An Introduction to Satisfiability Modulo Theories

Clark Barrett and Sanjit Seshia

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.

Congruence Closure and QF_UF

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 $\sim$ with respect to the congruence property:

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

- $\Gamma \cup \Delta$ is satisfiable iff for each $s \neq t \in \Delta$, $s \not\sim^* t$.

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.

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

A Solver for QF_UF

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

Example

$$f(f(a)) = a \;\wedge\; f(f(f(a))) = a \;\wedge\; g(a,b) \neq g(f(a),b)$$

t	find(t)	sig(t)
a	a	a
$f(a)$	$f(a)$	$f(a)$
$f(f(a))$	$f(f(a))$	$f(f(a))$
$f(f(f(a)))$	$f(f(f(a)))$	$f(f(f(a)))$
b	b	b
$g(a,b)$	$g(a,b)$	$g(a,b)$
$g(f(a),b)$	$g(f(a),b)$	$g(f(a),b)$

Example

$$f(f(a)) = a \;\wedge\; f(f(f(a))) = a \;\wedge\; g(a,b) \neq g(f(a),b)$$

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

Example

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

t	find(t)	sig(t)
a	a	a
$f(a)$	$f(a)$	$f(a)$
$f(f(a))$	a	$f(f(a))$
$f(f(f(a)))$	$f(f(f(a)))$	$f(f(f(a)))$
b	b	b
$g(a,b)$	$g(a,b)$	$g(a,b)$
$g(f(a),b)$	$g(f(a),b)$	$g(f(a),b)$

Example

$$f(f(a)) = a \;\wedge\; f(f(f(a))) = a \;\wedge\; g(a,b) \neq g(f(a),b)$$

t	find(t)	sig(t)
a	a	a
$f(a)$	$f(a)$	$f(a)$
$f(f(a))$	a	$f(f(a))$
$f(f(f(a)))$	$f(f(f(a)))$	$f(f(f(a)))$
b	b	b
$g(a,b)$	$g(a,b)$	$g(a,b)$
$g(f(a),b)$	$g(f(a),b)$	$g(f(a),b)$

Example

$$f(f(a)) = a \;\wedge\; f(f(f(a))) = a \;\wedge\; g(a,b) \neq g(f(a),b)$$

t	find(t)	sig(t)
a	a	a
$f(a)$	$f(a)$	$f(a)$
$f(f(a))$	a	$f(f(a))$
$f(f(f(a)))$	$f(f(f(a)))$	$f(a)$
b	b	b
$g(a,b)$	$g(a,b)$	$g(a,b)$
$g(f(a),b)$	$g(f(a),b)$	$g(f(a),b)$

Example

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

t	find(t)	sig(t)
a	a	a
$f(a)$	$f(a)$	$f(a)$
$f(f(a))$	a	$f(f(a))$
$f(f(f(a)))$	$f(f(f(a)))$	$f(a)$
b	b	b
$g(a,b)$	$g(a,b)$	$g(a,b)$
$g(f(a),b)$	$g(f(a),b)$	$g(f(a),b)$

Example

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

t	*find*(t)	*sig*(t)
a	a	a
$f(a)$	$f(a)$	$f(a)$
$f(f(a))$	a	$f(f(a))$
$f(f(f(a)))$	$f(a)$	$f(a)$
b	b	b
$g(a,b)$	$g(a,b)$	$g(a,b)$
$g(f(a),b)$	$g(f(a),b)$	$g(f(a),b)$

Example

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

t	find(t)	sig(t)
a	a	a
$f(a)$	$f(a)$	$f(a)$
$f(f(a))$	a	$f(f(a))$
$f(f(f(a)))$	$f(a)$	$f(a)$
b	b	b
$g(a,b)$	$g(a,b)$	$g(a,b)$
$g(f(a),b)$	$g(f(a),b)$	$g(f(a),b)$

Example

$$f(f(a)) = a \;\wedge\; f(f(f(a))) = a \;\wedge\; g(a,b) \neq g(f(a),b)$$

t	find(t)	sig(t)
a	a	a
$f(a)$	$f(a)$	$f(a)$
$f(f(a))$	a	$f(f(a))$
$f(f(f(a)))$	$f(a)$	$f(a)$
b	b	b
$g(a,b)$	$g(a,b)$	$g(a,b)$
$g(f(a),b)$	$g(f(a),b)$	$g(f(a),b)$

Example

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

t	find(t)	sig(t)
a	a	a
$f(a)$	a	$f(a)$
$f(f(a))$	a	$f(f(a))$
$f(f(f(a)))$	a	$f(a)$
b	b	b
$g(a,b)$	$g(a,b)$	$g(a,b)$
$g(f(a),b)$	$g(f(a),b)$	$g(f(a),b)$

Example

$$f(f(a)) = a \;\wedge\; f(f(f(a))) = a \;\wedge\; g(a,b) \neq g(f(a),b)$$

t	*find*(t)	*sig*(t)
a	a	a
$f(a)$	a	$f(a)$
$f(f(a))$	a	$f(f(a))$
$f(f(f(a)))$	a	$f(a)$
b	b	b
$g(a,b)$	$g(a,b)$	$g(a,b)$
$g(f(a),b)$	$g(f(a),b)$	$g(f(a),b)$

Example

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

t	find(t)	sig(t)
a	a	a
$f(a)$	a	$f(a)$
$f(f(a))$	a	$f(a)$
$f(f(f(a)))$	a	$f(a)$
b	b	b
$g(a,b)$	$g(a,b)$	$g(a,b)$
$g(f(a),b)$	$g(f(a),b)$	$g(a,b)$

Example

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

t	find(t)	sig(t)
a	a	a
$f(a)$	a	$f(a)$
$f(f(a))$	a	$f(a)$
$f(f(f(a)))$	a	$f(a)$
b	b	b
$g(a,b)$	$g(a,b)$	$g(a,b)$
$g(f(a),b)$	$g(f(a),b)$	$g(a,b)$

Example

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

t	find(t)	sig(t)
a	a	a
$f(a)$	a	$f(a)$
$f(f(a))$	a	$f(a)$
$f(f(f(a)))$	a	$f(a)$
b	b	b
$g(a,b)$	$g(a,b)$	$g(a,b)$
$g(f(a),b)$	$g(a,b)$	$g(a,b)$

Example

$$f(f(a)) = a \;\wedge\; f(f(f(a))) = a \;\wedge\; g(a,b) \neq g(f(a),b)$$

t	find(t)	sig(t)
a	a	a
$f(a)$	a	$f(a)$
$f(f(a))$	a	$f(a)$
$f(f(f(a)))$	a	$f(a)$
b	b	b
$g(a,b)$	$g(a,b)$	$g(a,b)$
$g(f(a),b)$	$g(a,b)$	$g(a,b)$

Example

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

t	find(t)	sig(t)
a	a	a
$f(a)$	a	$f(a)$
$f(f(a))$	a	$f(a)$
$f(f(f(a)))$	a	$f(a)$
b	b	b
$g(a,b)$	$g(a,b)$	$g(a,b)$
$g(f(a),b)$	$g(a,b)$	$g(a,b)$

Example

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

t	$\textit{find}(t)$	$\textit{sig}(t)$
a	a	a
$f(a)$	a	$f(a)$
$f(f(a))$	a	$f(a)$
$f(f(f(a)))$	a	$f(a)$
b	b	b
$g(a,b)$	$g(a,b)$	$g(a,b)$
$g(f(a),b)$	$g(a,b)$	$g(a,b)$

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