L'ordinateur q

L'ordinateur quantique verra-t-il le jour ? En 1996, La Recherche *répercutait le discours sceptique de certains chercheurs. Dix ans plus tard, des progrès sensibles ont été accomplis. Mais aucun calcul complexe n'est encore en vue. Il va falloir franchir un « abysse », selon un des ténors du domaine. C'est cependant possible. La théorie est bien en place, les pistes pour débusquer le meilleur support d'information quantique ne manquent pas, et les expériences se multiplient. Autre signe favorable, les programmes de recherche subventionnés par les États et les industriels ne cessent de se multiplier.*

uantique

EN DEUX MOTS À l'échelle de l'atome, des effets quantiques perturbent le fonctionnement des composants électroniques. Au contraire, un « ordinateur quantique » tirerait profit des lois régissant l'infiniment petit. En particulier, un système quantique peut se trouver dans une superposition d'états. En manipulant de tels systèmes, les théoriciens montrent comment le calcul quantique résout des problèmes plus rapidement que les ordinateurs actuels.

1 Comment calculer « quantique »

Calculer plus vite et résoudre des problèmes hors de portée de nos ordinateurs : ce sont les promesses de l'informatique quantique. Ce domaine de recherche connaît un véritable essor, et les exemples illustrant la supériorité du calcul quantique sont nombreux.

Julia Kempe, Sophie Laplante et Frédéric Magniez sont membres du laboratoire de recherche en informatique, à Orsay.
kempe@lri.fr
laplante@lri.fr
magniez@lri.fr

En novembre 2005, des mathématiciens allemands réussissaient à factoriser un nombre de 193 chiffres, remportant ainsi un défi lancé par la société américaine RSA [1]. Cette compagnie, experte en cryptographie, a bâti la fiabilité de ses codes sur la difficulté de factoriser des grands nombres. La performance affichée par les Allemands a d'ailleurs nécessité de gros moyens : cinq mois de calculs complexes réalisés sur plus de 80 ordinateurs en réseau ont été nécessaires. Avec un ordinateur « quantique », dont le principe consiste à utiliser les lois de la physique quantique pour manipuler l'information d'une manière plus efficace, quelques secondes auraient suffi pour remporter ce défi !

Le commerce électronique et la confidentialité des transactions financières sont-ils menacés, à terme, par le calcul quantique ? Certains n'hésitent pas à l'envisager. Car depuis la découverte par l'informaticien américain Peter Shor, en 1994, d'un « algorithme quantique » permettant de factoriser des grands nombres en un temps relativement court, les recherches dans le domaine de l'informatique quantique ont pris un essor considérable.

