SMT: quantifiers, and future prospects

Pascal Fontaine (University of Liège)

Based on joint works with many, including
Haniel Barbosa, Jasmin Blanchette, Daniel El Ouraoui, Mathias Fleury, Mikolás Janota, Cezary Kaliszyk, Andrew Reynolds, Hans-Jörg Schurr, Sophie Tourret...

...and built on the work of many others (see citations)

IPAM Workshop, UCLA, February 2023

Outline

Outline

Motivation

- Formal proofs should not be mostly about proving easy things
- Automated theorem provers (ATPs) should prove the easy things for you
- ATP proofs can be replayed: confidence is not compromised
- E.g. Sledgehammer
- Proof obligations often use quantifiers

SMT = SAT + expressiveness

- SAT solvers
$$\neg\big[\,(p \Rightarrow q) \Rightarrow \big[\,(\neg p \Rightarrow q) \Rightarrow q\big]\big]$$
- Congruence closure (uninterpreted symbols + equality)
$$a = b \wedge \big[f(a) \neq f(b) \vee (q(a) \wedge \neg q(b))\big]$$
- and with arithmetic
$$a \leq b \wedge b \leq a + x \wedge x = 0 \wedge \big[f(a) \neq f(b) \vee (q(a) \wedge \neg q(b + x))\big]$$
- ...
- What about quantifiers?

Quantifiers in SMT

- ☹ Full first-order logic is undecidable
- ☺ First-order logic is semi-decidable
  refutationally complete procedures terminate on UNSAT
- ☺ If finite model property, then decidable
- ☹ Presburger with even one unary predicate is not even semi-decidable [Halper91]
- ☺ Pragmatic approaches are quite successful

Why does the pragmatic SMT approach work?

- Verification problems are big and shallow
- SMT appropriate for long, mostly ground, uninterpreted function reasoning

Working hypothesis

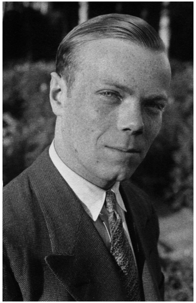
Quantifier handling for pure FOL will work most of the time sufficiently for SMT

Outline

Outline

Herbrand

Unlike superposition-based FOL provers, SMT solvers essentially based on instantiation



1908-1931

Herbrand instance of a Skolem formula $\forall \bar{x} \varphi(\bar{x})$: any ground formula $\varphi(\bar{t})$, where $\bar{t}$ are terms in the language

Theorem (Herbrand)

A finite set of Skolem formulas is unsatisfiable if and only if there exists a finite unsatisfiable set of Herbrand instances

Caveats

- there should be at least one constant available for every sort
- holds for pure FOL, might not in presence of theories

Example

Is this syllogism correct?

$$\frac{\text{All humans are mortal} \quad \text{All Greeks are humans}}{\text{Then all Greeks are mortal}}$$

Artistotle
384–322 BC

Example

Is this syllogism correct?

All humans are mortal
All Greeks are humans

Then all Greeks are mortal

Translate to FOL

Artistotle
384–322 BC

Example

Is this syllogism correct?

$$\frac{\begin{array}{l}\text{All humans are mortal}\\ \text{All Greeks are humans}\end{array}}{\text{Then all Greeks are mortal}}$$

Translate to FOL

$$\frac{\begin{array}{l}\forall x.\, H(x) \Rightarrow M(x)\\ \forall x.\, G(x) \Rightarrow H(x)\end{array}}{\forall x.\, G(x) \Rightarrow M(x)}$$

Artistotle
384–322 BC

Example

Is this syllogism correct?

$$\frac{\begin{array}{l}\text{All humans are mortal}\\ \text{All Greeks are humans}\end{array}}{\text{Then all Greeks are mortal}}$$

Translate to FOL

$$\frac{\begin{array}{l}\forall x.\, H(x) \Rightarrow M(x)\\ \forall x.\, G(x) \Rightarrow H(x)\end{array}}{\forall x.\, G(x) \Rightarrow M(x)}$$

Artistotle
384–322 BC

- Checking the validity of this formula
  $\Big((\forall x.\, H(x) \Rightarrow M(x)) \wedge (\forall x.\, G(x) \Rightarrow H(x))\Big) \Rightarrow \forall x.\, G(x) \Rightarrow M(x)$

Example

Is this syllogism correct?

$$\frac{\text{All humans are mortal} \quad \text{All Greeks are humans}}{\text{Then all Greeks are mortal}}$$

Translate to FOL

$$\frac{\forall x.\, H(x) \Rightarrow M(x) \quad \forall x.\, G(x) \Rightarrow H(x)}{\forall x.\, G(x) \Rightarrow M(x)}$$

Artistotle
384–322 BC

- Checking the validity of this formula
  $$\Big((\forall x.\, H(x) \Rightarrow M(x)) \wedge (\forall x.\, G(x) \Rightarrow H(x)) \Big) \Rightarrow \forall x.\, G(x) \Rightarrow M(x)$$
- Checking the unsatisfiability of
  $$\forall x.\, H(x) \Rightarrow M(x), \forall x.\, G(x) \Rightarrow H(x), \neg\forall x.\, G(x) \Rightarrow M(x)$$

Example

Is this syllogism correct?

$$\frac{\begin{array}{l}\text{All humans are mortal}\\ \text{All Greeks are humans}\end{array}}{\text{Then all Greeks are mortal}}$$

Translate to FOL

$$\frac{\begin{array}{l}\forall x.\, H(x) \Rightarrow M(x)\\ \forall x.\, G(x) \Rightarrow H(x)\end{array}}{\forall x.\, G(x) \Rightarrow M(x)}$$

Artistotle
384–322 BC

- Checking the validity of this formula
  $\Big((\forall x.\, H(x) \Rightarrow M(x)) \wedge (\forall x.\, G(x) \Rightarrow H(x))\Big) \Rightarrow \forall x.\, G(x) \Rightarrow M(x)$
- Checking the unsatisfiability of
  $\forall x.\, H(x) \Rightarrow M(x), \forall x.\, G(x) \Rightarrow H(x), \neg\forall x.\, G(x) \Rightarrow M(x)$
- Skolemize
  $\forall x.\, H(x) \Rightarrow M(x), \forall x.\, G(x) \Rightarrow H(x), \neg(G(s) \Rightarrow M(s))$

Example

Is this syllogism correct?

$$\frac{\begin{array}{l}\text{All humans are mortal}\\ \text{All Greeks are humans}\end{array}}{\text{Then all Greeks are mortal}}$$

Translate to FOL

$$\frac{\begin{array}{c}\forall x.\, H(x) \Rightarrow M(x)\\ \forall x.\, G(x) \Rightarrow H(x)\end{array}}{\forall x.\, G(x) \Rightarrow M(x)}$$

Artistotle
384–322 BC

- Checking the validity of this formula
  $\Big((\forall x.\, H(x) \Rightarrow M(x)) \wedge (\forall x.\, G(x) \Rightarrow H(x))\Big) \Rightarrow \forall x.\, G(x) \Rightarrow M(x)$
- Checking the unsatisfiability of
  $\forall x.\, H(x) \Rightarrow M(x), \forall x.\, G(x) \Rightarrow H(x), \neg\forall x.\, G(x) \Rightarrow M(x)$
- Skolemize
  $\forall x.\, H(x) \Rightarrow M(x), \forall x.\, G(x) \Rightarrow H(x), \neg(G(s) \Rightarrow M(s))$
- Instantiate: add the two formulas (Herbrand instances)
  $H(s) \Rightarrow M(s), G(s) \Rightarrow H(s)$

Example

Is this syllogism correct?

$$\frac{\begin{array}{l}\text{All humans are mortal}\\ \text{All Greeks are humans}\end{array}}{\text{Then all Greeks are mortal}}$$

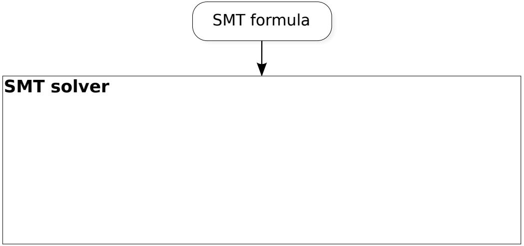
Translate to FOL

$$\frac{\begin{array}{c}\forall x.\, H(x) \Rightarrow M(x)\\ \forall x.\, G(x) \Rightarrow H(x)\end{array}}{\forall x.\, G(x) \Rightarrow M(x)}$$

Artistotle
384–322 BC

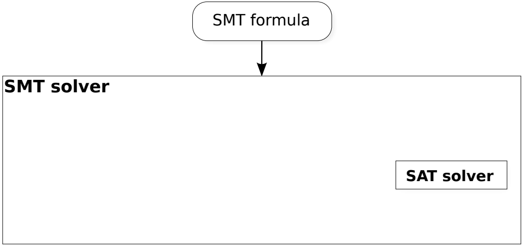
- Checking the validity of this formula
  $\Big((\forall x.\, H(x) \Rightarrow M(x)) \wedge (\forall x.\, G(x) \Rightarrow H(x))\Big) \Rightarrow \forall x.\, G(x) \Rightarrow M(x)$
- Checking the unsatisfiability of
  $\forall x.\, H(x) \Rightarrow M(x), \forall x.\, G(x) \Rightarrow H(x), \neg\forall x.\, G(x) \Rightarrow M(x)$
- Skolemize
  $\forall x.\, H(x) \Rightarrow M(x), \forall x.\, G(x) \Rightarrow H(x), \neg(G(s) \Rightarrow M(s))$
- Instantiate: add the two formulas (Herbrand instances)
  $H(s) \Rightarrow M(s), G(s) \Rightarrow H(s)$
- A ground (SAT/SMT) solver will deduce unsatisfiability.

