UNIVERSITÉ DE SHERBROOKE

Département d'informatique

IGL 501/IGL 710 – Méthodes formelles en génie logiciel

Plan d'activité pédagogique
Automne 2018

Enseignant

Richard St-Denis

Courriel :	Richard.St-Denis@USherbrooke.ca
Local :	D4-2005
Téléphone :	(819) 821-8000 poste 62847
Site :	http://www.usherbrooke.ca/informatique/personnel/professeurs/professeurs/richard-st-denis/
Disponibilité :	horaire de consultation affiché sur ma porte

Responsable(s) : Marc Frappier

Horaire

Exposé magistral :	mardi	10 h 30 à 12 h 20	salle D4-2023
	mercredi	9 h 30 à 10 h 20	salle D4-2023

Description officielle de l'activité pédagogique [1]

Cibles de formation :	Connaître et utiliser les méthodes formelles de spécification, de validation et de vérification.
Contenu :	Rappels mathématiques. Spécification à base de modèles. Algèbre de processus. Techniques de vérification : analyse formelle des spécifications, correction et preuve de spécifications, preuve de correction d'une implémentation, vérification par exploration de l'espace d'états (model checking). Techniques de validation : exécution de spécifications formelles, prototypage.
Crédits	3
Organisation	3 heures d'exposé magistral par semaine 6 heures de travail personnel par semaine
Préalable	(GEN 700 et GLO 700) ou IFT 159

1. https://www.usherbrooke.ca/admission/fiches-cours/igl501

1 Présentation

Cette section présente les cibles de formation spécifiques et le contenu détaillé de l'activité pédagogique. Cette section, non modifiable sans l'approbation d'un comité de programme du Département d'informatique, constitue la version officielle.

1.1 Mise en contexte

La construction de systèmes de qualité tout en respectant les contraintes de temps et de budget représente toujours un formidable défi pour les informaticiens. Dans les domaines où la sécurité des personnes et des biens est en cause, ce défi est encore plus grand. Une des approches proposées pour résoudre ce problème consiste à utiliser des *outils mathématiques* pour spécifier, valider et vérifier les systèmes informatiques. On désigne communément ces approches basées sur les mathématiques comme des *méthodes formelles*.

Le choix des mathématiques s'explique par le besoin de rigueur et de précision dans la description du comportement de systèmes complexes, et par la nécessité de disposer de mécanismes d'abstraction pour juguler la complexité. Les méthodes formelles permettent également de palier les faiblesses des méthodes traditionnelles de tests qui ne peuvent traiter de manière exhaustive tous les cas possibles d'utilisation d'un système.

On distingue deux approches pour vérifier la cohérence d'un système par rapport à sa spécification: la preuve et la vérification. La preuve consiste à démontrer de manière systématique, en utilisant les règles d'inférence d'une logique, un théorème de correction. La vérification (appelée *model checking* en anglais) consiste à vérifier, de manière exhaustive en parcourant tous les états possibles du système, que le théorème est satisfait. Ces deux approches seront abordés dans le cadre du cours en utilisant des outils logiciels appropriés.

Après plus de trois décennies de recherche, la communauté scientifique a proposé plusieurs méthodes formelles de construction de systèmes. Certaines d'entre elles sont maintenant utilisées pour concevoir des systèmes critiques en milieu industriel comme le transport, les télécommunications, l'énergie nucléaire, les circuits intégrés et les appareils médicaux. Toutefois, l'utilisation de méthodes formelles demeure peu répandue, et leur utilisation à grande échelle nécessitera encore plusieurs investissements au niveau de la recherche, mais également au niveau de la formation des informaticiennes et informaticiens.

1.2 Cibles de formation spécifiques

À la fin de cette activité pédagogique, l'étudiante ou l'étudiant sera capable :

1. traduire les exigences d'un cahier des charges (analyse des besoins) en une spécification formelle;
2. raffiner une spécification;
3. implémenter une spécification;
4. comprendre les principes de base de la preuve;
5. comprendre les principes de base de la vérification;
6. spécifier des propriétés en logique temporelle;
7. comprendre l'apport des méthodes formelles pour la production de logiciel de qualité;
8. identifier les situations où l'utilisation de méthodes formelles est souhaitable.

1.3 Contenu détaillé

Voir la section suivante.

2 Organisation

Cette section propre à l'approche pédagogique de chaque enseignante ou enseignant présente la méthode pédagogique, le calendrier, le barème et la procédure d'évaluation ainsi que l'échéancier des travaux. Cette section doit être cohérente avec le contenu de la section précédente.

