Little Engines of Proof: Combination Methods

N. Shankar, L. de Moura, H. Ruess, A. Tiwari

shankar@csl.sri.com

URL: http://www.csl.sri.com/~shankar/LEP.html

Computer Science Laboratory
SRI International
Menlo Park, CA

Overview

So far, we have examined decision procedures for the satisfiability of conjunctions of equality and disequality literals in individual theories.

Equalities over uninterpreted constants and function symbols were treated using union-find and congruence closure.

For the case of interpreted symbols, decision procedures for a number of canonizable and solvable (Shostak) theories such as linear arithmetic, lists, finite sequences, and bit-vectors were presented through a generalized Gaussian elimination method.

Many applications involve symbols from several theories.

Combining Theories

Typical examples of theory combinations include linear arithmetic, arrays, lists, pure equality,

$car(x) = cdr(x) - 4 \wedge x = cons(y, 7) \wedge y \neq 3$

$A[i := j][j] = A[i] \wedge A[i] \neq A[j] \wedge i \neq j$

$A[j-3] = i + 4 \wedge A[(i+2) := j-1][j-3] \neq i + 4$

$i + 3 = j - 2 \wedge A[(i+2) := j - i][j-3] \neq 5$

$i - 1 = j + 2 \wedge f(i+3) \neq f(j+6)$

$f(f(i-j)) = j \wedge i = 2 * j \wedge f(f(f(f(A[2 * j := j][i])))) \neq j$

Nelson–Oppen Combination

Given two theories: T_1 over signature Σ_1, and T_2 over Σ_2, with $\Sigma_1 \cap \Sigma_2 = \emptyset$, to decide satisfiability of Γ over $T_1 \cup T_2$:

$\dfrac{\Gamma}{\Gamma_1;\Gamma_2}$	Purification
$\dfrac{\Gamma_1;\Gamma_2}{A;\Gamma_1;\Gamma_2}$	for some arrangement A
$\dfrac{A;\Gamma_1;\Gamma_2}{\bot}$	if $T_i \models A, \Gamma_i \Rightarrow \bot, i = 1, 2$

If $\simeq$ the equivalence relation generated by some partition P of the shared constants, then A_P is $\bigwedge_{\{i,j:k_i \simeq k_j\}} k_i = k_j \wedge \bigwedge_{\{i,j:k_i \not\simeq k_j\}} k_i \neq k_j$.

Examples

$$i - 1 = j + 2 \wedge f(i+3) \neq f(j+6)$$

$$k_1 = i - 1, k_2 = j + 2, k_3 = i + 3, k_4 = j + 6, k_1 = k_2, k_5 \neq k_6;$$
$$k_5 = f(k_3), k + 6 = f(k_4)$$

$$\ldots \mid \{k_1 = k_2, k_3 = k_4, k_5 \neq k_6, \ldots \mid \ldots\}$$

$$\bot \mid \ldots \mid \bot \mid \ldots \mid \bot$$

$$i - 1 = j + 2 \wedge f(i+3) \neq f(j+4)$$

$$k_1 = i - 1, k_2 = j + 2, k_3 = i + 3, k_4 = j + 4, k_1 = k_2, k_5 \neq k_6;$$
$$k_5 = f(k_3), k + 6 = f(k_4)$$

$$\ldots \mid \{k_1 = k_2, k_3 = k_4, k_5 \neq k_6, k_2 \neq k_3, k_3 \neq k_5, \ldots\} \mid \ldots$$

An Abstract Component Inference System (AC)

The inference system AC consists of

1. The input equalities/disequalities G;
2. The equalities/disequalities on shared constants V;
3. The set of shared constants K;
4. The theory-specific equalities and disequalities E.

The inference state will be represented as $[K : G; V] : E$ to indicate that $[K : G; V]$ is shared.

We assume oracles $\models V \Rightarrow k_i = k_j$ on constants, and $T \models V; E \Rightarrow k_i = k_j$ for the theory T.