From SAT to SMT,...



Input: $a \leq b \wedge b \leq a + x \wedge x = 0 \wedge \left[f(a) \neq f(b) \vee (q(a) \wedge \neg q(b + x))\right]$

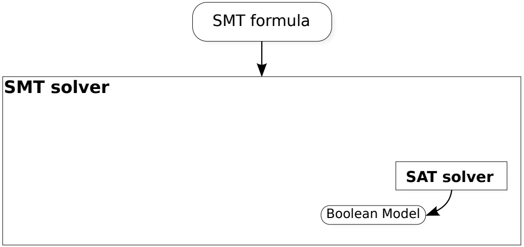
From SAT to SMT,...



Input: $a \leq b \wedge b \leq a + x \wedge x = 0 \wedge \big[f(a) \neq f(b) \vee (q(a) \wedge \neg q(b + x))\big]$

To SAT solver: $p_{a \leq b} \wedge p_{b \leq a+x} \wedge p_{x=0} \wedge \big[\neg p_{f(a)=f(b)} \vee \big(p_{q(a)} \wedge \neg p_{q(b+x)}\big)\big]$

From SAT to SMT,...

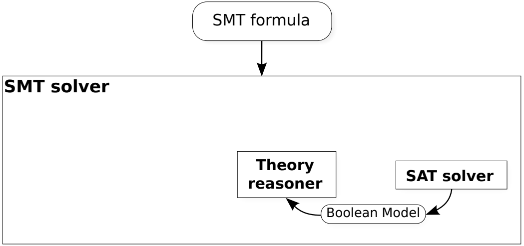


Input: $a \leq b \wedge b \leq a + x \wedge x = 0 \wedge \left[f(a) \neq f(b) \vee (q(a) \wedge \neg q(b + x)) \right]$

To SAT solver: $p_{a \leq b} \wedge p_{b \leq a+x} \wedge p_{x=0} \wedge \left[\neg p_{f(a)=f(b)} \vee \left(p_{q(a)} \wedge \neg p_{q(b+x)} \right) \right]$

Boolean model: $p_{a \leq b}, p_{b \leq a+x}, p_{x=0}, \neg p_{f(a)=f(b)}$

From SAT to SMT,...



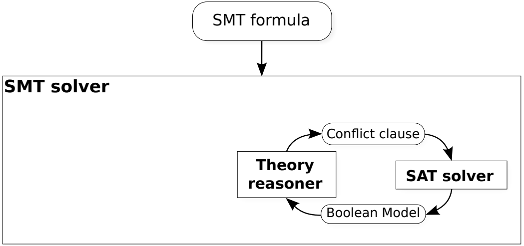
Input: $a \leq b \wedge b \leq a + x \wedge x = 0 \wedge \left[f(a) \neq f(b) \vee (q(a) \wedge \neg q(b + x)) \right]$

To SAT solver: $p_{a \leq b} \wedge p_{b \leq a+x} \wedge p_{x=0} \wedge \left[\neg p_{f(a)=f(b)} \vee \left(p_{q(a)} \wedge \neg p_{q(b+x)} \right) \right]$

Boolean model: $p_{a \leq b}, p_{b \leq a+x}, p_{x=0}, \neg p_{f(a)=f(b)}$

Theory reasoner: $a \leq b, b \leq a + x, x = 0, f(a) \neq f(b)$ unsatisfiable

From SAT to SMT,...



Input: $a \leq b \wedge b \leq a + x \wedge x = 0 \wedge \left[f(a) \neq f(b) \vee (q(a) \wedge \neg q(b+x)) \right]$

To SAT solver: $p_{a \leq b} \wedge p_{b \leq a+x} \wedge p_{x=0} \wedge \left[\neg p_{f(a)=f(b)} \vee \left(p_{q(a)} \wedge \neg p_{q(b+x)} \right) \right]$

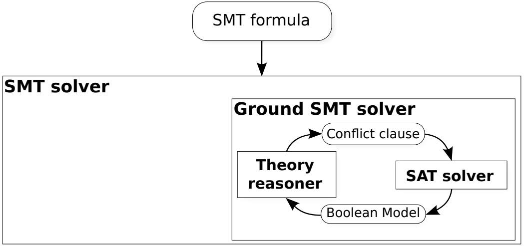
Boolean model: $p_{a \leq b}, p_{b \leq a+x}, p_{x=0}, \neg p_{f(a)=f(b)}$

Theory reasoner: $a \leq b, b \leq a + x, x = 0, f(a) \neq f(b)$ unsatisfiable

New clause: $\neg p_{a \leq b} \vee \neg p_{b \leq a+x} \vee \neg p_{x=0} \vee p_{f(a)=f(b)}$

Conflict clauses are negation of unsatisfiable conjunctive sets of literals

From SAT to SMT,... and then to quantified SMT



Input: $a \leq b \wedge b \leq a + x \wedge x = 0 \wedge \left[f(a) \neq f(b) \vee (q(a) \wedge \neg q(b + x))\right]$

To SAT solver: $p_{a \leq b} \wedge p_{b \leq a+x} \wedge p_{x=0} \wedge \left[\neg p_{f(a)=f(b)} \vee \left(p_{q(a)} \wedge \neg p_{q(b+x)}\right)\right]$

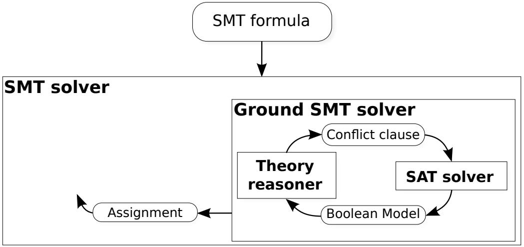
Boolean model: $p_{a \leq b}, p_{b \leq a+x}, p_{x=0}, \neg p_{f(a)=f(b)}$

Theory reasoner: $a \leq b, b \leq a + x, x = 0, f(a) \neq f(b)$ unsatisfiable

New clause: $\neg p_{a \leq b} \vee \neg p_{b \leq a+x} \vee \neg p_{x=0} \vee p_{f(a)=f(b)}$

Conflict clauses are negation of unsatisfiable conjunctive sets of literals

From SAT to SMT,... and then to quantified SMT



Input: $a \leq b \wedge b \leq a + x \wedge x = 0 \wedge \left[f(a) \neq f(b) \vee (q(a) \wedge \neg q(b + x))\right]$

To SAT solver: $p_{a \leq b} \wedge p_{b \leq a+x} \wedge p_{x=0} \wedge \left[\neg p_{f(a)=f(b)} \vee \left(p_{q(a)} \wedge \neg p_{q(b+x)}\right)\right]$

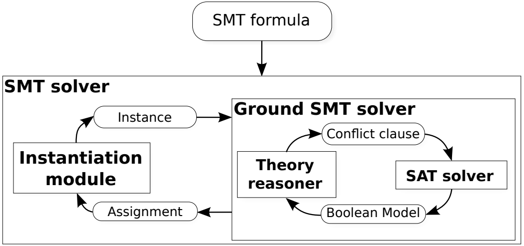
Boolean model: $p_{a \leq b}, p_{b \leq a+x}, p_{x=0}, \neg p_{f(a)=f(b)}$

Theory reasoner: $a \leq b, b \leq a + x, x = 0, f(a) \neq f(b)$ unsatisfiable

New clause: $\neg p_{a \leq b} \vee \neg p_{b \leq a+x} \vee \neg p_{x=0} \vee p_{f(a)=f(b)}$

Conflict clauses are negation of unsatisfiable conjunctive sets of literals

From SAT to SMT,. . . and then to quantified SMT



Input: $a \leq b \wedge b \leq a + x \wedge x = 0 \wedge \left[f(a) \neq f(b) \vee (q(a) \wedge \neg q(b + x))\right]$

To SAT solver: $p_{a \leq b} \wedge p_{b \leq a+x} \wedge p_{x=0} \wedge \left[\neg p_{f(a)=f(b)} \vee \left(p_{q(a)} \wedge \neg p_{q(b+x)}\right)\right]$

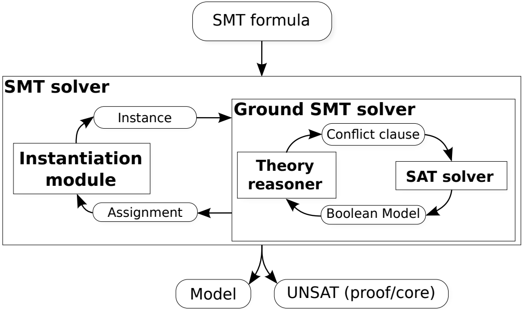
Boolean model: $p_{a \leq b}, p_{b \leq a+x}, p_{x=0}, \neg p_{f(a)=f(b)}$

Theory reasoner: $a \leq b, b \leq a + x, x = 0, f(a) \neq f(b)$ unsatisfiable

New clause: $\neg p_{a \leq b} \vee \neg p_{b \leq a+x} \vee \neg p_{x=0} \vee p_{f(a)=f(b)}$

