

Semestre 1, Master Informatique spécialité RIF

Description des Cours

Programmes des cours d'introduction

Semestre 2

Complexité

Responsables : Emmanuel Kounalis (PR, UNS)

Intervenant(s) :

Programme pédagogique :

Ce cours est une introduction à la théorie de la complexité. Nous aborderons les points suivants :

- Les problèmes comme langages formels
- Classes de complexités (P, NP, Co-NP..)
- La NP-complétude

Cryptographie et sécurité

Responsable : Bruno MARTIN

Programme pédagogique :

Cet enseignement de première année de master informatique constitue une introduction à la cryptographie et à la sécurité. L'objectif principal est de comprendre l'utilisation et le fonctionnement des outils qui permettent d'assurer la sécurité d'un ensemble de services à l'intérieur d'un réseau local.

Nous présentons différents aspects de la sécurité informatique (menaces et contre-mesures). Nous introduisons brièvement la cryptographie à clé secrète, la cryptographie à clé publique et les différents mécanismes qui permettent d'assurer la confidentialité, l'intégrité et la disponibilité des services qu'on souhaite protéger face aux risques identifiés. Nous montrons comment on peut combiner ces différents mécanismes de sécurité pour réaliser des services de sécurité qui sont utilisés dans les protocoles sécurisés comme https ou ssh. Nous montrons le rôle d'une politique de sécurité et comment on peut la réaliser (sécurisation de quelques services cruciaux comme le web ou le mail, réalisation d'un coupe-feu sur une passerelle).

Cet enseignement constitue une bonne introduction aux cours "cryptographie et sécurité", "sécurité des réseaux", et "vérification et sécurité" qui sont dispensés en seconde année du master et qui approfondissent les notions introduites dans ce cours.

Vérification de Programmes et Preuve sur Ordinateur

Responsable : Yves Bertot

Programme pédagogique :

Ce cours illustre la vérification formelle de programmes et d'algorithmes récursifs en se concentrant sur une approche pratique de l'utilisation du système de preuve Coq. Il s'agit dans un premier temps d'apprendre à programmer dans un style fonctionnel, typé, et reposant sur des "types inductifs" pour définir de nouvelles structures de données. Dans un deuxième temps, il s'agit d'apprendre à raisonner sur ces programmes, en couvrant tous les cas prévus par les structures de données et en utilisant la récurrence pour prendre en compte les ensembles de données infinis. Les concepts abordés contiendront: la définition de fonctions, les constructions de filtrage et le traitement par cas, les formules logiques de premier ordre et d'ordre supérieur, la preuve dirigée par les buts, les tactiques de raisonnement sur les connecteurs logiques et sur les programmes, les types inductifs et les types dépendants.

Optimisation Discrète Combinatoire

Responsable : Jean-Charles Régim (UNS)

Programme pédagogique :

Le cours présentera certaines des méthodes les plus connues pour résoudre les problèmes d'optimisation combinatoire discrète.

On insistera sur le caractère complet ou incomplet de la méthode utilisée, mais aussi sur le côté exact et inexact des méthodes.

Les méthodes heuristiques et les métaheuristiques seront abordées. On peut notamment citer le recuit-simulé, la recherche tabou, les colonies de fourmis, les algorithmes évolutionnistes. Des méthodes complètes à vocation générale, comme la programmation linéaire en nombres entiers, ou plus spécifiques, comme la résolution de cliques maximum ou le coloriage de graphes, seront également étudiées.

Logique et calcul

Responsable : Grégory Lafitte (MC, Univ. Provence)

Programme pédagogique :

Le cours porte sur les notions introduites pour l'étude du phénomène d'incomplétude de Gödel. Nous commencerons par rappeler les résultats classiques de la théorie de la calculabilité. Nous introduirons ensuite les notions de logiques (langages, logiques, théories, modèles, ...).

Divers théories liées à la calculabilité (Robinson (Q), Peano Arithmetic (PA), Primitive Recursive Arithmetic (PRA), ...) seront introduites.

Ensuite, nous introduirons les notions élémentaires de la théorie des ensembles (le type ensemble, les ordinaux, le système Zermelo-Fraenkel (ZF), l'axiome du choix (C), les cardinaux et les modèles de ZFC).

Nous montrerons les théorèmes d'incomplétude de Gödel aussi bien du point de vue de la logique que de celui de la calculabilité et nous introduirons la notion de forcing pour pouvoir montrer des résultats d'indépendance.

Enfin, nous introduirons les notions nécessaires à la compréhension de résultats récents sur des problèmes indépendants de théories au delà de PA.