An Abstract Component Inference System (AC)

$\dfrac{[K : G; V] : E}{\bot}$	if $\models V, E \Rightarrow \bot$
$\dfrac{[K : k_1 = k_2, G; V] : E}{[K : G; V, k_1 = k_2] : E}$	
$\dfrac{[K : k_1 \neq k_2, G; V] : E}{[K : G; V, k_1 \neq k_2] : E}$	
$\dfrac{[K : G\{a\}; V] : E}{[K : G\{k\}; V] : E}$	if $T \models E, V \Rightarrow k = a$ for pure Σ-term $a, k \in K$
$\dfrac{[K : G\{a\}; V] : E}{[K, k : G\{k\}; V] : E, k = a}$	for pure Σ-term a, and fresh k
$\dfrac{[K : G; V] : E}{[K : G; V, k_1 = k_2], E \mid [K : G; V, k_1 \neq k_2], E}$	if $\not\models V \Rightarrow k_1 = k_2$ and $\not\models V \Rightarrow k_1 \neq k_2$

Correctness

Check that the inference rules are well-founded.

Check that the inference rules are model-preserving.

Check that if $[K : G; V] : E$ is irreducible, then each formula in G contains non-Σ symbols, and $V; E$ is satisfiable.

Congruence Closure as a Component

A pure term has the form $f(c_1, \ldots, c_n)$ for an uninterpreted function f and constants $c_1, \ldots, c_n$.

The inference system from Lecture 11 can be recast as an instance of an abstract component.

This component can be formally proved to be a refinement of an abstract component, as defined later.

Congruence Closure Component (CC)

$\dfrac{c = d, G; U; V}{G; U; V}$ if $V(c) \equiv V(d)$
$\dfrac{c = d, G; U; V}{G; (U; V) \circ \{V(c) = V(d)\}}$ if $V(c) \not\equiv V(d)$
$\dfrac{s \neq t, G; U; V}{\bot}$ if $S[s] \equiv S[t]$ for $S = U; V$
$\dfrac{(s = t)\{f(c_1, \ldots, c_n)\}, G; U; V}{(s = t)\{c\}, G; U; V}$ if $c = f(c'_1, \ldots, c'_n) \in U, c'_i = V(c_i)$
$\dfrac{(s = t)\{f(c_1, \ldots, c_n)\}, G; U; V}{(s = t)\{c\}, G; U \cup \{c = f(c'_1, \ldots, c'_n)\}; V}$ if $c = f(c'_1, \ldots, c'_n) \notin U,$ c fresh, $c'_i = V(c_i)$ for $1 \leq i \leq n$
$\dfrac{G; U; V}{G; (U; V) \circ \{c = d\}}$ if $U(c) \equiv U(d)$ for $V(c) \not\equiv V(d)$

Refining Inference Systems

Given an abstract inference system $\vdash_I$ and a concrete one $\vdash_J$ (known to be well-founded), we say that J *refines* I iff

1. There is a total refinement relation α between concrete states ϕ, and abstract states ψ, such that ϕ and ψ are equisatisfiable when $\alpha(\phi, \psi)$.
2. Each concrete inference step $\phi \vdash_J \phi'$ can be simulated by zero or more abstract steps so that for any ψ such that $\alpha(\phi, \psi)$, there exists a ψ' such that $\psi \vdash_I^* \psi'$ and $\alpha(\phi', \psi')$.
3. If ϕ is irreducible in J, then for all ψ such that $\alpha(\phi, \psi)$, there is an irreducible ψ' with $\psi \vdash_I^* \psi'$ in I.

Exercise: Prove that J is sound and complete if I is. Show that CC refines AC(Eq), where Eq is the theory of equality.

Composition of Inference Components

Given two theories T_1 and T_2 with disjoint signatures Σ_1 and Σ_2, and inference systems I_1 and I_2, respectively.

The composition $I_1 \otimes I_2$ of two abstract inference components I_1 given by $[K : G; V] : E_1$ and I_2 given by $[K; G; V] : E_1$ is the union of the inference rules with respect to the combined state $[K : G; V] : E_1; E_2$.

The inference rules for I_i leave E_j unchanged for $i \neq j$.

Branching on Equality/Disequality

Branching on equalities/disequalities over shared constants is essential.

For example, if theory T_1 requires $\forall x : x = f(x) \vee x = f(f(x))$, and E_1 contains $k_2 = f(k_1), k_3 = f(f(k_1))$, the theory T_2 requires $\forall x : x \neq g(x)$, and E_2 contains $k_2 = g(k_1)$.

