Automated Reasoning 2020

Lecture 21: Theory combination

Instructor: Ashutosh Gupta

IITB, India

Compile date: 2020-11-13

Theory combination

A formula may have terms that involved multiple theories.

Example 21.1

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

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 21.1

Nelson-Oppen method

Nelson-Oppen method conditions

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

1. The signatures S_i are disjoint.
2. The theories are stably infinite
3. The formulas are conjunction of quantifier-free literals

Stably infinite theories

Definition 21.1

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

Example 21.2

Let us suppose we have the following axiom in a theory

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

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 S_i is i-symbol.

Definition 21.2

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

Definition 21.3

An i-atom is

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

Definition 21.4

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

Exercise 21.1

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*
- $f(x) = 3 + y$ *is*
- $z = 3 + y$ *is*
- $z \neq 3 + y$ *is*

Nelson-Oppen method terminology II

Definition 21.5

An occurrence of a term t in i-term/literal is i-alien if t is a j-term for $i \neq j$ and all of its super-terms are i-terms.

Definition 21.6

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

Exercise 21.2

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

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

Nelson-Oppen method: convert to separate form

Let F be a 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. $F := F \cup \{\ell[t \mapsto z], z = t\}$.
4. go to step 1.

Example 21.3

Consider $1 \leq x \leq 2 \wedge f(x) \neq f(2) \wedge f(x) \neq f(1)$ *of theory* $Cn(\mathcal{T}_E \cup \mathcal{T}_Z)$.

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

In separate form, $F_E = f(x) \neq f(z) \wedge f(x) \neq f(y)$ $F_Z = 1 \leq x \leq 2 \wedge y = 1 \wedge z = 2$

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 21.7
Let S be a set of terms and equivalence relation $\sim$ over S.

$$F[\sim] := \bigwedge\{t = s | t \sim s \text{ and } t, s \in S\} \land \bigwedge\{t \neq s | t \not\sim s \text{ and } t, s \in S\}$$

$F[\sim]$ 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 $F_1 \wedge F_2$.
2. Guess an equivalence relation $\sim$ over variables $vars(F_1) \cap vars(F_2)$.
3. Run $DP_1(F_1 \wedge F[\sim])$
4. Run $DP_2(F_2 \wedge F[\sim])$

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

Otherwise F is unsatisfiable.

Exercise 21.3

Extend the above method for k theories.

Example: non-deterministic Nelson-Oppen method

Example 21.4

We had the following formula in separate form.

$F_E = f(x) \neq f(z) \wedge f(x) \neq f(y)$ $\qquad$ $F_Z = 1 \leq x \leq 2 \wedge y = 1 \wedge z = 2$

Common variables x, y, and z.

Five potential $F[\sim]$s

1. $x = y \wedge y = z \wedge z = x$: *Inconsistent with* F_E
2. $x = y \wedge y \neq z \wedge z \neq x$: *Inconsistent with* F_E
3. $x \neq y \wedge y \neq z \wedge z = x$: *Inconsistent with* F_E
4. $x \neq y \wedge y = z \wedge z \neq x$: *Inconsistent with* F_Z
5. $x \neq y \wedge y \neq z \wedge z \neq x$: *Inconsistent with* F_Z

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

Topic 21.2

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 21.8

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

Homomorphisms and isomorphism of models

Definition 21.9

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

- *for each* $f/n \in \mathsf{F}$ *and* $(d_1, .., d_n) \in D_m^n$, $h(f_m(d_1, .., d_n)) = f_{m'}(h(d_1), .., h(d_n))$
- *for each* $P/n \in \mathsf{R}$ *and* $(d_1, .., d_n) \in D_m^n$, $(d_1, .., d_n) \in P_m$ *iff* $(h(d_1), .., h(d_n)) \in P_{m'}$
- *for each* $v \in V$, $h(v_m) = v_{m'}$

Definition 21.10

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 21.1

Let F_i be a 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

$$m_1|_{S_1 \cap S_2, V_1 \cap V_2} \textit{ is isomorphic to } m_2|_{S_1 \cap S_2, V_1 \cap V_2}.$$

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 $m_1|_{S_1 \cap S_2, V_1 \cap V_2}$ to $m_2|_{S_1 \cap S_2, V_1 \cap V_2}$.