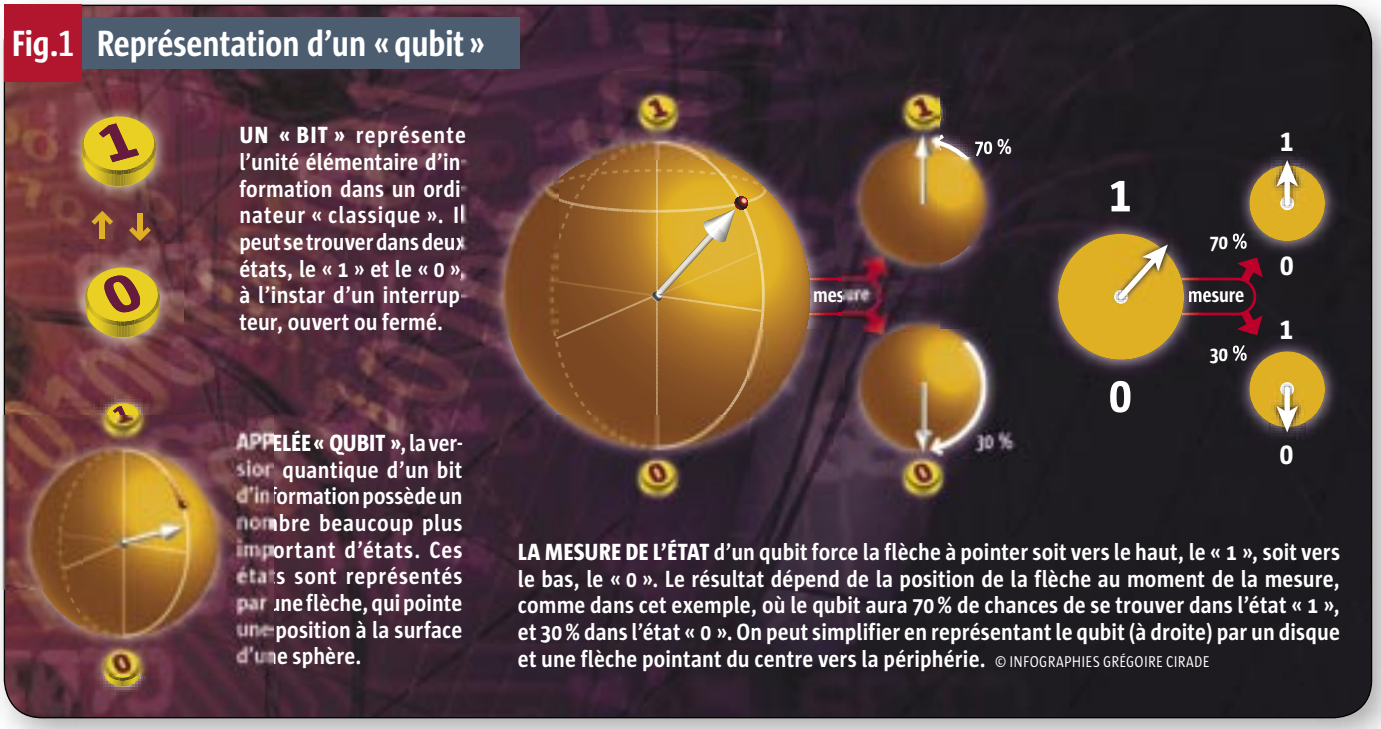
Algorithmes divers

De nombreux informaticiens, physiciens et mathématiciens travaillent aujourd'hui ensemble afin d'éliminer les obstacles, tant théoriques qu'expérimentaux, qui s'opposent encore à la réalisation d'une telle machine. Déjà, des progrès sont notables au-delà de la factorisation des grands nombres : d'autres algorithmes ont été élaborés, et pourraient être utilisés dans un ordinateur quantique si celui-ci venait à voir le jour. Pas encore de quoi crier victoire, mais les ⇨

[1] www.crypto-world.com/announcements/rsa640.txt

L'ORDINATEUR QUANTIQUE 1

Fig.1 Représentation d'un « qubit »



© INFOGRAPHIES GRÉGOIRE CIRADE

⇨ spécialistes de la sécurité informatique suivent, pas à pas, le développement de ces recherches.

Retour à la situation actuelle. Dans nos ordinateurs, l'information est stockée physiquement dans des transistors, composants électroniques se comportant comme des interrupteurs. Ils se trouvent dans un état « allumé » ou « éteint », selon qu'ils permettent ou non le passage du courant électrique. C'est par ces deux états, désignés, par convention par « 1 » ou « 0 », que la quantité élémentaire d'information est définie : le « bit ». Tout calcul effectué par un ordinateur se décompose en une suite d'opérations qui agissent sur l'état de quelques bits à la fois.

Plus le nombre d'informations à traiter est important, plus le nombre d'opérations doit être grand. Telle est l'épine principale dans le pied de l'informaticien. D'autant plus que, pour certaines tâches, le temps de calcul augmente exponentiellement avec la quantité d'information. Certes, la miniaturisation fait croître les performances des ordinateurs selon l'empirique « loi de Moore » : le nombre de transistors sur une puce de silicium double tous les dix-huit mois. Mais cette évolution ne pourra se poursuivre indéfiniment. À l'horizon 2020, la taille des transistors approchera celle de l'atome. À cette échelle, les effets quantiques perturbent le fonctionnement des composants électroniques. Un obstacle technologique à ce jour incontournable.

Au lieu de les considérer comme « nuisibles », un ordinateur quantique utiliserait les lois de la physique quantique pour calculer plus rapidement, et résoudre des problèmes hors de portée des ordinateurs « classiques ». Pour la plupart, ces lois n'ont pas d'équivalents dans le monde sensible. Selon l'« équation de Schrödinger », par exemple, qui doit son nom au physicien autrichien qui l'a formulée, et qui décrit, en fonction du temps, le comportement d'un système quantique, des combinaisons d'états possibles correspondent de façon égale à un état possible. Ainsi, aussi étrange que cela puisse paraître, une particule peut se trouver, au même moment, dans deux états à la fois !

> La « superposition quantique » permet de calculer plus rapidement

Pour expliquer le passage du monde quantique au monde « classique », les physiciens ont recours à la théorie de la « décohérence » : plus un système physique interagit avec son environnement, comme c'est le cas pour les objets macroscopiques, plus les phénomènes quantiques s'estompent. C'est pour cette raison que l'état de superposition d'une particule est détruit dès que ses propriétés sont observées par un appareil de mesure. La particule se retrouve alors dans un état déterminé. Les chercheurs espèrent tirer profit du phénomène de superposition quantique pour manipuler l'information d'une manière plus efficace. Le support physique de l'information n'est plus un transistor, mais n'importe quelle particule susceptible de posséder deux états en superposition : un électron, un photon, et même un atome.

En informatique quantique, de tels systèmes sont appelés « qubit ». On peut les représenter par un disque, au centre duquel part une flèche qui pointe une position de la circonférence [fig. 1]. Cette position correspond à l'état quantique du système. Si la flèche pointe le haut du disque, le qubit est dans l'état « 1 » ; si elle pointe vers le bas, il est dans l'état « 0 ». Pour tous les autres états, le qubit est en superposition quantique. La position de la flèche détermine la « proportion » de l'état « 1 » et de l'état « 0 » dans le qubit.

Qubit flexible

Comme le postulent les lois de la mécanique quantique, en mesurant l'état du qubit, la superposition est détruite. La flèche est instantanément projetée sur le « 1 » ou le « 0 », avec une probabilité qui dépend de sa position avant la mesure. Plus la flèche est proche d'un pôle, plus la probabilité que celle-ci soit projetée sur ce pôle est grande. Si la flèche est en position horizontale, elle est projetée avec une probabilité égale vers le « 1 » ou le « 0 ».

