Theory Combination

Clark Barrett

barrett@cs.nyu.edu

New York University

Combining Theory Solvers

Given a theory T, a Theory Solver for T takes as input a set (interpreted as an implicit conjunction) Φ of literals and determines whether Φ is T-satisfiable.

We are often interested in using two or more theories at the same time. A natural question is: can we combine two theory solvers to get a theory solver for the combined theory?

Example (combining $T_{\mathcal{E}}$ and $T_{\mathcal{Z}}$):

$\Phi = \{1 \leq x, x \leq 2, f(x) \neq f(1), f(x) \neq f(2)\}$.

Roadmap

- The Nelson-Oppen Method
- Example
- Correctness of Nelson-Oppen
- Extensions

The Nelson-Oppen Method

A very general method for combining theory solvers is the Nelson-Oppen method.

This method is applicable when

1. The signatures Σ_i are disjoint.
2. The theories T_i are stably-infinite.

   A Σ-theory T is stably-infinite if every T-satisfiable quantifier-free Σ-formula is satisfiable in an infinite model.
3. The formulas to be tested for satisfiability are conjunctions of quantifier-free literals.

Extensions exist that can relax each of these restrictions in some cases.

The Nelson-Oppen Method

Definitions

1. A member of Σ_i is an i-symbol.
2. A term t is an i-term if it starts with an i-symbol.
3. An atomic i-formula is an application of an i-predicate , an equation whose lhs is an i-term, or an equation whose lhs is a variable and whose rhs is an i-term.
4. An i-literal is an atomic i-formula or the negation of one.
5. An occurrence of a term t in either an i-term or an i-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.
6. An expression is pure if it contains only variables and i-symbols for some i.

The Nelson-Oppen Method

Now we can explain step one of the Nelson-Oppen method:

1. Conversion to Separate Form

Given a conjunction of literals, ϕ, we desire to convert it into a separate form: a T-equisatisfiable conjunction of literals $\phi_1 \wedge \phi_2 \wedge \cdots \wedge \phi_n$, where each ϕ_i is a Σ_i-formula.

The following algorithm accomplishes this:

1. Let ψ be some literal in ϕ.
2. If ψ is a pure i-literal, for some i, remove ψ from ϕ and add ψ to ϕ_i; if ϕ is empty then stop; otherwise goto step 1.
3. Otherwise, ψ is an i-literal for some i. Let t be a term occuring i-alien in ψ. Replace t in ϕ with a new variable z, and add $z = t$ to ϕ. Goto step 1.

The Nelson-Oppen Method

It is easy to see that ϕ is T-satisfiable iff $\phi_1 \wedge \cdots \wedge \phi_n$ is T-satisfiable.

Furthermore, because each ϕ_i is a Σ_i-formula, we can run Sat_i on each ϕ_i.

Clearly, if Sat_i reports that any ϕ_i is unsatisfiable, then ϕ is unsatisfiable.

But the converse is not true in general.

We need a way for the decision procedures to communicate with each other about shared variables.

First a definition: If S is a set of terms and $\sim$ is an equivalence relation on S, then the arrangement of S induced by $\sim$ is $Ar_\sim = \{x = y \mid x \sim y\} \cup \{x \neq y \mid x \not\sim y\}$.

The Nelson-Oppen Method

Suppose that T_1 and T_2 are theories with disjoint signatures Σ_1 and Σ_2 respectively. Let $T = \bigcup T_i$ and $\Sigma = \bigcup \Sigma_i$. Given a Σ-formula ϕ and decision procedures *Sat*$_1$ and *Sat*$_2$ for T_1 and T_2 respectively, we wish to determine if ϕ is T-satisfiable. The non-deterministic Nelson-Oppen algorithm for this is as follows:

1. Convert ϕ to its separate form $\phi_1 \wedge \phi_2$.
2. Let S be the set of variables shared between ϕ_1 and ϕ_2. Guess an equivalence relation $\sim$ on S.
3. Run *Sat*$_1$ on $\phi_1 \cup Ar_\sim$.
4. Run *Sat*$_2$ on $\phi_2 \cup Ar_\sim$.

The Nelson-Oppen Method

If there exists an equivalence relation $\sim$ such that both Sat_1 and Sat_2 succeed, then ϕ is T-satisfiable.

