CMPT 477 - D100 Introduction to Formal Verification

Instructor(s): Eugenia Ternovska

Calendar Objective/Description:
Introduces, at an accessible level, a formal framework for symbolic model checking, one of the most important verification methods. The techniques are illustrated with examples of verification of reactive systems and communication protocols. Students learn to work with a model checking tool.

Instructor’s Objectives:
(Please note that this course is cross-listed with CMPT 777) Real software systems are extremely complex. In the software industry, formal verification methods are increasingly used to verify that a model of a software system satisfies the requirements. The course concentrates on contemporary applications of logic to the verification of software systems. The objective is to introduce, at an accessible level, a mathematical framework for symbolic model checking, one of the most important verification methods. The techniques are illustrated with examples of verification of reactive systems and communication protocols. Students learn to work with the model checking tool SMV.

Prerequisites:
CMPT 275 or 276.

Topics:
- Model checking as a verification technique
- Model checking with Computational Tree Logic (CTL)
- Representing practically relevant specifications in CTL
- The NuSMV (`symbolic model verifier`) system
- Alternatives and extensions of CTL
- Model checking with fairness
- Efficient representation of boolean functions - binary decision diagrams
- Use of binary decision diagrams in symbolic model checking
- Model checking for the relational mu-calculus

Grading:
To be discussed the first week of classes

Required Books:

Reference Books:


Academic Honesty Statement::

Academic honesty plays a key role in our efforts to maintain a high standard of academic excellence and integrity. Students are advised that ALL acts of intellectual dishonesty will be handled in accordance with the SFU Academic Honesty and Student Conduct Policies (http://www.sfu.ca/policies/gazette/student.html).