

## Informatique Quantique Théorique

### Cours

Titre: Informatique quantique théorique  
Sigle: PHY-732  
Crédits: 3

### Place du cours dans le programme

Type de cours: optionel  
Cours préalable: PHQ-330, PHQ-430

### Professeur

Nom: David Poulin  
Bureau: D3-2044  
Tél: 62054  
Courriel: David.Poulin@USherbrooke.ca

### Charge de travail hebdomadaire

3 heures en classe d'exposés magistraux  
1 heure en classe de travaux dirigés  
2 heures de lecture des notes  
4 heures pour réaliser les devoirs

### Mise en contexte du cours

*L'information est physique* disait R. Landauer ; il ne peut y avoir d'information sans système physique pour la contenir. Cette indissociabilité du contenu et du contenant a des répercussions physiques importantes. Par exemple, elle permet de résoudre l'énigme du démon de Maxwell en thermodynamique à l'aide d'arguments de la théorie de l'information. En contrepartie, cette indissociabilité suggère aussi que les lois de la physique doivent encadrer les principes informatiques. Puisque les lois de la nature sont fondamentalement quantiques, il s'en suit que les règles régissant le traitement de l'information doivent être dictées par la mécanique quantique. Au cours des dernières décennies, de nombreuses expériences ont démontré la possibilité de contrôler des systèmes quantiques individuels de façon cohérente. Cet exploit fut d'ailleurs souligné par l'attribution du prix Nobel en 2012.

L'informatique quantique vise d'abord à comprendre et exploiter les possibilités offertes par la mécanique quantique à des fins de traitement d'information. Il est maintenant bien établi qu'en principe, la communication réalisée à partir de l'échange de particules quantiques permet d'accomplir certaines tâches qui sont impossibles dans un monde classique. De même, un ordinateur pouvant exploiter le principe de superposition permet en principe d'accomplir certains calculs beaucoup plus rapidement que ce que nous croyons être possible avec un ordinateur classique. Ces avantages peuvent être attribués au principe de superposition quantique et à l'existence d'intrication quantique.

## Objectifs

Acquérir une connaissance approfondie des principaux sujets de l'informatique quantique théoriques. Maîtriser les concepts qui s'y rattachent et comprendre leur formalisme.

## Contenu

Théorie quantique de l'information, tolérance aux fautes, complexité du calcul, modèles théoriques du calcul quantique.

## Objectifs spécifiques

À la fin de ce cours, pour atteindre les objectifs, l'étudiant devra être capable de :

- Comprendre les différentes notions de capacité d'un canal quantique et connaître les formules entropiques qui s'y rattachent. Pouvoir démontrer la validité de ces formules dans des cas simples;
- Connaître les classes de complexités liées au calcul quantique, savoir démontrer l'appartenance et la complétude d'un problème pour ces classes.
- Maîtriser les concepts fondamentaux de la tolérance aux fautes, savoir analyser le seuil d'un protocole tolérant les fautes.
- Décrire les différents modèles théoriques de calcul quantiques et savoir démontrer leur équivalence.

## Méthode pédagogique

La méthode pédagogique utilisée sera principalement un exposé magistral théorique parsemé d'exercices ou de discussions.

## Évaluation

- Pondération: Devoirs 20%, Intra 30%, Projet 15%, Final 35%.
- Date de l'examen intratrimestriel : elle sera fixée par la Faculté des sciences et vous sera communiquée au cours de la session.
- Date de l'examen final : elle sera fixée par la Faculté des sciences et vous sera communiquée en novembre.
- Critères d'évaluation : les devoirs et les examens consistent de problèmes à résoudre en se basant sur les concepts généraux appris en classe et de démonstrations formelles d'énoncés. Les réponses sont évalués selon la façon de formuler le problème mathématiquement, l'exactitude de l'analyse et la validité de l'interprétation. Les preuves seront évaluées selon la validité et la simplicité du raisonnement et l'exactitude de l'analyse.

## Contenu détaillé

Temps alloué	Sujet
3 semaines	<b>Information quantique</b> : théorie de Shannon, compression de Schumacher, information accessible, Borne de Holevo, mesure d'intrication
3 semaines	<b>Tolérance aux fautes</b> : formalisme stabilisateur, mesure de syndromes, portes transverses, seuil d'erreur, distillation d'états magiques.
3 semaine	<b>Complexité</b> : P, NP, BQP, QMA, notion de problème complet, état fondamental.
3 semaine	<b>Modèles de calcul quantique</b> : circuits, calcul quantique adiabatique, calcul quantique topologique, calcul par mesures.

## Bibliographie

1. J. Preskill, Lecture notes on quantum computation, disponible sur Internet à l'adresse <http://www.theory.caltech.edu/people/preskill/ph229/>
2. M.A. Nielsen et I.L. Chuang, Quantum computation and quantum information, Cambridge University Press, 2000 [QA 76.889 N54].
3. D.A. Lidar et T.A. Brun, éditeurs, Quantum Error Correction, Cambridge University Press, 2013.
4. N.D. Mermin, Quantum computer science: an introduction, Cambridge University Press, New York, 2007 [QA 76.889 M47].
5. U. Vazirani, Lecture notes on quantum computation, disponible sur Internet à l'adresse <http://www.cs.berkeley.edu/~vazirani/f04quantum/quantum.html>
6. J. Watrous, Quantum Computational Complexity, Springer Encyclopedia of Complexity and Systems Science, disponible à <http://arxiv.org/abs/0804.3401v1> .
7. A. Yu. Kitaev, A.H. Shen et M.N. Vyalyi, Classical and quantum computation, American Mathematical Society, 2002.
8. D.E. Browne et H.J. Briegel, One-way Quantum Computation — a tutorial introduction, disponible à <http://arxiv.org/abs/quant-ph/0603226> .
9. J. Kempe, A. Yu. Kitaev, Alexei et O. Regev, The Complexity of the Local Hamiltonian Problem, SIAM Journal on Computing 35 (5): 1070–1097 (2006), disponible à arXiv:quant-ph/0406180v2