

CODE CORRECTEUR D'ERREUR DE PETER SHOR

Dans le code correcteur d'erreur classique le plus simple, on triple chaque information : on remplace 0 par (0, 0, 0) et 1 par (1, 1, 1). Quand on le juge nécessaire, on teste si les trois bits d'un tel triplet sont égaux et si ce n'est pas le cas on inverse le bit en exemplaire unique : si on lit (0,0,1) on rétablit (0,0,0), si on lit (1,0,1), on rétablit (1,1,1). Une telle méthode corrige toutes les erreurs simples. Si la probabilité d'une erreur simple est petite alors celle d'une erreur double ou triple (non-corrigée par la méthode) sera très petite et on la néglige. L'adaptation par Peter Shor de ce code correcteur commence par remplacer chaque qubit $|0\rangle$ par le 3-qubit $|000\rangle$ et chaque qbit $|1\rangle$ par le 3-qubit $|111\rangle$. La méthode classique de correction est inapplicable car il faudrait lire chacune des composantes des 3-qubit, ce qui est impossible sans perturber fatalement les 3-qubits. En revanche une mesure collective non destructive de deux composantes est possible par la méthode de Shor.

Si on a le qubit $|x,y,z\rangle$ on peut par exemple connaître $x \text{ XOR } y$ ($x \text{ XOR } y$ désigne le OU exclusif, aussi dénommé NON contrôlé, entre x et y qui vaut 0 si x et y sont égaux et 1 sinon). L'idée de Shor est de calculer la paire $[y \text{ XOR } z, x \text{ XOR } z]$.

Un petit calcul montre que si une seule des composantes a basculé (0 devenu 1, ou 1 devenu 0) dans un 3-qubit composé de trois fois la même composante, alors la paire de Shor donne l'écriture en binaire du numéro du bit qui a changé. On peut alors effectuer la correction.

Exemple : Pour (0,1,0) $y \text{ XOR } z$ vaut 1, $x \text{ XOR } z$ vaut 0, donc la paire de Shor est [1,0], qui donne 10, l'écriture binaire de 2, le numéro de la composante à corriger.

Le secret de la méthode de correction (sans contradiction avec le principe de non-duplication) réside dans le fait (a) qu'on ne lit aucune composante individuellement, (b) qu'on trouve le numéro de la composante à corriger, et (c) qu'on la corrige sans même savoir si on change un 0 en 1 ou l'inverse.

(moins de 100 kilomètres). En cryptographie quantique, on utilise des photons qu'on fait circuler dans des fibres optiques, où ils sont inévitablement atténués par absorption. L'idée d'utiliser des répéteurs classiques qui lisent le signal et l'amplifient est inapplicable, car les photons qui circulent sont dans des états quantiques inconnus et, encore une fois, pour les amplifier, il faudrait les lire. La technique de téléportation résout en principe le problème et autorise la conception de nouveaux répéteurs qui «ré-émettent» sans lire les photons envoyés.

Mémoriser l'information : la superposition et le qubit

Après ces considérations générales sur les propriétés de la transmission quantique, examinons le support de cette information. Le support élémentaire classique est le bit : un 0 ou un 1 ; son analogue quantique est le qubit, le *quantum bit*. Classiquement ou quantiquement, le bit est l'état de n'importe quel système matériel pouvant prendre un parmi deux états différents, par exemple un curseur tourné vers le haut ou vers le bas, un carré noir ou blanc sur un papier, un accumulateur électrique chargé ou non, le spin d'un noyau

d'atome orienté vers le haut ou vers le bas, etc. Quelle est alors la différence entre un bit et un qubit?

Les principes de la mécanique quantique autorisent qu'un chat soit à la fois mort et vivant – ce que l'on appelle la superposition d'états. Aussi le qubit décrit, avec deux nombres a et b , un état $a|0\rangle + b|1\rangle$ (a et b sont des nombres complexes). Il mémorise ainsi plus d'informations qu'un bit classique. Le N -bit, de la forme 00101011... est décrit complètement par n choix de chiffres 0 ou 1, le N -qubit est spécifié par 2^N choix de nombres complexes (voir *Les propriétés de l'information quantique*, page précédente).

