Université de Montréal

Département d'informatique et de recherche opérationnelle

# IFT 3155/6155 — Informatique quantique — H22

**Professeur :** Gilles Brassard, brassard@iro.umontreal.ca
**Démonstrateur :** Rémi Ligez, remi.ligez@hotmail.com
**Site web du cours :** https://studium.umontreal.ca/course/view.php?id=219552

**Description :** Malgré la richesse indéniable de l'informatique traditionnelle, celle-ci prend résolument ses racines dans la physique classique de Newton et Einstein, 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 théorie 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 théorie 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 pseudotélépathie, 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 théorie 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 théorie 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 Richard 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 pseudotélépathie 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 sera indispensable au fonctionnement fiable de l'ordinateur quantique du futur.

**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 théorie 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. Et, sans blague, il vous faudra être familier avec l'alphabet grec ! Mais surtout, venez avec un esprit ouvert afin de donner libre cours à vos rêves et à votre imagination : sachez qu'Einstein a dit que l'imagination est plus importante que la connaissance. Je suis bien d'accord.

**Documentation :** Le cours sera basé sur une version préliminaire de mon livre *Quantum Information Science for Computer Scientists* (disponible sous StudiUM au fur et à mesure de l'avancement du cours), le livre *L'Impensable Hasard* de Nicolas Gisin, ainsi que sur des articles scientifiques et notes de cours qui seront placés sur StudiUM au moment opportun.

**Horaire des cours et des examens :**
Mardis de 12h30 à 14h20 et mercredis 13h30 à 15h20, salle S–144 du pavillon Roger-Gaudry **ou** ID de réunion Zoom 860 6459 0769, code secret 791954, selon l'évolution de la situation.
Examen de mi-session le mercredi 9 mars 2022 de 13h30 à 15h20 au S-144, Roger-Gaudry ;
Examen final le mercredi 20 avril 2022 de 13h30 à 16h20 au 1355, André-Aisenstadt.

**Attention :** Les cours commenceront sur Zoom et se continueront possiblement en présentiel au S-144. Si un examen de mi-session en présentiel est impossible, il sera remplacé par des questions spontanées, possiblement administrées sur StudiUM. Mais à moins de catastrophe majeure, *l'examen final sera en présentiel*. **Ne vous inscrivez pas** au cours si vous ne pouvez pas garantir votre présence physique à Montréal le 20 avril 2022.

Université de Montréal

Département d'informatique et de recherche opérationnelle

# IFT 3155/6155 — Informatique quantique — H22

## *Mode d'évaluation*

**Professeur :** Gilles Brassard, `brassard@iro.umontreal.ca`.
**Démonstrateur :** Rémi Ligez, `remi.ligez@hotmail.com`
**Site web du cours :** https://studium.umontreal.ca/course/view.php?id=219552

Le mode d'évaluation de ce cours (qui ne demande pas de programmation) dépendra de la possibilité ou non de faire un examen de mi-session en présentiel. Si ce n'est pas possible, celui-ci sera remplacé par des questions spontanées (voir ci-dessous).

Il faut aussi savoir que le mode d'évaluation est différent selon que vous soyez inscrit(e)s à IFT3155 (trois crédits) ou IFT6155 (quatre crédits). Les critères d'évaluation seront les suivants, bien que le dernier d'entre eux n'est pertinent que des étudiants de IFT6155. Une description plus détaillée se trouve à la page suivante (ou au verso).

- Examen de mi-session le 9 mars 2022 au S-144 du pavillon Roger-Gaudry *ou* vingt-cinq questions spontanées posées pendant les cours sans préavis, à raison d'un point par question *ou* une combinaison des deux. **Attention :** Ceci est une nouvelle date pour l'examen de mi-session car il était prévu à l'origine pour le 23 février.
- Devoirs variés au cours de la session. On peut s'attendre à environ 7 devoirs.
- Examen final le 20 avril 2022, 13h30–16h20, salle 1355 du Pavillon André-Aisenstadt.
- Lecture d'un article scientifique et présentation en classe de ce qu'il contient.

