz.

Ces aimants étant plongé dans ces enceintes contenant de l'hélium liquide à -269°C et ne dissipant pas de chaleur (effet joule nul), l'avantage de ce système est de ne pas consommer d'électricité pour générer les champs magnétiques. La seule contrainte est qu'il faut régulièrement remplacer l'hélium et l'azote liquides pour assurer la supra-conductivité car les produits ont tendance à s'évaporer.

Un ordinateur quantique utilisant la technologie RMN est réduit à une molécule et ces qubits sont représentés par les noyaux atomiques contenus dans la molécule. En fait pour effectuer les calculs le système n'utilise pas une seule molécule mais une “soupe” ou une “tasse” de molécules liquides. **L'avantage de cette méthode est d'éviter tout risque d'erreur : même si les molécules du liquide sautent dans un autre état, l'état de spin des noyaux qu'elles contiennent restent inchangés.** Le problème de la décohérence reste toutefois présent, mais il apparaît beaucoup plus tard que dans toute autre technique entrevue jusqu'à présent.



"Ordinateur" moléculaire RMN constitué de 5 qubits.
© S.J.Glaser/U.T.Munich - Tous droits de reproduction interdit

Les premiers résultats probants furent obtenus par Isaac Chuang en 1998. Avec son équipe il parvint à créer un ordinateur quantique à 2 qubits dans un dé à coudre de chloroforme et parvint à calculer les différentes périodicités d'une fonction. Il parvint également à retrouver une donnée parmi quatre en une seule étape en appliquant l'algorithme de Grover.

Le travail actuel des chercheurs consiste à réaliser des tâches plus complexes qui requièrent un plus grand nombre de qubits, donc plus de molécules et plus de nucléi.
En 2001 Chuang et son équipe sont parvenus à créer un système contenant 7 qubits qui leur permit de réaliser la factorisation du nombre 15 grâce à l'algorithme de Shor. En pratique cela correspond à contrôler un milliard de milliards de molécules !

Chuang et Gershenfield n'envisagent toutefois pas de solutions au delà de 15 ou 20 qubits du fait que les signaux magnétiques qui mesurent l'orientation des spins et déterminent les états quantiques deviennent excessivement faibles à mesure que le nombre de qubits augmentent, faiblissant d'un facteur voisin de 2 pour chaque qubit supplémentaire.

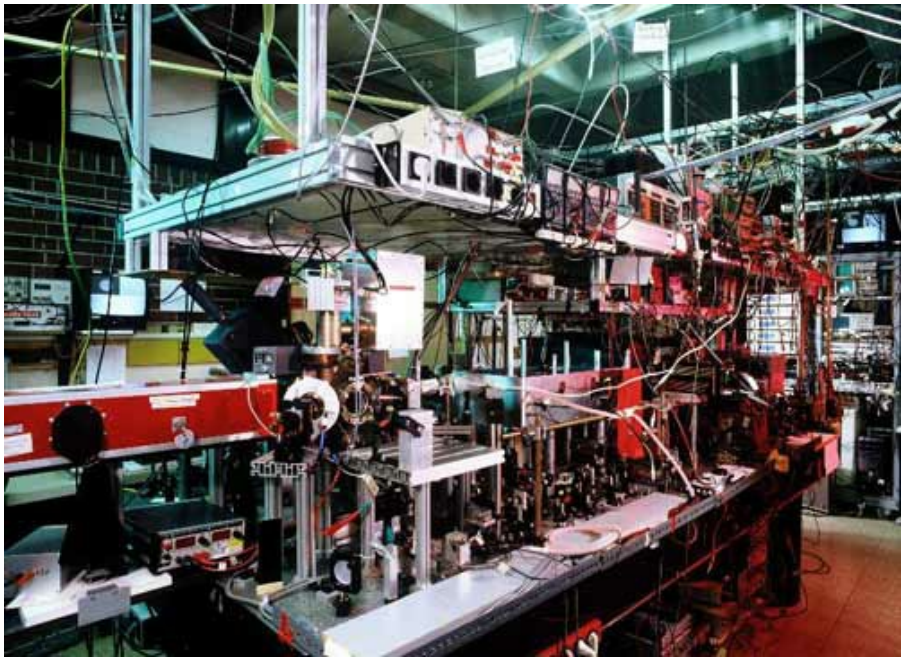
- **C - Les semi-conducteurs**

Voyant les limites de la RMN, Colin Williams du JPL de la NASA a suggéré de fixer les qubits dans des semi-conducteurs ou sur des photons piégés dans des cavités optiques.

