Automated Reasoning 2018

Lecture 19: Theory combination

Instructor: Ashutosh Gupta

IITB, India

Compile date: 2018-10-10

Theory combination

A formula may have terms that involved multiple theories.

Example 19.1

$$\neg P(y) \wedge s \approx store(t, i, 0) \wedge x - y - z \approx 0 \wedge$$
$$z + s[i] \approx f(x - y) \wedge P(x - f(f(z)))$$

The above formula involves theory of

- *equality* $\mathcal{T}_E$
- *linear integer arithmetic* $\mathcal{T}_Z$
- *arrays* $\mathcal{T}_A$

How to check satisfiability of the formula?

Combination solving

Let suppose a formula refers to theories $\mathcal{T}_1$,....,$\mathcal{T}_k$.

We will assume that we have decision procedures for each quantifier-free $\mathcal{T}_i$.

We will present a method that combines the decision procedures and provides a decision procedure for quantifier-free $Cn(\mathcal{T}_1 \cup \ldots \cup \mathcal{T}_k)$.

Topic 19.1

Nelson-Oppen method

Nelson-Oppen method conditions

The Nelson-Oppen method combines theories that satisfy the following conditions

1. The signatures $\mathbf{S}_i$ are disjoint.
2. The theories are stably infinite
3. The formulas are conjunction of quantifier-free literals

Stably infinite theories

Definition 19.1

A theory is stably infinite if each quantifier-free satisfiable formula under the theory is satisfiable in an infinite model.

Example 19.2

Let us suppose we have the following axiom in a theory

$$\forall x, y, z. \, (x \approx y \vee y \approx z \vee z \approx x)$$

The above formula says that there are at most two elements in the domain of a satisfying model. Therefore, the theory is not stably infinite.

Nelson-Oppen method terminology I

We call a function of predicate in $\mathbf{S}_i$ is i-symbol.

Definition 19.2

A term t is an i-term if the top symbol is an i-symbol.

Definition 19.3

An i-atom is

- *an i-predicate atom,*
- *$s \approx t$, where s is an i-term, or*
- *$v \approx t$, v is a variable and t is an i-term.*

Definition 19.4

An i-literal is an i-atom or the negation of one.

Exercise 19.1

Let $\mathcal{T}_E$, $\mathcal{T}_Z$, and $\mathcal{T}_A$ are involved in a formula.

- $x + y$ *is*
- $store(A, x, f(x + y))$ *is*
- $A[3] \leq f(x)$ *is*
- $f(x) \approx 3 + y$ *is*
- $z \approx 3 + y$ *is*
- $z \not\approx 3 + y$ *is*

Nelson-Oppen method terminology II

Definition 19.5
An occurrence of a term t in either an i-term/literal is i-alien if t is a j-term with $i \neq j$ and all of its super-terms (if any) are i-terms.

Definition 19.6
An expression is pure if it contains only variables and i-symbols for some i.

Exercise 19.2
Let $\mathcal{T}_E$, $\mathcal{T}_Z$, and $\mathcal{T}_A$ are involved in a formula. Find the alien term.

- In $A[3] \approx f(x)$,
- In $z \approx 3 + y$,
- In $f(x) \neq f(2)$,
- In $f(x) \approx A[3]$,
- In $store(a, x + y, f(z))$,

Nelson-Oppen method: convert to separate form

Let input F be conjunction of literals.
We produce an equiv-satisfiable $F_1 \wedge \cdots \wedge F_k$ such that F_i is a $\mathcal{T}_i$ formula.

1. Pick an i-literal $\ell \in F$ for some i. $F := F - \{\ell\}$.
2. If ℓ is pure, $F_i := F_i \cup \{\ell\}$.
3. Otherwise, there is a term t occurring i-alien in ℓ.
   Let z be a fresh variable. $F := F \cup \{\ell[t \mapsto z], z \approx t\}$.
4. go to step 1.

Example 19.3

Consider $1 \leq x \leq 2 \wedge f(x) \not\approx f(2) \wedge f(x) \not\approx f(1)$ *of theory* $Cn(\mathcal{T}_E \cup \mathcal{T}_Z)$.

Alien terms are $\{2, 1\}$.

