Université de Montréal

Département d'informatique et de recherche opérationnelle

IFT 3155/6155 — Informatique quantique — A18

Professeur : Charles Bédard, AA-3366, charles.alexandre.bedard@umontreal.ca
Démonstrateur : Sophie Berthelette, AA-3363, sophie.berthelette@umontreal.ca

Description : 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. En effet, 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. Plus d'un siècle 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 complexité de la communication quantique, de pseudo-télépathie, de distillation 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 ni lue ni copiée sans être perturbée irrémédiablement, elle ne peut pas 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 — et au calcul réversible classique, nous serons prêts à plonger dans le monde mystérieux de l'*ordinateur quantique*. Le *principe de superposition* permet à un *bit quantique* (appelé *qubit*) de prendre simultanément les valeurs 0 et 1. Il s'en suit qu'un *registre quantique* formé de n qubits peut être en superposition des 2^n valeurs classiques possibles. Par la magie du *parallélisme quantique* — qui n'est rien d'autre, mathématiquement parlant, qu'une manifestation de la linéarité de la mécanique quantique — il est possible de calculer simultanément sur toutes ces valeurs. Ceci permet d'effectuer une quantité exponentielle de calculs dans le temps qu'il faudrait classiquement pour en réaliser un seul. 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 savons comment faire 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 Shor, qui permet la factorisation rapide de très grands entiers (avec des conséquences dramatiques sur la cryptographie classique) et celui de 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 spectaculairement la quantité d'information qui doit être échangée entre deux ou plusieurs participants afin de collaborer à un calcul commun. Ceci donne lieu au phénomène dit de pseudo-télépathie lorsque cette réduction est poussée à son ultime limite : aucune communication.

Nous étudierons également d'autres aspects de la théorie de l'information quantique à l'état pur. Nous verrons comment téléporter l'information quantique et comment la distiller afin de 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.

Public cible : Ce cours s'adresse à tous ceux et celles 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 théorie des probabilités et en algèbre linéaire. Une connaissance préalable des nombres complexes et de la façon de les manipuler sera présumée. Mais surtout, venez avec un esprit ouvert afin de donner libre cours à vos rêves et à votre imagination !

Documentation : Le cours sera basé sur une version préliminaire de mon livre *Quantum Information Science for Computer Scientists* (disponible au fur et à mesure de l'avancement du cours dans le sous-répertoire `livre` du site web mentionné ci-dessus), le livre *L'Impensable Hasard* de Nicolas Gisin (éditions Odile Jacob), ainsi que sur des articles scientifiques et notes de cours qui seront distribués au fur et à mesure.

Horaire : mardi et jeudi de 12h30 à 14h20. Le local reste à déterminer.

Le premier cours aura lieu le mardi 4 septembre 2018 à 12h30.
Il s'agira d'une présentation grand-public de la discipline à laquelle vous pouvez venir sans que ceci vous engage à quoi que cela soit. **Avis aux curieux...** Venez nombreux !