Les méthodes pour y parvenir sont variées : les uns utilisent des électrons confinés dans des nanostructures semi-conductrices, les autres des noyaux associés avec des impuretés mono-atomiques dans un semi-conducteur ou encore des flux électroniques ou magnétiques circulant dans des supra-conducteurs.

Page 7/10 - Applications des ordinateurs quantiques

Admettons que notre ordinateur quantique soit fonctionnel. Si nous lançons un calcul sur base d'un algorithme classique sur un ordinateur quantique, le processus ne tournera pas plus vite quoi qu'on fasse. Par quelle magie alors un ordinateur quantique peut-il accélérer les calculs ?



Qu'est-ce que ce fatras de cables et d'appareils de mesures me demandez-vous ? Et bien...un ordinateur quantique ! Il a récemment été développé par le groupe d'Optique Quantique et de spectroscopie de l'Université d'Innsbruck (UIBK) en Autriche

Tout programmeur sait par exemple que si un calcul de multiplication est programmé sur un ordinateur supportant un encodage sur 8 bits, à vitesse CPU identique il n'ira pas plus vite s'il l'exécute sur une plate-forme 32-bits. Pour obtenir le résultat plus rapidement il doit recompiler le programme pour la nouvelle plate-forme afin de tirer avantage des nouvelles opérations sur 32-bits.

C'est la même chose avec un ordinateur quantique. **Pour qu'un ordinateur quantique exécute une tâche plus rapidement qu'un ordinateur classique, il faut exploiter sa puissance de calcul en parallélisme quantique.** Ces algorithmes sont difficiles à élaborer et on peut les compter aujourd'hui sur les doigts d'une main, parmi lesquels l'algorithme de Shor et celui de Grover.
On a estimé qu'un ordinateur classique requiert 10 millions de milliards de milliards d'années pour factoriser un nombre constitué de 1000 chiffres. En appliquant l'algorithme de Shor, notre programmeur obtiendra son résultat en... 20 minutes !

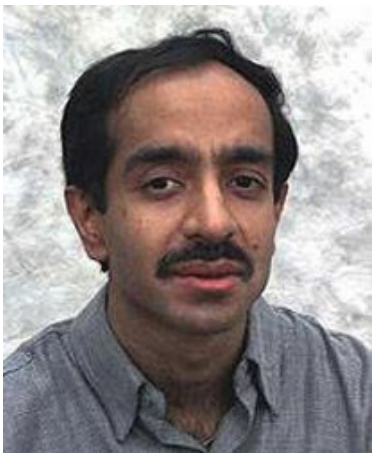
- **A - Les algorithmes de Shor et de Grover**

Nous n'allons malheureusement pas décrire les algorithmes de Peter Shor et de Lov Grover qui sortent du cadre de cet article mais vous trouverez suffisamment d'information sur Internet puisqu'ils sont aujourd'hui inséparables de l'évolution des ordinateurs quantiques.

Dr Peter Shor, mathématicien au MIT.

En quelques mots disons que l'algorithme inventé par Peter Shor en 1995 permet de factoriser rapidement de grands nombres. Il est principalement utilisé en cryptographie et trouvera sans nul doute des applications dans l'encryption des clés publiques telles que RSA (la clé publique permet d'encrypter un message tandis que la clé privée permet de le décrypter).

L'algorithme de Lov Grover a été conçu avant tout pour rechercher des informations dans des bases de données non indexées (triées) plus rapidement qu'un ordinateur conventionnel.


Dr Lov K. Grover, physcien aux Bell Labs/Lucent Technologies

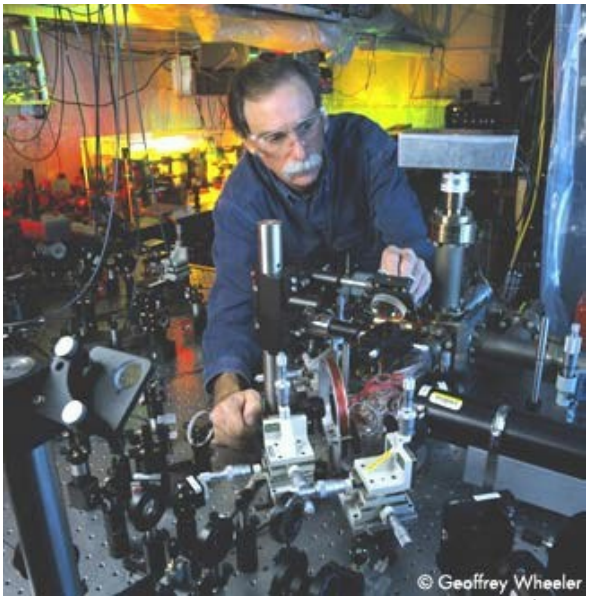
Normalement, il faut N/2 recherches pour trouver un enregistrement dans une base de données contenant N entrées. L'algorithme de Grover trouve la donnée en un temps √ N.