Conflict clauses are negation of unsatisfiable conjunctive sets of literals

From SAT to SMT,... and then to quantified SMT



Input: $a \leq b \wedge b \leq a + x \wedge x = 0 \wedge \left[f(a) \neq f(b) \vee (q(a) \wedge \neg q(b + x))\right]$

To SAT solver: $p_{a \leq b} \wedge p_{b \leq a+x} \wedge p_{x=0} \wedge \left[\neg p_{f(a)=f(b)} \vee (p_{q(a)} \wedge \neg p_{q(b+x)})\right]$

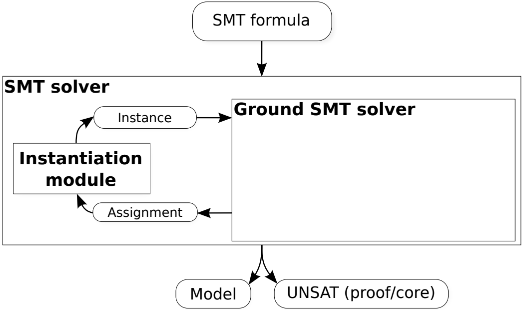
Boolean model: $p_{a \leq b}, p_{b \leq a+x}, p_{x=0}, \neg p_{f(a)=f(b)}$

Theory reasoner: $a \leq b, b \leq a + x, x = 0, f(a) \neq f(b)$ unsatisfiable

New clause: $\neg p_{a \leq b} \vee \neg p_{b \leq a+x} \vee \neg p_{x=0} \vee p_{f(a)=f(b)}$

Conflict clauses are negation of unsatisfiable conjunctive sets of literals

From SAT to SMT,... and then to quantified SMT



Input: $a \leq b \wedge b \leq a + x \wedge x = 0 \wedge \left[f(a) \neq f(b) \vee (q(a) \wedge \neg q(b + x))\right]$

To SAT solver: $p_{a \leq b} \wedge p_{b \leq a+x} \wedge p_{x=0} \wedge \left[\neg p_{f(a)=f(b)} \vee (p_{q(a)} \wedge \neg p_{q(b+x)})\right]$

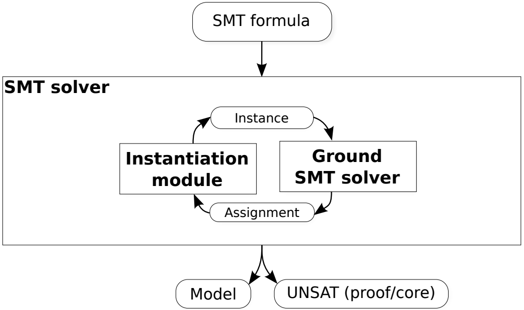
Boolean model: $p_{a \leq b}, p_{b \leq a+x}, p_{x=0}, \neg p_{f(a)=f(b)}$

Theory reasoner: $a \leq b, b \leq a + x, x = 0, f(a) \neq f(b)$ unsatisfiable

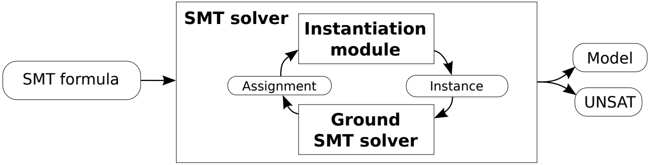
New clause: $\neg p_{a \leq b} \vee \neg p_{b \leq a+x} \vee \neg p_{x=0} \vee p_{f(a)=f(b)}$

Conflict clauses are negation of unsatisfiable conjunctive sets of literals

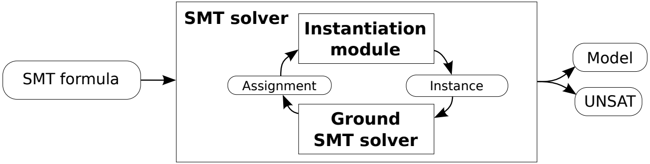
From SAT to SMT,... and then to quantified SMT



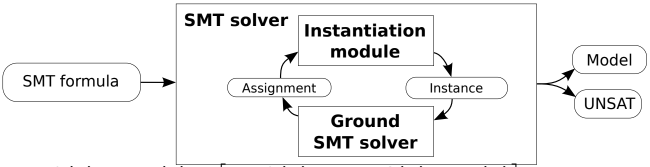
From SAT to SMT,... and then to quantified SMT



Instance?

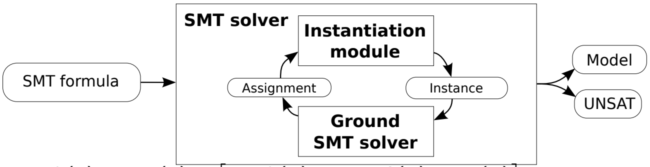

SMT formula
SMT solver
Instantiation module
Instance
Ground SMT solver
Assignment
Model
UNSAT

Instance?



Input: $a = b \wedge S(b) \wedge \neg Q(a) \wedge \neg R(a) \wedge \left[\forall x\, Q(x) \vee \forall x\,.\, S(x) \equiv R(x)\right]$

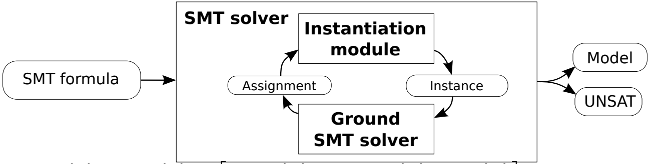
Instance?



Input: $a = b \wedge S(b) \wedge \neg Q(a) \wedge \neg R(a) \wedge \left[\forall x\, Q(x) \vee \forall x\,.\, S(x) \equiv R(x)\right]$

To SAT solver: $p_{a=b} \wedge p_{S(b)} \wedge \neg p_{Q(a)} \wedge \neg p_{R(a)} \wedge \left[p_{\forall x\, Q(x)} \vee p_{\forall x\,.\, S(x) \equiv R(x)}\right]$

Instance?

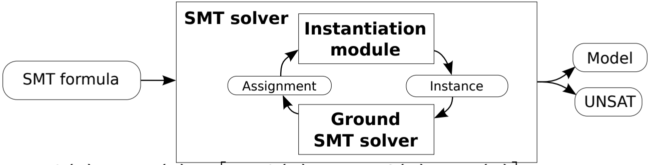


Input: $a = b \wedge S(b) \wedge \neg Q(a) \wedge \neg R(a) \wedge \left[\forall x\, Q(x) \vee \forall x\, .\, S(x) \equiv R(x)\right]$

To SAT solver: $p_{a=b} \wedge p_{S(b)} \wedge \neg p_{Q(a)} \wedge \neg p_{R(a)} \wedge \left[p_{\forall x\, Q(x)} \vee p_{\forall x\, .\, S(x) \equiv R(x)}\right]$

Boolean model: $p_{a=b}, p_{S(b)}, \neg p_{Q(a)}, \neg p_{R(a)}, p_{\forall x\, .\, S(x) \equiv R(x)}$

Instance?



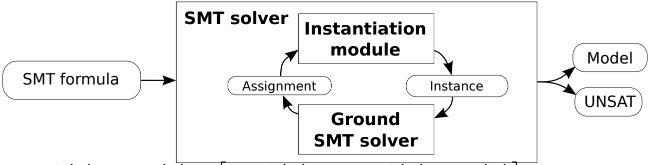
Input: $a = b \wedge S(b) \wedge \neg Q(a) \wedge \neg R(a) \wedge \left[\forall x\, Q(x) \vee \forall x\,.\,S(x) \equiv R(x)\right]$

To SAT solver: $p_{a=b} \wedge p_{S(b)} \wedge \neg p_{Q(a)} \wedge \neg p_{R(a)} \wedge \left[p_{\forall x\, Q(x)} \vee p_{\forall x\,.\,S(x)\equiv R(x)}\right]$

Boolean model: $p_{a=b}, p_{S(b)}, \neg p_{Q(a)}, \neg p_{R(a)}, p_{\forall x\,.\,S(x)\equiv R(x)}$

Theory reasoner: fine! ...but does not understand $\forall x\,.\,S(x) \equiv R(x)$

Instance?



Input: $a = b \wedge S(b) \wedge \neg Q(a) \wedge \neg R(a) \wedge \left[\forall x\, Q(x) \vee \forall x\,.\, S(x) \equiv R(x)\right]$

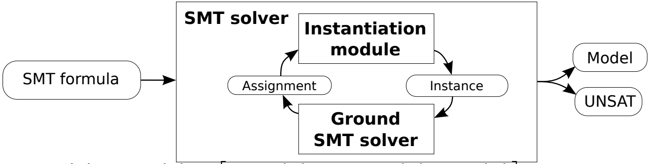
To SAT solver: $p_{a=b} \wedge p_{S(b)} \wedge \neg p_{Q(a)} \wedge \neg p_{R(a)} \wedge \left[p_{\forall x\, Q(x)} \vee p_{\forall x\,.\, S(x) \equiv R(x)}\right]$

Boolean model: $p_{a=b}, p_{S(b)}, \neg p_{Q(a)}, \neg p_{R(a)}, p_{\forall x\,.\, S(x) \equiv R(x)}$

Theory reasoner: fine! ...but does not understand $\forall x\,.\, S(x) \equiv R(x)$

Instantiation module: there is something to do with $\forall x\,.\, S(x) \equiv R(x)$

Instance?



