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

The Story So Far

We are interested in deciding

1. Word problems (WP) $\models s = t$.
2. Uniform word problems (UWP) $\models \bigwedge \Gamma \Rightarrow s = t$, where Γ is a set of equations.
3. Clausal validity problems (CVP) $\models \bigvee \Gamma$, where Γ is a set of equations and disequations.

Many natural decision problems involve combinations of decidable theories.

Nelson–Oppen Combination

The Nelson–Oppen method combines decision procedures for disjoint theories by communicating equalities and disequalities between variables.

A high-level version of the method consists of three phases:

1. Purification of Γ into the conjunction of Γ_1 in T_1 and Γ_2 in T_2
2. Guessing, an arrangement A as a consistent conjunction of equalities and disequalities between shared constants
3. Checking the individual satisfiability of $A; \Gamma_i$ in T_i.

This high-level method was refined to be an online procedure in terms of abstract components and refinements of these components to achieve more efficient branching rules than guessing an arrangement.

Nelson–Oppen Refinements

We presented the Nelson–Oppen combination in terms of an abstract component $AC(T)$ for a theory T operating over a state $[K : G; V]; E$.

We presented a three levels of refinement:

1. $AC(T)$ has a general splitting rule on constant equalities/disequalities.
2. $AC_b(T)$ has a branching rule on implied disjuncts of equalities.
3. $AC_c(T)$ has a propagation rule for implied equalities.

We saw the refinement ordering $AC_c(T) \sqsubseteq AC_b(T) \sqsubseteq AC(T)$.

An Abstract Component Inference System (AC(T))

$\dfrac{[K : G; V]; E}{\bot}$ 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 $\not\models V \Rightarrow k_1 \neq k_2$

Abstract Components with Branching and Propagation

$AC_b(T)$:

$$\frac{[K : G; V]; E}{[K : G; V, l_1 = k_1]; E \mid \ldots \mid [K : G; V, l_n = k_n]; E}$$

if $T \models V; E \Rightarrow \bigvee_{i=1}^{n} l_i = k_i$ but $\not\models V \Rightarrow l_i = k_i$, for $1 \leq i \leq n$

$AC_c(T)$:

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

Complexity

The number of partitions of a set of n elements is given by Bell's number $B(n)$ which is computed in terms of Stirling numbers (of the second kind) as follows: where

$$\begin{aligned} B(n) &= \Sigma_{k=0}^{n} S_n^{(k)} \\ S_{n+1}^{(k+1)} &= S_n^{(k)} + (k+1) * S_n^{(k+1)}, \text{ for } k < n \\ S_n^n &= 1 \\ S_n^0 &= 1 \end{aligned}$$

Each partition is representable in n literals.

Complexity for $AC(T_1) \otimes AC(T_2)$: $O(B(n) * (C_1(n) + C_2(n)))$, where C_i is the complexity of procedure i. Note that $B(n) \leq 2^{n^2}$

Further Exercises

Prove that the union of disjoint, stably infinite, consistent theories is consistent and stably infinite.

Prove that the union of disjoint convex theories is convex.

Prove that the worst-case complexity of $AC_c(T_1) \otimes AC_c(T_2)$ is $O(n^4 * (C_1(n) + C_2(n)))$.

Combining Shostak Theories

We already saw that several interesting theories possess canonizers and solvers, and can be captured within a schematic decision procedure.

Shostak presented an algorithm the union of disjoint Shostak theories based on combining solvers and canonizers.

Unfortunately, this does not work. The union of disjoint Shostak theories may not be Shostak. Canonizers can usually be combined but solvers, rarely.

We present a combination method for Shostak theories as a refinement of the Nelson–Oppen combination for convex theories.

Canonizers

The canonizer σ for a theory T solves the word problem for the theory, i.e., $T \models s = t$ iff $\sigma(s) \equiv \sigma(t)$

A term s is *canonical* if $\sigma(s) = s$.

Additionally, σ must satisfy the conditions

1. $\mathit{free}(\sigma(s)) \subseteq \mathit{free}(s)$
2. Every subterm of $\sigma(s)$ is canonical.

Example canonizers: ordered sum-of-products form for linear and nonlinear polynomials, simplification axioms for lists, arrays.

Solvers

Canonizers solve the word problem (WP) $T \models s = t$, but the interesting problem is the uniform word problem $T \models \bigwedge \Gamma \Rightarrow s = t$.

A solver processes an equality $s' = t'$ in Γ (that can be assumed to be canonical form) into a solved form $S = \mathit{solve}(s' = t')$.

Given a Σ-solution set S Define

$$\begin{aligned} S[k] &= S(k) \\ S[f(s_1, \ldots, s_n)] &= \sigma(f(S[s_1], \ldots, S[s_n])) \end{aligned}$$

Solvers

In some cases, like $0 = 1$ or $x = x - 1$, the given equality might be unsolvable, and solve returns $\bot$.

Otherwise, the solved form S returned by $\mathit{solve}(s' = t')$ must be a solution set of the form $\{k_1 = u_1, \ldots, k_m = u_m\}$ where each k_i is in $\mathit{free}(s' = t')$ and does not occur in $\mathit{free}(u_j)$ for any i, j, $1 \leq i, j \leq m$.