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 $m|_{\mathsf{S}_1, V_1} = m_1$.

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

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

... similarly for predicates.

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

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

Equality preserving models ensure combined satisfiability

Theorem 21.2

Let F_i be a S_i-formula with variables V_i for $i \in \{1,2\}$. Let $S_1 \cap S_2 = \emptyset$. $F_1 \wedge F_2$ 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 $h : (V_1 \cap V_2)_{m_1} \to (V_1 \cap V_2)_{m_2}$ 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 21.4 *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 21.3

Let $\mathcal{T}_i$ be stably infinite S_i-theory and F_i be S_i a formula with variables V_i for $i \in \{1, 2\}$. Let $\mathrm{S}_1 \cap \mathrm{S}_2 = \emptyset$. $F_1 \wedge F_2$ 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. $\square$

Topic 21.3

Implementation of Nelson-Oppen

Searching $\sim$

Enumerating $\sim$ over shared variables S is very expensive.

Exercise 21.5

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

The goal is to minimize the search.

- Reduce the size of S by simplify simplification formulas.
- Efficient strategy of finding $\sim$

Commentary: In the simplification, we replace alien terms with native terms as much as possible.

Efficient search for $\sim$

We can use DPLL like search for $\sim$.

- Decision: Incrementally add a (dis)equality in $\sim$.
- Backtracking: backtrack if a theory finds inconsistency and ensure early detection of inconsistency.
- Propagation: If an (dis)equality is implied by a current $F_i \wedge F[\sim]$ add them to $\sim$.

For convex theories, this strategy is very efficient. There is no need for decisions.

Commentary: We have a choice in the propagation step. We may be eager or lazy for deriving equalities. Eager propagation may require a lot of work in each theory. During backtracking we can use interpolation based method to lazily identify inferred equality/disequalities. C. Barrett.Checking Validity of Quantifier-Free Formulas in Combinations of First-Order Theories. PhD thesis, Stanford University,03

Convex theories

Definition 21.11
$\mathcal{T}$ is convex if for a conjunction literals F and variables $x_1, \dots, x_n$, $y_1, \dots, y_n$, $F \Rightarrow_{\mathcal{T}} x_1 = y_1 \lor \dots \lor x_n = y_n$ implies for some $i \in 1..n$, $F \Rightarrow_{\mathcal{T}} x_i = y_i$.

Example 21.5
$\mathcal{T}_{\mathbb{Q}}$ is convex and unfortunately $\mathcal{T}_{\mathbb{Z}}$ is not convex. Consider the following implication in $\mathcal{T}_{\mathbb{Z}}$.

$$1 \leq x \leq 2 \land y = 1 \land z = 2 \Rightarrow y = x \lor z = x$$

From the above we can not conclude that the LHS implies any of the equality in RHS.

Exercise 21.6
Is the theory of arrays convex?Hint: apply axiom 2

Exercise 21.7
Prove that if all theories are convex, there is no need for decision step in the previous slide?

(Hint: Introduce disequalities between equivalence classes. Show due to convexity, F_is will remain satisfiable.)

Incremental theory combination

Let F be a conjunctive input formula. Let S be a set of terms at the start.

1. If F is empty, return satisfiable.
2. Pick an i-literal $\ell \in F$ for some i. $F := F - \{\ell\}$.
3. Simplify and purify ℓ to ℓ' and add the fresh variable names for alien terms to S
4. $F_i := F_i \cup \{\ell'\}$.
5. If F_i is unsatisfiable, return unsatisfiable.
6. For each $s, t \in S$, check if $F_i \Rightarrow t = s$ or $F_i \Rightarrow t \neq s$, add the fact to the other F_js.
7. go to step 1.

