EXERCISE #32

BOOLEAN SATISFIABILITY REVIEW

Write your name and answer the following on a piece of paper

Apply DPLL to determine if there is a satisfying assignment to the following Boolean formula

$$(a \vee b) \wedge (a \vee c) \wedge (\neg b \vee \neg c) \wedge (\neg d \vee \neg c) \wedge (\neg d \vee \neg b) \wedge (c)$$

EXERCISE #32 SOLUTION

BOOLEAN SATISFIABILITY REVIEW

Write your name and answer the following on a piece of paper

Apply DPLL to determine if there is a satisfying assignment to the following Boolean formula

$$(a \lor b) \land (a \lor c) \land (\neg b \lor \neg c) \land (\neg d \lor \neg c) \land (\neg d \lor \neg b) \land (c)$$

ADMINISTRIVIA AND ANNOUNCEMENTS

SMT SOLVING

EECS 677: Software Security Evaluation

Drew Davidson

PREVIOUSLY : SATISFIABILITY

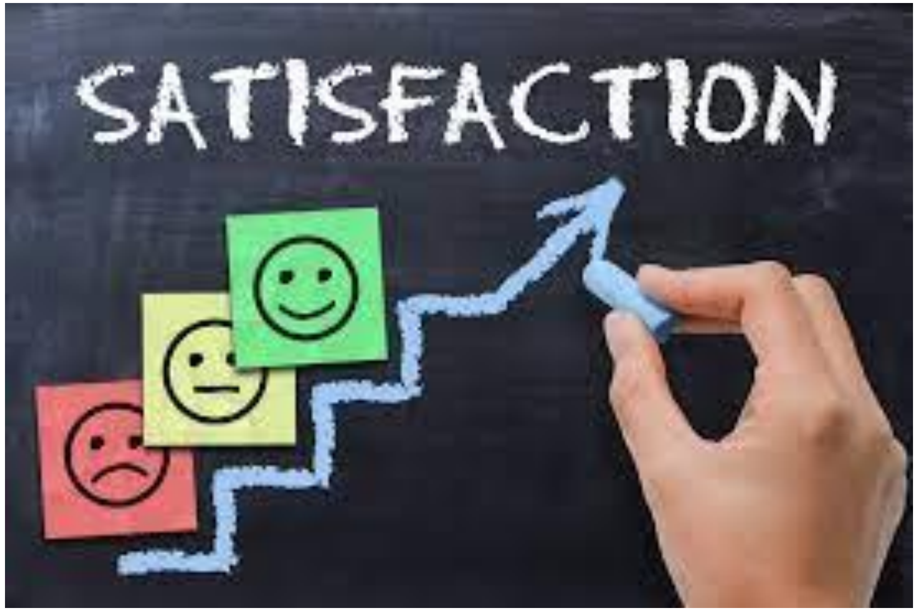
OUTLINE / OVERVIEW

THE MAGIC THAT MADE SYMBOLIC EXECUTION WORK WAS THE SOLVER

A COMPUTATIONALLY HARD PROBLEM

Famously NP-complete (the progenitor of that complexity class!)

Obvious exponential loose upper bound (brute force)



THIS LECTURE

SMT SOLVING

SATISFIABILITY BEYOND SIMPLE BOOLEAN EXPRESSIONS

Gets us (closer) to the real programs that we want to analyze

KEY PRINCIPLES

Formulating constraints modularize a concern to a theory

Considering individual theory solvers

THEORY SOLVERS

SMT SOLVING

Some example theories

Theory of linear integer arithmetic

Theory of bitvectors

Theory of arrays

Theory of strings

Theory of equality on uninterpreted (mathematical) functions

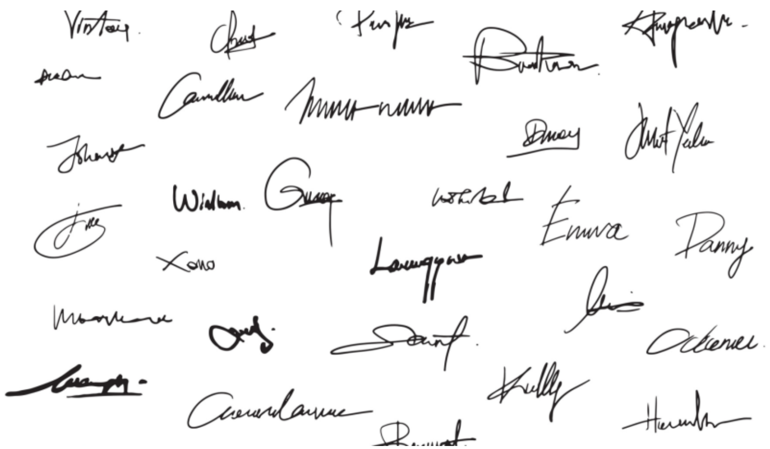
Often possible (+ convenient / necessary) to abstract away the actual behavior of a function

