Réalisations physiques

Un ordinateur quantique pourrait être implémenté à partir de toute particule pouvant avoir deux états *à la fois* ***excité*** *et* ***non excité*** *au même moment*. Ils peuvent être construits à partir de photons *présents* à deux endroits au même moment, ou à partir de protons et de neutrons ayant un spin positif, négatif *ou les deux en même temps* tant qu'ils ne sont pas observés.

Contraintes physiques

On pourrait imaginer utiliser une molécule microscopique, pouvant contenir plusieurs millions de protons et de neutrons, comme ordinateur quantique. Celui-ci contenant plusieurs millions de qubits. Mais le calcul quantique exige du système qui le porte deux contraintes fortes pour être utilisable :

- il doit être *totalement isolé du monde extérieur* pendant la phase calcul (on parle alors de *calcul adiabatique*), toute observation *ou tout effacement de données* perturbant le processus47. On ne le laisse communiquer à l'extérieur qu'avant (introduction des données) et après (lecture des résultats, ou plus exactement *du* résultat) ; l'isolement thermique total ne peut exister, mais si l'on arrive à le maintenir le temps du calcul, celui-ci peut avoir lieu sans interférence. Ce phénomène d'interférence est appelédécohérence, c'est le principal obstacle à la réalisation d'un calculateur quantique. Le temps de décohérence correspond pour un système quantique au temps pendant lequel ses propriétés quantiques ne sont pas corrompues par l'environnement.
- il doit se faire sans la moindre perte d'information. En particulier *tout circuit de calcul quantique doit être réversible*. Dans les circuits logiques "classiques" certaines portes ne vérifient pas cette propriété (porte NAND par exemple). Cependant des astuces de construction permettent de contourner cette difficulté en conservant des informations supplémentaires non directement utiles. Toutes les portes classiques ont un équivalent quantique (voir Porte quantique **(en)**).

Il existe des systèmes quantiques isolés naturellement comme les noyaux de certains atomes. Certains, comme le carbone 13, possèdent un moment cinétique, un spin, et peuvent donner lieu à différents états quantiques. Les cristaux de diamant qui contiennent des isotopes du carbone 12 (les noyaux du diamant sont composés jusqu'à 1 % de noyaux de carbone 13) permettraient théoriquement à température ambiante de stocker et de manipuler de l'information quantique. Une première technique consiste à manipuler par laser le spin des électrons d'un atome d'azote constituant les impuretés du diamant, et ainsi agir sur le couplage entre le spin de ces électrons et celui des noyaux du carbone 1348.

vitesse de l'ordinateur se trouve augmentée d'une façon exponentielle, car il peut traiter simultanément tous les états à la fois. Par exemple, un ordinateur classique possédant 4 bits pourrait créer une des 16 (2 exposant 4) combinaisons possibles; 0000, 0001, 0010 etc. Puisque le qubit peut être une superposition de zéro et de un, l'avantage de l'ordinateur quantique est qu'il pourra approximer les 16 états d'un même coup.

Idées de la mécanique quantique

Les fonctions d'onde, qui décrivent l'état d'un système, sont issues de calculs *déterministes*. La source d'aléa est dans *l'acte d'observation lui-même*, c'est-à-dire la *mesure*. Suite à une mesure, le système quantique se fixe dans un état classique avec une certaine probabilité. On peut éliminer cette incertitude en formulant des expressions ne se traduisant que par oui ou par non (par exemple : « cette combinaison est compatible avec la clé » / « cette combinaison ne peut pas être la clé ». Pour certains algorithmes, il est nécessaire d'effectuer les calculs plusieurs fois jusqu'à ce que la réponse vérifie une certaine propriété.

En mécanique quantique, une particule peut posséder de multiples états simultanément : l'état de la particule est une superposition d'états possibles. Ce principe est illustrée par la métaphore du chat de Schrödinger qui est, *avant observation*, à la fois mort et/ou vivant.

La mécanique quantique n'est pas un modèle rendant compte de notre ignorance du système ; il décrit l'état réel des systèmes. Les particules possèdent bien cet état superposé et il en découle quelques propriétés inhabituelles à notre échelle. Une mesure sur un système quantique va fixer le système, avec des probabilités données par la fonction d'onde, dans *un* des états possibles, qui sera alors constatable par tous les autres observateurs sans aléa. L'interprétation d'Everett propose une signification possible de ce phénomène.

Le qubit

La mémoire d'un ordinateur classique est faite de bits. Chaque bit porte soit un 1 soit un 0. La machine calcule en manipulant ces bits. Un ordinateur quantique travaille sur un jeu de qubits. Un qubit peut porter soit un un, soit un zéro, soit une superposition d'un un et d'un zéro (ou, plus exactement, il porte une distribution de *phase*, angle qui pour 0° lui fait prendre la valeur 1, pour 90° la valeur 0, et entre les deux la superposition d'états dans les proportions du sin2 et du cos2 de la phase). L'ordinateur quantique calcule en manipulant ces distributions. On n'a donc pas trois états en tout mais une infinité.

