# Modélisation et vérification

**Groupe 30**
Mercredi, de 13h30 à 16h30 SB-R430 (cours)

## Responsable(s) du cours

**Nom du coordonnateur :** VILLEMAIRE, Roger

**Nom de l'enseignant :** VILLEMAIRE, Roger
**Local :** PK-4615
**Téléphone :** (514) 987-3000 #6744
**Disponibilité :**
**Courriel :** villemaire.roger@uqam.ca
**Site Web :** http://intra.info.uqam.ca/personnels/Members/villemaire_r

## Description du cours

Modélisation de systèmes informatiques en vue de faire une vérification automatique de leurs propriétés. Objectifs de la vérification. Introduction à un outil et descriptions de systèmes. Formalisation de propriétés à l'aide de logiques. Algorithmes de vérification: diagrammes de décision binaires, algorithme DPLL, démonstrateurs de théorèmes.

## Objectifs du cours

- Ce cours vise à rendre l'étudiant apte à représenter un système informatique à l'aide d'un outil de vérification ainsi qu'à être capable de décrire des propriétés informatiques significatives à l'aide de symbolismes logiques. De plus, l'étudiant devra maîtriser les concepts théoriques sur lesquels reposent le fonctionnement des outils.
- Les compétences développées dans le cadre de ce cours rendront l'étudiant(e) capable:
    - de modéliser un système informatique en justifiant ses choix en fonction des objectifs de vérification
    - de représenter des propriétés significatives avec des logiques
    - d'utiliser un outil de façon effective pour réaliser une vérification
    - d'être en mesure d'utiliser et d'expliquer les structures de données et les algorithmes utilisés en vérification
    - d'être en mesure d'apprécier les besoins algorithmiques spécifiques de la modélisation et de la vérification, en particulier au niveau de la performance

## Contenu du cours

Introduction: Les objectifs de la vérification et de la spécification de systèmes informatiques. Bref survol des différentes approches existantes.
Modélisation de systèmes informatiques: Structures de Kripke. Quelques modélisations simples. L'outil NuSMV.
La logique LTL (Linear Temporal Logic): Chemins d'une exécution. Syntaxe et sémantique de LTL. Descriptions de propriétés

représentatives. Dualités. Modélisations et vérifications avec l'outil. Le problème de la négation.
Modélisation et vérification: Exemples et exercices plus avancés de modélisation et de vérification à l'aide de NuSMV. Systèmes synchrones et asynchrones. Le problème de l'équité. Utilisation des macros m4.
Vérification symbolique de modèles: Encodage des structures de Kripke sous forme de formules booléennes. Représentations des variables du système, des états initiaux et des transitions.
Méthode SAT : Vérification de modèles bornée et vérification d'une formule LTL par la satisfaction d'une formule booléenne. Méthode de Tseitin pour mettre en forme normale conjonctive. Satisfaction de formules booléennes et algorithme de Davis-Putman-Logemann-Loveland (DPLL). Usage de l'outil en mode BMC.
La logique CTL (Computation Tree Logic).: Propriétés de chemins et propriétés d'états. Syntaxe et sémantique de CTL. Descriptions de propriétés représentatives. Comparaisons pratiques et théoriques avec LTL. La logique CTL*. Usage de l'outil avec CTL.
Les BDD (diagrammes de décisions binaires): Définition et construction des BDD. Le problème de l'ordre des variables. Comparaison avec les tables de vérité et les formes normales disjonctive et conjonctive. Remarque sur le problème SAT et P=NP. Vérification de formules CTL à l'aide des BDD.
Le déroulement du cours inclus des séances de laboratoire obligatoires. Nous nous déplacerons quelques fois au laboratoire pour utiliser des outils permettant de mettre en pratique les notions vues.

## Modalités d'évaluation

| Description sommaire | Date | Pondération |
|---|---|---|
| Examen intra | | 25% |
| Examen final | | 25% |
| Travail de session: travail de recherche, dont le sujet devra être approuvé par le professeur | | 50% |

Les règlements concernant le plagiat seront strictement appliqués. Pour plus de renseignements, consultez le site suivant :http://www.sciences.uqam.ca/etudiants/integrite-academique.html

**Politique d'absence aux examens**

**L'autorisation de reprendre un examen en cas d'absence est de caractère exceptionnel. Pour obtenir un tel privilège, l'étudiant-e doit avoir des motifs sérieux et bien justifiés.**

Il est de la responsabilité de l'étudiant-e de ne pas s'inscrire à des cours qui sont en conflit d'horaire, tant en ce qui concerne les séances de cours ou d'exercices que les examens. **De tels conflits d'horaire ne constituent pas un motif justifiant une demande d'examen de reprise.**

Dans le cas d'une absence pour raison médicale, l'étudiant-e doit joindre un certificat médical original et signé par le médecin décrivant la raison de l'absence à l'examen. Les dates d'invalidité doivent être clairement indiquées sur le certificat. Une vérification de la validité du certificat pourrait être faite. Dans le cas d'une absence pour une raison non médicale, l'étudiant-e doit fournir les documents originaux expliquant et justifiant l'absence à l'examen – par exemple, lettre de la Cour en cas de participation à un jury, copie du certificat de décès en cas de décès d'un proche, etc. Toute demande incomplète sera refusée. Si la direction du programme d'études de l'étudiant-e constate qu'un étudiant a un comportement récurrent d'absence aux examens, l'étudiant-e peut se voir refuser une reprise d'examen.

