3IF2220 - Sémantique et preuve des programmes

Responsables : **Frederic BOULANGER**

Langues d'enseignement : **FRANCAIS**

Campus où le cours est proposé : **CAMPUS DE PARIS - SACLAY**

Nombre d'heures d'études élèves (HEE) : **40**

Nombre d'heures présentielles d'enseignement (HPE) : **21**

Année académique : **2024-2025**

Niveau avancé : **non**

Présentation, objectifs généraux du cours :

La valeur d'un modèle tient au sens qu'il porte et aux outils qu'on peut lui appliquer. Il est primordial que les différents outils interprètent un modèle donné de la même façon. Ce cours présente les techniques sémantiques qui permettent de définir le sens d'un langage, et donc le sens des modèles exprimés dans ce langage. On y verra comment modéliser la syntaxe abstraite d'un langage (en connexion avec le cours de traitement des langages), choisir un domaine sémantique (en général une logique), et comment établir une correspondance entre les éléments syntaxiques et les éléments sémantiques. Les différents styles de sémantiques (opérationnel, dénotationnel, axiomatique) seront présentés, ainsi que les relations de consistance et de complétude relatives. Ce cours s'appuie sur le cours de logique et systèmes déductifs, et suit une approche pragmatique avec une mise en œuvre concrète des concepts et des méthodes dans l'assistant de preuve Isabelle/HOL. 16 heures de travail personnel sont dédiées à la prise en main de l'outil (tutoriel à suivre) et à des exercices. Deux créneaux de 3 heures en présentiel sont consacrés à une pratique encadrée (travaux pratiques) afin d'ancrer les notions abstraites dans leur mise en œuvre concrète sur un cas d'étude. Deux autres créneaux de 3h sont consacrés à la preuve de programmes C avec Frama-C afin de montrer comment les techniques vues dans ce cours s'appliquent dans un contexte industriel.

Période(s) du cours (n° de séquence ou hors séquence) :

SM11

Prérequis :

Cours de logique et systèmes déductifs de la mention Science du logiciel

Plan détaillé du cours (contenu) :

7 créneaux de 3h (21 HPE).

- Créneau 1 : Introduction, initiation à Isabelle/HOL
  - Logique d'ordre supérieur
  - Principes fondamentaux d'Isabelle/HOL
  - Tutoriel sur la définition de types inductifs, de fonctions et les techniques de preuve.
- Créneau 2 : Sémantique opérationnelle (avec exercices sur machine)
  - Syntaxe et sémantique

    - Rappel sur le langage Niklaus
    - Modélisation de la syntaxe abstraite de Niklaus en Isabelle/HOL
    - Choix du domaine sémantique
    - Correspondance syntaxe abstraite <-> domaine sémantique
    - Sémantique des expressions Niklaus
    - Approche fonctionnelle, problème de la terminaison
    - Approche inductive
    - Sémantique à petits pas ou à grands pas
    - Sémantique à grands pas de Niklaus
- Créneau 3 : Sémantique dénotationnelle
    - Problème des définitions récursives
    - Définitions récursives de la factorielle
    - Fonctionnelles et points fixes
    - Application à la sémantique dénotationnelle du while
    - Sémantique dénotationnelle de Niklaus
- Créneau 4 : sémantique axiomatique
    - Triplets de Hoare
    - Validité et dérivabilité
    - Plus faible précondition, notion d'invariant
    - Sémantique axiomatique de Niklaus
    - Preuves de programmes
- Créneau 5 : Finalisation des projets
    - Compléments sur les définitions sémantiques
    - Tactiques de preuve
    - Déblocage sur des problèmes techniques
    - Finalisation des exercices sur la simplification d'expressions arithmétique et sur les expressions régulières
- Créneaux 6 et 7 : bureau d'étude Frama-C (Nikolaï Kosmatov)
    - Preuve de programmes C

Déroulement, organisation du cours :

- Site web présentant le matériel du cours ainsi que des éléments d'initiation et d'approfondissement
- Auto-formation aux outils par un tutoriel afin d'être prêt à suivre les cours
- Cours magistraux pour présenter les concepts
- Cours sur machine pour mettre en œuvre les concepts avec l'assistance d'un enseignant
- Bureaux d'étude avec réalisations concrètes pour mettre en œuvre les concepts et se les approprier

Organisation de l'évaluation :

L'évaluation se fait en contrôle continu sur la qualité des rendus d'exercices (tutoriel, en autres), sur la participation aux bureaux d'étude et sur les rendus finaux.

Moyens :

Les moyens mis en œuvre pour ce cours combinent tutoriels pour se familiariser avec une problématique, cours magistraux pour définir les concepts, cours sur machine pour les mettre en œuvre avec l'assistance d'un enseignant et bureaux d'étude pour une pratique plus autonome. Un travail personnel d'approfondissement du contenu des bureaux d'étude est attendu.

Acquis d'apprentissage visés dans le cours :

À l'issue de ce cours, les élèves seront capables :

- de donner un sens précis et formel à un modèle,
- de choisir l'approche sémantique adaptée au problème à traiter,
- d'établir les bases de la définition de cette sémantique dans un assistant de preuve,
- d'exploiter cette sémantique pour vérifier des propriétés d'un modèle ou d'un programme.

Description des compétences acquises à l'issue du cours :

C1.2 Use and develop appropriate models, choose the right modeling scale to capture the phenomenon, choose the relevant simplifying assumptions
- capture the essential elements of model semantics
- represent them in a manner appropriate to the problem at hand
- build several models at different levels of abstraction and link them together

C2.1 Deeper understanding of a domain in the fundamental or engineering sciences
- master logic as a modeling tool

C5.2 Listen to, understand and be understood by various audiences (training, trades, cultures...) by using the appropriate means of communication.
- analyse with rigour the different meanings that a model can have, define the logical model that corresponds to what the users think.

C7.1 Convice about what matters. Be clear about the objectives and the expected results. Structure ideas and arguments
- clear up things thanks to formal logics
- avoid monolithic models, structure the different levels of abstraction.
- be explicit about the compromise between expressivity and solving capabilities

Bibliographie :

https://wdi.centralesupelec.fr/semantique/