THEORY SIGNATURES

SMT SOLVING

The set of (non-logical) symbols and their meanings defined by that theory

Example: Theory of linear integer arithmetic:
(integer constants, literals, $+, -, \times, \div, \leq, \geq, <, >, =$)



HOW TO (NOT) USE THEORIES

SMT SOLVING

Shortcuts: The name of the game

We'd really like to **not** invoke the theory solvers as much as possible, and we really want theories to **not** intermingle

To this end, we'll try to get our formula (i.e. path constraint) to separate concerns into theories

DPLL(T)

SMT SOLVING

"Strategize" about which constraints to solve using DPLL

- Abstract non-logical clauses
- Reason about a set of "sufficient" set of sub-formulae to satisfy

Note: still need to run the theory solvers to discard contradiction in the theories

Example

p1 p2 p3 p4

$x \geq 0 \land y = x + 1 \land (y > 2 \lor y < 1)$

Abstract all non-logical clauses

$p1 \land p2 \land (p3 \lor p4)$

DPLL

p1:true $x \geq 0$
p2:true $y = x + 1$
p3:false ~~$y < 2$~~
p4: true $y < 1$

Linear Solver: contradiction!

Add information and start over

$p1 \land p2 \land (p3 \lor p4) \land (\neg p1 \lor \neg p2 \lor \neg p3)$

SEPARATING CONCERNS

SMT SOLVING

Occasionally a clause will mix multiple theories.

That's bad! It means that none of the solvers can apply

Goal: break down the constraint system to match our core (logical) theory at the top level, with individual clauses potentially in our theory signatures

Logical symbols
– Parentheses: (,)
– Propositional connectives: ∨, ∧, ¬, →, ↔
– Variables: v1, v2, . . .
– ~~Quantifiers: ∀, ∃~~

Non-logical symbols
– Equality: =
– Functions: +, -, %, bit-wise &, f(), concat, ...
– Predicates: ·, is_substring, ...
– Constant symbols: 0, 1.0, null`

NELSON-OPPEN

SMT SOLVING

A METHOD FOR WORKING ACROSS THEORIES

Big idea:

Put the formula into *separated form* (each clause belongs entirely in a theory signature)

Apply axioms of the theory to create new clauses

Communicate information between theories across equality

EXAMPLE

SMT SOLVING

$f(f(x) - f(y)) = a$

$\wedge$

$f(0) = a + 2$

$\wedge$

$x = y$

Signature of linear integer arithmetic:

- integer constants, literals
- $+, -, \times, \div, \leq, \geq, <, >, =$

Signature of EUF

- The predicate =
- All literal and function symbols

Credit: this example due to Oliveras and Rodriguez-Carbonell, additional work by Aldrich

EXAMPLE

SMT SOLVING

Basic idea: replace operations with fresh propositional variables and add the operation as a new constraint on the abstract variable

$f(f(x) - f(y)) = a$
$\wedge$
$f(0) = a + 2$
$\wedge$
$x = y$

$f(e_1) = a$
$\wedge$
$e_1 = f(x) - f(y)$
$\wedge$
$f(0) = a + 2$
$\wedge$
$x = y$

$f(e_1) = a$
$\wedge$
$e_1 = e_2 - e_3$
$\wedge$
$e_2 = f(x)$
$\wedge$
$e_3 = f(y)$
$\wedge$
$f(0) = a + 2$
$\wedge$
$x = y$

EXAMPLE

SMT SOLVING

$f(e_1) = a$
$\wedge$
$e_1 = e_2 - e_3$
$\wedge$
$e_2 = f(x)$
$\wedge$
$e_3 = f(y)$
$\wedge$
$f(0) = a + 2$
$\wedge$
$x = y$

$f(e_1) = a$
$\wedge$
$e_1 = e_2 - e_3$
$\wedge$
$e_2 = f(x)$
$\wedge$
$e_3 = f(y)$
$\wedge$
$f(e_4) = a + 2$
$\wedge$
$e_4 = 0$
$\wedge$
$x = y$