2.1 Méthode pédagogique

L'activité pédagogique *Méthodes formelles en génie logiciel* est avant tout orientée vers la présentation de méthodes et d'outils qui sont extraits de livres ou d'articles scientifiques.

2.2 Calendrier

Semaines	Thèmes	Références	Devoirs
1	introduction: modélisation, vérification, synthèse	chap, 1 de [1]	
2	modélisation: système à transition (Uppaal)	chap, 2 de [1]	devoir #1
3	modélisation: système à transition (Uppaal)	chap, 2 de [1]	
4	logique propositionnelle (exemple avec Alloy)	[3]	
5	propriétés (invariant, sûreté, vivacité, équité)	chap, 2 de [1]	devoir #2
6	logique relationnelle et Alloy	[3]	devoir #3
7	examen périodique		
8	synthèse et application à SCT	[2–4]	devoir #4
9	logique temporelle linéaire (LTL)	chap, 5 de [1]	
10	logique temporelle linéaire (LTL)	chap, 5 de [1]	devoir #5
11	logique arborescente (CTL)	chap, 6 de [1]	
12	logique arborescente (CTL)	chap, 6 de [1]	devoir #6
13	automate temporisé (Uppaal)	chap, 9 de [1]	
14	automate temporisé (Uppaal)	chap, 9 de [1]	
15–16	examen final		

SCT : Supervisory Control Theory
Alloy : `alloy.mit.edu`
Uppaal : `www.uppaal.org`

2.3 Évaluation

Devoirs	30%
Examen périodique	30%
Examen final	40%
Qualité du français	0%

Toute documentation est permise aux examens. Toutefois, les appareils électroniques (calculatrice, portable, téléphone cellulaire) sont interdits.

Conformément à l'article 17 du règlement facultaire d'évaluation des apprentissages des étudiantes et des étudiants

(https://www.usherbrooke.ca/sciences/fileadmin/sites/sciences/Etudiants_actuels/Informations_academiques_et_reglements/2017-10-27_Reglement_facultaire_-_evaluation_des_apprentissages.pdf),

l'enseignant peut retourner à l'étudiante ou à l'étudiant tout travail non conforme aux exigences quant à la qualité de la langue et aux normes de présentation.

Toute situation de plagiat sera traitée en conformité, entre autres, avec l'article 9.4.1 du *Règlement des études* de l'Université de Sherbrooke disponible à l'adresse

https://www.usherbrooke.ca/registraire/droits-et-responsabilites/reglement-des-etudes/

Vous trouverez en annexe un document d'information relatif à l'intégrité intellectuelle qui fait état de l'article 9.4.1. En particulier,

> Un document dont le texte et la structure se rapporte à des textes intégraux tirés d'un livre, d'une publication scientifique ou même d'un site Internet, doit être référencé adéquatement. Lors de la correction de tout travail individuel ou de groupe une attention spéciale sera portée au plagiat, défini dans le *Règlement des études* comme « le fait, dans une activité pédagogique évaluée, de faire passer indûment pour siens des passages ou des idées tirés de l'oeuvre d'autrui ». Le cas échéant, le plagiat est un délit qui contrevient à l'article 9.4.1 du *Règlement des études* : « tout acte trompeur ou toute tentative de commettre un tel acte, quant au rendement scolaire ou à une exigence relative à une activité pédagogique. » À titre de sanction disciplinaire, les mesures suivantes peuvent être imposées : a) l'obligation de reprendre un travail, un examen ou une activité pédagogique et b) l'attribution de la note E ou de la note 0 pour un travail, un examen ou une activité évaluée. Tout travail suspecté de plagiat sera référé au Secrétaire de la Faculté des sciences.

2.4 Échéancier des travaux

Les directives, la date de remise et le barème relatifs aux devoirs seront connus à la remise de l'énoncé de chaque d'eux aux étudiantes et aux étudiants.

Directives particulières : Les devoirs peuvent être faits individuellement ou par équipe de deux personnes. Aucun devoir ne peut être remis par courrier électronique. Les devoirs non remis reçoivent automatiquement la note zéro.

La correction des devoirs et des examens est entre autres basée sur le fait que chacune de vos réponses soit :

— claire, c'est-à-dire lisible et compréhensible pour le correcteur ;
— précise, c'est-à-dire exacte ou sans erreur ;
— complète, c'est-à-dire que toutes les étapes de résolution du problème sont présentes ;
— concise, c'est-à-dire que la méthode de résolution est la plus courte possible.

2.5 Utilisation d'appareils électroniques et du courriel

Selon le Règlement complémentaire des études (complément à la section 4.2.3) l'utilisation d'ordinateurs, de cellulaires ou de tablettes pendant une prestation est interdite à condition que leur usage soit explicitement permise dans le plan de cours.