Input: $a = b \wedge S(b) \wedge \neg Q(a) \wedge \neg R(a) \wedge \left[\forall x\, Q(x) \vee \forall x\,.\,S(x) \equiv R(x)\right]$

To SAT solver: $p_{a=b} \wedge p_{S(b)} \wedge \neg p_{Q(a)} \wedge \neg p_{R(a)} \wedge \left[p_{\forall x\, Q(x)} \vee p_{\forall x\,.\,S(x)\equiv R(x)}\right]$

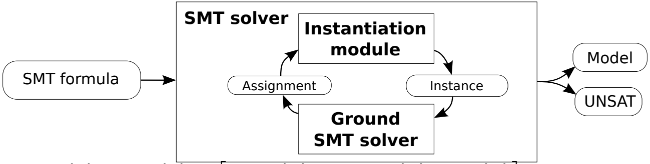
Boolean model: $p_{a=b}, p_{S(b)}, \neg p_{Q(a)}, \neg p_{R(a)}, p_{\forall x\,.\,S(x)\equiv R(x)}$

Theory reasoner: fine! ... but does not understand $\forall x\,.\,S(x) \equiv R(x)$

Instantiation module: there is something to do with $\forall x\,.\,S(x) \equiv R(x)$

New clause: $\neg p_{a=b}, \neg p_{S(b)} \vee p_{R(a)} \vee \neg p_{\forall x\,.\,S(x)\equiv R(x)}$

Instance?



Input: $a = b \land S(b) \land \neg Q(a) \land \neg R(a) \land \left[\forall x\, Q(x) \lor \forall x\,.\, S(x) \equiv R(x)\right]$

To SAT solver: $p_{a=b} \land p_{S(b)} \land \neg p_{Q(a)} \land \neg p_{R(a)} \land \left[p_{\forall x\, Q(x)} \lor p_{\forall x\,.\, S(x) \equiv R(x)}\right]$

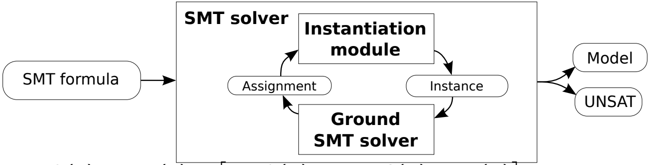
Boolean model: $p_{a=b}, p_{S(b)}, \neg p_{Q(a)}, \neg p_{R(a)}, p_{\forall x\,.\, S(x) \equiv R(x)}$

Theory reasoner: fine! . . . but does not understand $\forall x\,.\, S(x) \equiv R(x)$

Instantiation module: there is something to do with $\forall x\,.\, S(x) \equiv R(x)$

New clause:$\neg p_{a=b}, \neg p_{S(b)} \lor p_{R(a)} \lor \neg p_{\forall x\,.\, S(x) \equiv R(x)}$
. . . too complicated to find/generate

Instance?



Input: $a = b \wedge S(b) \wedge \neg Q(a) \wedge \neg R(a) \wedge \left[\forall x\, Q(x) \vee \forall x \,.\, S(x) \equiv R(x)\right]$

To SAT solver: $p_{a=b} \wedge p_{S(b)} \wedge \neg p_{Q(a)} \wedge \neg p_{R(a)} \wedge \left[p_{\forall x\, Q(x)} \vee p_{\forall x \,.\, S(x)\equiv R(x)}\right]$

Boolean model: $p_{a=b}, p_{S(b)}, \neg p_{Q(a)}, \neg p_{R(a)}, p_{\forall x \,.\, S(x)\equiv R(x)}$

Theory reasoner: fine! ... but does not understand $\forall x \,.\, S(x) \equiv R(x)$

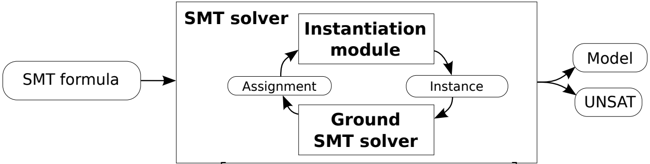
Instantiation module: there is something to do with $\forall x \,.\, S(x) \equiv R(x)$

New clause:$\neg p_{a=b}, \neg p_{S(b)} \vee p_{R(a)} \vee \neg p_{\forall x \,.\, S(x)\equiv R(x)}$

... too complicated to find/generate

What is the right formula to generate?

Instance?



Input: $a = b \wedge S(b) \wedge \neg Q(a) \wedge \neg R(a) \wedge \left[\forall x\, Q(x) \vee \forall x\,.\,S(x) \equiv R(x)\right]$

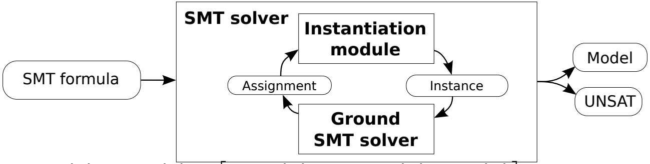
To SAT solver: $p_{a=b} \wedge p_{S(b)} \wedge \neg p_{Q(a)} \wedge \neg p_{R(a)} \wedge \left[p_{\forall x\, Q(x)} \vee p_{\forall x\,.\,S(x) \equiv R(x)}\right]$

Boolean model: $p_{a=b}, p_{S(b)}, \neg p_{Q(a)}, \neg p_{R(a)}, p_{\forall x\,.\,S(x) \equiv R(x)}$

Instantiation module: there is something to do with $\forall x\,.\,S(x) \equiv R(x)$

What is the right formula to generate?

Instance?



Input: $a = b \wedge S(b) \wedge \neg Q(a) \wedge \neg R(a) \wedge \left[\forall x\, Q(x) \vee \forall x\, .\, S(x) \equiv R(x)\right]$

To SAT solver: $p_{a=b} \wedge p_{S(b)} \wedge \neg p_{Q(a)} \wedge \neg p_{R(a)} \wedge \left[p_{\forall x\, Q(x)} \vee p_{\forall x\, .\, S(x) \equiv R(x)}\right]$

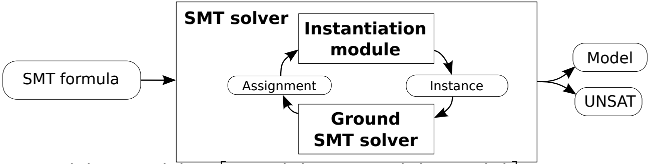
Boolean model: $p_{a=b}, p_{S(b)}, \neg p_{Q(a)}, \neg p_{R(a)}, p_{\forall x\, .\, S(x) \equiv R(x)}$

Instantiation module: there is something to do with $\forall x\, .\, S(x) \equiv R(x)$

What is the right formula to generate?

$S(a) \equiv R(a)$ is not right

Instance?



Input: $a = b \wedge S(b) \wedge \neg Q(a) \wedge \neg R(a) \wedge \left[\forall x\, Q(x) \vee \forall x\,.\, S(x) \equiv R(x)\right]$

To SAT solver: $p_{a=b} \wedge p_{S(b)} \wedge \neg p_{Q(a)} \wedge \neg p_{R(a)} \wedge \left[p_{\forall x\, Q(x)} \vee p_{\forall x\,.\, S(x) \equiv R(x)}\right]$

Boolean model: $p_{a=b}, p_{S(b)}, \neg p_{Q(a)}, \neg p_{R(a)}, p_{\forall x\,.\, S(x) \equiv R(x)}$

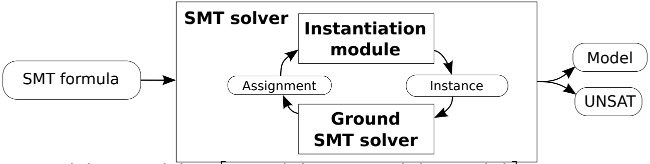
Instantiation module: there is something to do with $\forall x\,.\, S(x) \equiv R(x)$

What is the right formula to generate?

$S(a) \equiv R(a)$ is not right

We want $S(a) \equiv R(a)$ whenever $p_{\forall x\,.\, S(x) \equiv R(x)}$ is in the Boolean model

Instance?



Input: $a = b \wedge S(b) \wedge \neg Q(a) \wedge \neg R(a) \wedge \left[\forall x\, Q(x) \vee \forall x\, .\, S(x) \equiv R(x)\right]$

To SAT solver: $p_{a=b} \wedge p_{S(b)} \wedge \neg p_{Q(a)} \wedge \neg p_{R(a)} \wedge \left[p_{\forall x\, Q(x)} \vee p_{\forall x\, .\, S(x) \equiv R(x)}\right]$

Boolean model: $p_{a=b}, p_{S(b)}, \neg p_{Q(a)}, \neg p_{R(a)}, p_{\forall x\, .\, S(x) \equiv R(x)}$

Instantiation module: there is something to do with $\forall x\, .\, S(x) \equiv R(x)$

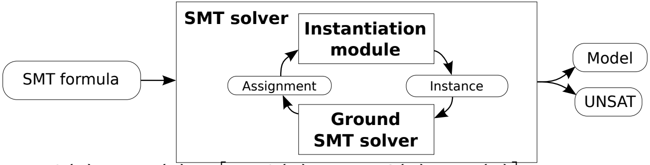
What is the right formula to generate?

$S(a) \equiv R(a)$ is not right

We want $S(a) \equiv R(a)$ whenever $p_{\forall x\, .\, S(x) \equiv R(x)}$ is in the Boolean model

$(\forall x\, .\, S(x) \equiv R(x)) \Rightarrow (S(a) \equiv R(a))$ would do

Instance?



