Département d'informatique et de recherche opérationnelle

Université de Montréal

IFT 6195 — Sujets en informatique quantique — H09

Professeur : Gilles Brassard, 2215 André–Aisenstadt, brassard@iro.umontreal.ca

Horaire des cours : mardi de 14h30 à 16h20 au 1175 du Pavillon André-Aisenstadt et mercredi de 14h30 à 16h20 au D–225 du Pavillon Roger-Gaudry.

Le premier cours, ***accessible à tous****, aura lieu le mercredi 7 janvier 2009 à 14h30.*

Attention... Prévoyez 15 minutes pour vous rendre au D-225 la première fois !

Description : Le monde dans lequel nous vivons est soumis aux lois parfois étranges de la mécanique quantique. 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 afin de profiter pleinement des merveilles de Mère Nature ! Les rudiments de l'informatique quantique sont présentés dans le cours d'introduction, IFT 6155, alors que ce cours de *sujets*, IFT 6195, y fait normalement suite pour approfondir certains aspects de la discipline. La liste spécifique des sujets traités n'est pas fixée d'avance car elle dépendra en partie de l'intérêt des étudiants inscrits. Ceci étant dit, les sujets seront tirés au moins en partie de la liste suivante.

- *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 altération 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, qui ont été implantées de façon expérimentale avec grand succès sur plus d'une centaine de kilomètres, sont désormais disponibles commercialement.

  Après avoir présenté les rudiments de la distribution quantique de clefs, tel le protocole « BB84 » (que plusieurs auront déjà vu), nous aborderons les preuves de sécurité et les attaques contre des implantations imparfaites. Nous verrons entre autres qu'il y avait une faille aussi fondamentale qu'étonnante dans les premières preuves de sécurité. Nous discuterons également des aspect pratiques de cette technologie.

- *La cryptographie quantique au-delà de BB84.* Tout comme la cryptographie classique va bien au-delà de la transmission confidentielle d'information (suivez le cours IFT 6180, qui se donne en parallèle, si vous voulez en savoir davantage), il en va de même de la cryptographie quantique. Nous pourrions passer toute la session à discuter de sujets aussi fascinants que le tirage à pile ou face, la mise en gage, le transfert équivoque, le partage de secrets, le *zero knowledge*, les puzzles de Merkle quantiques, le calcul multi-partie, la transmission anonyme quantique...

- L'*intrication* est la plus éblouissante des manifestations non-classiques de la mécanique quantique. Quelle est son épopée ? Comment peut-on la quantifier ? La simuler en profitant des échappatoires ? La manipuler ? La distiller ? Que nous apprend-elle sur notre univers ? Permet-elle d'expliquer le phénomène de la mesure ? Certaines formes de nonlocalité causales peuvent-elles être plus fortes que l'intrication ?

- Vous connaissez tous les *algorithmes de Shor et de Grover* ainsi que la transformée de Fourier quantique. Mais il y a d'autres techniques d'algorithmique quantique ! L'*amplification de l'amplitude*, qui est une généralisation fertile de l'algorithme de Grover, a fait place à certaines *marches aléatoires quantiques* et *chaînes de Markov quantiques*, qui procurent parfois une accélération exponentielle.

- Le modèle du *circuit quantique* n'est pas le seul à exister. Il est parfois plus intéressant de considérer le calcul quantique comme un *phénomène continu*; c'est ainsi par exemple que certains nouveaux algorithmes ont été découverts. De même, le *modèle basé sur la mesure* procure une perspective différente dont la fertilité a été démontrée à maintes reprises, incluant dans des contextes cryptographiques.

- *Bornes inférieures.* L'ordinateur quantique peut accélérer certains calculs, mais il n'est pas omnipuissant. Plusieurs techniques ont été développées pour démontrer certaines limitations intrinsèques à sa puissance : argument hybride, méthode polynomiale, argument d'adversaire...

- Dans les modèles de *preuves interactives* à un ou plusieurs prouveurs, l'intrication est-elle une bénédiction qui permet de prouver certains énoncés plus efficacement, ou au contraire une malédiction qui permet à des prouveurs sans scrupules de tricher ?

- Grâce au mécanisme dit de *locking*, une grande quantité d'information classique, enfermée de façon apparemment inaccessible dans un état quantique, peut être libérée par la révélation d'une courte clef.

- À travers tout ceci, la question qui me fascine le plus concerne les *fondements de la mécanique quantique*. Bien sûr, celle-ci nous offre une fantastique panoplie pour améliorer nos capacités à traiter l'information. Mais se peut-il que l'informatique quantique en vienne un jour à repayer sa dette envers la physique en nous permettant enfin de faire mentir Richard Feynman lorsqu'il proclamait fièrement : « I think I can safely say that nobody understands quantum mechanics » ?

Public cible : Ce cours s'adresse aux étudiant(e)s qui ont déjà des connaissances de base en informatique quantique, préférablement (mais pas nécessairement) ayant suivi le cours préalable IFT 6155 — Informatique quantique.

Documentation : Le cours sera basé sur une collection d'articles scientifiques qui seront distribués au fur et à mesure.

Évaluation : L'évaluation sera basée principalement sur la participation en classe et la présentation d'une conférence accompagnée d'un document écrit.