Combinations of decision procedures

- G. Nelson and D.C. Oppen Simplification by cooperating decision procedures, ACM Trans. on Programming Languages and Systems, 1(2):245–257, 1979
- C. Tinelli and M. Harandi A new correctness proof of the Nelson-Oppen combination procedure, Proceedings FroCos'96
- F. Baader and K. Schulz Combining constraint solving, Proceedings CCL'99, LNCS 2002:104–158, 2001

Presented by: Viorica Sofronie-Stokkermans

Example

Nelson & Oppen, 1979

Theories

$\mathcal{R}$	theory of rationals	$\Sigma_{\mathcal{R}} = \{\leq, +, -, 0, 1\}$	$=$
$\mathcal{L}$	theory of lists	$\Sigma_{\mathcal{L}} = \{=, \mathsf{car}, \mathsf{cdr}, \mathsf{cons}\}$	$=$
$\mathcal{E}$	theory of equality	Σ: free function and predicate symbols	$=$

Problem

Is the following conjunction:

$$x \leq y \ \wedge \ y \leq x + \mathsf{car}(\mathsf{cons}(0, x)) \ \wedge \ P(h(x) - h(y)) \ \wedge \ \neg P(0)$$

satisfiable in $\mathcal{R} \cup \mathcal{L} \cup \mathcal{E}$?

General combination problem

Given: Theories $\mathcal{T}_1, \ldots, \mathcal{T}_n$ over signatures $\Sigma_1, \ldots, \Sigma_n$

ϕ formula in the signature $\Sigma_1 \cup \cdots \cup \Sigma_n$

Task: Decide if $\mathcal{T}_1 \cup \cdots \cup \mathcal{T}_n \models \phi$

or:

Decide if ϕ satisfiable in $\mathcal{T}_1 \cup \cdots \cup \mathcal{T}_n$

Definitions

Signature: $\Sigma = \Sigma_P \cup \Sigma_F$ Variables: X countably infinite

Σ-Terms: $T_\Sigma(X)$ Σ-Formulae: $\mathsf{Fma}_\Sigma(X)$

First-order Σ-theory: set of closed Σ-formulae

Σ-structure $\mathcal{A} = (A, \{f_A\}_{f \in \Sigma_F}, \{P_A\}_{P \in \Sigma_P})$

$f_A : A^{a(f)} \to A$ interpretation of the function symbol $f \in \Sigma_F$

$P_A \subseteq A^{a(P)}$ interpretation of the predicate symbol $P \in \Sigma_P$

Valuation $v : X \to A$ t Σ-term $\mapsto$ $\overline{v}(t)$

ϕ Σ-formula $\mapsto$ $\overline{v}(\phi)$

$\mathcal{A}, v \models \phi$ iff $\overline{v}(\phi) = 1$

$\mathcal{A}, v \models \mathcal{T}$ iff $\mathcal{A}, v \models \phi$ for all $\phi \in \mathcal{T}$

$\mathcal{A}$ is a model of $\mathcal{T}$ iff $\mathcal{A}, v \models \mathcal{T}$ for all $v : X \to A$

Definitions

$\mathcal{T} \models \phi$ iff for all Σ-structures $\mathcal{A}$ if $\mathcal{A} \models \mathcal{T}$ then $\mathcal{A} \models \phi$

ϕ is satisfiable in $\mathcal{A}$ if there exists $v : X \to A$ such that $\overline{v}(\phi) = 1$.

ϕ is satisfiable in $\mathcal{T}$ iff satisfiable in some model of $\mathcal{T}$.