Input: $a = b \wedge S(b) \wedge \neg Q(a) \wedge \neg R(a) \wedge \left[\forall x\, Q(x) \vee \forall x\, .\, S(x) \equiv R(x)\right]$

To SAT solver: $p_{a=b} \wedge p_{S(b)} \wedge \neg p_{Q(a)} \wedge \neg p_{R(a)} \wedge \left[p_{\forall x\, Q(x)} \vee p_{\forall x\, .\, S(x) \equiv R(x)}\right]$

Boolean model: $p_{a=b}, p_{S(b)}, \neg p_{Q(a)}, \neg p_{R(a)}, p_{\forall x\, .\, S(x) \equiv R(x)}$

Instantiation module: there is something to do with $\forall x\, .\, S(x) \equiv R(x)$

What is the right formula to generate?

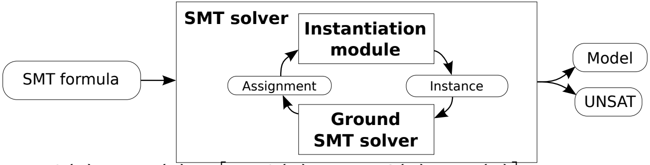
$S(a) \equiv R(a)$ is not right

We want $S(a) \equiv R(a)$ whenever $p_{\forall x\, .\, S(x) \equiv R(x)}$ is in the Boolean model

$(\forall x\, .\, S(x) \equiv R(x)) \Rightarrow (S(a) \equiv R(a))$ would do

$\neg p_{\forall x\, .\, S(x) \equiv R(x)} \vee \left(p_{S(a)} \equiv p_{R(a)}\right)$ at the propositional level

Instance?



Input: $a = b \wedge S(b) \wedge \neg Q(a) \wedge \neg R(a) \wedge \left[\forall x\, Q(x) \vee \forall x \,.\, S(x) \equiv R(x)\right]$

To SAT solver: $p_{a=b} \wedge p_{S(b)} \wedge \neg p_{Q(a)} \wedge \neg p_{R(a)} \wedge \left[p_{\forall x\, Q(x)} \vee p_{\forall x \,.\, S(x) \equiv R(x)}\right]$

Boolean model: $p_{a=b}, p_{S(b)}, \neg p_{Q(a)}, \neg p_{R(a)}, p_{\forall x \,.\, S(x) \equiv R(x)}$

Instantiation module: there is something to do with $\forall x \,.\, S(x) \equiv R(x)$

What is the right formula to generate?

$S(a) \equiv R(a)$ is not right

We want $S(a) \equiv R(a)$ whenever $p_{\forall x \,.\, S(x) \equiv R(x)}$ is in the Boolean model

$(\forall x \,.\, S(x) \equiv R(x)) \Rightarrow (S(a) \equiv R(a))$ would do

$\neg p_{\forall x \,.\, S(x) \equiv R(x)} \vee \left(p_{S(a)} \equiv p_{R(a)}\right)$ at the propositional level

Together with $\forall x\, Q(x) \Rightarrow Q(a)$, this grounds the problem

Instance in an SMT context

$$\forall \bar{x}\, \varphi(\bar{x}) \Rightarrow \varphi\sigma$$

where σ is a ground substitution for variables $\bar{x}$

E.g. $\forall \bar{x}\, \varphi(\bar{x})$ is $\forall x\,.\, S(x) \equiv R(x)$, σ is $x \mapsto a$, $\varphi\sigma$ is $S(a) \equiv R(a)$

Remarks

- Above formula is a FOL tautology. E.g. $(\forall x\,.\, S(x) \equiv R(x)) \Rightarrow (S(a) \equiv R(a))$
- $\forall \bar{x}\, \varphi(\bar{x})$ gets abstracted as a propositional variable in the SAT solver, that has a meaning only for the instantiation module
- $\varphi\sigma$ gets abstracted as a Boolean combination of propositional variables. . .
- . . . that have meaning at the level of the *ground* theory reasoner
- $\varphi\sigma$ gets "activated"/relevant only in the models where $p_{\forall \bar{x}\, \varphi(\bar{x})}$ is true.

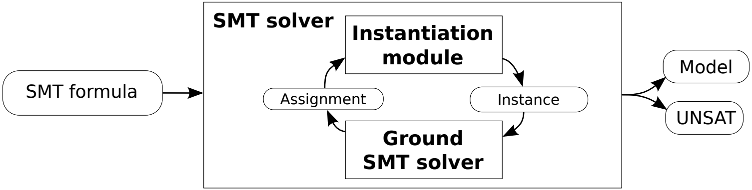
We might refer to $\varphi\sigma$ as the instance, but remember: all is fine at the level of the SAT solver/ground SMT solver

Outline

Outline

Instantiation techniques

The framework



Ground SMT solver enumerates assignments $E \cup Q$

- E set of ground literals
- Q set of quantified clauses

Instantiation module generates instances of Q that will further feed E

classic Herbrand Theorem: instantiate with all possible terms in language

Outline

E-matching/Trigger-based instantiation (**e**) [Detlefs05, deMoura07]

Search for relevant instances according to a set of triggers and E-matching

E-matching/Trigger-based instantiation (**e**) [Detlefs05, deMoura07]

Search for relevant instances according to a set of triggers and E-matching

- $E = \{\neg P(a), \neg P(b), P(c), \neg R(b)\}$ and $Q = \{\forall x.\, P(x) \vee R(x)\}$
- Assume trigger $P(x)$
- Find substitution σ for x such $P(x)$ is a know term (in E)
- Three suitable substitutions: $x \mapsto a$, $x \mapsto b$, or $x \mapsto c$
  E.g. $E \models P(x)[x/a] = P(a)$ and $P(a) \in E$
- Formally

$\mathbf{e}(E, \forall \bar{x}.\, \varphi)$

1. Select a set of triggers $\{\bar{t}_1, \ldots \bar{t}_n\}$ for $\forall \bar{x}.\, \varphi$
2. For each $i = 1, \ldots, n$, select a set of substitutions S_i s.t for each $\sigma \in S_i$, $E \models \bar{t}_i\sigma = \bar{g}_i$ for some tuple $\bar{g}_i \in \mathcal{T}_E$.
3. Return $\bigcup_{i=1}^{n} S_i$

E-matching/Trigger-based instantiation

Ideal for expanding definitions/rewriting rules

- Example

  $$\forall x \forall y \,.\, \mathrm{sister}(x, y) \equiv \\ (\mathrm{female}(x) \wedge \mathrm{mother}(x) = \mathrm{mother}(y) \wedge \mathrm{father}(x) = \mathrm{father}(y))$$

  $\mathrm{sister}(\mathrm{Eliane}, \mathrm{Eloïse})$

  $\mathrm{sister}(\mathrm{Eloïse}, \mathrm{Elisabeth})$

  $\neg\mathrm{sister}(\mathrm{Eliane}, \mathrm{Elisabeth})$

- Choosing instantiation trigger $\mathrm{sister}(x, y)$ suffices for SMT solver to prove unsatisfiability

Remarks

- Decision procedure for, e.g., expressive arrays, lists [Dross16]
- Mostly efficient (see later evaluation)
- But can easily blow or miss the right instances
- Requires triggers (human or auto-generated)

E-matching/Trigger-based instantiation, prospects

Machine learning for instance filtering

- Instantiation method issue: number of useless generated instances
- It often occurs that $> 99\%$ of 100k generated instances are useless

E-matching/Trigger-based instantiation, prospects

Machine learning for instance filtering

- Instantiation method issue: number of useless generated instances
- It often occurs that $> 99\%$ of 100k generated instances are useless

An opportunity for machine learning

separate the wheat from the chaff: select the useful instances

E-matching/Trigger-based instantiation, prospects

Machine learning for instance filtering

- Instantiation method issue: number of useless generated instances
- It often occurs that $> 99\%$ of 100k generated instances are useless

An opportunity for machine learning

separate the wheat from the chaff: select the useful instances

- We investigated XGBoost to filter instances [Blanchette19]

E-matching/Trigger-based instantiation, prospects

Machine learning for instance filtering

- Instantiation method issue: number of useless generated instances
- It often occurs that $> 99\%$ of 100k generated instances are useless

An opportunity for machine learning

separate the wheat from the chaff: select the useful instances

- We investigated XGBoost to filter instances [Blanchette19]
- Trained on successful proofs (good instance $\leftarrow$ survives pruning of proof)

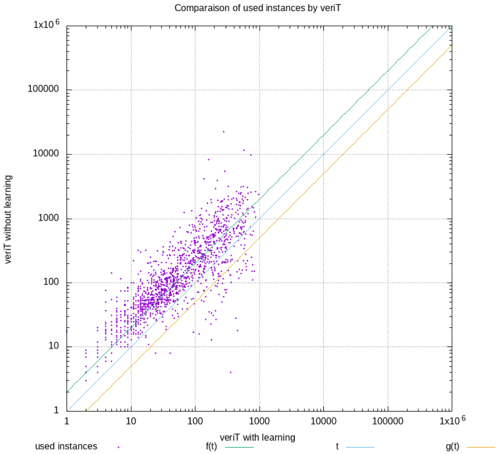
ML for instance filtering: experimental results

