EXERCISE #32

BOOLEAN SATISFIABILITY REVIEW

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

Apply the pure literal elimination technique to the following Boolean expression until no pure literals remain

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

ADMINISTRIVIA AND ANNOUNCEMENTS

Quiz 3

In-class Friday

SMT SOLVING

EEC 677: Software Security Evaluation

Drew Davidson

WHERE WE’RE AT

TOOLS / TECHNIQUES UNDERLYING SYMBOLIC EXECUTION

PREVIOUSLY : SATISFIABILITY

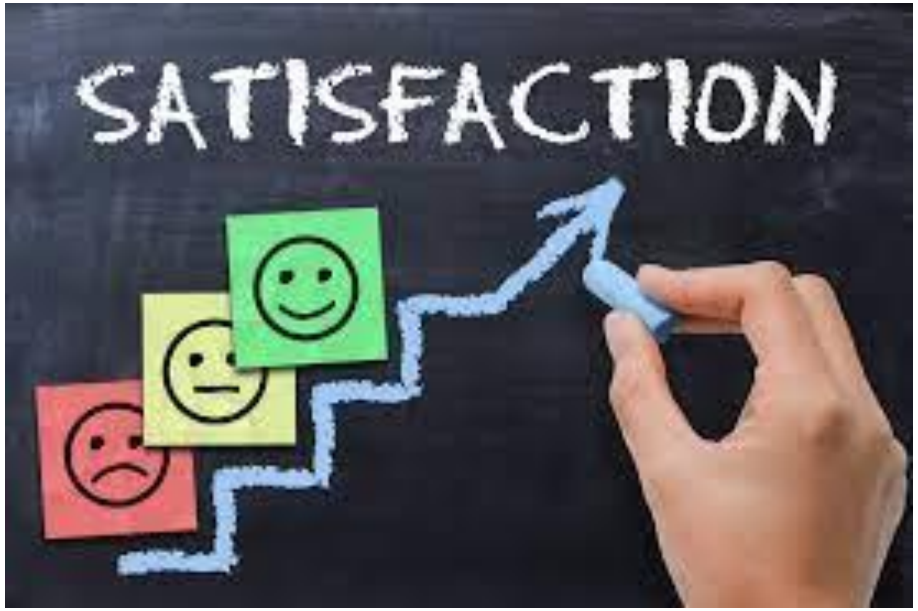
OUTLINE / OVERVIEW

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

Individual theory solvers

Formulating constraints modularize a concern to a theory

THEORY SOLVERS

SMT SOLVING

SOME EXAMPLE THEORIES

Theory of linear integer arithmetic

Theory of bitvectors

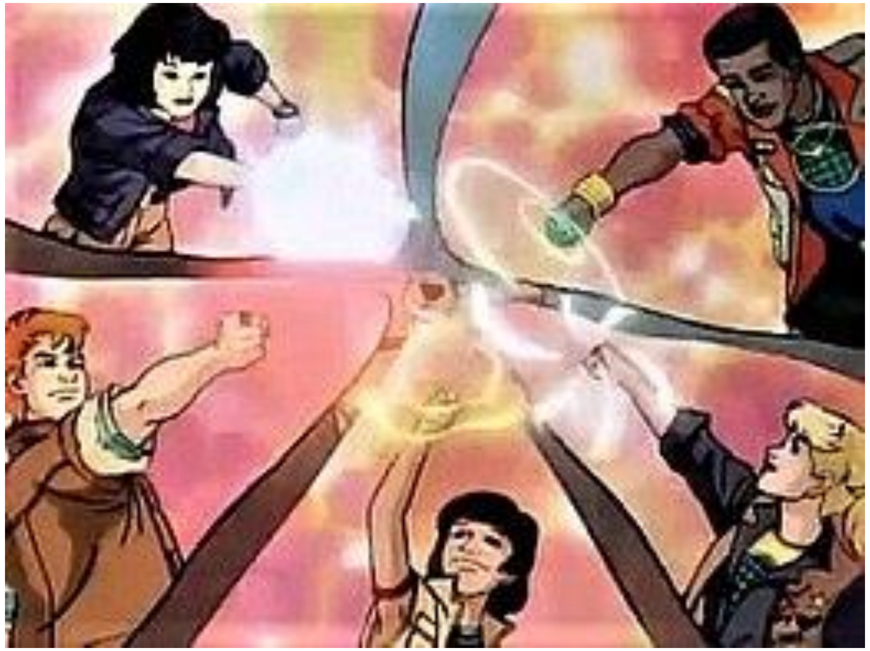
Theory of arrays

Theory of strings

EUF

Theory of equality on uninterpreted (mathematical) functions

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



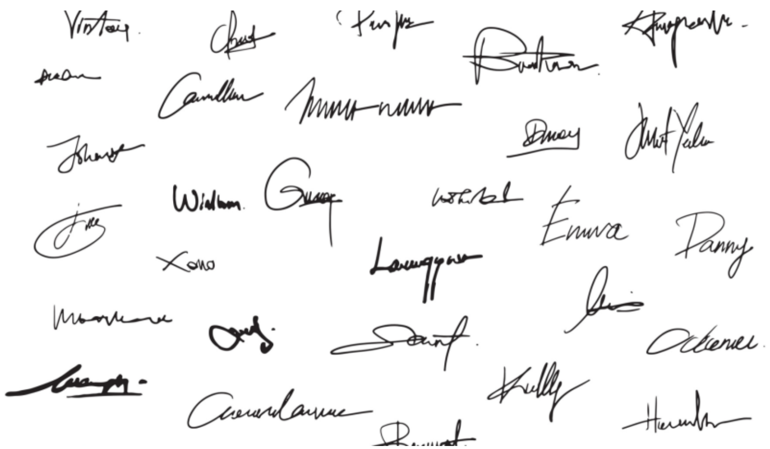
THEORY SIGNATURES

SMT SOLVING

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

Example: Theory of linear integer arithmetic: $(0, 1, +, -, \leq)$ interpreted over $\mathbb{Z}$

Once we have a set of signatures, we'll try to get our formula (i.e. path constraint) to separate concerns into theories



SEPARATING CONCERNS

SMT SOLVING

Note: we will only deal with constraints in Quantifier-Free First-Order Logic

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: $\vee$, $\wedge$, $\neg$, $\rightarrow$, $\leftrightarrow$
- Variables: v1, v2, . . .
- ~~Quantifiers: $\forall$, $\exists$~~

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

EXAMPLE

SMT SOLVING

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

$\land$

$f(0) = a + 2$

$\land$

$x = y$

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

EXAMPLE

SMT SOLVING

Step 1: Nelson-Oppen procedure to separate theories

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

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

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

EXAMPLE

SMT SOLVING

Step 1: Nelson-Oppen procedure to separate theories

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

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

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

EXAMPLE

SMT SOLVING

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

EXAMPLE

SMT SOLVING

$f(e_1) = a$

$\wedge$

$e_1 = e_2 - e_3$

$\wedge$

$e_2 = f(x)$

$\wedge$