Grâce au phénomène de superposition et à la multiplicité d'états dans lequel un qubit peut se trouver, il peut être manipulé d'une manière beaucoup plus flexible qu'un bit d'information. Dans un ordinateur classique, les calculs sont effectués par l'intermédiaire de circuits électroniques, qui modifient l'état des transistors selon des opérations de la logique booléenne*. Celles-ci sont appelées « portes logiques ». Pour qu'un transistor passe de l'état « 1 » à l'état « 0 », par exemple, une seule porte est possible : les informaticiens l'appellent « NON ».

En informatique quantique, une opération similaire consisterait à modifier l'état d'un qubit de sorte que la flèche pivote de 180°. Mais d'autres manipulations, ou « portes logiques quantiques », sont aussi possibles. Par exemple, celle qui consiste à faire tourner la flèche de 90° dans le sens des aiguilles d'une montre est appelée « racine carrée de NON ». En partant d'un état déterminé (le « 0 » ou le « 1 »), deux opérations de ce type (90° + 90° = 180°) équivalent ainsi à une porte NON classique [fig. 2].

Cette porte quantique conduit à des résultats surprenants. En effet, une seule opération suivie d'une mesure de l'état du qubit renvoie celui-ci en position « 0 » ou « 1 », avec une probabilité de 50 %. Autrement dit, en partant d'un état déterminé, on arrive dans un état apparemment « désordonné ». Si cet état n'est pas mesuré, il est possible de répéter l'opération. On revient alors à un état déterminé ! Ce processus est d'autant plus étonnant qu'il semble violer le deuxième principe de la thermodynamique*, qui prédit l'accroissement du désordre pour un système. Cette porte logique n'a en fait aucune contrepartie en physique classique.

Des résultats remarquables peuvent être obtenus à l'aide d'un seul qubit, mais le calcul quantique prend tout son intérêt avec la manipulation de plusieurs qubits à la fois. Dans le cas classique, 3 bits d'information correspondent à 3 transistors indépendants, allumés ou éteints. En informatique quantique, 3 qubits ne sont pas équivalents à 3 disques autonomes. Ils correspondent à une sorte de « super-disque » multidimensionnel. Pour trouver le nombre d'états accessibles classiquement, on multiplie le nombre d'états d'un qubit par lui-même autant de fois que l'on a de qubits : on obtient 2 x 2 x 2 = 8 états.

Mais un système composé de 3 qubits peut être dans une superposition de ces 8 états. Dans ce cas, le système prend « simultanément » toutes les valeurs possibles. De plus, les qubits ne sont pas indépendants. Agir sur l'un d'entre eux produit un effet sur les autres : ce phénomène s'appelle l'« intrication quantique ». Certes, après une mesure, seules les valeurs classiques (3 bits d'information) pourront être extraites. Il n'en demeure pas moins que la manipulation « astucieuse » d'un ou de plusieurs qubits permet d'arriver à des résultats étonnants. C'est le physicien britannique David Deutsch qui, le premier, vers le milieu des années 1980, imagina un algorithme quantique illustrant ce principe [fig. 3]. Le problème que son algorithme permettait de résoudre était cependant très théorique, et l'avantage minime. Mais, grâce à ce que l'on appelle aujourd'hui le « problème de Deutsch », preuve venait d'être faite de la supériorité du calcul quantique pour un problème donné (lire l'entretien p. 35) [2].

Jusqu'au début des années 1990, seul un petit nombre de chercheurs poursuivent la piste proposée par D. Deutsch. Parmi eux, André Berthiaume et Gilles ⇨

*** La logique booléenne** permet de manipuler des formules sur des variables logiques qui prennent la valeur « vrai » ou « faux », à l'aide de symboles comme ET, OU et NON.

*** Le deuxième principe de la thermodynamique** est une loi qui établit l'irréversibilité de certains phénomènes physiques, en particulier lors des échanges de chaleur.

[2] D. Deutsch, *Proc. Roy. Soc. London Ser. A, 400*, 97, 1985.

Fig.2 Portes logiques quantiques

UNE PORTE LOGIQUE permet d'effectuer des opérations sur les unités élémentaires d'information. Dans un ordinateur classique, la porte « NON » fait basculer un transistor de l'état « 0 » à l'état « 1 », et inversement. En informatique quantique, la même opération consiste à modifier l'état d'un qubit de sorte que la flèche pivote de 180°. Mais d'autres manipulations sont possibles. La porte « √NON », par exemple, qui n'a aucun équivalent en informatique classique, entraîne une rotation de 90° dans le sens des aiguilles d'une montre. Une mesure de cet état donnera 0 et 1 avec la même probabilité de 50 %. Il faut appliquer deux fois √NON pour changer complètement l'état d'un qubit.