In separate form,
$F_E = f(x) \not\approx f(z) \wedge f(x) \not\approx f(y)$
$F_Z = 1 \leq x \leq 2 \wedge y \approx 1 \wedge z \approx 2$

Theory solvers need to coordinate

Let DP_i be the decision procedure of theory $\mathcal{T}_i$.

F is unsatisfiable if for some i, $DP_i(F_i)$ returns unsatisfiable.

However, if all $DP_i(F_i)$ return satisfiable, we can not guarantee satisfiability.

The decision procedures need to coordinate to check the satisfiability.

Equivalence constraints

Definition 19.7
Let S be a set of terms and equivalence relation $\sim$ over S.

$$F[\sim] := \bigwedge\{t \approx s | t \sim s\} \wedge \bigwedge\{t \not\approx s | t \not\sim s\}$$

$F[\sim]$ will be used for the coordination.

Non-deterministic Nelson-Oppen method

Let $\mathcal{T}_1$ and $\mathcal{T}_2$ be two theories with disjoint signature.

Let F be a conjunction of literals for theory $Cn(\mathcal{T}_1 \cup \mathcal{T}_2)$.

1. Convert F to separate form $F_1 \land F_2$.
2. Guess an equivalence relation $\sim$ over variables $vars(F_1) \cap vars(F_2)$.
3. Run $DP_1(F_1 \land F[\sim])$
4. Run $DP_2(F_2 \land F[\sim])$

If there is a $\sim$ such that both steps 3 and 4 return satisfiable, F is satisfiable.

Otherwise F is unsatisfiable.

Exercise 19.3

Extend the above method for k theories.

Example: non-deterministic Nelson-Oppen method

Example 19.4

We had the following formula in separate form.
$F_E = f(x) \not\approx f(z) \land f(x) \not\approx f(y)$
$F_Z = 1 \leq x \leq 2 \land y \approx 1 \land z \approx 2$

Common variables x, y, and z.

Five potential $F[\sim]$s

1. $x \approx y \land y \approx z \land z \approx x$: *Inconsistent with F_E*
2. $x \approx y \land y \not\approx z \land z \not\approx x$: *Inconsistent with F_E*
3. $x \not\approx y \land y \not\approx z \land z \approx x$: *Inconsistent with F_E*
4. $x \not\approx y \land y \approx z \land z \not\approx x$: *Inconsistent with F_Z*
5. $x \not\approx y \land y \not\approx z \land z \not\approx x$: *Inconsistent with F_Z*

Since all $\sim$ are causing inconsistency, the formula is unsatisfiable.

Topic 19.2

Correctness of Nelson-Oppen

model and assignment

We have noticed if there are no quantifiers, variables behave like constants.

In the lecture, we will refer models and assignments together as models.

Definition 19.8

Let m be a model of signature $\mathbf{S}$ and variables V. Let $m|_{\mathbf{S}',V'}$ be the restriction of A to the symbols in $\mathbf{S}'$ and the variables in V'.

Homomorphisms and isomorphism of models

Definition 19.9

Consider signature $\mathbf{S} = (\mathbf{F}, \mathbf{R})$ *and a variables* V. *Let* m *and* m' *be* $\mathbf{S}, V$*-models. A function* $h : D_m \rightarrow D_{m'}$ *is a homomorphism of* m *into* m' *if the following holds.*

- *for each* $f/n \in \mathbf{F}$, *for each* $(d_1, .., d_n) \in D_m^n$

$$h(f_m(d_1, .., d_n)) = f_{m'}(h(d_1), .., h(d_n))$$

- *for each* $P/n \in \mathbf{R}$, *for each* $(d_1, .., d_n) \in D_m^n$

$$(d_1, .., d_n) \in P_m \quad iff \quad (h(d_1), .., h(d_n)) \in P_{m'}$$

- *for each* $v \in V$, $h(v_m) = v_{m'}$

Definition 19.10

A homomorphism h *of* m *into* m' *is called isomorphism if* h *is one-to-one.* m *and* m' *are called isomorphic if an* h *exists that is also onto.*

Isomorphic models ensure combined satisfiability

Theorem 19.1

Let F_i be a $\mathbf{S}_i$-formula with variables V_i for $i \in \{1,2\}$. $F_1 \wedge F_2$ is satisfiable iff there are $m_1 \models F_1$ and $m_2 \models F_2$ such that

$$m_1|_{\mathbf{S}_1 \cap \mathbf{S}_2, V_1 \cap V_2} \text{ is isomorphic to } m_2|_{\mathbf{S}_1 \cap \mathbf{S}_2, V_1 \cap V_2}.$$

Proof.

