CS719: Topics in Mathematical Foundations of Formal Verification

- Offering: Autumn Semester 2010
- Instructor: Supratik Chakraborty
  - Office: CFDVS (basement of Mathematics Dept)
  - Email: supratik@cse.iitb.ac.in
- TA: Rahul Srinivasan
  - Email: rahulsrini@cse.iitb.ac.in
- Course web page:
  - http://www.cse.iitb.ac.in/~supratik/courses/cs719
- Moodle: http://moodle.iitb.ac.in

CS719: Overview

- Formal Verification and Reasoning:
  - Reasoning about behaviour of systems in mathematically precise and rigorous manner
  - Allows **proving** properties of systems, as opposed to demonstrating properties on some input cases
  - Based on several sub-disciplines of mathematics and computer science
- This course aims at covering (some of) the mathematical background to facilitate advanced studies and projects in formal verification & related areas.

CS719: Under the hood

- High-level topics intended to be covered
  - First order logic (FOL) and some of its intricacies
    - FOL as a description language for interesting structures that arise in Computer Science
    - Completeness, Compactness, Interpolation, Definability and other key results in FOL
    - Decision procedures for useful fragments of FOL
    - Connections with Model Theory (depending on time)

CS719: Under the hood

- High level topics intended to be covered
  - Lattices and partial orders
    - Basics, homomorphisms, ideals & filters
    - Interesting results and partial ordered sets
    - Boolean and distributive lattices
    - Complete lattices and Galois connections, fixpoint theorems
    - Well quasi orders and applications (depending on time)

CS719: Under the hood

- Process algebras and transition systems
  - Basic process theory and transition systems
  - Simulation and preorder relations
  - Specialized automata and transition systems (depending on time)

Prerequisites

- Basic familiarity with propositional logic and some familiarity with first order logic
- Undergraduate level course on discrete structures
- Interest in mathematical reasoning and symbolic reasoning in particular
- Willingness to read beyond what is taught in class to understand a topic better

References

- Shawn Hedman, A First Course in Logic, Oxford University Press, 2006
- Peter B. Andrews, An Introduction to Mathematical Logic and Type Theory: To Truth Through Proof, 2nd edition, Springer, 2002
- B. A. Davey and H. A. Priestley, Introduction to Lattices and Orders, Second edition, Cambridge University Press, 2001
- D. Kroening and O. Strichman, Decision Procedures: An Algorithmic Point of View, Springer, 2008
- J.C.M. Baeten and W.P. Wiejland, Process Algebra, Cambridge Tracts in Theoretical Computer Science, Cambridge University Press, 1990
- Papers etc to be provided in class