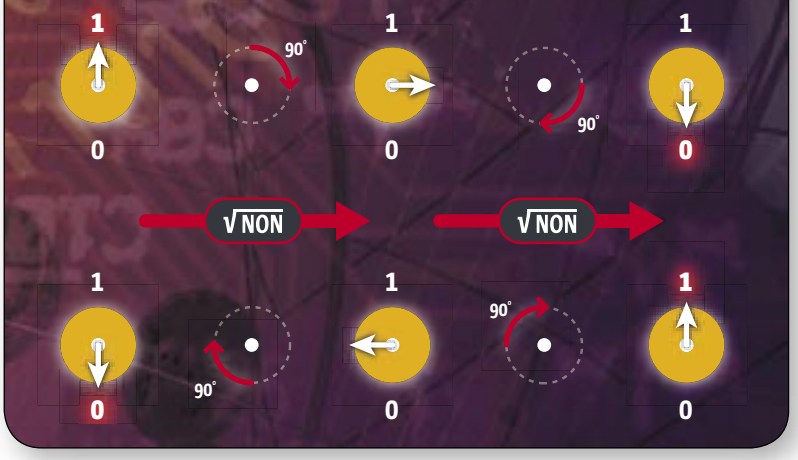
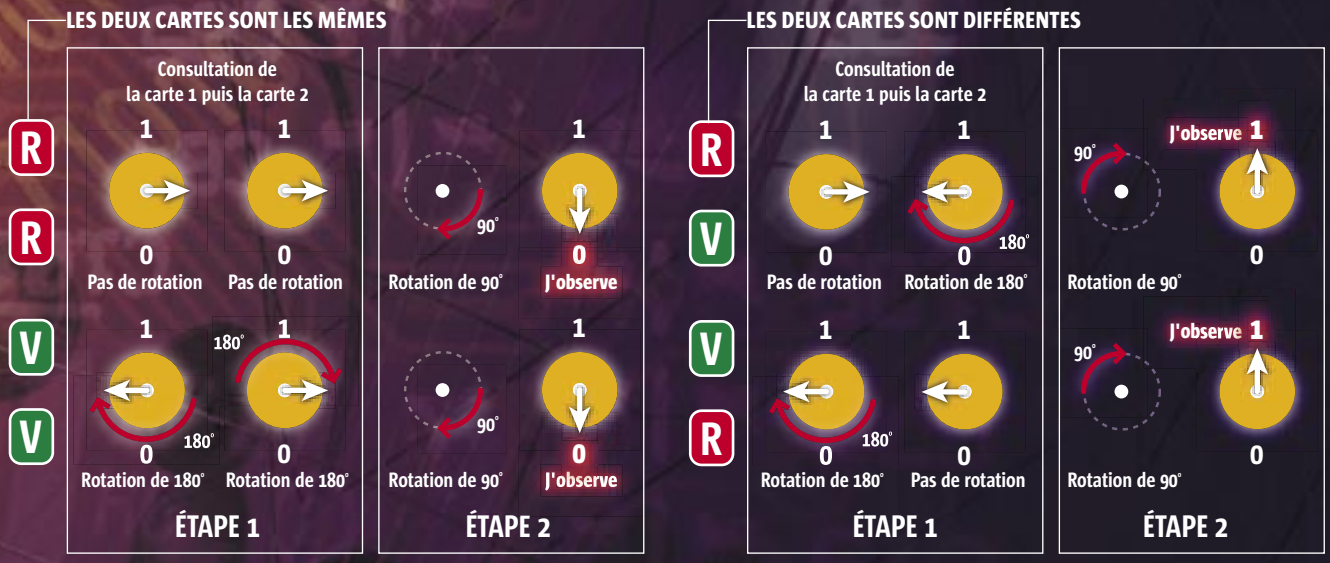


Fig.3 Le problème de Deutsch

UN CROUPIER DISPOSE DE DEUX CARTES MASQUÉES, ROUGES OU VERTES. Il faut deviner si les deux cartes sont de la même couleur ou pas. Même quand le croupier permet de découvrir l'une des deux cartes, on n'a pas plus d'une chance sur deux de gagner. Dans le monde quantique, on peut résoudre un problème analogue où la consultation des cartes est une opération quantique qui permet de les consulter simultanément.

CONSULTATION DES CARTES. On utilise un qubit en état de superposition de 0 et 1 : 0 désigne la consultation de la première carte ; 1 la consultation de la seconde. Les propriétés de la mécanique quantique permettent alors de regarder les deux cartes en superposition (à gauche). Le phénomène de superposition permet au qubit de recueillir l'information sur les deux cartes à la fois, même si, à ce moment, aucune information classique n'est extraite. Ensuite, si la carte est rouge, l'état du qubit reste inchangé ; si elle est verte, la flèche pivote de 180° (à droite).



L'ALGORITHME. On procède en deux étapes. D'abord, une opération quantique permet de consulter les cartes (étape1), et le résultat de la consultation est stocké dans le qubit. Ensuite, on manipule le qubit, et on le mesure (étape2). Lorsque les cartes ont la même couleur (à gauche), si elles sont rouges, le qubit ne change pas d'état ; si elles sont vertes, le qubit effectue deux rotations de 180° : il revient à l'état initial. Lorsque les cartes sont de couleur différente (à droite), si l'une est rouge et l'autre verte, le qubit ne change pas de position, puis la flèche pivote de 180°. Si l'une est verte et l'autre rouge, la flèche pivote de 180°, puis ne change pas de position. La deuxième étape consiste à faire effectuer au qubit une rotation de 90° dans le sens horaire. Quand on mesure le qubit, on obtient 0 si les deux cartes sont de même couleur ; on obtient 1, si elles étaient de couleur différente. La mesure du qubit donne le bon résultat dans 100 % des cas.