If theories were convex then the above algorithm returns the answer. Otherwise, we need to explore far reduced space for $\sim$ in case of satisfiable response.

Example: Nelson-Oppen on convex theories == (Dis)Equality exchange

Example 21.6

Consider formula: $f(f(x) - f(y)) \neq f(z) \land x \leq y \land y + z \leq x \land 0 \leq z$

After separation we obtain two formulas in theory of equality and $\mathbb{Q}$*:*

$F_E = f(w) \neq f(z) \land u = f(x) \land v = f(y)$ $\quad$ $F_{\mathbb{Q}} = x \leq y \land y + z \leq x \land 0 \leq z \land u - v = w$

Common symbols $S = \{w, u, v, z, x, y\}$.

Action	$\mathcal{T}_{\mathbb{Q}}$	$\mathcal{T}_E$
Equality discovery:	$F_{\mathbb{Q}} \Rightarrow x = y$	
Equality exchange and discovery:		$F_E \land x = y \Rightarrow u = v$
Equality exchange and discovery:	$F_Q \land u = v \Rightarrow w = z$ *(why?)*	
Equality exchange:		$F_E \land x = y \land w = z \Rightarrow \perp$

Contradiction. The formula is unsatisfiable.

Example: Nelson-Oppen on non-convex theories == (Dis)Equality exchange + case split

Example 21.7

Consider formula in $\mathcal{T}_E \cup \mathcal{T}_{\mathbb{Z}}$*:* $1 \leq x \leq 2 \wedge f(x) \neq f(1) \wedge f(x) \neq f(2)$

After separation we obtain two formulas in theory of equality and $\mathbb{Q}$*:*

$F_E = f(x) \neq f(y) \wedge f(x) \neq f(z)$ $\quad$ $F_{\mathbb{Z}} = 1 \leq x \leq 2 \wedge y = 1 \wedge z = 2$

Common symbols $S = \{x, y, z\}$.

Action	$\mathcal{T}_{\mathbb{Z}}$	$\mathcal{T}_E$
Disjunctive equality discovery:	$F_{\mathbb{Z}} \Rightarrow x = y \vee x = z$	
Equality case $x = y$*:*		$F_E \wedge x = y \Rightarrow \bot$
Equality case $x = z$*:*		$F_E \wedge x = z \Rightarrow \bot$

Contradiction. The formula is unsatisfiable.

Example: a satisfiable formula

Example 21.8

Consider formula in $\mathcal{T}_E \cup \mathcal{T}_{\mathbb{Z}}$*:* $1 \leq x \leq 3 \wedge f(x) \neq f(1) \wedge f(x) \neq f(3) \wedge f(1) \neq f(2)$

After separation we obtain two formulas in theory of equality and $\mathbb{Q}$*:*

$F_E = f(x) \neq f(y) \wedge f(x) \neq f(w) \wedge f(y) \neq f(z)$ $\quad$ $F_{\mathbb{Z}} = 1 \leq x \leq 3 \wedge y = 1 \wedge z = 2 \wedge w = 3$

Common symbols $S = \{x, y, z, w\}$.

Action	$\mathcal{T}_{\mathbb{Z}}$	$\mathcal{T}_E$
Equality discovery:	$F_{\mathbb{Z}} \Rightarrow x = y \vee x = z \vee x = w$	
	$F_{\mathbb{Z}} \Rightarrow distinct(y, z, w)$	
Equality case $x = y$*:*		$F_E \wedge x = y \wedge distinct(y, z, w) \Rightarrow \perp$
Equality case $x = w$*:*		$F_E \wedge x = w \wedge distinct(y, z, w) \Rightarrow \perp$
Equality case $x = z$*:*		$F_E \wedge x = z \wedge distinct(y, z, w) \not\Rightarrow \perp$

Commentary: $distinct(y, z, w) \triangleq y \neq z \wedge z \neq w \wedge w \neq y$

End of Lecture 21