UNIVERSITÉ DE SHERBROOKE

Département d'informatique

IGL 501 / IGL 710 – Méthodes formelles en génie logiciel

Plan d'activité pédagogique

Automne 2021

Enseignant

Marc Frappier	
Courriel :	marc.frappier@usherbrooke.ca
Local :	D4-1010-08
Téléphone :	+1 819 821-8000 x62096
Disponibilités :	Sur rendez-vous par courriel

Responsable(s) : Marc Frappier et Michael Blondin

Site web du cours : http://info.usherbrooke.ca/mfrappier/igl501/igl501.html

Horaire

Exposé magistral :	Lundi	13h30 à 14h20	salle D3-2035
	Jeudi	13h30 à 15h20	salle D3-2040

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
Particularités	Aucune

[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 du 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, une propriété d'un logiciel. La vérification (appelée model checking en anglais) consiste à vérifier, de manière exhaustive en parcourant les états du système, que la propriété est satisfaite. 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. de traduire les exigences d'un cahier des charges (analyse des besoins) en une spécification formelle ;
2. de raffiner une spécification ;
3. d'implémenter une spécification ;
4. de comprendre les principes de base de la preuve ;
5. de comprendre les principes de base de la vérification ;
6. de spécifier des propriétés en logique temporelle ;
7. de comprendre l'apport des méthodes formelles pour la production de logiciel de qualité ;
8. d'identifier les situations où l'utilisation de méthodes formelles est souhaitable.

1.3 Contenu détaillé

Thème	Contenu	Nbr. d'heures	Objectifs	Travaux	Lectures
1	Mathématiques discrètes pour la spécification : Logique, ensemble, relation, fonction, séquence	5	1 à 8	✔	[5] [7]
2	Spécification à base de modèle et vérification : Exemples : B, Event-B, Z, ASM, TLA+, VDM	5	1, 4, 7 et 8	✔	[5] [10]
3	Raffinement de spécification : Exemples : Raffinement algorithmique, de données et de systèmes d'actions ; illustration avec B et/ou Event-B, ou l'équivalent	6	1, 2, 3, 4, 7 et 8	✔	[5] [6] [10]
4	Preuve de correction d'un logiciel : Exemples : WP-calcul, calcul de raffinement	6	3, 4, 7 et 8	✔	[5] [6] [8]
5	Modélisation et vérification avec des approches purement logique : Exemples : Alloy, Coq, PVS, HOL, solveur SMT	6	4, 5, 7 et 8	✔	[11] [4] [2]
6	Modélisation avec des algèbres de processus : Exemples : CSP, π-calcul, LOTOS, ACP	6	1, 2, 3, 4, 7 et 8	✔	[3] [9]
7	Logique temporelle (LTL et CTL) et vérification : Logique temporelle (LTL et CTL) et vérification.	6	6, 7 et 8	✔	[1]

1. Le cours doit comprendre au moins cinq travaux pratiques couvrant tous les sujets marqués «✔» dans le tableau.
2. Les lectures indiquées ne sont là qu'à titre indicatif. L'enseignant est libre de choisir un autre document de référence.

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

- Une semaine comprend normalement 3 heures de cours constituées d'un exposé magistral de 2 heures en télé-enseignement synchrone et d'une séance d'exercices de 1 heure effectuée aussi en télé-enseignement synchrone. Lorsque possible, les cours seront donnés en mode comodal (présentiel et en ligne).
- Le cours comporte 5 travaux pratiques à remettre avec TurninWeb.
- Un site Moodle sera aussi utilisé pour des quizz lors des séances de télé-enseignement.

Compte tenu du contexte actuel (pandémie due au COVID-19), il se peut que le cours ait lieu en totalité ou en partie à distance d'une façon différente de ce qui est énoncé ci-dessus. Notez que vous en serez informés rapidement si tel est le cas.