Lorsque les bases de données deviennent très volumineuses, le temps gagné devient très appréciable du fait que la toute la base de données est distribuée dans une multitude d'univers permettant d'effectuer une seule recherche dans chacun d'eux pour trouver le résultat. L'algorithme de Grover est également utilisé en cryptographie.

- **B - Simulation des systèmes quantiques**

En 1982, Richard Feynman imaginait qu'il serait un jour possible d'utiliser des ordinateurs quantiques pour simuler des systèmes quantiques avec bien plus de précision qu'il ne sera jamais possible de le faire avec des ordinateurs conventionnels.

Il imaginait ainsi qu'un ordinateur quantique de quelques dizaines de qubits pourrait réaliser des simulations quantiques qu'il serait vain de vouloir faire tourner sur des ordinateurs classiques en raison du temps nécessaire aux calculs.



Le physicien David Wineland du NIST ajustant un faisceau laser UV qui sera utilisé pour manipuler des ions piégés dans une chambre à vide. Ce dispositif est utilisé pour démontrer les fonctions de base d'un ordinateur quantique. © NIST - Tous droits de reproduction interdit

Sur un ordinateur classique, la dynamique d'un système quantique est d'ordinaire simulée par approximations. A l'inverse, un ordinateur quantique peut être “programmé” pour simuler le comportement d'un système en inférant les interactions entre ses variables; il imite en l'occurrence les propriétés du système en question. Un ordinateur quantique pourrait par exemple simuler le modèle de Hubbard, les mouvements des électrons dans un cristal, une simulation aujourd'hui impossible à simuler avec un ordinateur conventionnel.

- **C - La communication quantique**

Cette nouvelle technologie part du fait que l'information peut être encodée dans l'état de polarisation des photons (dans l'orientation de leur plan d'oscillation), chaque plan d'oscillation représentant un état quantique 0 ou 1. Ces deux modes de polarisation sont bien connus, il s'agit du mode rectilinéaire (propre aux polarisations verticales et horizontales) et du mode diagonal (polarisations à 45 et 135°).

Les données pourraient être encodées dans la polarisation des photons. **Pour recevoir ou lire les données il suffit que le plan de polarisation du filtre corresponde à celui des photons.** Si le plan de polarisation du récepteur est incorrect, s'il est rectilinéaire par exemple alors que celui du photon envoyé est diagonal, le résultat sera totalement aléatoire et le message sera illisible. En utilisant cette technique il est possible d'éviter toute écoute ou lecture indiscrète d'un message, le secret est maintenu.

En pratique, une transmission quantique s'établit en plusieurs étapes. **Tout d'abord l'émetteur envoie son message sans se préoccuper du mode de polarisation. Le récepteur enregistre l'information avec sa polarisation aléatoire.**

L'émetteur envoie ensuite au récepteur l'information sur la polarisation qu'il utilisa à travers un canal public. Le récepteur et l'émetteur comparent alors une sélection aléatoire parmi les informations reçues. Si un intermédiaire a intercepté puis retransmis l'information, l'émetteur et le récepteur seront avertis car il y aura un taux d'erreur beaucoup plus important que la normale. Dans ce cas tout le processus sera répété.

Ainsi dans un message dont on estime la réception correcte à 50%, il existe 50% d'information aléatoires. Imaginons qu'un pirate intercepte le message quantique puis le retransmette au destinataire. **En fait rien qu'en regardant le message, il altère son contenu puisqu'il s'agit d'un système quantique en superpositions d'états. Il est donc obligé de le retransmettre comme si de rien n'était. Erreur, le piratage est déjà enregistré ! Voyons pourquoi.**

Si la moitié des informations sont aléatoires, cela signifie dans le meilleur des cas que 75% des informations peuvent être interceptées par un tiers puis retransmises. Si le bruit est négligeable sur la ligne (0%), la tentative de ce pirate sera reconnue car l'information que le destinataire recevra contiendra dans ce cas plus de 25% d'erreurs. Il obtiendra cette information en comparant une sélection aléatoire du message avec le message original transmis par le canal public.