$\mathcal{T} \models \phi$ iff $\neg\phi$ unsatisfiable in $\mathcal{T}$

$\phi(x_1, \ldots, x_n)$ quantifier-free, with variables $x_1, \ldots, x_n$

$\mathcal{T} \models \forall x_1 \ldots \forall x_n \phi(x_1, \ldots, x_n)$ iff $\exists x_1 \ldots \exists x_n \neg\phi(x_1, \ldots, x_n)$ unsatisfiable

Combination problem

Given: First-order theories $\mathcal{T}_1, \ldots, \mathcal{T}_n$ over signatures $\Sigma_1, \ldots, \Sigma_n$

ϕ quantifier-free formula in the signature $\Sigma_1 \cup \cdots \cup \Sigma_n$

Task: Decide if $\mathcal{T}_1 \cup \cdots \cup \mathcal{T}_n \models \phi$

Difficult, even if $\mathcal{T}_1, \ldots, \mathcal{T}_n$ are decidable and ϕ is very simple

An undecidable combination of decidable theories

Word problem for a theory $\mathcal{T}$: Decide if $\mathcal{T} \models s \approx t$

There exists a finitely-presented semigroup with an undecidable word problem [Matijasevic, 1967]

Example:

$\mathcal{A}$: theory of associativity

$\mathcal{G}$: finite set of ground equations (presentation for semigroup with undecidable word problem)

Word problem: decidable for $\mathcal{A}, \mathcal{G}$

undecidable for $\mathcal{A} \cup \mathcal{G}$

Simpler instances of combination

The Nelson-Oppen combination procedure

- $\mathcal{T}_1, \ldots, \mathcal{T}_n$ first-order theories
- $\Sigma_1, \ldots, \Sigma_n$ disjoint signatures
- ϕ quantifier-free formula

Combinations of theories sharing constructors

Combinations of unification algorithms

The Nelson-Oppen procedure

Combine decision procedures for the validity of universal sentences
in first-order theories over disjoint signatures

Given

- $\mathcal{T}_1, \mathcal{T}_2$ first-order theories with signatures Σ_1, Σ_2
- $\Sigma_1 \cap \Sigma_2 = \emptyset$
- ϕ quantifier-free formula

Question:

How can decision procedures for validity in $\mathcal{T}_1, \mathcal{T}_2$ be used
to obtain a decision procedure for validity in $\mathcal{T}_1 \cup \mathcal{T}_2$?

The Nelson-Oppen procedure

Combine decision procedures for the satisfiability of quantifier-free formulae
in first-order theories over disjoint signatures

Given

- $\mathcal{T}_1, \mathcal{T}_2$ first-order theories with signatures Σ_1, Σ_2
- $\Sigma_1 \cap \Sigma_2 = \emptyset$
- ϕ quantifier-free formula

Question:

How can decision procedures for satisfiability in $\mathcal{T}_1, \mathcal{T}_2$ be used
to obtain a decision procedure for satisfiability in $\mathcal{T}_1 \cup \mathcal{T}_2$?

Note: Restrict to conjunctive quantifier-free formulae

$\phi \mapsto DNF(\phi)$

$DNF(\phi)$ satisfiable in $\mathcal{T}$ iff one of the disjuncts satisfiable in $\mathcal{T}$

An Example

	$\mathcal{R}$	$\mathcal{L}$	$\mathcal{E}$
Σ	$\{\leq, +, -, 0, 1\}$	$\{\mathsf{car}, \mathsf{cdr}, \mathsf{cons}\}$	$F \cup P$
Axioms	$x + 0 = x$ $x - x = 0$ $+$ is A, C $\leq$ is R, T, A $x \leq y \vee y \leq x$ $x \leq y \rightarrow x + z \leq y + z$	$\mathsf{car}(\mathsf{cons}(x, y)) = x$ $\mathsf{cdr}(\mathsf{cons}(x, y)) = y$ $\mathsf{at}(x) \vee \mathsf{cons}(\mathsf{car}(x), \mathsf{cdr}(x)) = x$ $\neg\mathsf{at}(\mathsf{cons}(x, y))$	

Is the following conjunction:

$$x \leq y \ \wedge \ y \leq x + \mathsf{car}(\mathsf{cons}(0, x)) \ \wedge \ P(h(x) - h(y)) \ \wedge \ \neg P(0)$$

satisfiable in $\mathcal{R} \cup \mathcal{L} \cup \mathcal{E}$?