2.2 Calendrier

Semaine	Date	Thème	Lectures
1	2021-08-30	1	[7]
2	2021-09-06	2	[5]
3	2021-09-13	2	[5]
4	2021-09-20	3	[5]
5	2021-09-27	3	[5]
6	2021-10-04	4	[5]
7	2021-10-11	4	[5]
8	2021-10-18	Examen périodique	
9	2021-10-25	Relâche	
10	2021-11-01	6	[9] [3]
11	2021-11-08	6	[9] [3]
12	2021-11-15	5	
13	2021-11-22	5	
14	2021-11-29	7	
15	2021-12-06	7	
16	2021-12-13	Examen final	

2.3 Évaluation

Devoirs	20 %
Examen intra	40 %
Examen final	40 %

- Les dates de soumission et remise des devoirs seront fournies au fur et à mesure de l'avancement dans le cours. Il faut prévoir un devoir aux 2 semaines environ.
- Les devoirs sont remis avec TurninWeb (soumission par courriel refusée).
- Aucun retard accepté ; la note 0 sera attribuée à tout devoir remis en retard.
- Vous pouvez soumettre votre devoir autant de fois que vous voulez avec TurninWeb ; la dernière soumission remplace la précédente ; il faut resoumettre tous les fichiers.
- Il vaut mieux soumettre un devoir incomplet à temps qu'un devoir complet en retard.
- Les devoirs se font en équipe de 4 personnes.

2.3.1 Qualité de la langue et de la présentation

Conformément à l'article 17 du règlement facultaire d'évaluation des apprentissages[2] l'enseignante ou 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.

2.3.2 Plagiat

Le plagiat consiste à utiliser des résultats obtenus par d'autres personnes afin de les faire passer pour sien et dans le dessein de tromper l'enseignant. Vous trouverez en annexe un document d'information relatif à l'intégrité intellectuelle qui fait état de l'article 9.4.1 du Règlement des études[3]. Lors de la correction de tout travail individuel ou de groupe une attention spéciale sera portée au plagiat. Si une preuve de plagiat est attestée, elle sera traitée en conformité, entre autres, avec l'article 9.4.1 du Règlement des études de l'Université de Sherbrooke. L'étudiante ou l'étudiant peut s'exposer à de graves sanctions qui peuvent être soit l'attribution de la note E ou de la note zéro (0) pour un travail, un examen ou une activité évaluée, soit de reprendre un travail, un examen ou une activité pédagogique. Tout travail suspecté de plagiat sera transmis au Secrétaire de la Faculté des sciences. Ceci n'indique pas que vous n'ayez pas le droit de coopérer entre deux équipes, tant que la rédaction finale des documents et la création du programme restent le fait de votre équipe. En cas de doute de plagiat, l'enseignante ou l'enseignant peut demander à l'équipe d'expliquer les notions ou le fonctionnement du code qu'elle ou qu'il considère comme étant plagié. En cas d'incertitude, ne pas hésiter à demander conseil et assistance à l'enseignante ou l'enseignant afin d'éviter toute situation délicate par la suite.

2.4 Échéancier des travaux

Les dates de remise des travaux seront indiquées sur les énoncés.

2.5 Utilisation d'appareils électroniques et du courriel

Selon le règlement complémentaire des études, section 4.2.3 [4], 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, l'usage de téléphones cellulaires, de tablettes ou d'ordinateurs est autorisées. Cette permission peut être retirée en tout temps si leur usage entraîne des abus.

Tel qu'indiqué dans le règlement universitaire des études, section 4.2.3[5], toute utilisation d'appareils de captation de la voix ou de l'image exige la permission du professeur.

Note : L'utilisation du courriel est recommandée pour poser vos questions.

3 Matériel nécessaire pour l'activité pédagogique

Nous utiliserons les logiciels ProB, Atelier B, Alloy et FDR. Vous pouvez les installer sur votre ordinateur personnel ; la page web du cours donne des pointeurs vers les sites pour le téléchargement de ces logiciels.

4 Références

[1] Baier, Christel and Katoen, Joost-Pieter : *Principles of Model Checking (Representation and Mind Series)*. The MIT Press, 2008.

[2] Dennis Yurichev : SAT/SMT by Example). https://yurichev.com/writings/SAT_SMT_by_example.pdf, 2019.