Dans ce cours le complément facultaire du règlement 4.2.3 s'applique à moins d'avoir obtenu personnellement l'autorisation du professeur. Cette permission peut être retirée en tout temps, si l'appareil n'est pas uniquement utilisé à des fins d'apprentissage.

En particulier, toute utilisation d'appareils de captation de la voix ou de l'image exige la permission du professeur.

Le Règlement des études et le Règlement complémentaire au Règlement des études sont disponibles sur l'Intranet de la Faculté des sciences. [2]

Note: je ne réponds à aucun courriel.

2. https://www.usherbrooke.ca/registraire/droits-et-responsabilites/reglement-des-etudes/
https://www.usherbrooke.ca/sciences/fileadmin/sites/sciences/documents/Intranet/Informations_academiques/Sciences_Reglement_complementaire_2017-05-09.pdf

3 Matériel nécessaire pour l'activité pédagogique

Aucun manuel n'est obligatoire. Certains documents sont disponibles dans le répertoire public `Public/Cours` dont l'accès est décrit dans la page Web

http://www.usherbrooke.ca/informatique/intranet/ressources-et-documentation/faq/acces-aux-lecteurs-reseaux/

4 Références

[1] C. BAIER et J.-P. KATOEN : *Principles of Model Checking*. MIT Press, Cambridge, MA, 2008.

[2] B. FRAIKIN, M. FRAPPIER et R. ST-DENIS : Supervisory control theory with Alloy. *Science of Computer Programming*, 94:217–237, 2014.

[3] D. JACKSON : *Software Abstractions : Logic, Language, and Analysis, Revised edition*. MIT Press, Cambridge, MA, 2012.

[4] W. M. WONHAM : *Supervisory Control of Discrete-Event System*. Electrical & Computer Engineering, University of Toronto, 2013.

UNIVERSITÉ DE SHERBROOKE

L'intégrité intellectuelle passe, notamment, par la reconnaissance des sources utilisées. À l'Université de Sherbrooke, on y veille!

Extrait du Règlement des études

8.1.2 Relativement aux activités pédagogiques

L'expression délit désigne d'abord tout acte ou toute manœuvre visant à tromper quant au rendement scolaire ou quant à la réussite d'une exigence relative à une activité pédagogique.

Sans restreindre la portée générale de ce qui précède, est considéré comme un délit :

a) la substitution de personnes ou l'usurpation d'identité lors d'une activité évaluée ou obligatoire;
b) le plagiat, soit le fait, dans une activité évaluée, de faire passer indûment pour siens des passages ou des idées tirés de l'œuvre d'autrui;
c) l'obtention par vol ou par toute autre manœuvre frauduleuse de document ou de matériel, la possession ou l'utilisation de tout matériel non autorisé avant ou pendant un examen ou un travail faisant l'objet d'une évaluation;
d) le fait de fournir ou d'obtenir toute aide non autorisée, qu'elle soit collective ou individuelle, pour un examen ou un travail faisant l'objet d'une évaluation;
e) le fait de soumettre, sans autorisation préalable, une même production comme travail à une deuxième activité pédagogique;
f) la falsification d'un document aux fins d'obtenir une évaluation supérieure dans une activité ou pour l'admission à un programme.

Par plagiat, on entend notamment :

- Copier intégralement une phrase ou un passage d'un livre, d'un article de journal ou de revue, d'une page Web ou de tout autre document en omettant d'en mentionner la source ou de le mettre entre guillemets
- Reproduire des présentations, des dessins, des photographies, des graphiques, des données… sans en préciser la provenance et, dans certains cas, sans en avoir obtenu la permission de reproduire
- Utiliser, en tout ou en partie, du matériel sonore, graphique ou visuel, des pages Internet, du code de programme informatique ou des éléments de logiciel, des données ou résultats d'expérimentation ou toute autre information en provenance d'autrui en le faisant passer pour sien ou sans en citer les sources
- Résumer ou paraphraser l'idée d'un auteur sans en indiquer la source
- Traduire en partie ou en totalité un texte en omettant d'en mentionner la source ou de le mettre entre guillemets
- Utiliser le travail d'un autre et le présenter comme sien (et ce, même si cette personne a donné son accord)
- Acheter un travail sur le Web ou ailleurs et le faire passer pour sien
- Utiliser sans autorisation le même travail pour deux activités différentes (autoplagiat)

Autrement dit : mentionnez vos sources.

Document informatif V.2 (juin 2012) Groupe de travail anti-plagiat