⇨ Brassard, de l'université de Montréal, formalisent en 1992 la notion de complexité (une théorie qui permet d'évaluer la « difficulté » d'un calcul) pour les ordinateurs quantiques [3]. Au même moment, D. Deutsch et Richard Jozsa, tous deux à l'université d'Oxford, généralisent le « problème de Deutsch » à grande échelle [4]. L'année suivante, Ethan Bernstein et Umesh Vazirani, de l'université Berkeley, commencent à étudier les limites de la puissance de calcul d'un (hypothétique) ordinateur quantique [5].

L'idée de Peter Shor

Malgré ces premiers succès, rares étaient les chercheurs qui, à l'époque, croyaient à la faisabilité pratique d'un ordinateur quantique : entamer une thèse de doctorat dans le domaine de l'informatique quantique était alors très risqué. Seuls quelques chercheurs bien établis ont eu le loisir de s'y investir pleinement.

L'année 1994 constitua un tournant pour la discipline. Peter Shor, de la compagnie américaine AT&T, montra comment un algorithme quantique pourrait factoriser un nombre en un temps beaucoup plus court qu'au moyen des meilleurs algorithmes classiques [6]. L'algorithme de Shor est composé de deux parties. La première transforme le problème de factorisation en un problème de recherche de la périodicité d'une fonction mathématique, ce qui peut être réalisé de manière « classique ». La seconde partie trouve la période à l'aide d'une opération appelée « transformée de Fourier quantique* ». L'intérêt de cette transformation pour les problèmes de périodicité venait d'être mis en évidence par Daniel Simon, alors à l'université de Montréal [7].

[3] A. Berthiaume et G. Brassard, *Proc. IEEE Conference on Structure in Complexity Theory*, 132, 1992.

[4] D. Deutsch et R. Jozsa, *Proc. Roy. Soc. London A, 439*, 553, 1992.

[5] E. Bernstein et U. Vazirani, *Proc. ACM Symposium on the Theory of Computing*, 11, 1993.

L'article de P. Shor eut un impact retentissant du côté des cryptographes ! En effet, la plupart des protocoles, comme ceux utilisés pour assurer la confidentialité d'une carte bancaire par exemple, reposent sur la complexité de la factorisation ou d'opérations mathématiques similaires. Bien sûr, en 1994 (c'est encore vrai aujourd'hui), aucune machine capable d'utiliser l'algorithme de Shor n'existait. L'inquiétude des experts en sécurité informatique était néanmoins sensible.

Mais le scepticisme dominait. Nombre de physiciens, et non des moindres, se sont empressés de dénoncer l'impraticabilité de l'algorithme de Shor. « *Face à certaines promesses irréalistes d'applications pratiques en un domaine où tant de prévisions excessivement optimistes ont déjà été formulées,* écrivaient dans nos colonnes en 1996 Serge Haroche et Jean-Michel Raimond, de l'École normale supérieure, *nous estimons nécessaire une mise en garde… Plutôt que de nous apprendre comment fabriquer un ordinateur quantique de grande taille, il est plus vraisemblable que de telles expériences nous renseignent sur les processus qui feraient en définitive échouer une telle entreprise* [8] ».

Les physiciens « sceptiques » se focalisaient sur la fragilité de l'information quantique. Dans un ordinateur classique, en effet, la nature binaire de l'information rend celle-ci très « robuste ». Pour que des erreurs de calcul se produisent, la seule manière est qu'un transistor bascule spontanément de l'état « 0 » à l'état « 1 », ce qui est extrêmement rare. En revanche, un bit quantique se trouve dans un état particulièrement fragile, car le système physique qui le porte doit être soumis à des contraintes sévères. En particulier, le qubit doit être bien isolé de son environnement, afin que le phénomène de décohérence ne se produise pas. Auquel cas, l'état de superposition quantique serait détruit. En outre, une variation même infime de l'état de superposition se propagerait aux autres qubits.

Les interactions avec l'environnement menacent l'intégrité des qubits

Les tenants de l'informatique quantique ne se découragèrent pas pour autant. Dès 1995, des solutions permettant de corriger et de stabiliser l'information contenue dans un qubit ont été proposées. Grâce aux travaux de P. Shor, la discipline a gagné en crédibilité, et plusieurs physiciens et informaticiens de renom se sont lancés dans la course à l'ordinateur quantique. Les financements, tant publics que privés, affluèrent. Les militaires furent également de la partie, en raison du potentiel de déchiffrage rapide pour les communications secret-défense que laissait entrevoir l'informatique quantique.

Depuis une dizaine d'années, les recherches deviennent plus nombreuses et attractives. Les expérimentateurs tentent de déterminer le système physique le plus effi- ⇨

*** La transformée de Fourier** est une technique algorithmique permettant de déterminer le spectre de fréquences d'un signal.

[6] P. Shor, *Proc. IEEE Symposium on the Foundations of Computer Science,* 124, 1994.

[7] D. Simon, *Proc. IEEE Symposium on the Foundations of Computer Science,* 116, 1994.

[8] S. Haroche et J.-M. Raimond, « L'ordinateur quantique : rêve ou cauchemar ? », *La Recherche,* novembre 1996, p. 58.