If no such equivalence relation exists, then ϕ is T-unsatisfiable.

The generalization to more than two theories is straightforward.

Roadmap

- The Nelson-Oppen Method
- Example
- Correctness of Nelson-Oppen
- Extensions

Example

Consider the following $\Sigma_{\mathcal{E}} \cup \Sigma_{\mathcal{Z}}$ formula:

$$\phi = 1 \leq x \wedge x \leq 2 \wedge f(x) \neq f(1) \wedge f(x) \neq f(2).$$

Example

Consider the following $\Sigma_{\mathcal{E}} \cup \Sigma_{\mathcal{Z}}$ formula:

$$\phi = 1 \leq x \wedge x \leq 2 \wedge f(x) \neq f(1) \wedge f(x) \neq f(2).$$

We first convert ϕ to a separate form:

$$\phi_{\mathcal{E}} = f(x) \neq f(y) \wedge f(x) \neq f(z)$$
$$\phi_{\mathcal{Z}} = 1 \leq x \wedge x \leq 2 \wedge y = 1 \wedge z = 2$$

The shared variables are $\{x, y, z\}$. There are 5 possible arrangements based on equivalence classes of x, y, and z.

Example

$\phi_{\mathcal{E}} = f(x) \neq f(y) \wedge f(x) \neq f(z)$
$\phi_{\mathcal{Z}} = 1 \leq x \wedge x \leq 2 \wedge y = 1 \wedge z = 2$

1. $\{x = y, x = z, y = z\}$
2. $\{x = y, x \neq z, y \neq z\}$
3. $\{x \neq y, x = z, y \neq z\}$
4. $\{x \neq y, x \neq z, y = z\}$
5. $\{x \neq y, x \neq z, y \neq z\}$

Example

$\phi_{\mathcal{E}} = f(x) \neq f(y) \wedge f(x) \neq f(z)$
$\phi_{\mathcal{Z}} = 1 \leq x \wedge x \leq 2 \wedge y = 1 \wedge z = 2$

1. $\{x = y, x = z, y = z\}$: inconsistent with $\phi_{\mathcal{E}}$.
2. $\{x = y, x \neq z, y \neq z\}$
3. $\{x \neq y, x = z, y \neq z\}$
4. $\{x \neq y, x \neq z, y = z\}$
5. $\{x \neq y, x \neq z, y \neq z\}$

Example

$\phi_{\mathcal{E}} = f(x) \neq f(y) \wedge f(x) \neq f(z)$
$\phi_{\mathcal{Z}} = 1 \leq x \wedge x \leq 2 \wedge y = 1 \wedge z = 2$

1. $\{x = y, x = z, y = z\}$: inconsistent with $\phi_{\mathcal{E}}$.
2. $\{x = y, x \neq z, y \neq z\}$: inconsistent with $\phi_{\mathcal{E}}$.
3. $\{x \neq y, x = z, y \neq z\}$
4. $\{x \neq y, x \neq z, y = z\}$
5. $\{x \neq y, x \neq z, y \neq z\}$

Example

$\phi_{\mathcal{E}} = f(x) \neq f(y) \wedge f(x) \neq f(z)$
$\phi_{\mathcal{Z}} = 1 \leq x \wedge x \leq 2 \wedge y = 1 \wedge z = 2$

1. $\{x = y, x = z, y = z\}$: inconsistent with $\phi_{\mathcal{E}}$.
2. $\{x = y, x \neq z, y \neq z\}$: inconsistent with $\phi_{\mathcal{E}}$.
3. $\{x \neq y, x = z, y \neq z\}$: inconsistent with $\phi_{\mathcal{E}}$.
4. $\{x \neq y, x \neq z, y = z\}$
5. $\{x \neq y, x \neq z, y \neq z\}$

Example

$\phi_{\mathcal{E}} = f(x) \neq f(y) \wedge f(x) \neq f(z)$
$\phi_{\mathcal{Z}} = 1 \leq x \wedge x \leq 2 \wedge y = 1 \wedge z = 2$