($\Rightarrow$) trivial.(why?)

($\Leftarrow$).
We have models $m_1 \models F_1$ and $m_2 \models F_2$.
Let h be the onto isomorphism from $m_1|_{\mathbf{S}_1 \cap \mathbf{S}_2, V_1 \cap V_2}$ to $m_2|_{\mathbf{S}_1 \cap \mathbf{S}_2, V_1 \cap V_2}$.

We construct a model m for $F_1 \wedge F_2$. ...

Isomorphic models ensure combined satisfiability II

Proof(contd.)

Let $D_m = D_{m_1}$ and $m|_{\mathbf{S}_1,V_1} = m_1$.

For $v \in V_2 - V_1$, $v_m = h^{-1}(v_{m_2})$

For $f/n \in \mathbf{S}_2 - \mathbf{S}_1$, $f_m(d_1, .., d_n) = h^{-1}(f_{m_2}(h(d_1), .., h(d_n)))$

... similarly for predicates.

Clearly $m \models F_1$. We can easily check $m \models F_2$.

Therefore, $m \models F_1 \wedge F_2$. □

Equality preserving models ensure combined satisfiability

Theorem 19.2

Let F_i be a $\mathbf{S}_i$-formula with variables V_i for $i \in \{1, 2\}$. Let $\mathbf{S}_1 \cap \mathbf{S}_2 = \emptyset$.
$F_1 \wedge F_2$ is satisfiable iff there are $m_1 \models F_1$ and $m_2 \models F_2$ such that

- $|D_{m_1}| = |D_{m_2}|$ *and*
- $x_{m_1} = y_{m_1}$ *iff* $x_{m_2} = y_{m_2}$ *for each* $x, y \in V_1 \cap V_2$

Proof.

($\Rightarrow$) trivial.(why?)

($\Leftarrow$).
Let $V_m = \{v_m | v \in V\}$.
Let $h : (V_1 \cap V_2)_{m_1} \rightarrow (V_1 \cap V_2)_{m_2}$ be defined as follows

$$h(v_{m_1}) := v_{m_2} \qquad \text{for each } v \in V_1 \cap V_2.$$

h is well-defined(why?), one-to-one(why?), and onto(why?). ...

Exercise 19.4 *Prove the above whys*

Equality preserving models ensure combined satisfiability II

Proof(contd.)

Therefore, $|(V_1 \cap V_2)_{m_1}| = |(V_1 \cap V_2)_{m_2}|$

Therefore, $|D_{m_1} - (V_1 \cap V_2)_{m_1}| = |D_{m_2} - (V_1 \cap V_2)_{m_2}|$

Therefore, we can extend h to $h' : D_{m_1} \mapsto D_{m_2}$ that is one-to-one and onto.(why?)

By construction, h' is isomorphism from $m_1|_{V_1 \cap V_2}$ to $m_2|_{V_1 \cap V_2}$.

Therefore, by the previous theorem, $F_1 \wedge F_2$ is satisfiable. $\square$

Nelson-Oppen correctness

Theorem 19.3

Let $\mathcal{T}_i$ be stably infinite $\mathbf{S}_i$-theory and F_i be $\mathbf{S}_i$ a formula with variables V_i for $i \in \{1, 2\}$. Let $\mathbf{S}_1 \cap \mathbf{S}_2 = \emptyset$. $F_1 \wedge F_2$ is $Cn(\mathcal{T}_1 \cup \mathcal{T}_2)$-satisfiable iff there is an equivalence relation $\sim$ over $V_1 \cap V_2$ such that $F_i \wedge F[\sim]$ is $\mathcal{T}_i$-satisfiable.

Proof.

($\Rightarrow$) trivial.(why?)

($\Leftarrow$). Suppose there is $\sim$ over $V_1 \cap V_2$ such that $F_i \wedge F[\sim]$ is $\mathcal{T}_i$-satisfiable.