$f(e_1) = a$
$\wedge$
$e_1 = e_2 - e_3$
$\wedge$
$e_2 = f(x)$
$\wedge$
$e_3 = f(y)$
$\wedge$
$f(e_4) = e_5$
$\wedge$
$e_4 = 0$
$\wedge$
$e_5 = a + 2$
$\wedge$
$x = y$

EXAMPLE

SMT SOLVING

$f(e_1) = a$	Theory of EUF
$\land$	
$e_1 = e_2 - e_3$	Theory of integer arithmetic
$\land$	
$e_2 = f(x)$	Theory of EUF
$\land$	
$e_3 = f(y)$	Theory of EUF
$\land$	
$f(e_4) = e_5$	Theory of EUF
$\land$	
$e_4 = 0$	Theory of integer arithmetic
$\land$	
$e_5 = a + 2$	Theory of integer arithmetic
$\land$	
$x = y$	Theory of EUF AND Theory of integer arithmetic

EXAMPLE

SMT SOLVING

$f(e_1) = a$

$\land$

$e_1 = e_2 - e_3$

$\land$

$e_2 = f(x)$

$\land$

$e_3 = f(y)$

$\land$

$f(e_4) = e_5$

$\land$

$e_4 = 0$

$\land$

$e_5 = a + 2$

$\land$

$x = y$

$\land$

$f(x) = f(y)$

Some EUF Axioms

Congruence:

$x = y \Rightarrow f(x) = f(y)$

Symmetry

$x = y \Rightarrow y = x$

Transitivity:

$x = y \land y = z \Rightarrow x = z$

...

EXAMPLE

SMT SOLVING

$f\ (e_1) = a$

$\wedge$

$e_1 = e_2 - e_3$

$\wedge$

$e_2 = f(x)$

$\wedge$

$e_3 = f(y)$

$\wedge$

$f\ (e_4) = e_5$

$\wedge$

$e_4 = 0$

$\wedge$

$e_5 = a + 2$

$\wedge$

$x = y$

$\wedge$

$f(x) = f(y)$

$\wedge$

$e_2 = e_3$

Some EUF Axioms

Congruence:

$x = y \Rightarrow f(x) = f(y)$

Symmetry

$x = y \Rightarrow y = x$

Transitivity:

$x = y \wedge y = z \Rightarrow x = z$

...

EXAMPLE

SMT SOLVING

$f(e_1) = a$
$\wedge$
$e_1 = e_2 - e_3$
$\wedge$
$e_2 = f(x)$
$\wedge$
$e_3 = f(y)$
$\wedge$
$f(e_4) = e_5$
$\wedge$
$e_4 = 0$
$\wedge$
$e_5 = a + 2$
$\wedge$
$x = y$
$\wedge$
$f(x) = f(y)$
$\wedge$
$e_2 = e_3$

$\wedge$
$e_2 - e_3 = 0$

Some EUF Axioms

Congruence:

$x = y \Rightarrow f(x) = f(y)$

Symmetry

$x = y \Rightarrow y = x$

Transitivity:

$x = y \wedge y = z \Rightarrow x = z$

…

EXAMPLE

SMT SOLVING

$f(e_1) = a$
$\land$
$e_1 = e_2 - e_3$
$\land$
$e_2 = f(x)$
$\land$
$e_3 = f(y)$
$\land$
$f(e_4) = e_5$
$\land$
$e_4 = 0$
$\land$
$e_5 = a + 2$
$\land$
$x = y$
$\land$
$f(x) = f(y)$
$\land$
$e_2 = e_3$

$\land$
$e_2 - e_3 = 0$
$\land$
$e_1 = 0$

Some EUF Axioms

Congruence:

$x = y \Rightarrow f(x) = f(y)$

Symmetry

$x = y \Rightarrow y = x$

Transitivity:

$x = y \land y = z \Rightarrow x = z$

…

EXAMPLE

SMT SOLVING

$f(e_1) = a$
$\land$
$e_1 = e_2 - e_3$
$\land$
$e_2 = f(x)$
$\land$
$e_3 = f(y)$
$\land$
$f(e_4) = e_5$
$\land$
$e_4 = 0$
$\land$
$e_5 = a + 2$
$\land$
$x = y$
$\land$
$f(x) = f(y)$
$\land$
$e_2 = e_3$
$\land$
$e_2 - e_3 = 0$
$\land$
$e_1 = 0$
$\land$
$e_1 = e_4$

Some EUF Axioms

Congruence:

$x = y \Rightarrow f(x) = f(y)$

Symmetry

$x = y \Rightarrow y = x$

Transitivity:

$x = y \land y = z \Rightarrow x = z$

...