La **pondération** dépend du cours suivi selon le barême ci-dessous.

| | Examen de mi-session *ou* Questions spontanées | Devoirs | Examen final | Lecture et présentation |
|---|---|---|---|---|
| IFT3155 | 25 % | 40 % | 35 % | — |
| IFT6155 | 20 % | 35 % | 30 % | 15 % |

**Important :** Il s'agit d'un barème avec seuil à 40%, ce qui veut dire que vous devez obtenir un minimum de 40% de moyenne pondérée aux examens *ou* aux questions spontanées et à l'examen final, selon le cas, pour que les devoirs (et la présentation le cas échéant) soient pris en compte.

# Explication des critères d'évaluation

- Les **questions spontanées**, s'il y a lieu, seront administrées pendant les séances de cours. Elles tirent leur nom du fait qu'elles peuvent survenir à n'importe quel moment, sans préavis. Elles demanderont de démontrer votre compréhension des notions de base qui viennent d'être expliquées (ou qui ont été expliquées aux cours précédents récents), le plus souvent sans demander aucun calcul. Elles sont conçues pour que la réponse vienne immédiatement si, effectivement, vous avez compris. Par conséquent, vous n'aurez qu'une minute ou deux pour répondre (selon la question). Étant donné que ces questions seront administrées sur le site StudiUM du cours, vous *devez* être branché(e)s en permanence sur votre StudiUM pendant que vous assistez au cours, tant que celui-ci se déroulera sur Zoom (ensuite on verra, si ensuite it y a...). Ces questions pourront être regroupées en mini-tests, c'est-à-dire en rafales de plusieurs questions.

- Les **devoirs** consisteront en un certain nombre de questions à développement, le plus souvent (mais pas toujours) tirées du livre. Ils seront à remettre sur StudiUM tant que le cours sera sur Zoom, mais sur papier dès que le cours redeviendra en présentiel, s'il y a lieu. Dans tous les cas, les devoirs devront être remis avant le *début* du cours indiqué sur l'énoncé, généralement de 6 à 8 jours après avoir été assignés. **Aucun retard ne sera accepté** puisque les solutions aux problèmes des devoirs seront souvent donnés à ce cours-là. Certains de ces devoirs seront à faire individuellement alors que certains autres pourront également être remis par équipes de deux. Toutefois, vous êtes **très** fortement encouragé(e)s à travailler chaque question par vous-même car c'est ainsi qu'on assimile la matière. Sinon, vous pourriez le regretter lors d'évaluations subséquentes.

- L'**examen final** aura lieu le mercredi 20 avril **en présentiel** de 13h30 à 16h20 au 1355 du pavillon André-Aisenstadt, en autant que la situation sanitaire le permette. Si vous ne prévoyez pas être à Montréal ce jour-là, il est *essentiel* que vous renonciez dès maintenant à prendre le cours cette session-ci. En effet, *aucune* excuse du genre « Je n'ai pas pu me rendre à Montréal » ne sera acceptée le moment venu. Vous aurez été prévenus...

- La **lecture et présentation d'un article scientifique** n'est requise que pour les étudiants du cours IFT6155 afin qu'ils méritent leur quatrième crédit. Les modalités de cette activité seront annoncées dans un document subséquent. Notez que les présentations se feront en dehors des heures de cours selon un horaire qui conviendra à tous les intervenants. Étant donné le grand nombre d'inscriptions au IFT6155 cette année (une treizaine en date du 4 janvier 2022), le temps de parole de chacun sera limité à 25 petites minutes. Ce sera l'occasion de pratiquer la concision ! Vous pourrez néanmoins disposer de 50 minutes pour présenter un sujet en vous associant à un binôme (pas de Newton!).