Since $\mathcal{T}_i$ is stably infinite, there is an infinite model $m_i \models F_i \wedge F[\sim]$.

Due to LST (a standard theorem), $|m_1|$ and $|m_2|$ are infinity of same size.

Due to $m_1 \models F[\sim]$ and $m_2 \models F[\sim]$, $x_{m_1} = y_{m_1}$ iff $x_{m_2} = y_{m_2}$ for each $x, y \in V_1 \cap V_2$.

Due to the previous theorem, $F_1 \wedge F_2$ is $Cn(\mathcal{T}_1 \cup \mathcal{T}_2)$-satisfiable. □

Topic 19.3

Implementation of Nelson-Oppen

No need for explicit separation step

Instead of introducing the fresh names, we may keep the record of alien occurrences.

In DP_i, we need to treat alien occurrences as constants.

Example 19.5

Consider $\neg P(y) \land s \approx store(t, i, 0) \land x - y - z \approx 0 \land$
$z + s[i] \approx f(x - y) \land P(x - f(f(z)))$

We can separate the formulas and keep the record of alien terms
$F_E = \neg P(y) \land P(x - f(f(z)))$
$F_Z = x - y - z \approx 0 \land z + s[i] \approx f(x - y)$
$F_A = s \approx store(t, i, 0)$

Alien terms or shared variables:
$\{s[i], x - y, f(x - y), 0, y, z, f(f(z)), x - f(f(z))\}$

Searching $\sim$

Enumerating all $\sim$ is very expensive.

Exercise 19.5

Let $|S| = n$*. How many* $\sim$ *are there?*

The goal is to minimize the search.

- Reduce the size of S
- Efficient strategy of finding $\sim$

Reduce size of S

We apply simplifications in the formula and replace alien terms with native terms as much as possible.

Efficient search for $\sim$

Incremental construction of $\sim$ and backtrack if a theory finds inconsistency.

Ensure early detection of inconsistency.

For convex theories, this strategy is very efficient. Otherwise, we may have to explore the entire search space.

Definition 19.11

$\mathcal{T}$ is convex if for a conjunction literals F and variables $x_1, \dots, x_n$, $y_1, \dots, y_n$, $F \Rightarrow_{\mathcal{T}} x_1 \approx y_1 \vee \dots \vee x_n \approx y_n$ implies for some $i \in 1..n$

$$F \Rightarrow_{\mathcal{T}} x_i \approx y_i$$

Help from DP_is

We can use the theory decision procedures to find $\sim$.

DP_i can help us by providing currently implied (dis)equalities.

1. Pick an i-literal $\ell \in F$ for some i. $F := F - \{\ell\}$.
2. Simplify ℓ to ℓ' in current context
3. $F_i := F_i \cup \{\ell'\}$.
4. Add term t occurring i-alien in ℓ' to S.
5. For each $s, t \in S$, check if $F_i \Rightarrow t \approx s$ or $F_i \Rightarrow t \not\approx s$.
   Add the facts to F.
6. go to step 1.

Now we need to explore far reduced space for $\sim$ that are consistent with F_is.

Lazy $\sim$ search

The system maintains the current $\sim$ that is consistent with the current (dis)equalities present in the $F \cup F_i$s. Minimally updates it for new literals.

1. Pick an i-literal $\ell \in F$ for some i. $F := F - \{\ell\}$.
2. Simplify ℓ to ℓ' in current context
3. $F_i := F_i \cup \{\ell'\}$.
4. Add term t occurring i-alien in ℓ' to S.
5. If $F_i \wedge F[\sim]$ is unsatisfiable, Find (dis)equation literal ℓ'' such that $F_i \Rightarrow \ell''$ and $\ell'' \wedge F[\sim]$ is unsatisfiable.
    - Add the ℓ'' to F.
    - Update $\sim$ to make it compatible with ℓ'
6. go to step 1.

Finding ℓ'' is called interpolation

The above is a lazier version of the earlier algorithm.

C. Barrett.Checking Validity of Quantifier-Free Formulas in Combinations of First-Order Theories. PhD thesis, Stanford University,03

End of Lecture 19