EXAMPLE

SMT SOLVING

$f(e_1) = a$
$\land$
$e_1 = e_2 - e_3$
$\land$
$e_2 = f(x)$
$\land$
$e_3 = f(y)$
$\land$
$f(e_4) = e_5$
$\land$
$e_4 = 0$
$\land$
$e_5 = a + 2$
$\land$
$x = y$
$\land$
$f(x) = f(y)$
$\land$
$e_2 = e_3$
$\land$
$e_2 - e_3 = 0$
$\land$
$e_1 = 0$
$\land$
$e_1 = e_4$
$\land$
$f(0) = a$

Some EUF Axioms

Congruence:

$x = y \Rightarrow f(x) = f(y)$

Symmetry

$x = y \Rightarrow y = x$

Transitivity:

$x = y \land y = z \Rightarrow x = z$

…

EXAMPLE

SMT SOLVING

$f(e_1) = a$
$\wedge$
$e_1 = e_2 - e_3$
$\wedge$
$e_2 = f(x)$
$\wedge$
$e_3 = f(y)$
$\wedge$
$f(e_4) = e_5$
$\wedge$
$e_4 = 0$
$\wedge$
$e_5 = a + 2$
$\wedge$
$x = y$
$\wedge$
$f(x) = f(y)$
$\wedge$
$e_2 = e_3$

$\wedge$
$e_2 - e_3 = 0$
$\wedge$
$e_1 = 0$
$\wedge$
$e_1 = e_4$
$\wedge$
$f(0) = a$
$\wedge$
$f(0) = e_5$

Some EUF Axioms

Congruence:

$x = y \Rightarrow f(x) = f(y)$

Symmetry

$x = y \Rightarrow y = x$

Transitivity:

$x = y \wedge y = z \Rightarrow x = z$

…

EXAMPLE

SMT SOLVING

$f(e_1) = a$
∧
$e_1 = e_2 - e_3$
∧
$e_2 = f(x)$
∧
$e_3 = f(y)$
∧
$f(e_4) = e_5$
∧
$e_4 = 0$
∧
$e_5 = a + 2$
∧
$x = y$
∧
$f(x) = f(y)$
∧
$e_2 = e_3$
∧
$e_2 - e_3 = 0$
∧
$e_1 = 0$
∧
$e_1 = e_4$
∧
$f(0) = a$
∧
$f(0) = e_5$
∧
$e_5 = a$

Arithmetic Contradiction

Some EUF Axioms

Congruence:

$x = y \Rightarrow f(x) = f(y)$

Symmetry

$x = y \Rightarrow y = x$

Transitivity:

$x = y \land y = z \Rightarrow x = z$

...

"CONVENIENT" EQUALITIES

SMT SOLVING

$f(e_1) = a$
∧
$e_1 = e_2 - e_3$
∧
$e_2 = f(x)$
∧
$e_3 = f(y)$
∧
$f(e_4) = e_5$
∧
$e_4 = 0$
∧
$e_5 = a + 2$
∧
$x = y$
∧
$f(x) = f(y)$
∧
$e_2 = e_3$

∧
$e_2 - e_3 = 0$
∧
$e_1 = 0$
∧
$e_1 = e_4$
∧
$f(0) = a$
∧
$f(0) = e_5$
∧
$e_5 = a$

The lynchpin of our success was the existence of some useful equalities. What if they aren't in the original constraints?

Case split!

Can add logical predicates for all possible equalities...

$(e_1 = e_2 \lor e_1 \neq e_2)$
∧
$(e2 = e3 \lor e2 \neq e3)$
∧
$(e1 = e3 \lor e1 \neq e3)$
∧
...

and start making guesses

ARITHMETIC CONSTRAINTS

SMT SOLVING

We kinda danced around how the arithmetic solver works

Basic answer: Linear Algebra.

Also, something something Linear Optimization and the simplex algorithm

WRAP-UP

SMT SOLVERS

Hopefully I've convinced you that Solvers can be implemented

Not strictly magic, but they do employ some very clever techniques