

The Calculus of Computation

Zohar Manna

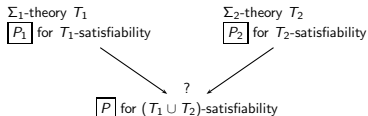
Spring 2009

Chapter 10: Combining Decision Procedures

Page 1 of 31

Page 2 of 31

Combining Decision Procedures



Problem:

Decision procedures are domain specific.
How do we combine them?

Page 3 of 31

Given

Theories T_i over signatures Σ_i
with corresponding decision procedures P_i for T_i -satisfiability.

Goal

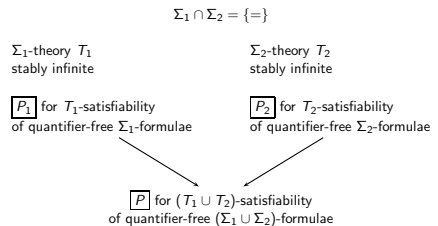
Decide satisfiability of a formula F in theory $\cup_i T_i$.

Example: How do we show that

$$F : 1 \leq x \wedge x \leq 2 \wedge f(x) \neq f(1) \wedge f(x) \neq f(2)$$

is $(T_E \cup T_{\mathbb{Z}})$ -unsatisfiable?

Nelson-Open Combination Method (N-O Method)



Page 4 of 31

Nelson-Oppen: Limitations

Given formula F in theory $T_1 \cup T_2$.

1. F must be quantifier-free.
2. Signatures Σ_i of the combined theory only share =, i.e.,

$$\Sigma_1 \cap \Sigma_2 = \{=\}$$

3. Theories must be stably infinite.

Note:

- ▶ Algorithm can be extended to combine arbitrary number of theories T_i — combine two, then combine with another, and so on.
- ▶ We restrict F to be conjunctive formula — otherwise convert to equivalent DNF and check each disjunct.

Example: T_E is stably infinite

Proof.

Let F be T_E -satisfiable quantifier-free Σ_E -formula with arbitrary satisfying T_E -interpretation $I : (D_I, \alpha_I)$.

α_I maps $=$ to $=_I$.

Let A be any infinite set disjoint from D_I . Construct new interpretation $J : (D_J, \alpha_J)$ such that

- ▶ $D_J = D_I \cup A$
- ▶ α_J agrees with α_I : the extension of functions and predicates for A is irrelevant, except $=_J$. For $v_1, v_2 \in D_J$,

$$v_1 =_J v_2 \equiv \begin{cases} v_1 =_I v_2 & \text{if } v_1, v_2 \in D_I \\ \text{true} & \text{if } v_1 \text{ is the same element as } v_2 \\ \text{false} & \text{otherwise} \end{cases}$$

J is a T_E -interpretation satisfying F with infinite domain.

Hence, T_E is stably infinite.

Stably Infinite Theories

A Σ -theory T is stably infinite iff

for every quantifier-free Σ -formula F :

if F is T -satisfiable

then there exists some T -interpretation that satisfies F with infinite domain

Example: Σ -theory T

$$\Sigma : \{a, b, =\}$$

Axiom

$$\forall x. x = a \vee x = b$$

For every T -interpretation I , $|D_I| \leq 2$ (by the axiom — at most two elements).

Hence, T is *not* stably infinite.

All the other theories mentioned so far are stably infinite.

Example

Consider quantifier-free conjunctive $(\Sigma_E \cup \Sigma_{\mathbb{Z}})$ -formula

$$F : 1 \leq x \wedge x \leq 2 \wedge f(x) \neq f(1) \wedge f(x) \neq f(2) .$$

The signatures of T_E and $T_{\mathbb{Z}}$ only share $=$. Also, both theories are stably infinite. Hence, the N-O combination of the decision procedures for T_E and $T_{\mathbb{Z}}$ decides the $(T_E \cup T_{\mathbb{Z}})$ -satisfiability of F .

Intuitively, F is $(T_E \cup T_{\mathbb{Z}})$ -unsatisfiable.

For the first two literals imply $x = 1 \vee x = 2$ so that $f(x) = f(1) \vee f(x) = f(2)$.

Contradict last two literals.