Variable abstraction

$$x \leq y \ \wedge \ y \leq x + \underbrace{\mathsf{car}(\mathsf{cons}(0, x))}_{g_1} \ \wedge \ P(\underbrace{\underbrace{h(x)}_{g_3} - \underbrace{h(y)}_{g_4}}_{g_2}) \ \wedge \ \neg P(\underbrace{0}_{g_5})$$

$\mathcal{R}$	$\mathcal{L}$	$\mathcal{E}$
$x \leq y$	$g_1 = \mathsf{car}(\mathsf{cons}(g_5, x))$	$P(g_2)$
$y \leq x + g_1$		$\neg P(g_5)$
$g_2 = g_3 - g_4$		$g_3 = h(x)$
$g_5 = 0$		$g_4 = h(y)$

Variable abstraction

Given: ϕ conjunctive quantifier-free formula over $\Sigma_1 \cup \Sigma_2$

Task: Find ϕ_1, ϕ_2 s.t. ϕ_i is a pure Σ_i-formula and $\phi_1 \wedge \phi_2$ equivalent with ϕ

Variable abstraction

$$
\begin{array}{lcl}
f(s_1,\ldots,s_n) = g(t_1,\ldots,t_m) & \mapsto & u{=}f(s_1,\ldots,s_n) \wedge u{=}g(t_1,\ldots,t_m) \\
f(s_1,\ldots,s_n) \neq g(t_1,\ldots,t_m) & \mapsto & u{=}f(s_1,\ldots,s_n) \wedge v{=}g(t_1,\ldots,t_m) \wedge u \neq v \\
(\neg)P(\ldots,s_i,\ldots) & \mapsto & (\neg)P(\ldots,u,\ldots) \wedge u{=}s_i \\
(\neg)P(\ldots,s_i[t],\ldots) & \mapsto & (\neg)P(\ldots,s_i[t \mapsto u],\ldots) \wedge u{=}t
\end{array}
$$

where $t = f(t_1,\ldots,t_n)$

Termination: obvious

Correctness: $\phi_1 \wedge \phi_2$ and ϕ satisfiable in exactly the same models of $\mathcal{T}_1 \cup \mathcal{T}_2$.

Propagate equality between shared variables

$$x \leq y \ \wedge \ y \leq x + \underbrace{\mathsf{car}(\mathsf{cons}(0, x))}_{g_1} \ \wedge \ P(\underbrace{\underbrace{h(x)}_{g_3} - \underbrace{h(y)}_{g_4}}_{g_2}) \ \wedge \ \neg P(\underbrace{0}_{g_5})$$

$\mathcal{R}$	$\mathcal{L}$	$\mathcal{E}$
$x \leq y$	$g_1 = \mathsf{car}(\mathsf{cons}(g_5, x))$	$P(g_2)$
$y \leq x + g_1$		$\neg P(g_5)$
$g_2 = g_3 - g_4$		$g_3 = h(x)$
$g_5 = 0$		$g_4 = h(y)$

deduce and propagate equalities between variables entailed by components

Propagate equality between shared variables

$$x \leq y \ \wedge \ y \leq x + \underbrace{\mathsf{car}(\mathsf{cons}(0, x))}_{g_1} \ \wedge \ P(\underbrace{\underbrace{h(x)}_{g_3} - \underbrace{h(y)}_{g_4}}_{g_2}) \ \wedge \ \neg P(\underbrace{0}_{g_5})$$

$\mathcal{R}$	$\mathcal{L}$	$\mathcal{E}$
$x \leq y$	$g_1 = \mathsf{car}(\mathsf{cons}(g_5, x))$	$P(g_2)$
$y \leq x + g_1$		$\neg P(g_5)$
$g_2 = g_3 - g_4$		$g_3 = h(x)$
$g_5 = 0$		$g_4 = h(y)$
$g_1 = g_5$	$g_1 = g_5$	$x = y$
$x = y$		$g_3 = g_4$
$g_2 = g_5$		$\bot$

The Nelson-Oppen algorithm

ϕ conjunction of literals

Step 1. Use variable abstraction to construct $\phi_1 \wedge \phi_2$

where ϕ_i is a pure Σ_i-formula and $\phi_1 \wedge \phi_2$ is equivalent to ϕ.

