C'est quoi, le quantique ?

Les lois physiques utilisées jusqu' à la fin du XIXe siècle pour décrire le monde sont, précision mise à part, simulables en temps polynomial par un ordinateur. Cela a amené à formuler l'hypothèse de Church-Turing forte : il n'y a pas de système physique classique qui permette de surpasser qualitativement les capacités de calcul d'une machine de Turing.

Au cours du siècle suivant furent inventés successivement la mécanique quantique puis l'ordinateur avec l'informatique théorique et la théorie de la complexité. En 1982, le physicien Feynman constatait ces deux points :

• Les ordinateurs ne font aucun usage des effets quantiques.

• L'évolution des systèmes d'après les lois de la mécanique quantique ne paraît pas simulable en un temps raisonnable par un ordinateur.

Il proposa alors d'étudier la possibilité d'intégrer des processus purement quantiques dans les calculateurs afin d'en augmenter la puissance – peut-être exponentiellement.

Aujourd'hui, si l'on ne sait toujours pas vraiment comment construire un ordinateur quantique, au moins le paradigme théorique est-il assez clairement établi.

• D'abord l'unité de base n'est plus le bit, mais le qubit. Les états de base du qubit sont toujours **0** et **1**, mais un qubit peut être dans une superposition de ces états. Techniquement, son état général peut être écrit $\alpha.\mathbf{0}+\beta.\mathbf{1}$, où α et β sont des nombres complexes dont la somme des carrés des modules vaut 1.

• Ensuite les transformations que l'on peut appliquer sont contraintes par les lois de la mécanique quantique. Si l'on veut conserver intacte la *cohérence* d'un système quantique, c'est-à-dire si l'on veut éviter de se retrouver dans un état classique, il faut lui appliquer des transformations *unitaires* ; en particulier, le calcul doit être réversible.

• Enfin la mesure devient une partie essentielle de l'algorithme. Il est bien connu qu'en mécanique quantique, l'observateur, en mesurant un système, le perturbe. On procède à une mesure, à la fin de la partie purement quantique, pour lire le résultat sous une forme classique ; cette opération est irréversible et essentiellement probabiliste. Plus précisément, mesurer le qubit $\alpha.\mathbf{0}+\beta.\mathbf{1}$ donne pour résultat **0** ou **1** avec probabilités respectives $|\alpha|^2$ et $|\beta|^2$, et le qubit est perdu dans l'opération.

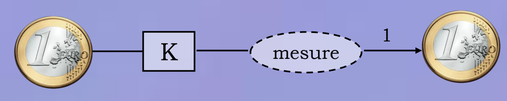
Classique	Quantique
bit	qubit
formule booléenne	transformation unitaire
lecture du résultat	mesure

Circuits quantiques

De même que l'on peut formaliser le calcul classique à l'aide des portes logiques habituelles – par exemple NOT et AND –, le calcul quantique peut être défini par des circuits, les opérations élémentaires consistant à appliquer une porte parmi un ensemble de base choisi à l'avance, au bon endroit et au bon moment.

Pour obtenir un jeu complet de portes quantiques, c'est-à-dire un ensemble de portes quantiques suffisant pour pouvoir approximer toute transformation quantique, il suffit par exemple d'ajouter à un jeu classique réversible complet deux portes opérant de manière plus étrange : H (la porte de Hadamard) et K.

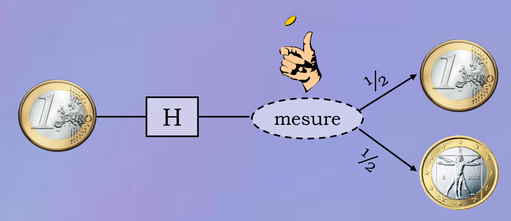
La porte K transforme le qubit $\alpha.\mathbf{0}+\beta.\mathbf{1}$ en $\alpha.\mathbf{0}+i\beta.\mathbf{1}$; elle n'a *a priori* pas d'effet classique évident.. Il faut pourtant l'appliquer quatre fois pour revenir dans l'état initial.



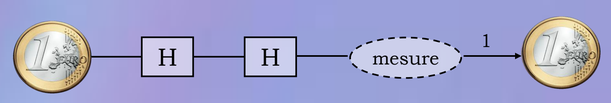
La porte de Hadamard transforme le qubit $\alpha.\mathbf{0}+\beta.\mathbf{1}$ en $\frac{\alpha+\beta}{\sqrt{2}}.\mathbf{0}+\frac{\alpha-\beta}{\sqrt{2}}.\mathbf{1}$

Elle a une curieuse propriété.

