INF7570 – Modélisation et vérification

Plan de cours – Automne 2012

GROUPE

(514) 987-3000

DESCRIPTION

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.

OBJECTIF

- ❏ 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

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%

CONTENU

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.

RÉFÉRENCES

m O R. Villemaire – *Modélisation et Vérification* – **2011.** – **http://www.info2.uqam.ca/~villemaire_r/7570/ModelisationEtVerification.pdf**
Manuel disponible en ligne.

V R 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**

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

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

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

V R D. Jackson – *Software Abstractions: Logic, Language, and Analysis* – **The MIT Press, 2006.**

V R R. Dechter – *Constraint Processing* – **Morgan Kaufmann, 2003.**

V R E.M. Clarke, O. Grumberg, D.A. Peled – *Model Checking* – **MIT Press, 2001.**

V R D.A. Peled – *Software Reliability Methods* – **Springer-Verlag, 2001.**

V R H. Kleine Büning, T. Lettmann – *Propositional Logic: Deduction and Algorithm* – **Cambridge University Press, 1999.**

V R T. Kropf – *Introduction to Formal Hardware Verification* – **Springer-Verlag, 1999.**

V R W. Kunz, D. Stoffel – *Reasoning in Boolean Networks* – **Kluwer Academic Publisher, 1997.**

A R Des articles de recherche seront mentionnés durant le cours.

L R *NuSMV* – **http://nusmv.fbk.eu/**

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

A : article – C : comptes rendus – L : logiciel – N : notes – R : revue – S : standard – U : uri – V : volume

C : complémentaire – O : obligatoire – R : recommandé