SAT/SMT Solvers for Software Engineering and Security

Instructor Bio and Course Outline

by

Vijay Ganesh

Assistant Professor, University of Waterloo, Canada.

Date: April 4-8, 2016

Venue: Moscow State University, Russia.

Brief Bio of Vijay Ganesh

- Studied mathematical logic and formal methods at Stanford, USA (PhD in computer science, 2007)
- Scientist at the Massachusetts Institute of Technology, USA (2007-2012)
- Assistant professor at the University of Waterloo, Canada (2012 – present)
- Research focus
  - Solvers and proof assistants for software engineering, security, and mathematics
  - Logic and complexity-theoretic questions that arise in software engineering
  - Foundations of mathematics

Key Contributions

Name	Key Concept	Impact	Pubs
STP Bit-vector & Array Solver[1,2]	Abstraction-refinement for solving	Concolic Testing	CAV 2007 CCS 2006 TISSEC 2008
HAMPI String Solver[1]	App-driven bounding for solving	Analysis of Web Apps	ISSTA 2009[3] TOSEM 2012 CAV 2011
Z3-str String and Numeric Solver[1]	Novel techniques for string + integer combination	Analysis of Web Apps	FSE 2013 CAV 2015[3]
Maple Series of SAT Solvers, and understanding SAT	Branching heuristics, and community structure	One of the fastest SAT solvers to-date	AAAI 2016 HVC 2015, SAT 2014[3]
MathCheck Conjecture Verifier	CAS+SAT combination	Finitely verified math conjectures	CADE 2015[3]
Taint-based Fuzzing	Data flow is cheaper than concolic	Scales better than concolic	ICSE 2009
Automatic Input Rectification	Automatic security envelope	New security approach	ICSE 2012
Undecidability results for theories over strings	New reductions	Solved open problems	HVC 2012

1. 100+ research projects use STP, HAMPI, and Z3str2. IBM Faculty Award 2015, Google Faculty Research Awards 2011/2013
2. STP won the SMTCOMP 2006/2010 and second in 2011/2014 competitions for bit-vector solvers
3. Won 7 best paper awards/honors at various conferences including SAT, DATE, SPLC, CAV, and CADE
4. Retargetable Compiler (DATE 1999, 2008). Ten Year Most-influential paper award at DATE 2008.

Current Projects

1. Understanding why conflict-driven clause-learning SAT solvers are so efficient
2. Theory and practice of solvers over strings, integers, and bit-vectors
3. MathCheck: SAT+CAS combination to verify math conjectures
4. Applications of SAT solvers to security
5. Formal verification of physics software
6. Attack-resistance

Syllabus

Lecture	Date	Contents
1	Apr 4th, 2016	Brief introduction to logic in software engineering and security. Introduction to SAT/SMT solvers and their applications, in particular, symbolic-execution based analysis and testing
2	Apr 5th, 2016	Internals of SAT Solvers
3	Apr 7th, 2016	Internals of SAT Solvers (continued)
4	Apr 8th, 2016	Internals of SAT Solvers (continued)
5	TBD	Introduction to first-order theories, and SMT solvers. DPLL(T) and combination of theories
6	TBD	Bit-vector and array solvers. Counter-example guided abstraction-refinement (CEGAR)
7	TBD	Solvers for theories over string equations (practice)
8	TBD	Solvers for theories over string equations (theory)

Course Requirements

- Attendance
- Final exam and tests
- Projects, if interested
- Grading to be determined by MSU faculty