Université de Montréal
Département d'informatique et de recherche opérationnelle

IFT 3375 / 6370 — Informatique théorique — A09

Professeur: Gilles Brassard, 2215 André–Aisenstadt
brassard@iro.umontreal.ca
http://www.iro.umontreal.ca/~brassard/

Horaire des cours: lundi et mardi, 15h30 –17h30, AA–1175
Premier cours: le mardi 1er septembre 2009

Ce cours fait suite à celui sur l'introduction à l'informatique théorique (IFT 2105). Il s'adresse aux étudiants des trois cycles intéressés par les aspects théoriques de l'informatique. Le contenu précis du cours n'est pas fixé dans le béton car il dépendra dans une certaine mesure des connaissances et intérêts des étudiants inscrits. Plusieurs des sujets suivants seront traités; d'autres pourraient l'être.

- ◇ *Degrés d'indécidabilité:* Vous savez déjà que certains problèmes ne peuvent pas être résolus quelles que soient les ressources dont on dispose. Nous verrons qu'il y a toute une hiérarchie à l'intérieur des problèmes indécidables: décider si un programme finit par arrêter sur toutes les données, par exemple, est encore plus indécidable que de savoir s'il boucle à l'infini sur toutes les données.

- ◇ *Complexité concrète:* Rappel de **NP**. Étude des principales classes de complexité déterministes, non-déterministes et probabilistes. Réductions et complétudes pour ces classes. Théorème de Ladner. Hiérarchie polynomiale.

- ◇ *Complexité axiomatique:* Lorsqu'on analyse la complexité d'un algorithme ou d'un problème, on tient le plus souvent compte du temps d'exécution ou de la mémoire. Toutefois, il y a bien d'autres mesures intéressantes. La théorie axiomatique de Blum va droit au cœur de *toutes* les mesures de complexité "raisonnables". Ceci permet entre autres de démontrer des théorèmes très généraux tels celui de l'accélération: Il existe des problèmes pour lesquels tout algorithme peut être accéléré exponentiellement... incluant la version accélérée de l'algorithme! Le théorème du trou noir de Borodin (*Gap Theorem*) est une autre merveille de cette théorie.

- ◇ *Complexité algorithmique:* Certaines chaînes de bits peuvent être comprimées algorithmiquement de façon importante alors que d'autres sont incompressibles. Cette notion permet de prouver certains théorèmes avec une surprenante simplicité. Nous discuterons également d'un oracle hautement incompressible qui permet de résoudre certains problèmes indécidables, mais qui ne permet curieusement pas d'accélérer la résolution des problèmes décidables davantage que ne le permettrait l'accès à une source purement aléatoire!

verso...

- ◇ *Preuves interactives:* En autant qu'une faible probabilité d'erreur soit tolérable, la notion classique de preuve mathématique peut être généralisée si une interaction est permise entre le prouveur et celui qui souhaite vérifier l'exactitude de l'énoncé à prouver. Cette théorie culmine par le fait que tout énoncé vérifiable en *espace* polynomial peut être démontré par une preuve interactive ne demandant au vérificateur qu'un *temps* polynomial. Une autre généralisation demande que la preuve puisse être vérifiée en ne regardant qu'un petit nombre de bits de celle-ci, choisis aléatoirement.

- ◇ *Lambda calcul:* Le lambda calcul est un formalisme étonnamment simple et amusant qui permet de définir la notion de ce qu'est une fonction calculable. Il est facile de définir l'exponentiation au moyen du lambda calcul. La multiplication est un peu plus difficile et l'addition plus difficile encore. Quant à la soustraction, c'est un cauchemar que Kleene n'a finalement pu résoudre que sur la chaise de son dentiste!

- ◇ *Calcul réversible:* Tout calcul peut être effectué de façon réversible, c'est-à-dire qu'il est possible à tout moment pendant le calcul de "renverser la vapeur" et faire marche arrière. Nous verrons les conséquences étonnantes de cette découverte. En particulier, tout calcul peut être effectué avec une quantité arbitrairement faible d'énergie.

- ◇ *Informatique quantique:* L'utilisation de la mécanique quantique pourrait conduire à une révolution sans précédent dans l'histoire de l'informatique. En particulier, l'information quantique peut se retrouver en superposition de différentes valeurs classiques. Ceci permet à une quantité exponentielle de calculs de prendre place simultanément. 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. L'information quantique peut également être utilisée pour fins cryptographiques.

- ◇ *Digressions:* Nous ferons à l'occasion des digressions pour la culture générale. Par exemple, j'ai discuté par le passé de sujets aussi variés que le constructivisme, la géométrie non Euclidienne, la cryptologie, l'auto-vérification de programmes (*Proof Checkers*), la génération pseudo-aléatoire, etc.

Support de cours et évaluation

Inutile de le préciser: aucun livre ne traite de tous ces sujets. Comme support de cours, nous utiliserons donc des copies d'articles et des notes diverses. Le mode d'évaluation reste à déterminer au cours des premières semaines: il dépendra du nombre d'étudiants inscrits. Il y aura toutefois un examen partiel le mardi 13 octobre de 15h30 à 17h20 au AA–1177, ainsi qu'un examen final cumulatif le mardi 15 décembre de 15h30 à 18h20 au AA–1360.