ECE 750-T28:
Computer-aided Reasoning for Software Engineering

Computer-aided reasoning tools, such as SAT/SMT solvers, have had a dramatic impact on software engineering and security in recent years. So much so that a very large number of software engineering tools these days are designed primarily using a SAT or SMT solver backend. The primary reason for this recent adoption of solvers in software engineering is the continued improvement in performance and expressive power of these solvers. Given both the foundational importance of computer-aided reasoning and their impact, it is important for any student wanting to do research in software engineering and/or security to have a thorough understanding of this topic.

In this course, we will cover the theory and practice of automated reasoning tools such as conflict-driven clause learning SAT solvers, SMT solvers, model-checkers, and theorem provers. We will also cover applications of automated reasoning tools in diverse areas such as automatic bug finding (e.g., concolic testing), symbolic execution, program analysis and synthesis, programming languages and formal methods.

The course will have 3 modules:

1. Mathematical logic and complexity theory basics
2. SAT/SMT solver and higher-order prover internals
3. Solver-based applications in testing, program analysis and formal verification

For a previous edition of the course please visit the following website:

https://ece.uwaterloo.ca/~vganesh/TEACHING/F2013/SATSMT/index.html