Ainsi, avec un 2-qubit, on mémorise simultanément 4 nombres complexes a, b, c, d , avec un 10-qubit, on mémorise un millier de nombres, avec un 30-qubit, on atteint le milliard, et avec un 40-qubit, on pourrait en principe stocker tout le contenu disponible actuellement sur le réseau Internet (qu'on évalue à 8 000 milliards de caractères, ce qui équivaut à une bibliothèque de 8 millions de livres).

Calculer avec des qubits revient finalement à faire simultanément plusieurs calculs à la fois : avec un 3-qubit par exemple on calculera la valeur d'une fonction en même temps pour

les huit jeux de données (0,0,0), (0,0,1), (0,1,0), (0,1,1), (1,0,0), (1,0,1), (1,1,0), (1,1,1), car calculer avec des états superposés, c'est faire des calculs simultanés. Bien sûr, la maîtrise de ces superpositions ne va pas de soi, mais on comprend l'intérêt d'y parvenir.

Il y a trois ans, certains théoriciens de la mécanique quantique pensaient que les phénomènes d'instabilité rendraient à jamais impossibles les calculs quantiques qui nécessitent la création de N -qubits, leur préservation durant des intervalles de temps significatifs, leur manipulation et leur lecture.

L'obstacle fondamental invoqué était la décohérence, c'est-à-dire la propension qu'un état quantique complexe (un N -qubit, par exemple) a d'interagir spontanément avec l'environnement, ce qui, en projetant son état sur l'un des états de base, détruit une partie de son contenu en information. Cette interaction agit comme une lecture conduisant à un état non superposé, par exemple celui codant (0,0,0), ce qui évidemment fait perdre tout son intérêt au N -qubit.

Tout a changé en 1996 et 1997, quand on a compris qu'on pouvait limiter toutes ces sources d'instabilité par des techniques de correction d'erreurs.

Les codes correcteurs d'erreurs

La théorie classique de la correction d'erreur conduit, même avec des composants imparfaits, à mener des calculs justes. Son adaptation au cas quantique est une avancée remarquable (voir l'encadré *Code correcteur d'erreur de Peter Shor*), qui offre la perspective d'une préservation parfaite d'états quantiques complexes, préservation jugée impossible à cause de processus irréversibles comme la relaxation par émission spontanée.

Dans un calcul utilisant des méthodes de correction, chaque élément d'un qubit pourrait être perdu et reconstitué. Peter Shor (inventeur de l'algorithme de factorisation quantique mentionné plus loin) et Andrew Steane remarquèrent, en 1995, que les méthodes classiques de correction d'erreurs s'adaptaient. Cela paraissait à première vue difficile, car le principe de non-duplication empêche la copie redondante d'une même information à préserver, copie qui est à la base de la correction d'erreur clas-

sique. Peter Shor remarqua qu'on peut détecter une erreur et la corriger sans avoir à en prendre connaissance en détail.

La méthode de Peter Shor a été généralisée et étendue aux diverses sources d'erreurs qu'on rencontre lors du déroulement d'un calcul quantique. Après trois ans de travaux, les chercheurs en sont arrivés à la conclusion ferme que, non seulement on peut corriger les erreurs, mais qu'on peut préserver un état quantique complexe et le manipuler pendant des intervalles de temps aussi longs qu'on le souhaite, avec un risque global d'erreur aussi petit qu'on le désire. Précisons toutefois qu'il s'agit d'une avancée théorique qui n'a pas aujourd'hui été expérimentalement mise en œuvre, ce qui demandera sans doute de nombreuses années.

L'intérêt de la superposition quantique et du calcul quantique est soumis à une objection grave fondée sur l'impossibilité de connaître complètement certains états quantiques : à quoi peut bien servir d'engendrer un état quantique contenant la superposition de $f(0,0,0)$, $f(0,0,1)$, $f(0,1,0)$, $f(0,1,1)$, $f(1,0,0)$, $f(1,0,1)$, $f(1,1,0)$, $f(1,1,1)$, si l'on ne peut pas en extraire – ce qui est le cas – la connaissance de $f(0,0,0)$?