$e_3 = f(y)$

$\wedge$

$f(e_4) = e_5$

$\wedge$

$e_4 = 0$

$\wedge$

$e_5 = a + 2$

$\wedge$

$x = y$

$\wedge$

$f(x) = f(y)$

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

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

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

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

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

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

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

$\wedge$
$e_2 - e_3 = 0$
$\wedge$
$e_1 = 0$
$\wedge$
$e_1 = e_4$

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

$f(e_1) = a$

$\wedge$

$e_1 = e_2 - e_3$

$\wedge$

$e_2 = f(x)$

$\wedge$

$e_3 = f(y)$

$\wedge$

$f(e_4) = e_5$

$\wedge$

$e_4 = 0$

$\wedge$

$e_5 = a + 2$

$\wedge$

$x = y$

$\wedge$

$f(x) = f(y)$

$\wedge$

$e_2 = e_3$

$\wedge$

$e_2 - e_3 = 0$

$\wedge$

$e_1 = 0$

$\wedge$

$e_1 = e_4$

$\wedge$

$f(0) = a$

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

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

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

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

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

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

Arithmetic Contradiction

Some EUF Axioms

Congruence:

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

Symmetry

$x = y \Rightarrow y = x$

Transitivity:

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

...

"CONVENIENT" EQUALITIES

SMT SOLVING

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

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

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...

$$(e_1 = e_2 \vee e_1 \neq e_2)$$
$$\wedge$$
$$(e2 = e3 \vee e2 \neq e3)$$
$$\wedge$$
$$(e1 = e3 \vee e1 \neq e3)$$
$$\wedge$$
$$\ldots$$

and start making guesses

"CONVENIENT" EQUALITIES

SMT SOLVING

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

Abstract all non-logical clauses

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

DPLL

p1:true
p2:true
p3:false
p4: true

Linear Solver: contradiction!

Add information and start over

$p1 \land p2 \land (p3 \lor p4) \land \underbrace{(\neg p1 \lor \neg p2 \lor \neg p3)}$

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...

$$(e_1 = e_2 \lor e_1 \neq e_2)$$
$$\land$$
$$(e2 = e3 \lor e2 \neq e3)$$
$$\land$$
$$(e1 = e3 \lor e1 \neq e3)$$
$$\land$$
$$\ldots$$

and start making guesses

smart

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