Hence, F is $(T_E \cup T_{\mathbb{Z}})$ -unsatisfiable.

Nelson-Oppen Method: Overview

Consider quantifier-free conjunctive $(\Sigma_1 \cup \Sigma_2)$ -formula F .

Two versions:

- ▶ nondeterministic — simple to present, but high complexity
- ▶ deterministic — efficient

Nelson-Oppen (N-O) method proceeds in two steps:

- ▶ Phase 1 (variable abstraction)
— same for both versions
- ▶ Phase 2
nondeterministic: guess equalities/disequalities and check
deterministic: generate equalities/disequalities by equality propagation

Phase 1: Variable abstraction

Given quantifier-free conjunctive $(\Sigma_1 \cup \Sigma_2)$ -formula F .

Transform F into two quantifier-free conjunctive formulae

$$\Sigma_1\text{-formula } F_1 \quad \text{and} \quad \Sigma_2\text{-formula } F_2$$

s.t. F is $(T_1 \cup T_2)$ -satisfiable iff $F_1 \wedge F_2$ is $(T_1 \cup T_2)$ -satisfiable

F_1 and F_2 are linked via a set of shared variables:

$$\text{shared}(F_1, F_2) = \text{free}(F_1) \cap \text{free}(F_2)$$

For term t , let $\text{hd}(t)$ be the root symbol, e.g. $\text{hd}(f(x)) = f$.

Generation of F_1 and F_2

For $i, j \in \{1, 2\}$ and $i \neq j$, repeat the transformations

- (1) if function $f \in \Sigma_i$ and $\text{hd}(t) \in \Sigma_j$,

$$F[f(t_1, \dots, t_n)] \Rightarrow F[f(t_1, \dots, w, \dots, t_n)] \wedge w = t$$

- (2) if predicate $p \in \Sigma_i$ and $\text{hd}(t) \in \Sigma_j$,

$$F[p(t_1, \dots, t_n)] \Rightarrow F[p(t_1, \dots, w, \dots, t_n)] \wedge w = t$$

- (3) if $\text{hd}(s) \in \Sigma_i$ and $\text{hd}(t) \in \Sigma_j$,

$$F[s = t] \Rightarrow F[w = t] \wedge w = s$$

$$F[s \neq t] \Rightarrow F[w \neq t] \wedge w = s$$

where w is a fresh variable in each application of a transformation.

Example

Consider $(\Sigma_E \cup \Sigma_Z)$ -formula

$$F : 1 \leq x \wedge x \leq 2 \wedge f(x) \neq f(1) \wedge f(x) \neq f(2) .$$

By transformation 1, since $f \in \Sigma_E$ and $1 \in \Sigma_Z$,

replace $f(1)$ by $f(w_1)$ and add $w_1 = 1$. Similarly,

replace $f(2)$ by $f(w_2)$ and add $w_2 = 2$.

Hence, construct the Σ_Z -formula

$$F_Z : 1 \leq x \wedge x \leq 2 \wedge w_1 = 1 \wedge w_2 = 2$$

and the Σ_E -formula

$$F_E : f(x) \neq f(w_1) \wedge f(x) \neq f(w_2) .$$

F_Z and F_E share the variables $\{x, w_1, w_2\}$.

$F_Z \wedge F_E$ is $(T_E \cup T_Z)$ -equisatisfiable to F .

Example

Consider $(\Sigma_E \cup \Sigma_Z)$ -formula

$$F : f(x) = x + y \wedge x \leq y + z \wedge x + z \leq y \wedge y = 1 \wedge f(x) \neq f(2) .$$

In the first literal, $\text{hd}(f(x)) = f \in \Sigma_E$ and $\text{hd}(x + y) = + \in \Sigma_Z$;
thus, by (3), replace the literal with

$$w_1 = x + y \wedge w_1 = f(x) .$$

In the final literal, $f \in \Sigma_E$ but $2 \in \Sigma_Z$, so by (1), replace it with

$$f(x) \neq f(w_2) \wedge w_2 = 2 .$$

Now, separating the literals results in two formulae:

$$F_Z : w_1 = x + y \wedge x \leq y + z \wedge x + z \leq y \wedge y = 1 \wedge w_2 = 2$$

is a Σ_Z -formula, and

$$F_E : w_1 = f(x) \wedge f(x) \neq f(w_2)$$

is a Σ_E -formula.

