CS 745 / ECE 725 Computer Aided Verification

Instructor: Richard Trefler
trefler@cs.uwaterloo.ca
DC 2336

Lectures: T & Th, 1:00 - 2:20pm, dc 2585

First Meeting: Sept. 5th

Computer hardware, software, embedded systems, and protocols play important roles in many ubiquitous computational systems: from computer operating systems to medical devices, from banking systems to communication protocols, from transportation control systems to telephony software --- these reactive systems are highly utilized and they are expected to operate reliably and robustly.

At the same time, designing and maintaining even a modestly sized system that operates in a manner that satisfies the system's basic specifications and requirements has significant challenges. Examples of systems suffering significant and evening devastating errors and bugs are wide spread.

Model checkers, and other automated and semi-automated program analysis engines, afford significant opportunities to increase the assurance that complex systems and protocols operate, substantially, as they were intended by their designers.

In this course we study the basic elements and challenges of fully-automated and semi-automated computer aided program analysis techniques.

This includes: specification languages to describe important aspects of system behavior; modeling techniques used to describe the behavior of reactive systems; and analysis techniques designed to show that systems behave as intended, or, if they do not behave as intended, then the analysis shows precisely how system behavior violates a specification.

Specific topics of study include: logic based specifications and notations; reactive system descriptions; semantics of reactive systems; fully automated and semi-automated system analysis techniques; compositional reasoning techniques; abstraction techniques; symmetry reduction; and analysis of parametrized systems.

Course text book:
Text book: Model Checking
Edmund M. Clarke, Orna Grumberg, Daniel Kroening, Doron Peled and Helmut Veith
MIT Press, 2018,

Grade:
Assignments: 35%
Presentation: 35% (based on papers selected from the literature)
Class Participation: 30%