We will fail to deduce that $k_1 = k_3$.

Stable-Infiniteness

The resulting procedure is still incomplete.

The theory T_1 with $\forall x, y, z : x = y \vee y = z \vee x = z$ has a 1 or 2-element model, while theory T_2 requires that $f(x) \neq x$ for each x.

Now, if we process $k \neq f(f(k))$, then this yields a state that is satisfiable in both theories, but needs at least a 3-element model in T_2.

The unsatisfiability is not detected.

The combination algorithm works only for *stably infinite* theories, i.e., theories where any satisfiable formula has a model of cardinality $\aleph_0$.

Correctness: Amalgamation

If theories T_1 and T_2 are *stably infinite* and the state $[K : G; V] : E_1, E_2$ is irreducible, then any satisfying assignment of values to the shared constants can map distinct equivalence classes in V to distinct domain elements.

We therefore have a satisfying interpretation $\mathcal{M}_1$ respecting T_1 for $V; E_1$ over the domain D_1, and $\mathcal{M}_2$ respecting T_2 for $V; E_2$ over the domain D_2.

Both domains can be placed in bijective correspondence (β_1 and β_2) with ω.

Let D be ω, and interpretation $\mathcal{M}(f)(a_1, \ldots, a_n) = \beta_i(\mathcal{M}_i(f)(\beta_i^{-1}(a_1), \ldots, \beta_i^{-1}(a_n))$.

Adding Uninterpreted Equality

The composition $CC \otimes I$ of the theory of uninterpreted equality, with an abstract inference component I is a sound and complete decision procedure for the union of the two theories.

Even without stable-infiniteness.

A non-$\perp$ irreducible state yields a partition V that must be satisfiable in each component.

Now the term model construction will not work for CC, but we can assign $\mathcal{M}(f)(a_1, \ldots, a_n)$ to a if there is some $k = f(k_1, \ldots, k_n)$ in U such that $\mathcal{M}_I(k_i) = a_i$ for $1 \leq i \leq n$, and $\mathcal{M}_I(k) = a$.

Otherwise, let $\mathcal{M}(f)(a_1, \ldots, a_n) = a$ for some $a \in D_I$.

Lazy Branching

The branching rule can be modified as

$$\frac{[K:G;V]:E}{[K:G;V,l_1=k_1]:E|\ldots\ |\ [K:G;V,l_n=k_n]:E}\quad \begin{array}{l}\text{if } T\models V;E\Rightarrow \bigvee_{i=1}^{n} l_i=k_i\\ \text{but } \not\models V\Rightarrow l_i=k_i,\\ \text{for } 1\leq i\leq n\end{array}$$

Ex: Show that branching simulates lazy branching.

Ex: Show that irreducibility under lazy branching can be simulated with branching.

Convexity

A theory T is *convex* if for any conjunction of literals A and equalities $A_1,\ldots A_n$, $T\models A\Rightarrow A_1\vee\ldots\vee A_n$ iff $T\models A_i$ for some i, $1\leq i\leq n$.

For a first-order theory with nontrivial models, convexity implies stable-infiniteness.

If not, there is a formula A that is only satisfiable in a model with at most m elements where $m>1$. Then, for some variables x_i, $0\leq i\leq m$ not occurring in A, $A\Rightarrow\bigvee_{0\leq i,j\leq m} x_i=x_j$. By convexity, $A\Rightarrow x_i=x_j$ for some i,j, so A is satisfiable only in the trivial one-element model. A contradiction.

By compactness, if A is satisfiable in an m-element model for each $m>1$, then it is satisfiable in an infinite model.

Combining Convex Theories

Branching can be eliminated when dealing with convex theories.

$$\frac{[K:G;V]:E}{[K:G;V,l=k]:E}\ \text{if } T\models V;E\Rightarrow l=k,\ \text{but } \not\models V\Rightarrow l=k$$

Ex: Show that the propagation rule above can be simulated with lazy branching.

Acknowledgment. The above presentation is partly based on ongoing joint work with Harald Ganzinger (MPI, Saarbrücken) and Harald Rueß (SRI). See also `http://www.csl.sri.com/users/ruess/slides/shostak/index.html` for a tutorial on this topic.