Département d'informatique et de recherche opérationnelle
Université de Montréal

# IFT 6155 — Informatique quantique — H00

**Professeur:** Gilles Brassard, 3349 André–Aisenstadt, brassard@iro.umontreal.ca

**Description:** Le monde dans lequel nous vivons est soumis aux lois parfois étranges de la mécanique quantique. C'est ainsi par exemple que certains objets peuvent traverser des barrières impénétrables ou se retrouver en plusieurs endroits simultanément. Toutefois, malgré la richesse indéniable de l'informatique traditionnelle, celle-ci prend résolument ses racines dans la physique classique, ce qui est au mieux un pâle reflet de la réalité. Ceci nous a largement empêchés de profiter pleinement de tout le potentiel offert par la nature pour fins de traitement de l'information. Presque cent ans après sa grande sœur la physique, le temps est venu pour l'informatique de prendre à son tour le virage quantique.

Dans ce cours, nous allons étudier toutes sortes d'approches basées sur la mécanique quantique qui ont le potentiel de révolutionner l'informatique. C'est ainsi que nous traiterons entre autres de cryptographie quantique, de calcul quantique, de téléportation quantique, de purification d'intrication, de correction d'erreur quantique, et de bien d'autres merveilles telle la possibilité théorique de calculer sans dépenser d'énergie!

L'information quantique est bien différente de sa contrepartie classique. L'information classique peut être lue et copiée sans restriction, elle peut être transmise à un nombre arbitraire de destinataires, mais elle ne peut pas voyager plus vite que la vitesse de la lumière. Par contraste, l'information quantique ne peut être lue ni copiée sans être perturbée irrémédiablement, elle ne peut être distribuée à plusieurs destinataires, mais elle *semble* en certains cas se propager instantanément et même à rebours du temps. De plus, l'information quantique peut se retrouver en *superposition* de différentes valeurs classiques.

Après une introduction aux fondements de la mécanique quantique — aucune connaissance préalable n'en sera présumée — nous verrons des exemples simples d'utilisation de l'information quantique pour l'accomplissement de tâches aussi spectaculaires que la possibilité de voir sans regarder et d'établir instantanément à distance des corrélations impossibles à expliquer classiquement. Ceci nous conduira à l'étude de la *cryptographie quantique*. Parce qu'il est impossible en général de mesurer un système quantique sans le perturber de façon irrémédiable, toute tentative d'espionnage sur une voie de communication quantique cause une perturbation inévitable qui peut être détectée par les usagers légitimes. Ceci permet de communiquer en toute confidentialité sous le nez d'une espionne, quelles que soient la puissance de calcul et la technologie dont celle-ci dispose. Ces techniques ont été implantées de façon expérimentale sur des distances de plusieurs dizaines de kilomètres.

Après un exposé sur les *ordinateurs réversibles*, ceci nous conduira à l'étude de l'*ordinateur quantique*. Le principe de superposition quantique permet à une quantité exponentielle de calculs de prendre place simultanément dans la même composante matérielle. L'exploitation de phénomènes d'interférence constructive et destructive permet de renforcer la probabilité d'obtention des résultats souhaités et d'annihiler celle des résultats parasites. Pour citer Feynman, c'est comme si "somehow or other it appears as if the probabilities would have to go negative". Nous verrons comment ceci permet la résolution de certains problèmes beaucoup plus rapidement que nous en sommes capables sur tout ordinateur classique. En principe, un ordinateur quantique capable de traiter de façon cohérente quelques milliers de bits quantiques serait capable d'effectuer des calculs hors de la portée d'un ordinateur classique dont la taille serait celle de l'Univers et dont chaque composante logique et chaque bit de mémoire auraient la taille d'une particule élémentaire. Après l'étude des algorithmes de Deutsch, de Deutsch–Jozsa et de Simon, cette partie du cours culminera par l'algorithme de Peter Shor, qui permet la factorisation rapide de très grands entiers, et celui de Lov Grover, qui permet de trouver une aiguille dans une botte de foin dans le temps requis pour la cuisson d'un soufflé. Nous verrons également comment l'emploi de l'information quantique permet dans certains cas de réduire exponentiellement la quantité d'information qui doit être échangée entre deux ou plusieurs participants afin de collaborer à un calcul commun. Ceci donne lieu à un phénomène de pseudo-télépathie.

Nous étudierons ensuite d'autres aspects de la théorie de l'information quantique à l'état pur. Nous verrons comment comprimer l'information quantique pour fins de transmission ou d'entreposage plus économique, comment téléporter l'information quantique non seulement d'un point vers un autre dans l'espace mais aussi dans le temps, et comment purifier l'information quantique pour corriger la possibilité d'erreurs de transmission ou de corruption malveillante. Ceci nous donnera des outils pour réaliser la correction d'erreurs sur données quantiques, ce qui est indispensable au fonctionnement fiable de tout ordinateur quantique. Nous aborderons également la question plus spéculative de la réalisation expérimentale des ordinateurs quantiques et des nombreux problèmes que cela pose.

**Public cible:** Ce cours s'adresse à tous ceux qui sont curieux de savoir à quoi ressemblera peut-être l'ordinateur de demain. Vous pouvez venir du département d'informatique et de recherche opérationnelle, bien entendu, mais également du département de mathématiques et de statistique ou du département de physique (cette liste ne se veut pas restrictive). Aucune connaissance préalable de la mécanique quantique ou de la cryptographie ne sera présumée. Par contre, une certaine maturité mathématique sera un atout, particulièrement en algèbre linéaire.

**Livre:** Le cours sera basé sur une version préliminaire de mon livre *Quantum Information Processing for Computer Scientists*, à paraître aux éditions MIT Press.

**Horaire:** Lundi de 9h30 à 11h20 au 1207 du pavillon André–Aisenstadt et mardi de 15h30 à 17h20 au Y–117 du pavillon principal. Premier cours le lundi 10 janvier 2000.