	30 s	60 s	120 s	180 s
veriT	2896	2913	2923	2929
veriT($\mathcal{M}$)	2907	2917	2925	2936
veriT($\mathcal{M}^2$)	2916	2927	2935	2944
veriT($\mathcal{M} + \mathcal{M}^2$)	2936	2959	2969	2975
veriT + portfolio	3181	3215	3228	3234
veriT($\mathcal{M} + \mathcal{M}^2$) + portfolio	3190	3247	3312	3322
Vampire smtcomp mode	3154	3165	3175	3197
CVC4 portfolio	3311	3345	3393	3404

Results on the benchmarks in the UF category of the SMT-LIB

- veriT: vanilla
- veriT($\mathcal{M}$): veriT with instance selection trained with veriT successes
- veriT($\mathcal{M}^2$): veriT with instance selection trained with veriT($\mathcal{M}$) successes
- veriT($\mathcal{M} + \mathcal{M}^2$): portfolio of above two
- veriT($\mathcal{M} + \mathcal{M}^2$) + portfolio of several strategies, with instance selection

ML for instance filtering: number of instances on test + training set



veriT on UF SMT-LIB benchmarks (with vs. without filtering)

ML for instance filtering: number of instances on test set only

veriT on UF SMT-LIB benchmarks (with vs. without filtering)

Outline

Conflict-based instantiation ($\mathbf{c}$)

[Reynolds14]

Search for *one* instance of one quantified formula in Q that is unsatisfiable together with E

Conflict-based instantiation ($\mathbf{c}$)

[Reynolds14]

Search for *one* instance of one quantified formula in Q that is unsatisfiable together with E

- $E = \{\neg P(a), \neg P(b), P(c), \neg R(b)\}$ and $Q = \{\forall x.\, P(x) \vee R(x)\}$
- Since E, $P(b) \vee R(b) \models \bot$, this strategy returns $x \mapsto b$
- Formally

  $\mathbf{c}(E, \forall \bar{x}.\, \varphi)$ Either return σ where $E \models \neg\varphi\sigma$, or return $\emptyset$

$\mathbf{c}$: solving the problem

$$E \wedge \psi\sigma \models \bot, \text{ for some } \forall \bar{x}\, \psi \in Q$$

c: solving the problem

$$E \models \neg\psi\sigma, \text{ for some } \forall\bar{x}\,\psi \in Q$$

$\mathbf{c}$: solving the problem

$$E \models \neg\psi\sigma, \text{ for some } \forall\bar{x}\,\psi \in Q$$

$$E = \{f(a) = f(b),\, g(b) \neq h(c)\},\; Q = \{\forall xyz.\; f(x) = f(z) \rightarrow h(y) = g(z)\}$$

C: solving the problem

$$E \models \neg\psi\sigma, \text{ for some } \forall\bar{x}\,\psi \in Q$$

$E = \{f(a) = f(b),\, g(b) \neq h(c)\},\ Q = \{\forall xyz.\ f(x) = f(z) \rightarrow h(y) = g(z)\}$

$$f(a) = f(b) \wedge g(b) \neq h(c) \models (f(x) = f(z) \wedge h(y) \neq g(z))\,\sigma$$

C: solving the problem

$$E \models \neg\psi\sigma, \text{ for some } \forall\bar{x}\,\psi \in Q$$

$E = \{f(a) = f(b),\ g(b) \neq h(c)\},\ Q = \{\forall xyz.\ f(x) = f(z) \to h(y) = g(z)\}$

$$f(a) = f(b) \wedge g(b) \neq h(c) \models (f(x) = f(z) \wedge h(y) \neq g(z))\,\sigma$$

- Each literal in the right hand side restricts σ

$\mathbf{c}$: solving the problem

$$E \models \neg\psi\sigma, \text{ for some } \forall\bar{x}\,\psi \in Q$$

$E = \{f(a) = f(b),\, g(b) \neq h(c)\},\ Q = \{\forall xyz.\ f(x) = f(z) \rightarrow h(y) = g(z)\}$

$$f(a) = f(b) \wedge g(b) \neq h(c) \models (f(x) = f(z) \wedge h(y) \neq g(z))\,\sigma$$

- Each literal in the right hand side restricts σ
  - $f(x) = f(z)$: either $x = z$ or $x = a \wedge z = b$ or $x = b \wedge z = a$

C: solving the problem

$$E \models \neg\psi\sigma, \text{ for some } \forall\bar{x}\,\psi \in Q$$

$E = \{f(a) = f(b),\, g(b) \neq h(c)\},\; Q = \{\forall xyz.\; f(x) = f(z) \rightarrow h(y) = g(z)\}$

$$f(a) = f(b) \land g(b) \neq h(c) \models (f(x) = f(z) \land h(y) \neq g(z))\,\sigma$$

- Each literal in the right hand side restricts σ
  - $f(x) = f(z)$: either $x = z$ or $x = a \land z = b$ or $x = b \land z = a$
  - $h(y) \neq g(z)$: $y = c \land z = b$

$\mathbf{c}$: solving the problem

$$E \models \neg\psi\sigma, \text{ for some } \forall\bar{x}\,\psi \in Q$$

$E = \{f(a) = f(b),\ g(b) \neq h(c)\},\ Q = \{\forall xyz.\ f(x) = f(z) \rightarrow h(y) = g(z)\}$

$$f(a) = f(b) \wedge g(b) \neq h(c) \models (f(x) = f(z) \wedge h(y) \neq g(z))\,\sigma$$

- Each literal in the right hand side restricts σ
  - $f(x) = f(z)$: either $\underline{x = z}$ or $x = a \wedge z = b$ or $x = b \wedge z = a$
  - $h(y) \neq g(z)$: $\underline{y = c \wedge z = b}$

$$\sigma = \{x \mapsto b,\ y \mapsto c,\ z \mapsto b\}$$

c: solving the problem

$$E \models \neg\psi\sigma, \text{ for some } \forall\bar{x}\,\psi \in Q$$

$E = \{f(a) = f(b),\ g(b) \neq h(c)\},\ Q = \{\forall xyz.\ f(x) = f(z) \rightarrow h(y) = g(z)\}$

$$f(a) = f(b) \wedge g(b) \neq h(c) \models (f(x) = f(z) \wedge h(y) \neq g(z))\,\sigma$$

- Each literal in the right hand side restricts σ
  - $f(x) = f(z)$: either $x = z$ or $\underline{x = a \wedge z = b}$ or $x = b \wedge z = a$
  - $h(y) \neq g(z)$: $\underline{y = c \wedge z = b}$

$$\sigma = \{x \mapsto b,\ y \mapsto c,\ z \mapsto b\}$$

or

$$\sigma = \{x \mapsto a,\ y \mapsto c,\ z \mapsto b\}$$

c: solving the problem

$$E \models \neg\psi\sigma, \text{ for some } \forall\bar{x}\,\psi \in Q$$

$E = \{f(a) = f(b),\, g(b) \neq h(c)\},\; Q = \{\forall xyz.\ f(x) = f(z) \rightarrow h(y) = g(z)\}$

$$f(a) = f(b) \wedge g(b) \neq h(c) \models (f(x) = f(z) \wedge h(y) \neq g(z))\,\sigma$$

- Each literal in the right hand side restricts σ
  - $f(x) = f(z)$: either $x = z$ or $x = a \wedge z = b$ or $\underline{x = b \wedge z = a}$
  - $h(y) \neq g(z)$: $\underline{y = c \wedge z = b}$

$$\sigma = \{x \mapsto b,\ y \mapsto c,\ z \mapsto b\}$$

or

$$\sigma = \{x \mapsto a,\ y \mapsto c,\ z \mapsto b\}$$

c: solving the problem with E-ground (dis)unification

Given conjunctive sets of equality literals E and L, with E ground, find substitution σ s.t. $E \models L\sigma$

c: solving the problem with E-ground (dis)unification

Given conjunctive sets of equality literals E and L, with E ground, find substitution σ s.t. $E \models L\sigma$

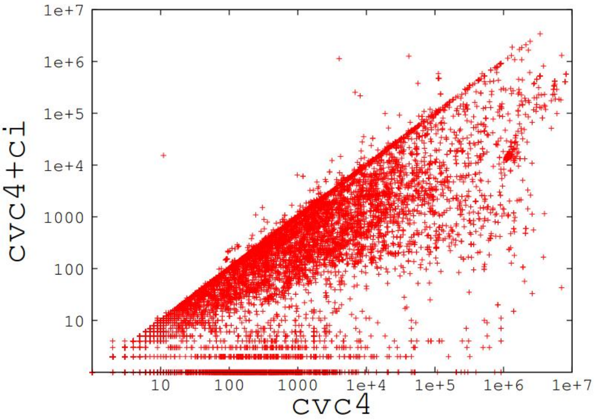
- Variant of classic (non-simultaneous) rigid E-unification

c: solving the problem with E-ground (dis)unification

Given conjunctive sets of equality literals E and L, with E ground, find substitution σ s.t. $E \models L\sigma$

- Variant of classic (non-simultaneous) rigid E-unification
- NP-complete
  - NP: solutions can be restricted to ground terms in $E \cup L$
  - NP-hard: reduction of 3-SAT
- CCFV: congruence closure with free variables [Barbosa17]
  - sound, complete and terminating calculus for solving E-ground (dis)unification
  - goal oriented
  - efficient in practice
- Still, 60% of time in veriT

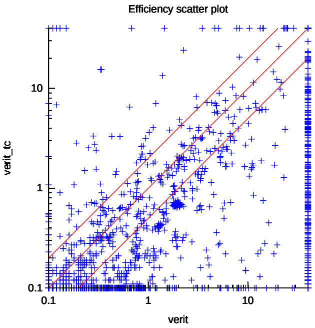
c evaluation (1/2) [Reynolds14]

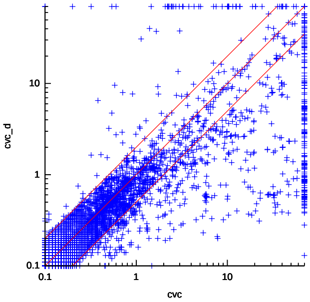


Reported number of instances.

