ICCAD 2009 Tutorial - p. 1/78

An Introduction to Satisfiability Modulo Theories

Clark Barrett and Sanjit Seshia

ICCAD 2009 Tutorial - p. 3/78

Theory Solvers

Given a theory T, a *Theory Solver* for T takes as input a set Φ of literals and determines whether Φ is T-satisfiable.

 Φ is T-satisfiable iff there is some model M of T such that each formula in Φ holds in M.

We next consider some examples of theory solvers.

Recall that QF UF is the theory with only equality and uninterpreted function symbols. If Γ is a set of equalities and Δ is a set of disequalities, then the satisfiability of $\Gamma \cup \Delta$ in QF_UF can be determined as follows [NO80, DST80]:

- Let τ be the set of terms appearing in $\Gamma \cup \Delta$.
- Let \sim be the equiavlence relation on τ induced by Γ (i.e. $t_1 \sim t_2$ iff $t_1 = t_2 \in \Gamma$ or $t_2 = t_1 \in \Gamma$).
- Let \sim^* be the *congruence closure* of \sim , obtained by closing ~ with respect to the congruence property:

$$\overline{s} = \overline{t} \to f(\overline{s}) = f(\overline{t}).$$

 $\Gamma \cup \Delta$ is satisfiable iff for each $s \neq t \in \Delta$, $s \nsim^* t$.

ICCAD 2009 Tutorial - p. 5/78

A Solver for QF_UF

union and find are abstract operations for manipulating equivalence classes. union(x,y) makes y the new equivalence class representative for x.

find(x) returns the unique representative for the equivalence class containing x.

 $sig(f(x_1, ..., x_n)) = f(find(x_1), ..., find(x_n)).$ The signature of a term is defined as:

```
if find(a) = find(b) for some a \neq b \in \Delta then
                                                                                                                                                                                                                                                                                         Let A be the set of terms containing
                                                                Remove some equality a=b from \Gamma;
                                                                                                                                                                                                                                                                                                                                                                                                                       if sig(x) = sig(y) for some y then
                                                                                                                                                                                                                                                                                                                                                                                                                                                     Merge(find(x), find(y));
                                                                                               {\sf Merge}({\it find}(a), {\it find}(b));
                                                                                                                                                                                                                                                                                                                              a as an argument
                                                                                                                                                                                                                                                            if a=b then return;
                                                                                                                                                                return False;
                                                                                                                                                                                                                                                                                                                                                                                           foreach x \in A
                                                                                                                                                                                                                                                                                                                                                        union(a,b);
                         while \Gamma 
eq \emptyset
                                                                                                                                                                                           return True;
                                                                                                                                                                                                                            	extit{Merge}(a,b)
\mathcal{CC}(\Gamma,\Delta)
```

ICCAD 2009 Tutorial - p. 7/78

Example

t	$ extit{find}(t)$	$oldsymbol{sig}(t)$
a	a	a
f(a)	f(a)	f(a)
f(f(a))	f(f(a))	f(f(a))
f(f(f(a)))	f(f(f(a)))	f(f(f(a)))
9	9	9
g(a,b)	g(a,b)	g(a,b)
g(f(a),b)	g(f(a),b)	g(f(a),b)

ICCAD 2009 Tutorial – p. 8/78

$$f(f(a)) = a \land f(f(f(a))) = a \land g(a,b) \neq g(f(a),b)$$

t	$ extit{find}(t)$	$oldsymbol{sig}(t)$
a	a	a
f(a)	f(a)	f(a)
f(f(a))	f(f(a))	f(f(a))
f(f(f(a)))	f(f(f(a)))	f(f(f(a)))
9	9	9
g(a,b)	g(a,b)	g(a,b)
g(f(a),b)	g(f(a),b)	g(f(a),b)

ICCAD 2009 Tutorial - p. 9/78

Example

t	$ extit{find}(t)$	$oldsymbol{sig}(t)$
a	a	a
f(a)	f(a)	f(a)
f(f(a))	a	f(f(a))
f(f(f(a)))	f(f(f(a)))	f(f(f(a)))
9	9	9
g(a,b)	g(a,b)	g(a,b)
g(f(a),b)	g(f(a),b)	g(f(a),b)

ICCAD 2009 Tutorial - p. 10/78

Example

t	$ extit{find}(t)$	$oldsymbol{sig}(t)$
a	a	a
f(a)	f(a)	f(a)
f(f(a))	a	f(f(a))
f(f(f(a)))	f(f(f(a)))	f(f(f(a)))
9	9	9
g(a,b)	g(a,b)	g(a,b)
g(f(a),b)	g(f(a),b)	g(f(a),b)

ICCAD 2009 Tutorial - p. 11/78

$$f(f(a)) = a \land f(f(f(a))) = a \land g(a,b) \neq g(f(a),b)$$

t	$ extit{find}(t)$	$\pmb{\mathit{sig}}(t)$
a	a	p
f(a)	f(a)	f(a)
f(f(a))	a	f(f(a))
f(f(f(a)))	f(f(f(a)))	f(a)
9	9	9
g(a,b)	g(a,b)	g(a,b)
g(f(a),b)	g(f(a),b)	g(f(a),b)