The conjunction $F_Z \wedge F_E$ is $(T_E \cup T_Z)$ -equisatisfiable to F .

Nondeterministic Version

Phase 2: Guess and Check

► Phase 1 separated $(\Sigma_1 \cup \Sigma_2)$ -formula F into two formulae:

$$\Sigma_1\text{-formula } F_1 \quad \text{and} \quad \Sigma_2\text{-formula } F_2$$

► F_1 and F_2 are linked by a set of shared variables:

$$V = \text{shared}(F_1, F_2) = \text{free}(F_1) \cap \text{free}(F_2)$$

► Let E be an equivalence relation over V .

► The arrangement $\alpha(V, E)$ of V induced by E is:

$$\alpha(V, E) : \bigwedge_{u, v \in V. uEv} u = v \quad \wedge \quad \bigwedge_{u, v \in V. \neg(uEv)} u \neq v$$

Nondeterministic Version

Lemma

the original formula F is $(T_1 \cup T_2)$ -satisfiable iff
there exists an equivalence relation E over V s.t.

(1) $F_1 \wedge \alpha(V, E)$ is T_1 -satisfiable, and

(2) $F_2 \wedge \alpha(V, E)$ is T_2 -satisfiable.

Otherwise, F is $(T_1 \cup T_2)$ -unsatisfiable.

Example 1

Consider $(\Sigma_E \cup \Sigma_Z)$ -formula

$$F : 1 \leq x \wedge x \leq 2 \wedge f(x) \neq f(1) \wedge f(x) \neq f(2)$$

Phase 1 separates this formula into the Σ_Z -formula

$$F_Z : 1 \leq x \wedge x \leq 2 \wedge w_1 = 1 \wedge w_2 = 2$$

and the Σ_E -formula

$$F_E : f(x) \neq f(w_1) \wedge f(x) \neq f(w_2)$$

with

$$V = \text{shared}(F_1, F_2) = \{x, w_1, w_2\}$$

There are 5 equivalence relations over V to consider, which we list
by stating the partitions:

Example 1

- 1. $\{\{x, w_1, w_2\}\}$, i.e., $x = w_1 = w_2$:
 $x = w_1$ and $f(x) \neq f(w_1) \Rightarrow F_E \wedge \alpha(V, E)$ is T_E -unsatisfiable.
- 2. $\{\{x, w_1\}, \{w_2\}\}$, i.e., $x = w_1, x \neq w_2$:
 $x = w_1$ and $f(x) \neq f(w_1) \Rightarrow F_E \wedge \alpha(V, E)$ is T_E -unsatisfiable.
- 3. $\{\{x, w_2\}, \{w_1\}\}$, i.e., $x = w_2, x \neq w_1$:
 $x = w_2$ and $f(x) \neq f(w_2) \Rightarrow F_E \wedge \alpha(V, E)$ is T_E -unsatisfiable.
- 4. $\{\{x\}, \{w_1, w_2\}\}$, i.e., $x \neq w_1, w_1 = w_2$:
 $w_1 = w_2$ and $w_1 = 1 \wedge w_2 = 2$
 $\Rightarrow F_{\mathbb{Z}} \wedge \alpha(V, E)$ is $T_{\mathbb{Z}}$ -unsatisfiable.
- 5. $\{\{x\}, \{w_1\}, \{w_2\}\}$, i.e., $x \neq w_1, x \neq w_2, w_1 \neq w_2$:
 $x \neq w_1 \wedge x \neq w_2$ and $x = w_1 = 1 \vee x = w_2 = 2$
(since $1 \leq x \leq 2$ implies that $x = 1 \vee x = 2$ in $T_{\mathbb{Z}}$)
 $\Rightarrow F_{\mathbb{Z}} \wedge \alpha(V, E)$ is $T_{\mathbb{Z}}$ -unsatisfiable.

Hence, F is $(T_E \cup T_{\mathbb{Z}})$ -unsatisfiable.