De plus, l'état de plusieurs qubits réunis n'est pas seulement une combinaison des états respectifs des qubits. En effet, si un qubit est dans une quelconque superposition d'états $\alpha \cdot |0\rangle + \beta \cdot |1\rangle$, deux qubits réunis sont quant à eux dans une superposition d'états $\alpha \cdot |00\rangle + \beta \cdot |01\rangle + \gamma \cdot |10\rangle + \delta \cdot |11\rangle$, avec $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$. Il s'agit cette fois d'employer la superposition des quatre états pour le calcul. C'est pourquoi la puissance de calcul théorique d'un ordinateur quantique double à chaque fois qu'on lui adjoint un qubit. Avec dix qubits, on a 1024 états superposables, et avec n qubits, 2^n.

Un ordinateur classique ayant trois bits de mémoire peut stocker uniquement trois chiffres binaires. À un moment donné, il pourrait contenir les bits « 101 » ou une autre combinaison des huit possibles (23). Un ordinateur quantique ayant trois qubits peut en fait stocker seize valeurs, assemblées deux par deux pour former huit nombres complexes (il est donc dans une superposition de ces huit états).

La somme des probabilités fait bien 1. S'il y avait eu n qubits, cette table aurait eu 2^n lignes. Pour un n aux alentours de 300, il y aurait eu plus de lignes que d'atomes dans l'univers observable.

La première colonne montre tous les états possibles pour trois bits. Un ordinateur classique peut seulement porter un de ces états à la fois. Un ordinateur quantique, lui, peut être dans une superposition de ces huit états à la fois. La deuxième colonne montre l'amplitude pour chacun des huit états. Ces huit nombres complexes sont un instantané du contenu d'un ordinateur quantique à un moment donné. Durant le calcul, ces trois nombres changeront et interagiront les uns avec les autres. En ce sens, un ordinateur quantique à trois qubits a bien plus de mémoire qu'un ordinateur classique à trois bits.

Cependant, il n'est pas possible de voir directement ces trois nombres. Quand l'algorithme est fini, une seule *mesure* est accomplie. La mesure retourne une simple chaîne de trois bits classiques et efface les huit nombres quantiques. La chaîne de retour est générée aléatoirement. La troisième colonne donne la probabilité pour chacune des chaînes possibles. Dans cet exemple, il y a 14 % de chance que la chaîne retournée soit « 000 », 4 % que ce soit « 001 », ainsi de suite. Chaque nombre complexe est nommé « ampere » et chaque probabilité une « amplitude carrée », parce qu'elle est égale à $a^2 + b^2$. La somme des huit probabilités est égale à un.

Typiquement, un algorithme d'un ordinateur quantique initialisera tous les nombres complexes à des valeurs égales, donc tous les états auront les mêmes probabilités. La liste des nombres complexes peut être imaginée comme un vecteur à huit éléments. À chaque étape de l'algorithme, le vecteur est modifié par son produit avec une matrice qui correspond à une opération quantique.

Avenir commercial ?

Même si les problèmes techniques posés par la réalisation de calculateurs quantiques étaient résolus à terme, leur avenir commercial immédiat ne se situe pas nécessairement dans le grand public, tout dépendant évidemment du coût auquel on arrive à les fabriquer.

En dehors des algorithmes de Shor pour le cassage de code et de Grover pour la recherche efficace dans des bases de données, ainsi qu'une classe de calculs en physique théorique, quelques applications seraient *peut-être* envisageables pour des simulations numériques qui butent aujourd'hui sur l'explosion combinatoire.

Il est à noter qu'un appareil électronique classique dédié exclusivement au calcul fortement combinatoire a existé dans les années 1970 où il servait à optimiser les roulements de la SNCF sous contraintes. Il s'agissait de l'"Optimateur" Cybco C100-1024, qui opérait par exploration câblée de toutes les solutions possibles en allégeant ses calculs par des considérations d'impossibilité et de symétrie57. Le besoin existe donc depuis déjà plusieurs décennies et sa résolution par des circuits spécialisés a même fait l'objet de brevets58.

En novembre 2008, Aram W. Harrow, Avinatan Hassidim et Seth Lloyd ont publié59 une méthode quantique permettant de résoudre des systèmes d'équations linéaires à matrices creuses en un temps O(log(n)) au lieu de O(n).

En réseaux de neurones, la méthode dite du *greedy learning*60 consomme également beaucoup de combinatoire et est donc signalée par D-Wave en 2009 comme une application possible61.