ICCAD 2009 Tutorial - p. 12/78

$$f(f(a)) = a \land f(f(f(a))) = a \land g(a,b) \neq g(f(a),b)$$

t	find(t)	$\pmb{\mathit{sig}}(t)$
a	a	p
f(a)	f(a)	f(a)
f(f(a))	a	f(f(a))
f(f(f(a)))	f(f(f(a)))	f(a)
9	9	9
g(a,b)	g(a,b)	g(a,b)
g(f(a),b)	g(f(a),b)	g(f(a),b)

ICCAD 2009 Tutorial - p. 13/78

Example

t	$\mathit{find}(t)$	$\pmb{\mathit{sig}}(t)$
a	a	p
f(a)	f(a)	f(a)
f(f(a))	a	f(f(a))
f(f(f(a)))	f(a)	f(a)
9	9	q
g(a,b)	g(a,b)	g(a,b)
g(f(a),b)	g(f(a),b)	g(f(a),b)

ICCAD 2009 Tutorial - p. 14/78

Example

t	$\mathit{find}(t)$	$\pmb{\mathit{sig}}(t)$
a	a	a
f(a)	f(a)	f(a)
f(f(a))	a	f(f(a))
f(f(f(a)))	f(a)	f(a)
9	9	9
g(a,b)	g(a,b)	g(a,b)
g(f(a),b)	g(f(a),b)	g(f(a),b)

ICCAD 2009 Tutorial - p. 15/78

$$f(f(a)) = a \land f(f(f(a))) = a \land g(a,b) \neq g(f(a),b)$$

t	$ extit{find}(t)$	$\pmb{\mathit{sig}}(t)$
a	p	p
f(a)	f(a)	f(a)
f(f(a))	a	f(f(a))
f(f(f(a)))	f(a)	f(a)
9	9	9
g(a,b)	g(a,b)	g(a,b)
g(f(a),b)	g(f(a),b)	g(f(a),b)

ICCAD 2009 Tutorial - p. 16/78

$$f(f(a)) = a \land f(f(f(a))) = a \land g(a,b) \neq g(f(a),b)$$

t	$\mathit{find}(t)$	$\pmb{\mathit{sig}}(t)$
a	a	p
f(a)	a	f(a)
f(f(a))	a	f(f(a))
f(f(f(a)))	a	f(a)
9	9	9
g(a,b)	g(a,b)	g(a,b)
g(f(a),b)	g(f(a),b)	g(f(a),b)

ICCAD 2009 Tutorial - p. 17/78

Example

t	$ extit{find}(t)$	$\pmb{sig}(t)$
a	p	a
f(a)	a	f(a)
f(f(a))	a	f(f(a))
f(f(f(a)))	a	f(a)
9	q	9
g(a,b)	g(a,b)	g(a,b)
g(f(a),b)	g(f(a),b)	g(f(a),b)

ICCAD 2009 Tutorial - p. 18/78

$$f(f(a)) = a \land f(f(f(a))) = a \land g(a,b) \neq g(f(a),b)$$

t	find(t)	$\mathbf{Sig}(t)$
a	a	a
f(a)	a	f(a)
f(f(a))	a	f(a)
f(f(f(a)))	a	f(a)
9	q	9
g(a,b)	g(a,b)	g(a,b)
g(f(a),b)	g(f(a),b)	g(a,b)

$$f(f(a)) = a \land f(f(f(a))) = a \land g(a,b) \neq g(f(a),b)$$

t	find(t)	$\mathbf{Sig}(t)$
a	a	a
f(a)	a	f(a)
f(f(a))	a	f(a)
f(f(f(a)))	a	f(a)
9	9	q
g(a,b)	g(a,b)	g(a,b)
g(f(a),b)	g(f(a),b)	g(a,b)

$$f(f(a)) = a \land f(f(f(a))) = a \land g(a,b) \neq g(f(a),b)$$

t	$ extit{find}(t)$	$oldsymbol{sig}(t)$
a	a	a
f(a)	a	f(a)
f(f(a))	a	f(a)
f(f(f(a)))	a	f(a)
9	9	9
g(a,b)	g(a,b)	g(a,b)
g(f(a),b)	g(a,b)	g(a,b)

ICCAD 2009 Tutorial - p. 21/78

$$f(f(a)) = a \land f(f(f(a))) = a \land g(a,b) \neq g(f(a),b)$$

t	$\mathit{find}(t)$	$oldsymbol{sig}(t)$
a	a	a
f(a)	a	f(a)
f(f(a))	a	f(a)
f(f(f(a)))	a	f(a)
9	9	9
g(a,b)	g(a,b)	g(a,b)
g(f(a),b)	g(a,b)	g(a,b)

ICCAD 2009 Tutorial - p. 22/78

Example

t	$ extit{find}(t)$	$oldsymbol{sig}(t)$
a	a	a
f(a)	a	f(a)
f(f(a))	a	f(a)
f(f(f(a)))	a	f(a)
9	q	9
g(a,b)	g(a,b)	g(a,b)
g(f(a),b)	g(a,b)	g(a,b)

Example

$$f(f(a)) = a \land f(f(f(a))) = a \land g(a,b) \neq g(f(a),b)$$

t	find(t)	$\mathbf{Sig}(t)$
a	a	a
f(a)	a	f(a)
f(f(a))	a	f(a)
f(f(f(a)))	a	f(a)
9	9	9
g(a,b)	g(a,b)	g(a,b)
g(f(a),b)	g(a,b)	g(a,b)

 $\mathit{find}(g(a,b)) = \mathit{find}(g(f(a),b)) \rightarrow \mathit{Unsatisfiable}$