Example 2

Consider the $(\Sigma_{\text{cons}} \cup \Sigma_{\mathbb{Z}})$ -formula

$$F : \text{car}(x) + \text{car}(y) = z \wedge \text{cons}(x, z) \neq \text{cons}(y, z) .$$

After two applications of (1), Phase 1 separates F into the Σ_{cons} -formula

$$F_{\text{cons}} : w_1 = \text{car}(x) \wedge w_2 = \text{car}(y) \wedge \text{cons}(x, z) \neq \text{cons}(y, z)$$

and the $\Sigma_{\mathbb{Z}}$ -formula

$$F_{\mathbb{Z}} : w_1 + w_2 = z ,$$

with

$$V = \text{shared}(F_{\text{cons}}, F_{\mathbb{Z}}) = \{z, w_1, w_2\} .$$

Example 2

Consider the equivalence relation E given by the partition

$$\{\{z\}, \{w_1\}, \{w_2\}\} .$$

The arrangement

$$\alpha(V, E) : z \neq w_1 \wedge z \neq w_2 \wedge w_1 \neq w_2$$

satisfies both F_{cons} and $F_{\mathbb{Z}}$:

$$F_{\text{cons}} \wedge \alpha(V, E) \text{ is } T_{\text{cons}}\text{-satisfiable, and}$$

$$F_{\mathbb{Z}} \wedge \alpha(V, E) \text{ is } T_{\mathbb{Z}}\text{-satisfiable.}$$

Hence, F is $(T_{\text{cons}} \cup T_{\mathbb{Z}})$ -satisfiable.

Practical Efficiency

Phase 2 was formulated as “guess and check”:

- 1. First, guess an equivalence relation E ,
- 2. then check the induced arrangement.

The number of equivalence relations grows super-exponentially with the # of shared variables. It is given by Bell numbers.
E.g., 12 shared variables $\Rightarrow$ over four million equivalence relations.

Solution: Deterministic Version

Deterministic Version

Phase 1 as before
Phase 2 asks the decision procedures P_1 and P_2 to propagate new equalities.

Example 3

Theory of equality T_E

P_E

Rational linear arithmetic T_Q

P_Q

$$F: f(f(x)-f(y)) \neq f(z) \wedge x \leq y \wedge y+z \leq x \wedge 0 \leq z$$

$$(T_E \cup T_Q)\text{-unsatisfiable}$$

Intuitively,
last 3 conjuncts $\Rightarrow x = y \wedge z = 0$
contradicts 1st conjunct

Phase 1: Variable Abstraction

Example 3

$$F: f(f(x)-f(y)) \neq f(z) \wedge x \leq y \wedge y+z \leq x \wedge 0 \leq z$$

Replace $f(x)$ by u , $f(y)$ by v , $u-v$ by w

$$F_E: f(w) \neq f(z) \wedge u = f(x) \wedge v = f(y) \quad \dots T_E\text{-formula}$$

$$F_Q: x \leq y \wedge y+z \leq x \wedge 0 \leq z \wedge w = u-v \quad \dots T_Q\text{-formula}$$

$$\text{shared}(F_E, F_Q) = \{x, y, z, u, v, w\}$$

Nondeterministic version — over 200 E s!
Let's try the deterministic version.

Phase 2: Equality Propagation

Example 3

$F_E: f(w) \neq f(z) \wedge u = f(x) \wedge v = f(y)$

$F_Q: x \leq y \wedge y+z \leq x \wedge 0 \leq z \wedge w = u-v$

P_Q

$F_Q \models x = y$

$\{ \}$

$\{x = y\}$

$\{x = y, u = v\}$

$\{x = y, u = v, z = w\}$

$\perp$

P_E

$F_E \wedge x = y \models u = v$

$F_Q \wedge u = v \models z = w$

$F_E \wedge z = w \models \perp$

Contradiction. Thus, F is $(T_Q \cup T_E)$ -unsatisfiable.
(If there were no contradiction, F would be $(T_Q \cup T_E)$ -satisfiable.)