Step 2. Test whether ϕ_i is satisfiable in $\mathcal{T}_i, i = 1, 2$

If ϕ_i unsatisfiable in $\mathcal{T}_i$ for $i = 1$ or $i = 2$ then return "unsatisfiable"

Step 3. Propagate equalities between different shared variables

If ϕ_1 entails an equality between variables not entailed by ϕ_2 then add the equality as a new conjunct to ϕ_2 (and vice-versa)

Step 4. Case split necessary?

If either ϕ_1 or ϕ_2 entails a disjunction $u_1{=}v_1 \vee \cdots \vee u_k{=}v_k$
without entailing any of the equalities alone,
then apply the procedure recursively to $\phi_1 \wedge \phi_2 \wedge u_i{=}v_i$, $1 \leq i \leq k$.

If any of these formulae is satisfiable

then return "satisfiable", else return "unsatisfiable".

The Nelson-Oppen algorithm

Termination: only finitely many shared variables to be identified

Completeness: If procedure answers "unsatisfiable" then ϕ is unsatisfiable

Soundness: Under additional hypotheses

Soundness

Example

E_1	E_2
$f(g(x), g(y)) = x$	$k(x) = k(x)$
$f(g(x), h(y)) = y$	
non-trivial	non-trivial

$g(x)=h(x) \wedge k(x)\neq x$ unsatisfiable

$g(x)=h(x)$ satisfiable in E_1

$k(x)\neq x$ satisfiable in E_2

no equations between shared variables; Nelson-Oppen answers "satisfiable"

A model of E_1 satisfies $g(x) = h(x)$ iff $\exists e \in A$ s.t. $g(e) = h(e)$.

Then, for all $a \in A$: $a = f_A(g(a), g(e)) = f_A(g(a), h(e)) = e$

Soundness

Another example

$\mathcal{T}_1$ theory admitting models of cardinality at most 2

$\mathcal{T}_2$ theory admitting models of any cardinality

$$f_1 \in \Sigma_1, f_2 \in \Sigma_2 \quad \text{such that} \quad \mathcal{T}_i \not\models \forall x, y \quad f_i(x) = f_i(y).$$

$f_1(x) \neq f_1(y) \quad \wedge \quad f_2(x) \neq f_2(z) \quad \wedge \quad f_2(y) \neq f_2(z)$ unsatisfiable

$$\phi_1 = f_1(x) \neq f_1(y) \qquad \phi_2 = f_2(x) \neq f_2(z) \ \wedge \ f_2(y) \neq f_2(z)$$

The Nelson-Oppen procedure returns "satisfiable"

$\mathcal{T}_1 \cup \mathcal{T}_2 \models \phi \rightarrow (x \neq y \wedge x \neq z \wedge y \neq z)$

Soundness

Cause of unsoundness

There exist formulae satisfiable in finite models of bounded cardinality

Solution Consider stably infinite theories.

Definition. $\mathcal{T}$ is stably infinite iff for every quantifier-free formula ϕ

ϕ satisfiable in $\mathcal{T}$ iff ϕ satisfiable in an infinite model of $\mathcal{T}$.

Note: This restriction is not mentioned in [Nelson Oppen 1979];

introduced by Oppen in 1980.

Fusions of structures

Assumption: $\Sigma_1 \cap \Sigma_2 = \emptyset$; $\mathcal{T}_i$ is a Σ_i-theory for $i = 1, 2$.

Definition. The $\Sigma_1 \cup \Sigma_2$-structure $\mathcal{A}$ is a fusion of the Σ_1-structure $\mathcal{A}_1$ and the Σ_2-structure $\mathcal{A}_2$ if $\mathcal{A}_{|\Sigma_i}$ is isomorphic to $\mathcal{A}_i$, $i = 1, 2$.