- Evaluation on SMT-LIB, TPTP, Isabelle benchmarks
- Using conflict-based instantiation (cvc4+ci), require an order of magnitude fewer instances to prove unsatisfiability w.r.t. E-matching alone

c evaluation (2/2) [Barbosa17]





veriT: + 800 out of 1 785 unsolved problems

CVC4: + 200 out of 745 unsolved problems

* experiments in the "UF", "UFLIA", "UFLRA" and "UFIDL" categories of SMT-LIB, which have 10 495 benchmarks annotated as *unsatisfiable*, with 30s timeout.

Conflicting instances, prospects

- Still, 60% of time in veriT
- CCFV is an NP-complete problem
- It can be encoded into SAT
- We expect careful encoding of CCFV into SAT will provide efficient procedure
- We are investigating a SAT-based algorithm for higher-order CCFV

- Conflicting instances only work for one instance
- Finding out a pair of instances that contradict a model?
- Maybe use superposition? Extend algorithm to find conflicts with several clauses?

Outline

Model-based instantiation/MBQI (**m**) [Ge09]

Build a candidate model for $E \cup Q$ and instantiate with counter-examples from model checking

Model-based instantiation/MBQI ($\mathbf{m}$) [Ge09]

Build a candidate model for $E \cup Q$ and instantiate with counter-examples from model checking

- $E = \{\neg P(a), \neg P(b), P(c), \neg R(b)\}$ and $Q = \{\forall x.\, P(x) \vee R(x)\}$
- Ground solver provides a partial model...
- ...extended to a full model s.t. $P^{\mathcal{M}} = \lambda x.\, \text{ite}(x = c, \top, \bot)$ and $R^{\mathcal{M}} = \lambda x.\, \bot$
- Since $\mathcal{M} \models \neg\,(P(a) \vee R(a))$, this strategy may return $x \mapsto a$
- Formally

$\mathbf{m}(E, \forall \bar{x}.\, \varphi)$ 1. Construct a model $\mathcal{M}$ for E

2. Return $\bar{x} \mapsto \bar{t}$ where $\bar{t} \in \mathcal{T}(E)$ and $\mathcal{M} \models \neg\varphi[\bar{x}/\bar{t}]$, or $\emptyset$ if none exists

Outline

Why can't we directly use Herbrand instantiation?

Theorem (Herbrand)

A finite set of Skolem formulas is unsatisfiable if and only if there exists a finite unsatisfiable set of Herbrand instances

Why can't we directly use Herbrand instantiation?

Theorem (Herbrand)

A finite set of Skolem formulas is unsatisfiable if and only if there exists a finite unsatisfiable set of Herbrand instances

- The earliest theorem provers relied on *Herbrand instantiation*
  - Instantiate with all possible terms in the language
- Enumerating all instances is unfeasible in practice!
- Enumerative instantiation was then discarded

Why can't we directly use Herbrand instantiation?

Theorem (Herbrand)

A finite set of Skolem formulas is unsatisfiable if and only if there exists a finite unsatisfiable set of Herbrand instances

- The earliest theorem provers relied on *Herbrand instantiation*
  - Instantiate with all possible terms in the language
- Enumerating all instances is unfeasible in practice!
- Enumerative instantiation was then discarded

Revisiting enumerative instantiation with benefits:

- strengthening of Herbrand theorem
- efficient implementation techniques

Theorem (Strengthened Herbrand)

If R is a (possibly infinite) set of instances of Q closed under Q-instantiation w.r.t. itself and if $E \cup R$ is satisfiable, then $E \cup Q$ is satisfiable.

Theorem (Strengthened Herbrand)

If there exists an infinite sequence of finite satisfiable sets of ground literals E_i and of finite sets of ground instances Q_i of Q such that

- $Q_i = \left\{ \varphi\sigma \;\middle|\; \forall \bar{x}.\, \varphi \in Q,\, \mathrm{dom}(\sigma) = \{\bar{x}\} \wedge \mathrm{ran}(\sigma) \subseteq \mathcal{T}(E_i) \right\}$;
- $E_0 = E,\ E_{i+1} \models E_i \cup Q_i$;

then $E \cup Q$ is satisfiable in the empty theory with equality

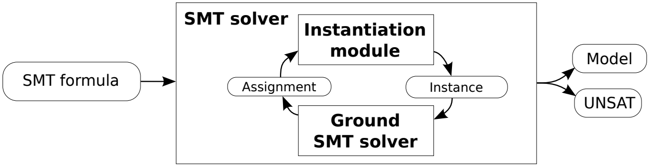
Theorem (Strengthened Herbrand)

If there exists an infinite sequence of finite satisfiable sets of ground literals E_i and of finite sets of ground instances Q_i of Q such that

- $Q_i = \{\varphi\sigma \mid \forall\bar{x}.\, \varphi \in Q,\ \mathrm{dom}(\sigma) = \{\bar{x}\} \wedge \mathrm{ran}(\sigma) \subseteq \mathcal{T}(E_i)\}$;
- $E_0 = E,\ E_{i+1} \models E_i \cup Q_i$;

then $E \cup Q$ is satisfiable in the empty theory with equality

Direct application to



- Ground solver enumerates assignments $E \cup Q$
- Instantiation module generates instances of Q

Enumerative instantiation ($\mathbf{u}$)

[Reynolds18]

$\mathbf{u}(E, \forall \bar{x}.\, \varphi)$

1. Choose an ordering $\preceq$ on tuples of ground terms
2. Return $\bar{x} \mapsto \bar{t}$ where $\bar{t}$ is a minimal tuple of terms w.r.t $\preceq$, such that $\bar{t} \in \mathcal{T}(E)$ and $E \not\models \varphi[\bar{x}/\bar{t}]$, or $\emptyset$ if none exist

- $E = \{\neg P(a), \neg P(b), P(c), \neg R(b)\}$ and $Q = \{\forall x.\, P(x) \vee R(x)\}$
- $\mathbf{u}$ chooses an ordering on tuples of terms, e.g. $a \prec b \prec c$
- Since $E \not\models P(a) \vee R(a)$, enumerative instantiation returns $x \mapsto a$

u as an alternative for **m**

- Enumerative instantiation plays a similar role to **m**
- It can also serve as a "completeness fallback" to **c** and **e**
- However, **u** has advantages over **m** for UNSAT problems
- And it is significantly simpler to implement
  - no model building
  - no model checking

Example

$$
\begin{array}{rcl}
E & = & \{\neg P(a),\ R(b),\ S(c)\} \\
Q & = & \{\forall x.\ R(x) \lor S(x),\ \forall x.\ \neg R(x) \lor P(x),\ \forall x.\ \neg S(x) \lor P(x)\} \\
M & = & \left\{ \begin{array}{rcl} P^{\mathcal{M}} & = & \lambda x.\ \bot, \\ R^{\mathcal{M}} & = & \lambda x.\ \mathrm{ite}(x = b,\ \top,\ \bot), \\ S^{\mathcal{M}} & = & \lambda x.\ \mathrm{ite}(x = c,\ \top,\ \bot) \end{array} \right\}, \qquad a \prec b \prec c
\end{array}
$$

φ	x s.t. $\mathcal{M} \models \neg\varphi$	x s.t. $E \not\models \varphi$	$\mathbf{m}(E, \forall x.\ \varphi)$	$\mathbf{u}(E, \forall x.\ \varphi)$
$R(x) \lor S(x)$	a	a	$x \mapsto a$	$x \mapsto a$
$\neg R(x) \lor P(x)$	b	a, b, c	$x \mapsto b$	$x \mapsto a$
$\neg S(x) \lor P(x)$	c	a, b, c	$x \mapsto c$	$x \mapsto a$

- **u** instantiates uniformly so that less new terms are introduced
- **m** instantiates depending on how model was built
- **u** directly leads to $E \land Q[x/a] \models \bot$

Advanced **u**: restricting enumeration space

- Strengthened Herbrand Theorem allows restriction to $\mathcal{T}(E)$

- *Sort inference* reduces instantiation space by computing more precise sort information
  - $E \cup Q = \{a \neq b,\ f(a) = c\} \cup \{P(f(x))\}$
    - $a, b, c, x : \tau$
    - $f : \tau \to \tau$ and $P : \tau \to \mathrm{Bool}$
  - This is equivalent to $E^s \cup Q^s = \{a_1 \neq b_1,\ f_{12}(a_1) = c_2\} \cup \{P_2(f_{12}(x_1))\}$
    - $a_1, b_1, x_1 : \tau_1$
    - $c_2 : \tau_2$
    - $f_{12} : \tau_1 \to \tau_2$ and $P : \tau_2 \to \mathrm{Bool}$

  - **u** would derive e.g. $x \mapsto c$ for $E \cup Q$, while for $E^s \cup Q^s$ the instantiation $x_1 \mapsto c_2$ is not well-sorted

Advanced $\mathbf{u}$: entailment checks

Two-layered method for checking whether $E \models \varphi[\bar{x}/\bar{t}]$ holds

- cache of instances already derived
- on-the-fly rewriting of $\varphi[\bar{x}/\bar{t}]$ modulo E
  with extension to other theories through theory-specific rewriting

Advanced $\mathbf{u}$: term ordering

Instances are enumerated according to the order

$$(t_1, \dots, t_n) \prec (s_1, \dots, s_n) \quad \text{if} \quad \begin{cases} \max_{i=1}^n t_i \prec \max_{i=1}^n s_i, \text{ or} \\ \max_{i=1}^n t_i = \max_{i=1}^n s_i \text{ and} \\ \qquad\qquad (t_1, \dots, t_n) \prec_{\text{lex}} (s_1, \dots, s_n) \end{cases}$$

for a given order $\preceq$ on ground terms.