Appliquée une fois à un qubit dans un état classique, elle le met dans un état classiquement équivalent à un bit aléatoire



Appliquée deux fois d'affilée, elle ne modifie pas le qubit.



Quelques problèmes

Considérons un tableau de taille N contenant des 0 et des 1.

• Y a t-il au moins un 1 dans le tableau ? Nous appelons cette question le **problème de recherche dans un tableau non trié**.

• Supposons maintenant que les éléments du tableau soient classés par ordre croissant : des 0 puis des 1. Quel est le numéro de la case contenant le premier 1 ? C'est le **problème de recherche dans un tableau trié**.

• Si le tableau contient des entiers, on peut se demander s'ils sont tous différents : c'est le problème de **recherche d'éléments identiques dans un tableau**.

• Supposons les cases du tableau indicées par $(Z/2Z)^n$ et contenant des éléments de ce même ensemble. On appelle f(x) le contenu de la case x et on suppose que soit f est une bijection, soit il existe un unique y tel que pour tout x on ait f(x)=f(x+y). Le **problème de Simon** est de savoir laquelle de ces deux propriétés possède le tableau.

Complexité en requêtes et adaptativité

On s'intéresse à la **complexité en requêtes** de ces problèmes. L'entrée, c'est-à-dire le tableau, n'est pas donnée en clair mais comme une boîte noire : il faut faire une requête pour lire ce qu'il y a dans une case du tableau. La complexité en requêtes d'un algorithme est le nombre de cases du tableau consultées par l'algorithme. La complexité en requêtes d'un problème est le nombre minimal de requêtes que doit faire un algorithme pour répondre correctement à la question.

Dans les cas probabiliste et quantique, les algorithmes doivent répondre à la question avec probabilité de réussite au moins 1/2.

Un **algorithme adaptatif** est un algorithme qui peut utiliser le résultat d'une requête, c'est-à-dire le contenu d'une case du tableau, pour décider de la requête suivante, c'est-à-dire du numéro de la prochaine case à regarder. Mais un **algorithme non-adaptatif** doit faire toutes ses requêtes en parallèle. Des calculs peuvent être effectués avant ou après les requêtes, mais pas entre les requêtes. Dans le cas de la recherche dans un tableau trié par exemple, un algorithme adaptatif peut procéder par dichotomie alors que ce n'est pas possible pour un algorithme non-adaptatif.

Dans le cas quantique, les requêtes doivent être des opérations réversibles. Si f(x) est le contenu de la case de numéro x, une requête au tableau f est l'opération qui a (x,y) associe (x,f(x)+y). Un algorithme quantique qui effectue n requêtes en parallèle est alors un algorithme utilisant l'opération qui a (x_1, ..., x_n, y_1, ..., y_n) associe (x_1, ..., x_n, y_1+f(x_1), ..., y_n+f(x_n)).

Comme nous le montrent les bornes supérieures et les bornes inférieures obtenues (voir le tableau ci-contre), c'est quelquefois l'utilisation du quantique qui donne les meilleurs résultats, quelquefois l'adaptativité, et quelquefois il faut les 2.

Complexité en requêtes	**recherche dans un tableau non trié**	**recherche d'éléments identiques dans le tableau**	**recherche dans un tableau trié**	**Problème de Simon**
Algorithme probabiliste	$\Theta(N)$	$\Theta(N)$	$\Theta(\log N)$	$\Theta(\sqrt{N})$
Algorithme probabiliste non-adaptatif	$\Theta(N)$	$\Theta(N)$	$\Theta(N)$	$\Theta(\sqrt{N})$
Algorithme quantique	$\Theta(\sqrt{N})$	$\Theta(N^{2/3})$	$\Theta(\log N)$	$\Theta(\log N)$
Algorithme quantique non-adaptatif	$\Theta(N)$	$\Theta(N)$	$\Theta(N)$	$\Theta(\log N)$

Bibliographie :

Vincent Nesme, **Complexité en requêtes et symétries**, Thèse de doctorat, mai 2007

Pascal Koiran, Vincent Nesme et Natacha Portier, **The quantum query complexity of the Abelian Subgroup Problem**, Theoretical Computer Science, 2007

Pascal Koiran, Jürgen Landes, Natacha Portier et Penghui Yao, **Adversary lower bounds for nonadaptive quantum algorithms**, JCSS special issue on Wollic'08

Pascal Koiran
Professeur ENS Lyon, LIP,
Equipe MC2

Jürgen Landes
Post-Doctorant INRA, Narbonne

Vincent Nesme
Post-Doctorant, Hanovre

Natacha Portier
Maîtresse de conférences ENS Lyon, LIP
Equipe MC2

Penghui Yao
Doctorant, Singapour