ENTRETIEN

David Deutsch : « J'ai démontré la supériorité du calcul quantique »

Considéré comme le « père » de l'ordinateur quantique, David Deutsch, physicien théoricien de l'université d'Oxford, est le premier à avoir démontré la supériorité du calcul quantique sur le calcul classique pour un problème donné.

Comment vous êtes-vous intéressé au calcul quantique ?

DAVID DEUTSCH : Vers le milieu des années 1970, j'effectuais mes études à l'université du Texas, dans un laboratoire où travaillaient Bryce DeWitt et John Wheeler. Comme la plupart des physiciens, la vision que ce dernier avait de la mécanique quantique était « non déterministe ». Pour preuve : le phénomène de superposition quantique, où une particule peut se trouver dans deux états à la fois. B. DeWitt défendait, lui, une interprétation de la mécanique quantique appelée « multi-mondes ». Elle suppose l'existence de particules « fantômes » qui interagissent de la même manière que dans le monde tangible, mais dans des… « univers parallèles ». Ces particules n'« apparaissent » dans notre monde qu'en de rares occasions, comme lors de phénomènes dits d'interférences quantiques. Plus je progressais dans mes recherches, plus je m'apercevais que l'approche non déterministe était physiquement et philosophiquement intenable. En 1977, j'ai démontré qu'en théorie il devrait être possible de réaliser une expérience prouvant l'existence de ces univers multiples. Le principe de ce montage correspond à ce que l'on appelle aujourd'hui un « ordinateur quantique ».

En quoi consiste-t-il ?

Cet « ordinateur » utilise des algorithmes qui manipulent l'information *via* des systèmes en état de superposition quantique, et non plus des bits d'information classiques. Plus tard, j'ai montré qu'un tel algorithme permet d'identifier les propriétés de certaines fonctions mathématiques en une seule opération, alors qu'un algorithme classique en a besoin d'au moins deux pour effectuer la même tâche. C'était la première fois que la supériorité du calcul quantique était prouvée. En outre, je défendais l'idée que la théorie du calcul quantique est une théorie universelle, dont le calcul « classique » n'est qu'une approximation.

Comment la communauté scientifique a-t-elle réagi ?

Considéré comme trop « spéculatif », le résultat de mes recherches sur les univers parallèles n'a été publié qu'en 1984. Cinq chercheurs, tout au plus, ont pris mon article au sérieux ! Quelques années plus tard, Arthur Eckert, de l'université d'Oxford, s'est penché sur mes travaux, et a développé de nombreux aspects de la théorie du calcul quantique. Surtout, il a convaincu de nombreux physiciens, théoriciens et expérimentateurs, de l'intérêt du calcul quantique. C'est grâce à lui que mes travaux ont eu ensuite un impact important.

Propos recueillis par Franck Daninos

Fig.4 L'algorithme de Grover

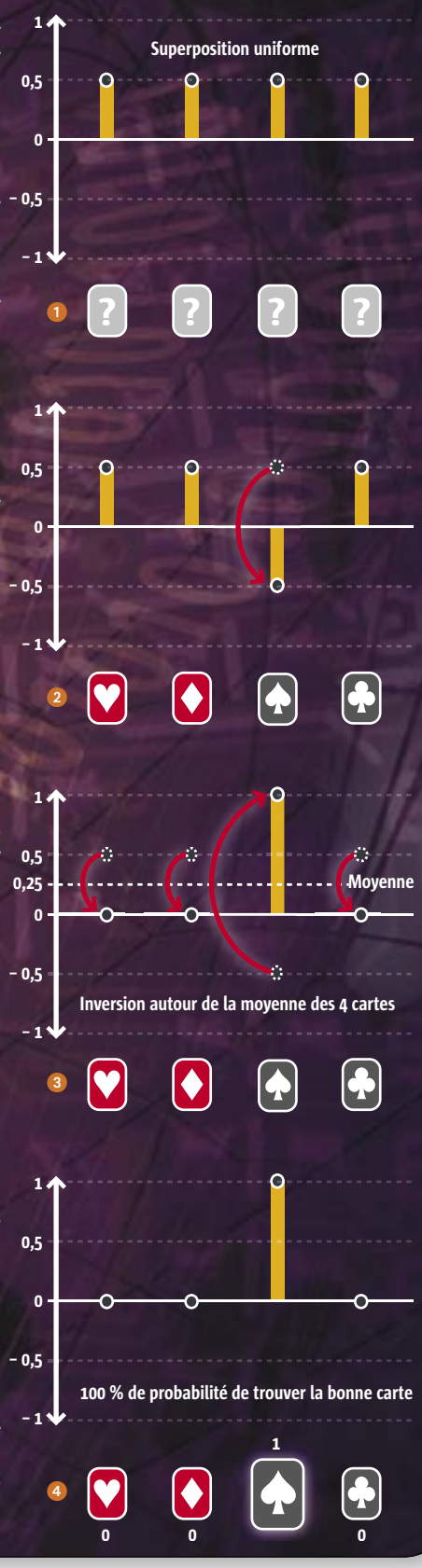
LES QUATRE AS d'un jeu de cartes sont sur la table, face invisible. Comment trouver l'as de pique en ne retournant qu'une carte ? On a seulement une chance sur quatre de gagner. Ce type de problème peut être transposé dans le monde quantique. Pour cela, on a besoin de deux qubits : ils forment un système qui peut se trouver en état de superposition de quatre états. Chacun de ces états interagit avec le système où sont codées les « cartes ». Les lois de la mécanique quantique permettent aux qubits de « consulter » en superposition les quatre cartes en même temps. Toutefois, aucune information classique ne peut encore être extraite.

