CS 745 Computer Aided Verification

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

Lectures: T & Th, 1:00 – 2:20pm, dc 2568

First Meeting: Sept. 7th

Computer hardware, software, embedded systems, and protocols play important roles in several, ubiquitous systems: from computer operating systems to medical devices, from banking systems to communication protocols, from transportation control systems to telephony software, these 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 widespread.

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

In this course we study the basic elements of fully-automated and semi-automated computer aided analysis techniques as they apply to computer hardware, software and embedded systems and protocols.

We study specification languages to describe important aspects of system behavior, modelling 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 system specifications.
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 parametrized system analysis.

Course text book:

Text book: Model Checking
Edmund M. Clarke, Orna Grumberg, Doron Peled

Grade:

Assignments: 50%
Presentation: 25% (based on papers selected from the literature)
Class Participation: 25%