Ainsi que le disent les chercheurs d'IBM, les actions indiscètes de la personne placée sur la ligne de communication sont déjouées grâce aux propriétés quantiques de la lumière.
© IBM - Tous droits de reproduction interdit

Et si le pirate renvoyait son propre message à la place de l'original, me demanderez-vous ? L'émetteur et le destinataire le découvriront également puisque la vérification qu'ils effectueront consistera à prélever un groupe aléatoire de valeurs. **Si un pirate a interposé son message, il ne sera de toute façon plus identique au message original.** Quoique le pirate puisse faire pour maquiller son message, l'expéditeur et le destinataire pourront toujours découvrir que leur ligne a été mise sur écoute.

Bien sûr cette méthode ne fonctionne que si le bruit sur la ligne de transmission est inférieur à la marge d'erreur. Actuellement un tel système existe déjà. British Telecom teste actuellement une ligne quantique présentant 9% d'erreurs sur une distance de 10 km. Le piratage des télécommunications sera bientôt une vieille histoire !

Page 8/10 - L'avenir

L'informatique “liquide” inventée par le Dr. Gershenfield et le Dr. Chuang permet d'envisager un avenir radieux à l'ordinateur quantique. Selon leurs estimations, celui-ci pourrait voir le jour dans moins d'une génération si les progrès à venir se maintiennent au taux actuel.

La bonne nouvelle dans ces développements est que les problèmes auxquels nous faisons face aujourd'hui sont considérés comme des problèmes techniques plutôt que fondamentaux.

Dessin extrait de l'article sur l'informatique quantique écrit par A.Barenco, A.Ekert, A. Sanpera et C.Machiavello dans La Recherche en novembre 1996.

Demain peut-être une éprouvette contenant une solution organique et un électro-aimant consisteront le coeur des ordinateurs quantiques.

Les modèles les plus compacts seront également des objets de décoration, faisant parfois office de presse-papier sur votre bureau. A l'occasion ils pourront se transformer en jus de fruit ou en tasse de café !

Reste la décohérence. Personne, ni à Los Alamos, au MIT, à Princeton ou chez IBM n'entrevoit de solution au delà de systèmes dépassant 10 qubits du fait que la décohérence rend les systèmes trop fragiles pour être exploitables.

Page 9/10 - En guise de conclusion

Si l'ordinateur conventionnel approche lentement de ses limites, l'ordinateur quantique nous promet de s'en affranchir en nous offrant une puissance de calcul et un temps d'exécution inimaginables jusqu'à présent.

L'ordinateur quantique devient théoriquement capable de simuler une infinité de processus physiques et il cache peut-être dans ces circuits atomiques le secret de la création de l'ordinateur doté d'intelligence artificielle.

Le XXIeme siècle est sans nul doute celui de l'information, une information qui s'affranchit ironiquement de tout risque de piratage. **Demain nos administrateurs réseau et nos équipes du support informatique devront peut-être maîtriser la physique quantique pour dépanner les utilisateurs et bientôt on apprendra ses rudiments à l'école primaire !** Finalement les cours préparatoires de physique quantique enseignés aux jeunes élèves de Star Trek n'est peut-être pas si utopique que cela...

La quantique et ses lois qui nous paraissent si étranges nous permettront peut-être de résoudre les problèmes les plus métaphysiques que se pose la science aujourd'hui à propos de l'esprit ou de l'univers. Car ses moyens nous permettent réellement d'appréhender des questions complexes, qu'aucun ordinateur conventionnel ne peut appréhender. **Reste bien sûr à le programmer correctement, ce qui fera certainement l'objet de bien des années de durs labeurs.** Mais un jour espérons-le, nous pourrons répondre à des questions qui sont aujourd'hui du ressort de la philosophie.

Avec une telle motivation, on ne peut qu'encourager les chercheurs qui s'investissent dans cette voie royale et leur souhaiter de réussir leur entreprise.

Page 10/10 - Pour en savoir plus

Important :

Un dossier préparé et publié avec l'accord de Thierry Lombry webmaster du site "Luxorion." Toute reproduction partielle, texte et image est interdite sans l'accord de l'auteur voir sa : FAQ.

FUTURA - SCIENCES .COM
Le savoir s'invite chez vous