ON PLACE LES QUBITS en état de superposition uniforme afin que la probabilité de trouver une carte sur quatre soit la même 1. En calcul quantique, on parle alors d'« amplitude » : elle est égale à la racine carrée de la probabilité de trouver la bonne carte ($\sqrt{0,25} = 0,5$).

L'ALGORITHME QUANTIQUE est défini de telle sorte que l'amplitude de l'état correspondant à la position de l'as de pique (dans ce schéma 2, la troisième carte) soit remplacée par sa symétrique par rapport à l'axe horizontal 0 : l'amplitude change donc de signe (-0,5). Pour les trois autres états, elle reste inchangée (0,5).

ON PROCÈDE ENSUITE 3 à une nouvelle inversion, mais cette fois-ci par rapport à la moyenne (0,25).

POUR L'ÉTAT CORRESPONDANT à la position de l'as de pique 4, l'amplitude devient égale à 1 (2(0,25)+0,5=1) ; elle vaut 0 pour les trois autres états (2(0,25)-0,5=0). Lorsque l'on mesure l'état quantique du système, on a 100 % de chances de trouver l'as de pique du premier coup : il est à la position correspondant au seul état d'amplitude 1.



⇨ cace pour stocker et manipuler un nombre suffisamment important de qubits (lire « Les constructeurs de qubits », p. 38). Les théoriciens, pour leur part, cherchent à identifier les problèmes susceptibles de bénéficier d'une résolution rapide à l'aide d'un ordinateur quantique. Ils doivent encore trouver le bon algorithme quantique, et prouver qu'aucun algorithme classique n'est à même de résoudre ces problèmes de manière efficace.

Pour cela, ils ont recours à la « théorie de la complexité ». Cette approche fondamentale de l'informatique théorique a pour objectif de classer les problèmes de calcul en fonction des ressources nécessaires pour les résoudre : le temps, l'espace mémoire, la quantité d'information, etc. Grâce à elle, il est souvent possible de prouver qu'en considérant une classe de problème et un certain type de ressources n'importe quel algorithme qui résout correctement un problème donné doit consommer, au minimum, une certaine quantité de ces ressources.

La méthodologie consiste à prendre un problème, ou une classe de problèmes liés, et de démontrer que, si un algorithme prétend le résoudre en mobilisant moins d'une certaine quantité de ressources, cet algorithme fera forcément des erreurs. On conclut alors que tout algorithme correct doit consommer plus que la quantité de ressources précédemment fixée.

Les « marches aléatoires »

Par cette méthode, la supériorité du calcul quantique pour la factorisation n'a pour le moment pas pu être démontrée. Certains informaticiens estiment même qu'un algorithme classique aussi efficace que l'algorithme quantique de Shor sera un jour découvert. En revanche, pour d'autres problèmes, comme la recherche d'une information pertinente au sein d'une base de données, par exemple, la supériorité d'un ordinateur quantique a été prouvée, grâce aux travaux réalisés depuis 1997 par Lov Grover, des laboratoires Bell, dans le New Jersey [9] [fig. 4].

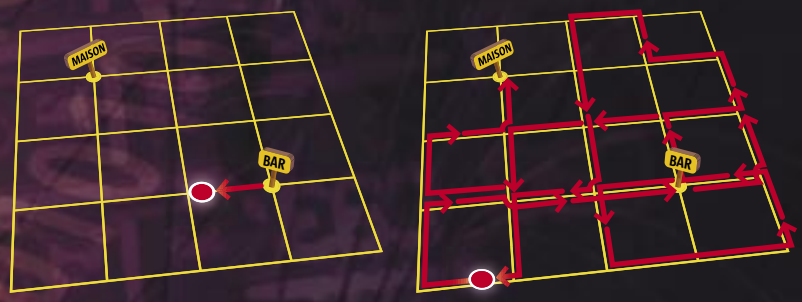
Plus récemment, l'algorithmique probabiliste a permis aux concepteurs d'algorithmes quantiques d'enregistrer d'autres succès remarquables, en s'inspirant notamment de l'approche dite des « marches aléatoires ». L'idée est que, lorsqu'un algorithme ne sait pas quel chemin de calcul adopter, autant qu'il choisisse celui-ci au hasard. Avec une certaine probabilité, un tel choix conduira à une impasse dans le calcul. Mais pour certains algorithmes, on peut montrer que cette stratégie est judicieuse dans l'immense majorité des cas.