[2] https://www.usherbrooke.ca/sciences/fileadmin/sites/sciences/Etudiants_actuels/Informations_academiques_et_reglements/2017-10-27_Reglement_facultaire_-_evaluation_des_apprentissages.pdf

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

[4] https://www.usherbrooke.ca/sciences/fileadmin/sites/sciences/documents/Intranet/Informations_academiques/Sciences_Reglement_complementaire_2017-05-09.pdf

[5] https://www.usherbrooke.ca/sciences/fileadmin/sites/sciences/Etudiants_actuels/Informations_academiques_et_reglements/2017-10-27_Reglement_facultaire_-_evaluation_des_apprentissages.pdf

[3] HOARE, C.A.R. : *Communicating Sequential Processes*. Prentice-Hall, 1985. http://info.usherbrooke.ca/mfrappier/IFT734/ref/csp/CSP-hoare-cspbook.pdf.

[4] JACKSON, DANIEL : *Software Abstractions : Logic, Language, and Analysis*. MIT Press, 2012.

[5] JEAN-RAYMOND ABRIAL : *The B-book : assigning programs to meanings*. Cambridge University Press, New York, NY, USA, 1996.

[6] JEAN-RAYMOND ABRIAL : *Modeling in Event-B : System and Software Engineering*. Cambridge University Press, Cambridge, UK, 2010.

[7] MARC FRAPPIER : MAT115 : Notes de cours. http://info.usherbrooke.ca/mfrappier/mat115/ref/mat115-notes-de-cours.pdf, 2019.

[8] MORGAN, C.C. : *Programming from Specifications*. Prentice-Hall, 1998. http://info.usherbrooke.ca/mfrappier/IFT734/ref/logique/morgan-pgm-from-spec.pdf.

[9] ROSCOE, A.W. : *The Theory and Practice of Concurrency*. Prentice-Hall, 2005. http://info.usherbrooke.ca/mfrappier/IFT734/ref/csp/CSP-roscoe-theory-concurrency.pdf.

[10] WOODCOCK, J. AND DAVIES, J. : *Using Z : Specification, Refinement, and Proof*. Prentice-Hall, 1996. http://info.usherbrooke.ca/mfrappier/IFT734/ref/logique/UsingZWoodcock.pdf.

[11] YVES BERTOT AND PIERRE CASTÉRAN : Le Coq'Art (V8). https://www.labri.fr/perso/casteran/CoqArt/coqartF.pdf, 2015.

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* (Règlement 2575-009)

9.4.1 DÉLITS RELATIFS AUX ÉTUDES

Un délit relatif aux études désigne tout acte trompeur ou toute tentative de commettre un tel acte, quant au rendement scolaire ou une exigence relative à une activité pédagogique, à un programme ou à un parcours libre.

Sont notamment considérés comme un délit relatif aux études les faits suivants :

a) commettre un plagiat, soit faire passer ou tenter de faire passer pour sien, dans une production évaluée, le travail d'une autre personne ou des passages ou des idées tirés de l'œuvre d'autrui (ce qui inclut notamment le fait de ne pas indiquer la source d'une production, d'un passage ou d'une idée tirée de l'œuvre d'autrui);

b) commettre un autoplagiat, soit soumettre, sans autorisation préalable, une même production, en tout ou en partie, à plus d'une activité pédagogique ou dans une même activité pédagogique (notamment en cas de reprise);

c) usurper l'identité d'une autre personne ou procéder à une substitution de personne lors d'une production évaluée ou de toute autre prestation obligatoire;

d) fournir ou obtenir toute aide non autorisée, qu'elle soit collective ou individuelle, pour une production faisant l'objet d'une évaluation;

e) obtenir par vol ou toute autre manœuvre frauduleuse, posséder ou utiliser du matériel de toute forme (incluant le numérique) non autorisé avant ou pendant une production faisant l'objet d'une évaluation;

f) copier, contrefaire ou falsifier un document pour l'évaluation d'une activité pédagogique;

[…]

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