

a) L'information unitaire classique est le bit : un objet qui vaut 0 ou 1.

b) L'information unitaire quantique est le qubit (quantum bit). C'est un vecteur dans un espace complexe de dimension 2 muni d'un produit scalaire (deux vecteurs dont le produit est nul sont orthogonaux). Les éléments d'une base orthogonale sont fixés et notés $|0\rangle$ et $|1\rangle$. Un qubit $|\phi\rangle$ se représente sous la forme $\alpha|0\rangle + \beta|1\rangle$ avec $|\alpha|^2 + |\beta|^2 = 1$, où α et β sont des nombres complexes (ainsi le qubit est déterminé par quatre nombres réels). Une mesure amène le qubit $|\phi\rangle$ sur l'un des vecteurs de la base $|0\rangle$, $|1\rangle$. Les règles de la mécanique quantique indiquent qu'on obtient, lors d'une mesure physique, $|0\rangle$ avec la probabilité $|\alpha|^2$ et $|1\rangle$ avec la probabilité $|\beta|^2$.

c) L'état quantique d'un N-qubit est un vecteur dans un espace analogue à celui du qubit, mais de dimension 2^N . On choisit une base orthogonale de cet espace. Pour un 3-qubit on choisit une base orthogonale dont les vecteurs sont : $|000\rangle$, $|001\rangle$, $|010\rangle$, $|011\rangle$, $|100\rangle$, $|101\rangle$, $|110\rangle$, $|111\rangle$. Un état général du 3-qubit est de la forme : $a_{000}|000\rangle + a_{001}|001\rangle + a_{010}|010\rangle + a_{011}|011\rangle + a_{100}|100\rangle + a_{101}|101\rangle + a_{110}|110\rangle + a_{111}|111\rangle$, où la somme des carrés des $|a_{ijk}|$ est égale à 1. La lecture du 3-qubit donne un vecteur de la base, chaque vecteur de la base étant obtenu avec une probabilité proportionnelle à $|a_{ijk}|$.

d) Réaliser un calcul quantique consiste à préparer un N-qubit dans un état initial standard, par exemple $|00\dots 0\rangle$ puis à appliquer à cet état une série de transformations unitaires (ce sont des opérations analogues en dimension quelconque aux rotations d'un vecteur). À la fin de cette suite de transformations, on mesure le N-qubit par une expérience qui l'amène dans un état correspondant à un vecteur de la base orthogonale, ce qui donne par exemple $|001\rangle$. Le résultat de cette mesure est probabiliste : on ne sait jamais ce que l'on va trouver. Tout l'art de la programmation quantique réside dans le choix des opérateurs qu'on applique de façon à ce qu'il se produise quelque chose d'intéressant (par exemple, la factorisation d'un entier). Le plus souvent, un calcul quantique commence par la création d'une superposition homogène de tous les états de la base. Pour un 3-qubit, par exemple, on commence par créer : $[|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle] / \sqrt{8}$. Un N-qubit est un objet difficile à décrire : il faut, pour le spécifier complètement, indiquer 2^N nombres complexes. Il n'était pas évident que les règles délicates du calcul quantique par transformations unitaires produisent des résultats intéressants. C'est pourtant ce qu'ont montré Peter Shor, Lov Grover et les algorithmiciens quantiques.

e) La non-localité : un résultat de Don Page

La possibilité de coder des informations globalement dans un N-qubit est mise en évidence par l'exemple suivant : un de vos amis choisit un 30-qubit et en prépare un très grand nombre d'exemplaires (comme il l'a choisi lui-même, cela ne contredit pas le principe de non-duplication). En faisant une série assez longue de mesures sur les divers exemplaires du 30-qubit on peut en reconstituer l'état avec exactitude. Mais, au lieu de cela, on divise chaque 30-qubit en trois sous-ensembles de 10-qubit qu'on envoie à Rennes, Lille et Marseille. En faisant des mesures localement et indépendamment dans ces trois villes (c'est-à-dire sans coordonner ni corrélérer les mesures), on ne peut, d'après un résultat de Don Page, tirer en moyenne que moins d'un millième de l'information contenue dans le 30-qubit, et cela quel que soit le nombre de copies dont on dispose. L'information contenue dans le 30-qubit est intrinsèquement non locale, les composantes sont corrélées, et seules des mesures collectives peuvent la révéler.

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-