L'algorithme quantique

Cette question est très gênante. La réponse n'est devenue claire que progressivement, par le développement d'algorithmes quantiques délicats qui exploitent astucieusement les superpositions d'états et les opérations que la théorie quantique autorise sur eux pour extraire des superpositions des informations utiles. Le premier résultat important (dû à Peter Shor en avril 1994) est un algorithme rapide pour la factorisation des nombres entiers. Comme aucun algorithme rapide classique n'existe, cette découverte créa un certain émoi chez les spécialistes et suscita une vague d'intérêt pour les ordinateurs quantiques (sauf en France, où l'on préféra se spécialiser dans l'explication de l'impossibilité à surmonter la décohérence).

Le second problème algorithmique important traité fut celui du repérage d'une donnée dans une liste non organisée par Lov Grover (voir l'article de N. Gershenfeld et I. Chuang dans ce numéro). Cet algorithme est

plus important encore que le premier car ses applications potentielles touchent cette fois non seulement la cryptographie, mais aussi le traitement général des données, quelle qu'en soit la nature.

Des résultats récents montrent aussi – comme on pouvait le présumer – qu'un ordinateur quantique n'aurait pas d'équivalent pour étudier les systèmes quantiques quelconques et qu'il permettrait de les simuler avec efficacité, ce qui est impossible avec un ordinateur classique.

D'autres algorithmes plus spécialisés sont proposés régulièrement et on commence à comprendre ce nouvel art de programmer que nécessiteront les ordinateurs quantiques. Cet ensemble de résultats a une incidence sur les fondements de la théorie du calcul, car il remet en cause une de ses bases : l'acceptation que tous les mécanismes de calcul sont sensiblement équivalents en puissance (en langage précis : que chacun est simulable en temps polynomial par chaque autre). La première victime de ce bouleversement est dès

LA TÉLÉPORTATION SERA-T-ELLE QUANTIQUE?

Si l'on pense qu'une personne humaine n'est pas seulement définie par l'état physique de son corps et de son cerveau (question philosophique) alors aucune discussion n'est possible. Supposons donc que l'intégrité d'une personne humaine n'est qu'une question physique. Deux cas apparaissent.

Cas 1. La mécanique quantique ne joue pas de rôle essentiel dans le fonctionnement du corps et du cerveau. En prenant connaissance à un niveau de détail assez fin de la position des atomes qui composent le voyageur (chose peut-être impossible mais qu'aujourd'hui aucun principe n'interdit) on pourrait transmettre cette information d'un point à un autre (par radio) et mener au point d'arrivée une reconstruction du voyageur. Dans un tel cas la téléportation fait voyager à la vitesse de la lumière. Les hypothèses mises en œuvre ici permettent en théorie de dupliquer une personne humaine (après avoir pris connaissance de sa définition on en reconstitue plusieurs copies), comme dans certains épisodes de Star Trek lorsque l'appareil de téléportation fonctionne mal.

La quantité d'information impliquée dans ces opérations est parfois évoquée pour dire qu'aucun canal d'information n'aura jamais assez de puissance pour transmettre l'information nécessaire qui serait au moins de 10^{30} bits. Cet argument néglige les possibilités de compression d'information : pour transmettre l'information décrivant un corps humain il n'est pas nécessaire par exemple de transmettre la description des chromosomes de chaque cellule puisque dans chacune des milliards de cellules d'un organisme vivant ce sont les mêmes chromosomes qu'on trouve.

Cas 2. La mécanique quantique joue un rôle essentiel dans le fonctionnement du corps et du cerveau qui utilise peut-être des atomes corrélés et des superpositions complexes d'états quantiques pour fonctionner. Aucune mesure complète de l'état instantané du voyageur ne sera possible et donc sa duplication sera impossible. En revanche, la technique de téléportation quantique s'appliquerait et produirait le déplacement à la vitesse de la lumière (mais pas plus, là encore) d'un voyageur (qui serait alors nécessairement détruit à son point de départ).

Précisons bien sûr qu'il se passera quelques siècles avant qu'on se pose sérieusement ces questions et que d'ici là d'autres obstacles seront peut-être apparus rendant impossible toute duplication humaine et toute téléportation.