If $a \prec b \prec c$, then

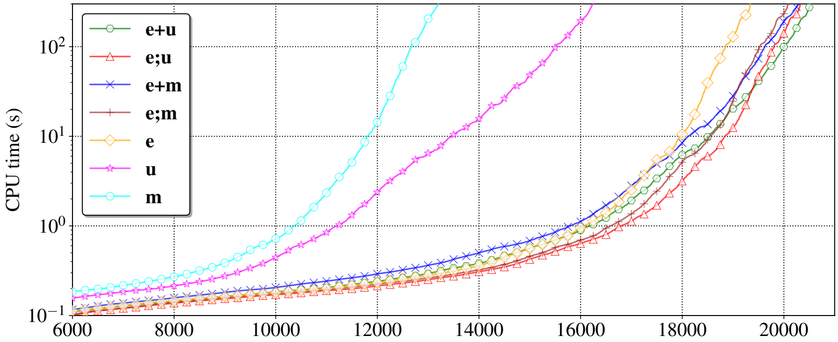
$$(a, a) \prec (a, b) \prec (b, a) \prec (b, b) \prec (a, c) \prec (c, b) \prec (c, c)$$

- instances with c considered only after considering all cases with a and b
- goal is to introduce new terms less often
- order on $\mathcal{T}(E)$ fixed for finite set of terms $t_1 \prec \dots \prec t_n$
  - instantiate in order with $t_1, \dots, t_n$
  - then choose new non-congruent term $t \in \mathcal{T}(E)$ and have $t_n \prec t$
- Still a lot of room for improvement (and ML?) [Janota21]

Outline

Experimental evaluation (UNSAT)

CVC4 configurations on unsatisfiable benchmarks



- 42 065 benchmarks: 14 731 TPTP + 27 334 SMT-LIB
- **e**+**u**: interleave **e** and **u**
- **e**;**u**: apply **e** first, then **u** if it fails
- All CVC4 configurations have **c**; as prefix

Experimental evaluation (SAT)

Library	#	**u**	**e;u**	**e+u**	**e**	**m**	**e;m**	**e+m**
TPTP	14731	471	492	464	17	930	808	829
UF	7293	39	42	42	0	70	69	65
Theories	20041	3	3	3	3	350	267	267
Total	42065	513	537	509	20	1350	1144	1161

Outline

Outline

Conclusion

- Quantifiers in SMT: handled in an ad hoc manner
- Techniques presented here are pure FOL with equality
  (i.e. not "Modulo Theories")
- Reasonably effective nonetheless

Future works and perspectives

- New instantiation techniques (Vampire-like attitude, in SMT?)
- Machine learning
- More convergence with state-of-the-art FOL techniques from saturation theorem proving
- Symbiosis with quantifier elimination for theory reasoning
- Convergence with FOL provers?
- Higher-order logic

Advertisement: European research network on digital proofs

COST EU Action EuroProofNet

`https://europroofnet.github.io/`

EuroProofNet aims at boosting
the interoperability and usability of
proof systems

Outline

Outline

References I

[Althaus09] Ernst Althaus, Evgeny Kruglov, and Christoph Weidenbach. Superposition modulo linear arithmetic SUP(LA). In Silvio Ghilardi and Roberto Sebastiani, editors, *Frontiers of Combining Systems (FroCoS)*, volume 5749 of *Lecture Notes in Computer Science*, pages 84–99. Springer, 2009.

[Baaz01] Matthias Baaz, Uwe Egly, and Alexander Leitsch. Normal form transformations. In John Alan Robinson and Andrei Voronkov, editors, *Handbook of Automated Reasoning*, volume I, chapter 5, pages 273–333. Elsevier Science B.V., 2001.

[Barbosa17] Haniel Barbosa, Pascal Fontaine, and Andrew Reynolds. Congruence closure with free variables. In Axel Legay and Tiziana Margaria, editors, *Tools and Algorithms for Construction and Analysis of Systems (TACAS)*, volume 10206 of *Lecture Notes in Computer Science*, pages 214–230. Springer, 2017.

[Baumgartner14] Peter Baumgartner. Model evolution-based theorem proving. *IEEE Intelligent Systems*, 29(1):4–10, 2014.

[Blanchette19] Jasmin Christian Blanchette, Daniel El Ouraoui, Pascal Fontaine, and Cezary Kaliszyk. Machine Learning for Instance Selection in SMT Solving. In *AITP 2019 - 4th Conference on Artificial Intelligence and Theorem Proving*, Obergurgl, Austria, 2019.

[Bonacina17] Maria Paola Bonacina and David A. Plaisted. Semantically-guided goal-sensitive reasoning: Inference system and completeness. *J. Autom. Reasoning*, 59(2):165–218, 2017.

References II

[deMoura07] Leonardo Mendonça de Moura and Nikolaj Bjørner. Efficient E-matching for SMT solvers. In Frank Pfenning, editor, *CADE*, volume 4603 of *LNCS*, pages 183–198, 2007.

[Detlefs05] David Detlefs, Greg Nelson, and James B. Saxe. Simplify: A Theorem Prover for Program Checking. *J. ACM*, 52(3):365–473, 2005.

[Dross16] Claire Dross, Sylvain Conchon, Johannes Kanig, and Andrei Paskevich. Adding decision procedures to SMT solvers using axioms with triggers. *J. Autom. Reasoning*, 56(4):387–457, 2016.

[Fiori19] Alberto Fiori and Christoph Weidenbach. SCL Clause Learning from Simple Models. *Automated Deduction - CADE 27,*, volume 11716 of *Lecture Notes in Computer Science*, pages 233–249. Springer, 2019.

[Fontaine21] Pascal Fontaine and Hans-Jörg Schurr. Quantifier simplification by unification in SMT. In Boris Konev and Giles Reger, editors, *Frontiers of Combining Systems (FroCoS)*, volume 12941 of *Lecture Notes in Computer Science*, pages 232–249. Springer, 2021.

[Ge09] Yeting Ge and Leonardo Mendonça de Moura. Complete instantiation for quantified formulas in satisfiabiliby modulo theories. In Ahmed Bouajjani and Oded Maler, editors, *Computer Aided Verification (CAV)*, volume 5643 of *Lecture Notes in Computer Science*, pages 306–320. Springer, 2009.

[Halper91] Joseph Y. Halpern. Presburger arithmetic with unary predicates is Π^1_1 complete. *The Journal of Symbolic Logic*, 56(2):637–642, June 1991.

References III

[Janota21] Mikolás Janota, Haniel Barbosa, Pascal Fontaine, and Andrew Reynolds. Fair and adventurous enumeration of quantifier instantiations. In *Formal Methods in Computer Aided Design (FMCAD)*, pages 256–260. IEEE, 2021.

[Korovin13] Konstantin Korovin. Inst-gen - A modular approach to instantiation-based automated reasoning. In Andrei Voronkov and Christoph Weidenbach, editors, *Programming Logics - Essays in Memory of Harald Ganzinger*, volume 7797 of *Lecture Notes in Computer Science*, pages 239–270. Springer, 2013.

[Nonnengart01] Andreas Nonnengart and Christoph Weidenbach. Computing small clause normal forms. In John Alan Robinson and Andrei Voronkov, editors, *Handbook of Automated Reasoning*, volume I, chapter 6, pages 335–367. Elsevier Science B.V., 2001.

[Reynolds18] Andrew Reynolds, Haniel Barbosa, and Pascal Fontaine. Revisiting enumerative instantiation. In Dirk Beyer and Marieke Huisman, editors, *Tools and Algorithms for Construction and Analysis of Systems (TACAS)*, volume 10806 of *Lecture Notes in Computer Science*, pages 112–131. Springer, 2018.

[Reynolds14] Andrew Reynolds, Cesare Tinelli, and Leonardo Mendonça de Moura. Finding conflicting instances of quantified formulas in SMT. In *Formal Methods In Computer-Aided Design (FMCAD)*, pages 195–202. IEEE, 2014.

References IV

[Reynolds13] Andrew Reynolds, Cesare Tinelli, Amit Goel, Sava Krstić, Morgan Deters, and Clark Barrett. Quantifier Instantiation Techniques for Finite Model Finding in SMT. In MariaPaola Bonacina, editor, *Proc. Conference on Automated Deduction (CADE)*, volume 7898 of *Lecture Notes in Computer Science*, pages 377–391. Springer, 2013.

[Voronkov14] Andrei Voronkov. AVATAR: the architecture for first-order theorem provers. In Armin Biere and Roderick Bloem, editors, *Computer Aided Verification (CAV)*, volume 8559 of *Lecture Notes in Computer Science*, pages 696–710. Springer, 2014.