Prenons un exemple simple de parcours de recherche aléatoire. Imaginons un village quadrillé par des rues horizontales et verticales, qui abritent 25 maisons. À chaque intersection se trouve une maison. Un soir, un homme ivre sort du bar à la recherche de son gîte. Il ne sait plus où celui-ci se situe, et pour le retrouver, il choisit une direction au hasard. Malheureusement,

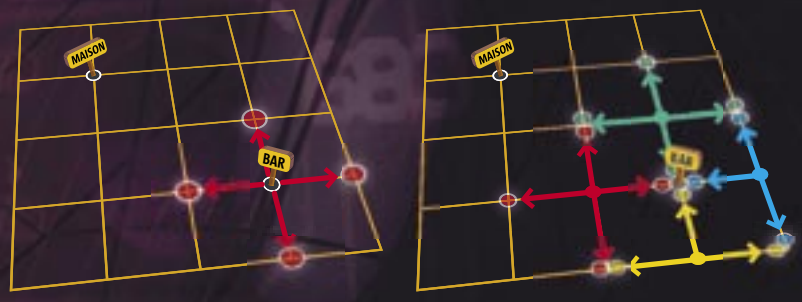
Fig.5 L'ivrogne quantique

LE CLIENT D'UN BAR cherche à regagner sa maison. Mais il est tellement ivre qu'il a oublié dans quelle direction aller. Pour la retrouver, il choisit une direction au hasard, et doit visiter, l'une après l'autre, les maisons de son village, représenté ici par un quadrillage (5 rues croisent 5 rues). Chaque intersection correspond à une maison. Ayant totalement perdu la mémoire, l'ivrogne peut très bien revenir sur ses pas. Un calcul statistique montre qu'après 25 étapes il est presque sûr de trouver sa maison.

DANS LE MONDE QUANTIQUE, pour explorer plus rapidement les différents points d'un quadrillage, on peut utiliser deux qubits en état de superposition quantique uniforme. Par analogie, ces qubits correspondent à un « ivrogne quantique » qui serait capable, en sortant du bar, de visiter les quatre maisons avoisinantes, en superposition quantique. En utilisant un algorithme quantique, on montre qu'après 5 « visites » en état de superposition quantique, il est tout aussi sûr d'arriver chez lui !



Après 25 étapes, il a de très fortes chances d'arriver chez lui



Après 5 étapes (ici, seules 2 étapes sont représentées), il a de très fortes chances d'arriver chez lui

son état l'empêche aussi de mémoriser les directions qu'il a prises. L'ivrogne effectue ainsi une marche aléatoire au sein d'une grille à deux dimensions. En moyenne, l'ivrogne devra visiter 25 maisons avant de réussir à trouver la sienne.

La marche aléatoire est souvent pertinente pour des algorithmes disposant d'une quantité de mémoire limitée. Elle peut être utilisée pour résoudre toute une classe de problèmes, comme savoir si deux points sont liés ou non par un chemin au sein d'un réseau de grande taille (voiries, Internet, etc.). Au Laboratoire de recherche en informatique, à Orsay, nous nous inspirons de cette approche pour élaborer de nouveaux algorithmes quantiques. Ainsi nous avons montré qu'en choisissant, dans l'exemple précédent, une superposition quantique de directions à chaque intersection du quadrillage, un « ivrogne quantique » trouvera sa maison en 5 étapes seulement [10] [fig. 5].

De plus en plus d'exemples illustrent la supériorité des algorithmes quantiques

Les exemples illustrant la supériorité du calcul quantique sont ainsi de plus en plus nombreux. Mais les recherches en informatique quantique ont eu aussi des retombées inattendues dans le domaine de l'informatique… classique ! Pour le comprendre, prenons l'exemple suivant. La « taille » d'une formule de la logique booléenne, permettant de décrire un problème donné, correspond au nombre minimal de symboles nécessaires pour écrire celui-ci à l'aide des portes logiques « ET », « OU », « NON ». Cette taille est donc une manière d'appréhender la difficulté d'un problème. Si l'on cherche, par exemple, à trouver l'as de pique dans un jeu de 52 cartes, une formule possible est : [la première carte est l'as de pique] OU [la deuxième carte est l'as de pique] OU [etc.] OU [la 52e carte est l'as de pique]. La taille de cette formule est proportionnelle au nombre de cartes. Ce problème de recherche se généralise pour une base de données contenant « N » éléments.

Existe-t-il un algorithme équivalent de plus petite taille ? Grâce au calcul quantique, on peut répondre, sans équivoque, par la négative. En effet, L. Grover a montré qu'un algorithme quantique permettait d'identifier l'élément recherché en un nombre de requêtes égal à la racine carrée des « N » données, et que cela était impossible avec un nombre inférieur [fig. 4]. Cela reste vrai pour n'importe quel problème, car le carré de la « complexité quantique » d'un problème est relié à la taille minimale de la formule classique correspondante [11]. En utilisant cette connexion, la taille de plusieurs formules classiques a pu être caractérisée.

Ce concept de « preuve quantique » est très prometteur. Elle offre des perspectives pour résoudre des problèmes ouverts en informatique classique. Même si l'ordinateur quantique restait en définitive un mythe, les recherches en informatique quantique laissent poindre des applications concrètes. ■ **J. K., S. L. et F. M.**

[9] L. Grover, *Proc. ACM Symposium on the Theory of Computing*, 212, 1996.

[10] A. Ambainis *et al.*, *Proc. ACM-SIAM Symposium on Discrete Algorithms*, 1099, 2005.

[11] S. Laplante *et al.*, *Proc. IEEE Conference on Computational Complexity*, 76, 2005.