Convex Theories

Definition

A Σ -theory T is *convex* iff
for every quantifier-free conjunctive Σ -formula F
and for every disjunction $\bigvee_{i=1}^n (u_i = v_i)$
if $F \Rightarrow \bigvee_{i=1}^n (u_i = v_i)$
then $F \Rightarrow u_i = v_i$, for some $i \in \{1, \dots, n\}$

Claim

Equality propagation is a decision procedure for convex theories.

Convex Theories

- ▶ $T_E, T_R, T_Q, T_{\text{cons}}$ are convex
- ▶ T_Z, T_A are not convex

Example: T_Z is not convex

Consider quantifier-free conjunctive Σ_Z -formula

$$F : 1 \leq z \wedge z \leq 2 \wedge u = 1 \wedge v = 2$$

Then

$$F \Rightarrow z = u \vee z = v$$

but

$$F \not\Rightarrow z = u$$

$$F \not\Rightarrow z = v$$

Convex Theories

Example: Theory of arrays T_A is not convex

Consider the quantifier-free conjunctive Σ_A -formula

$$F : a[i \triangleleft v][j] = v .$$

Then

$$F \Rightarrow i = j \vee a[j] = v ,$$

but

$$F \not\Rightarrow i = j$$

$$F \not\Rightarrow a[j] = v .$$

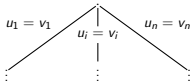
What if T is Not Convex?

Case split when:

$$F \Rightarrow \bigvee_{i=1}^n (u_i = v_i)$$

but $F \not\Rightarrow u_i = v_i$ for any $i = 1, \dots, n$

- ▶ For each $i = 1, \dots, n$, construct a branch on which $u_i = v_i$ is assumed.
- ▶ If all branches are contradictory, then **unsatisfiable**. Otherwise, **satisfiable**.



Claim: Equality propagation (with branching) is a decision procedure for non-convex theories too.

Example 1: Non-Convex Theory

T_Z not convex!

$$\boxed{P_Z}$$

T_E convex

$$\boxed{P_E}$$

$$F : 1 \leq x \wedge x \leq 2 \wedge f(x) \neq f(1) \wedge f(x) \neq f(2)$$

in $T_Z \cup T_E$.

- ▶ Replace $f(1)$ by $f(w_1)$, and add $w_1 = 1$.
- ▶ Replace $f(2)$ by $f(w_2)$, and add $w_2 = 2$.

Result:

$$F_Z : 1 \leq x \wedge x \leq 2 \wedge w_1 = 1 \wedge w_2 = 2$$

$$F_E : f(x) \neq f(w_1) \wedge f(x) \neq f(w_2)$$

and

$$V = \text{shared}(F_Z, F_E) = \{x, w_1, w_2\}$$

Example 4: Non-Convex Theory

Consider

$$F : 1 \leq x \wedge x \leq 3 \wedge \\ f(x) \neq f(1) \wedge f(x) \neq f(3) \wedge f(1) \neq f(2)$$

in $T_{\mathbb{Z}} \cup T_E$.

- ▶ Replace $f(1)$ by $f(w_1)$, and add $w_1 = 1$.
- ▶ Replace $f(2)$ by $f(w_2)$, and add $w_2 = 2$.
- ▶ Replace $f(3)$ by $f(w_3)$, and add $w_3 = 3$.

Result:

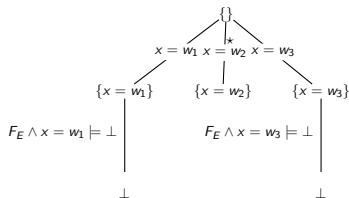
$$F_{\mathbb{Z}} : 1 \leq x \wedge x \leq 3 \wedge w_1 = 1 \wedge w_2 = 2 \wedge w_3 = 3$$

$$F_E : f(x) \neq f(w_1) \wedge f(x) \neq f(w_3) \wedge f(w_1) \neq f(w_2)$$

and

$$V = \text{shared}(F_{\mathbb{Z}}, F_E) = \{x, w_1, w_2, w_3\}$$

Example 4: Non-Convex Theory



$$\star : F_{\mathbb{Z}} \models x = w_1 \vee x = w_2 \vee x = w_3$$

No more equations on middle leaf $\Rightarrow F$ is $(T_{\mathbb{Z}} \cup T_E)$ -satisfiable.