1. $\{x = y, x = z, y = z\}$: inconsistent with $\phi_{\mathcal{E}}$.
2. $\{x = y, x \neq z, y \neq z\}$: inconsistent with $\phi_{\mathcal{E}}$.
3. $\{x \neq y, x = z, y \neq z\}$: inconsistent with $\phi_{\mathcal{E}}$.
4. $\{x \neq y, x \neq z, y = z\}$: inconsistent with $\phi_{\mathcal{Z}}$.
5. $\{x \neq y, x \neq z, y \neq z\}$

Example

$\phi_{\mathcal{E}} = f(x) \neq f(y) \wedge f(x) \neq f(z)$
$\phi_{\mathcal{Z}} = 1 \leq x \wedge x \leq 2 \wedge y = 1 \wedge z = 2$

1. $\{x = y, x = z, y = z\}$: inconsistent with $\phi_{\mathcal{E}}$.
2. $\{x = y, x \neq z, y \neq z\}$: inconsistent with $\phi_{\mathcal{E}}$.
3. $\{x \neq y, x = z, y \neq z\}$: inconsistent with $\phi_{\mathcal{E}}$.
4. $\{x \neq y, x \neq z, y = z\}$: inconsistent with $\phi_{\mathcal{Z}}$.
5. $\{x \neq y, x \neq z, y \neq z\}$: inconsistent with $\phi_{\mathcal{Z}}$.

Roadmap

- The Nelson-Oppen Method
- Example
- Correctness of Nelson-Oppen
- Extensions

Correctness of Nelson-Oppen

Recall that an interpretation of a signature Σ assigns meanings to each symbol in Σ as well as to all of the variables.

Two Σ-interpretations A and B are isomorphic if there exists an isomorphism h from A to B that preserves all of the meanings of the symbols in Σ and $h(x^A) = x^B$ for each variable x (where x^A signifies the value assigned to x by the interpretation A).

We furthermore define $A^{\Sigma,V}$ to be the restriction of A to the symbols in Σ and the variables in V.

Correctness of Nelson-Oppen

Theorem

Let Σ_1 and Σ_2 be signatures, and for $i = 1, 2$, let ϕ_i be a set of Σ_i-formulas, and V_i the set of variables appearing in ϕ_i. Then $\phi_1 \cup \phi_2$ is satisfiable iff there exists a Σ_1-interpretation A satisfying ϕ_1 and a Σ_2-interpretation B satisfying ϕ_2 such that:

$A^{\Sigma_1 \cap \Sigma_2, V_1 \cap V_2}$ is isomorphic to $B^{\Sigma_1 \cap \Sigma_2, V_1 \cap V_2}$.

Correctness of Nelson-Oppen

Proof

Let $\Sigma = \Sigma_1 \cap \Sigma_2$ and $V = V_1 \cap V_2$.
Suppose $\phi_1 \cup \phi_2$ is satisfiable. Let M be an interpretation satisfying $\phi_1 \cup \phi_2$. If we let $A = M^{\Sigma_1, V_1}$ and $B = M^{\Sigma_2, V_2}$, then clearly:

- $A \models \phi_1$
- $B \models \phi_2$
- $A^{\Sigma, V}$ is isomorphic to $B^{\Sigma, V}$

On the other hand, suppose that we have A and B satisfying the three conditions listed above. Let h be an isomorphism from $A^{\Sigma, V}$ to $B^{\Sigma, V}$.

Correctness of Nelson-Oppen

We define an interpretation M as follows:

- $\mathit{dom}(M) = \mathit{dom}(A)$
- For each variable or constant u, $u^M =$
$$\begin{cases} u^A & \text{if } u \in (\Sigma_1^C \cup V_1) \\ h^{-1}(u^B) & \text{otherwise} \end{cases}$$
- For function symbols of arity n,
$$f^M(a_1, \ldots, a_n) = \begin{cases} f^A(a_1, \ldots, a_n) & \text{if } f \in \Sigma_1^F \\ h^{-1}(f^B(h(a_1), \ldots, h(a_n))) & \text{otherwise} \end{cases}$$
- For predicate symbols of arity n,
$(a_1, \ldots, a_n) \in P^M$ iff $(a_1, \ldots, a_n) \in P^A$ if $P \in \Sigma_1^P$
$(a_1, \ldots, a_n) \in P^M$ iff $(h(a_1), \ldots, h(a_n)) \in P^B$
otherwise

Correctness of Nelson-Oppen

By construction, M^{Σ_1, V_1} is isomorphic to A. In addition, it is easy to verify that h is an isomorphism of M^{Σ_2, V_2} to B.