Logique Linéaire

Responsable : André Hirschowitz (PR, UNS)

Programme pédagogique :

La logique linéaire, son rapport avec les jeux, son rapport avec les autres logiques, ses preuves et ses modèles.

Analyse d'images

Responsable : Georges Drettakis (DR, INRIA) et Josiane Zérubia (DR, INRIA)

Programme pédagogique :

- Introduction aux champs de Markov : définitions, quelques modèles classiques, simulation des champs de Gibbs et méthodes MCMC.
- Processus ponctuels marqués : définitions, ppm pour la détection d'objets, simulation des ppm et méthode MCMC à sauts réversibles.
- Approche variationnelle : fonctionnelles de restauration et de segmentation d'image, calcul des variations, espace des fonctions à Variations Bornées, régularisation, algorithmes de minimisation, filtrage d'image par EDP non linéaires.
- Théorie des graphes : définitions, quelques méthodes classiques pour l'analyse d'image.

- Éclairage, ré-éclairage et perception
- Son 3D
- Textures et techniques procédurales
- Mini-projets

Imagerie médicale

Responsable : Xavier Pennec (DR, INRIA)

Programme pédagogique :

1. Introduction aux images médicales et à leur acquisition
2. Introduction au traitement des images médicales
3. Recalage rigide et non rigide
4. Introduction aux variétés Riemanniennes et groupes de Lie
5. Statistiques sur des variétés Riemanniennes
6. Imagerie du tenseur de diffusion
7. EDPs sur des images à valeur dans une variété
8. Anatomie algorithmique (variabilité du cerveau)
9. Les problèmes posés par des groupes de dimension infinie

Pavages et calcul

Responsables : Nicolas Ollinger (PR, Univ. D'Orléans)

Programme pédagogique :

Ce cours a pour objectif de présenter la théorie des pavages du plan discret et plus particulièrement son approche sous l'angle du calcul. Après une rapide présentation des définitions et outils topologiques sur les jeux de tuiles et pavages du plan complet, fini et périodique, le corps du cours se concentre sur l'apériodicité et les résultats d'indécidabilité associés (Berger 1964 et suivants). Après avoir discuté ces problèmes et leurs applications en dehors du cadre des pavages, nous poursuivons la description de la structure des pavages en construisant des pavages de complexité maximale en introduisant les résultats fondamentaux de la complexité de Kolmogorov.

Sémantique (des langages de programmation)

Responsable : Yves Bertot (DR, INRIA)

Programme pédagogique :

Le but de ce cours est d'apprendre à démontrer la correction d'outils de manipulation de programmes.

Trois outils sont visés: un outil de génération de conditions, un outil d'analyse statique, et un interprète. L'ensemble est décrit de manière à permettre une vérification par ordinateur et la génération automatique des outils à partir des spécifications et des preuves.

Unité 1 : description du langage de programmation, sémantique naturelle +sémantique à petit pas

Unité 2 : preuves par récurrence sur les dérivations, exemple sur l'équivalence entre sémantique naturelle et la sémantique à petits pas

Unité 3 : introduction orale à Coq, description en Coq des spécifications sémantiques, techniques de raisonnement par récurrence et inversion, encodage de la preuve d'équivalence.

Unité 4 : démonstration sur machine en Coq: preuve de correction d'une transformation de programmes

Unité 5 : introduction à la sémantique axiomatique, preuve de correction de la sémantique axiomatique (oralement en Coq).

Unité 6 : preuve de correction d'un générateur de conditions de vérification (décrit en Coq).

Unité 7 : introduction à l'interprétation abstraite: cas des intervalles (description de la preuve de correction)

Unité 8 : description formelle d'un interprète concret et vérification de sa correction vis-à-vis de la sémantique naturelle.

Anglais Scientifique

Responsable : Nuria Serrano

Programme pédagogique :

L'objectif de ce cours est d'amener les étudiants à s'exprimer clairement en anglais sur des sujets relatifs aux sciences en général, et à l'informatique en particulier, aussi bien à l'oral qu'à l'écrit.

Les étudiants assisteront à des séminaires d'informatique (Colloquium Morgenstern). Ils devront ensuite expliquer en anglais, à l'oral, de façon simple et concise le contenu des séminaires. Les étudiants devront également choisir un article scientifique en anglais, toujours dans le domaine de l'informatique et faire une présentation orale en anglais pour exposer l'article devant l'ensemble de la classe. Finalement des exercices de rédaction scientifique en anglais, comme par exemple la rédaction d'un résumé d'article, seront proposés. Certains points précis de grammaire ainsi que le vocabulaire nécessaire à une expression scientifique claire seront également abordés.