L'étudiant-e absent-e lors d'un examen doit, dans les cinq (5) jours ouvrables suivant la date de l'examen, présenter une demande de reprise en utilisant le formulaire prévu, disponible sur le site Web du département à l'adresse suivante : **http://info.uqam.ca/politiques/**

L'étudiant-e doit déposer le formulaire dûment complété au secrétariat de la direction de son programme d'études : PK-3150 pour les programmes de premier cycle, PK-4150 pour les programmes de cycles supérieurs. Pour plus de détails sur la politique d'absence aux examens du Département d'informatique, consultez le site web suivant : **http://info.uqam.ca/politiques**

## Intégrité académique

**PLAGIAT Règlement no 18 sur les infractions de nature académique. (extraits)**

**Tout acte de plagiat, fraude, copiage, tricherie ou falsification de document commis par une étudiante, un étudiant, de même que toute participation à ces actes ou tentative de les commettre, à l'occasion d'un examen ou d'un travail faisant l'objet d'une évaluation ou dans toute autre circonstance, constituent une infraction au sens de ce règlement.**

**La liste non limitative des infractions est définie comme suit :**

- **la substitution de personnes;**
- **l'utilisation totale ou partielle du texte d'autrui en la faisant passer pour sien ou sans indication de référence;**
- **la transmission d'un travail pour fins d'évaluatiion alors qu'il constitue essentiellement un travail qui a déjà été transmis pour fins d'évaluation académique à l'Université ou dans une autre institution d'enseignement, sauf avec l'accord préalable de l'enseignante, l'enseignant;**
- **l'obtention par vol, manoeuvre ou corruption de questions ou de réponses d'examen ou de tout autre document ou matériel non autorisés, ou encore d'une évaluation non méritée;**
- **la possession ou l'utilisation, avant ou pendant un examen, de tout document non autorisé;**
- **l'utilisation pendant un examen de la copie d'examen d'une autre personne;**
- **l'obtention de toute aide non autorisée, qu'elle soit collective ou individuelle;**
- **la falsification d'un document, notamment d'un document transmis par l'Université ou d'un document de l'Université transmis ou non à une tierce persone, quelles que aoient les circonstances;**
- **la falsification de données de recherche dans un travail, notamment une thèse, un mémoire, un mémoire-création, un rapport de stage ou un rapport de recherche;**
- **Les sanctions reliées à ces infrations sont précisées à l'article 3 du Règlement no 18.**

Les règlements concernant le plagiat seront strictement appliqués. Pour plus de renseignements, veuillez consulter les sites suivants : **http://www.sciences.uqam.ca/etudiants/integrite-academique.html** et **http://www.bibliotheques.uqam.ca/recherche/plagiat/index.html**

## Médiagraphie

VO R. Villemaire -- *Modélisation et Vérification* -- **2013.** Manuel disponible en ligne. http://www.info2.uqam.ca/~villemaire_r/7570/ModelisationEtVerification/mev.php

VR R. Cavada, A. Cimatti, C. A. Jochim, G. Keighren, E. Olivetti, M. Pistore, M. Roveri, A. Tchaltsev -- *NuSMV 2.5 User Manual, FBK-irst* -- **2010.** http://nusmv.fbk.eu/NuSMV/userman/v25/nusmv.pdf

VR A. Biere, M. Heule, H. Van Maaren, T. Walsh -- *Handbook of Satisfiability (Volume 185 Frontiers in Artificial Intelligence and Applications)* -- **IOS Press, 2009.**

VR D. Kroening, O. Strichman -- *Decision Procedures: An Algorithmic Point of View* -- **Springer, Series: Texts in Theoretical Computer Science. An EATCS Series, 2008.**

VR C. Baier, J-P. Katoen -- *Principles of Model Checking* -- **MIT Press 2008.**

VR D. Jackson -- *Software Abstractions: Logic, Language, and Analysis* -- **The MIT Press, 2006.**

VR R. Dechter -- *Constraint Processing* -- **Morgan Kaufmann, 2003.**

VR E.M. Clarke, O. Grumberg, D.A. Peled -- *Model Checking* -- **MIT Press, 2001.**

VR D.A. Peled -- *Software Reliability Methods* -- **Springer-Verlag, 2001.**

VR H. Kleine Büning, T. Lettmann -- *Propositional Logic: Deduction and Algorithm* -- **Cambridge University Press, 1999.**

VR T. Kropf -- *Introduction to Formal Hardware Verification* -- **Springer-Verlag, 1999.**

VR W. Kunz, D. Stoffel -- *Reasoning in Boolean Networks* -- **Kluwer Academic Publisher, 1997.**

AR Des articles de recherche seront mentionnés durant le cours.

LR -- *NuSMV* http://nusmv.fbk.eu/

UC http://www.info2.uqam.ca/~villemaire_r/7570.html
Site WEB du cours

| | |
|---|---|
| A : article - C : comptes rendus - L : logiciel<br>S: Standard - U : uri - V : volume | C : complémentaire - O : Obligatoire - R : recommandé |