It follows by the homomorphism theorem (a standard theorem of first-order logic) that M satisfies $\phi_1 \cup \phi_2$.

□

Correctness of Nelson-Oppen

Theorem

Let Σ_1 and Σ_2 be signatures, with $\Sigma_1 \cap \Sigma_2 = \emptyset$, and for $i = 1, 2$, let ϕ_i be a set of Σ_i-formulas, and V_i the set of variables appearing in ϕ_i. As before, let $V = V_1 \cap V_2$. Then $\phi_1 \cup \phi_2$ is satisfiable iff there exists an interpretation A satisfying ϕ_1 and an interpretation B satisfying ϕ_2 such that:

1. $|A| = |B|$, and
2. $x^A = y^A$ iff $x^B = y^B$ for every pair of variables $x, y \in V$.

Correctness of Nelson-Oppen

Proof

Clearly, if $\phi_1 \cup \phi_2$ is satisfiable in some interpretation M, then the only if direction holds by letting $A = M$ and $B = M$.

Consider the converse. Let $h : V^A \to V^B$ be defined as $h(x^A) = x^B$. This definition is well-formed by property 2 above.

In fact, h is bijective. To show that h is injective, let $h(a_1) = h(a_2)$. Then there exist variables $x, y \in V$ such that $a_1 = x^A$, $a_2 = y^A$, and $x^B = y^B$. By property 2, $x^A = y^A$, and therefore $a_1 = a_2$.

Correctness of Nelson-Oppen

To show that h is surjective, let $b \in V^B$. Then there exists a variable $x \in V^B$ such that $x^B = b$. But then $h(x^A) = b$.

Since h is bijective, it follows that $|V^A| = |V^B|$, and since $|A| = |B|$, we also have that $|A - V^A| = |B - V^B|$. We can therefore extend h to a bijective function h' from A to B.

By construction, h' is an isomorphism of A^V to B^V. Thus, by the previous theorem, we can obtain an interpretation satisfying $\phi_1 \cup \phi_2$.

□

Correctness of Nelson-Oppen

We can now prove the correctness of the non-deterministic Nelson-Oppen method:

Theorem

Let T_i be a stably-infinite Σ_i-theory, for $i = 1, 2$, and suppose that $\Sigma_1 \cap \Sigma_2 = \emptyset$. Also, let ϕ_i be a set of Σ_i literals, $i = 1, 2$, and let S be the set of variables appearing in both ϕ_1 and ϕ_2. Then $\phi_1 \cup \phi_2$ is $T_1 \cup T_2$-satisfiable iff there exists an equivalence relation $\sim$ on S such that $\phi_i \cup Ar_\sim$ is T_i-satisfiable, $i = 1, 2$.

Correctness of Nelson-Oppen

Proof

($\Rightarrow$) Suppose M is an interpretation satisfying $\phi_1 \cup \phi_2$. Define $x \sim y$ iff $x, y \in S$ and $x^M = y^M$. By construction, M is a T_i-interpretation satisfying $\phi_i \cup Ar_\sim$, $i = 1, 2$.

($\Leftarrow$) Suppose there exists $\sim$ such that $\phi_i \cup Ar_\sim$ is T_i-satisfiable, $i = 1, 2$. Since each T_i is stably-infinite, there is are infinite interpretations A and B such that A satisfies $\phi_1 \cup Ar_\sim$ and B satisfies $\phi_2 \cup Ar_\sim$.

By another standard theorem (LST), we can take the least upper bound of $|A|$ and $|B|$ and obtain interpretations of that cardinality.

Then we have $|A| = |B|$ and $x^A = y^A$ iff $x^B = y^B$ for every variable $x, y \in S$. By the previous theorem, there exists of a $(\Sigma_1 \cup \Sigma_2)$-interpretation satisfying $\phi_1 \cup \phi_2$. $\square$

Roadmap

- The Nelson-Oppen Method
- Example
- Correctness of Nelson-Oppen
- Extensions