Lemma. Let $\mathcal{A}_i$ be a Σ_i-structure, i = 1,2. T.f.a.e.:

(1) $\mathcal{A}_1$ and $\mathcal{A}_2$ have a fusion

(2) the domains of $\mathcal{A}_1$ and $\mathcal{A}_2$ have the same cardinality

Proposition. Let $\mathcal{T}_i$ be a Σ_i-theory, i = 1,2; $\mathcal{A}$ a $\Sigma_1 \cup \Sigma_2$-structure. Tfae:

(1) $\mathcal{A}$ is a model of $\mathcal{T}_1 \cup \mathcal{T}_2$

(2) $\mathcal{A}$ is a fusion of a model $\mathcal{A}_1$ of $\mathcal{T}_1$ and a model $\mathcal{A}_2$ of $\mathcal{T}_2$.

Soundness

Proposition. Let $\mathcal{T}_1$ and $\mathcal{T}_2$ be stably infinite theories over disjoint signatures;
ϕ_i quantifier-free Σ_i-formula $(i = 1, 2)$ in variables X.
If $\phi_i \wedge \Delta(X)$ is satisfiable in a model $\mathcal{A}_i$ of $\mathcal{T}_i, i = 1, 2$
then $\phi_1 \wedge \phi_2$ is satisfiable in a fusion of models of $\mathcal{T}_1, \mathcal{T}_2$

$$\Delta(X) = \bigwedge_{x,y \in X, distinct} x \neq y$$

Theorem. Let $\mathcal{T}_1$ and $\mathcal{T}_2$ be stably infinite theories over disjoint signatures.
Then the Nelson-Oppen combination procedure for $\mathcal{T}_1, \mathcal{T}_2$ is sound.

Theorem. Let $\mathcal{T}_1$ and $\mathcal{T}_2$ be stably infinite theories over disjoint signatures.
Assume that the universal theory of $\mathcal{T}_i$ is decidable, $i = 1, 2$
Then the universal theory of $\mathcal{T}_1 \cup \mathcal{T}_2$ is also decidable.

Complexity

Main sources of complexity:

(i) transformation of the formula in DNF

(ii) Step 3 (propagation of equalities between shared variables)

(a) decide if there is a disjunction of equalities between variables

(b) investigate different branches corresponding to disjunctions

Definition. $\mathcal{T}$ is convex iff for every quantifier-free formula ϕ,
$\phi \models \bigvee_i x_i = y_i$ implies $\phi \models x_j = y_j$ for some j.

no branching in Step 4.

Theorem. Let $\mathcal{T}_1$ and $\mathcal{T}_2$ be convex and stably infinite; $\Sigma_1 \cap \Sigma_2 = \emptyset$
Assume that the conjunctive universal theory of $\mathcal{T}_i$ is in PTIME
Then the conjunctive universal theory of $\mathcal{T}_1 \cup \mathcal{T}_2$ is also in PTIME

Complexity

In general: non-deterministic decision procedure

Theorem. Let $\mathcal{T}_1$ and $\mathcal{T}_2$ be stably infinite theories over disjoint signatures.

Assume that the universal theory of $\mathcal{T}_i$ is decidable in NP, $i = 1, 2$

Then the universal theory of $\mathcal{T}_1 \cup \mathcal{T}_2$ is also decidable in NP.

Conclusion

Nelson-Oppen decision procedure

- terminates
- complete
- sound for combinations of stably-infinite theories

Extensions and related work

- Shostak's procedure (more efficient)
- relax the disjointness requirement for the signatures
    - [Ringeissen'96]
    - combinations of theories sharing constructors
        - [Ringeissen & Tinelli'98 '99]
        - [Baader & Tinelli'97;'99;'00,'01] equational theories
- combinations of E-unification algorithms [Baader & Schulz 1996 – 2001]