The right-hand side terms u_j must be canonical and might contain "fresh" constants that don't appear in the input equality.

S and $s' = t'$ must be equivalent.

Ex: Show that if $\mathit{solve}(s' = t') = S \neq \bot$, then $S[s'] \equiv S[t']$.

Example Solvers

Linear Arithmetic: $solve(c_0 * x_0 + \ldots + c_n * x_n = 0)$ with $c_0 \neq 0$ return $x_0 = (-c_1/c_0) * x_1 + \ldots + (-c_n/c_0) * x_n$.

Lists: $S \circ_K R = (S \triangleright R) \cup R/K$, where R/K is R domain-restricted to K. $[\![E]\!]$ is the set of subterms of E. Initially, $K : E; \emptyset$ where $K = \mathit{free}(E)$.

$\dfrac{K : E; S}{K : \sigma(R[E]); S \circ R}$ if $car(k) \in [\![E]\!]$ or $cdr(k) \in [\![E]\!]$, $R = \{k = cons(k_1, k_2)\}, k_1, k_2$ fresh
$\dfrac{K : cons(r, s) = cons(r', s'), E; S}{K : r = r', s = s', E; S}$
$\dfrac{K : k = s, E; S}{K : \sigma(\{k = s\}(E)); S \circ_K \{k = s\}}$ if s is non-atomic $k \notin \mathit{free}(s)$
$\dfrac{K : k = k, E; S}{K : E; S}$
$\dfrac{K : k = s, \Gamma; S}{\bot}$ if s a constructor term $s \not\equiv k, k \in \mathit{free}(s)$

Inference System for a Shostak Theory (Sh(T))

Given Shostak theory T over signature Σ with canonizer σ and solver $solve$:

$\dfrac{[K : k = k', G; V]; S}{[K : G; V]; S}$ if $\models V \Rightarrow k = k'$
$\dfrac{[K : k \neq k', G; V]; S}{\bot}$ if $\models V \Rightarrow k = k'$
$\dfrac{[K : G\{s\}; V]; S}{[K : G\{k\}; V]; S}$ if $k' = S[s] \in S, \models V \Rightarrow k = k'$, for Σ-term s
$\dfrac{[K : G\{s\}; V]; S}{[K, k : G\{k\}; V]; S \circ \{k = S[s]\}}$ if $k' = S[s] \notin S$ for any k', for fresh k, Σ-term s
$\dfrac{[K : G; V]; S}{[K : G; l = k, V]; S}$ if $\not\models V \Rightarrow l = k$, but $S(l) \equiv S(k)$ for $l, k \in K$
$\dfrac{[K : G; V]; S}{[K : G; V]; S \circ R}$ if $\models V \Rightarrow l = k$, but $S(l) \not\equiv S(k)$ $R = solve(S(l) = S(k)) \neq \bot$, for $l, k \in K$
$\dfrac{[K : G; V]; S}{\bot}$ if $V(l) \equiv V(k)$, but $S(l) \not\equiv S(k)$ $solve(S[l] = S[k]) = \bot$, for $l, k \in K$

Shostak and Convexity

Shostak's method is complete only for UWP or, equivalently for CVP over convex theories.

There are non-convex Shostak theories: A 2-element theory with constant a_1, a_2, with axioms $a_1 \neq a_2$ and $(\forall x : x = a_1 \vee x = a_2)$, has a trivial canonizer and solver, but Shostak's method cannot establish the unsatisfiability of $k_1 \neq k_2 \wedge k_2 \neq k_3 \wedge k_3 \neq k_1$.

What about Boolean algebra? It is actually convex. Any disequality $s \neq t$ can be converted into an equality $s = \neg t$ so that the CVP can be turned into UWP.

Correctness for Convex Shostak Theories

The inference steps are terminating and model-preserving, since $solve$ is model-preserving.

Note that solved forms S are easily satisfiable: Pick an arbitrary assignment $\mathcal{M}(k)$ for right-hand side uninterpreted constants k, and for left-hand side constants l, let $\mathcal{M}(l) = \mathcal{M}[\![S(l)]\!]$.

For an irreducible configuration $[K : G, V]; S$, the conjunction of $l \neq k; V; S$ is satisfiable, for each disequality $l \neq k \in G$.

Since the theory is convex, this ensures completeness.

Canonical Term Models

Notice that if a Shostak theory is convex, then an irreducible configuration is satisfiable in a canonical term model where $D_S = \{s|\sigma(s) = s\}$, $\mathcal{M}_S(k) = S(k)$, and $\mathcal{M}_S(f)(a_1, \ldots, a_n) = \sigma(f(a_1, \ldots, a_n))$.

Conversely, if a Shostak theory admits canonical term models, it is convex.

Combinations

Since $Sh(T)$ refines $AC_c(T)$, combining a Shostak theory with uninterpreted function symbols is simply $Sh(T) \otimes CC$.

Similarly, combining multiple Shostak theories is just $Sh(T_1) \otimes Sh(T_2)$.

Correctness proof for combinations is easy since it has already been shown for the combination of abstract components.