Decision Procedures for Verification

Combinations of Decision Procedures (3)

6.02.2017

Viorica Sofronie-Stokkermans

sofronie@uni-koblenz.de

Last time

Combinations of Decision Procedures

Example

[Nelson & Oppen, 1979]

Theories

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

Problems:

1. $\mathcal{R} \cup \mathcal{L} \cup \mathcal{E} \models \forall x, y (x \leq y \wedge y \leq x + \text{car}(\text{cons}(0, x)) \wedge P(h(x) - h(y)) \rightarrow P(0))$
2. Is the following conjunction:

$$c \leq d \ \wedge \ d \leq c + \text{car}(\text{cons}(0, c)) \ \wedge \ P(h(c) - h(d)) \ \wedge \ \neg P(0)$$

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

Step 1: Purification

$$c \leq d \ \wedge \ d \leq c + \underbrace{\mathrm{car}(\mathrm{cons}(0, c))}_{c_1} \ \wedge \ P(\underbrace{\underbrace{h(c)}_{c_3} - \underbrace{h(d)}_{c_4}}_{c_2}) \ \wedge \ \neg P(\underbrace{\ 0\ }_{c_5})$$

Step 1: Purification

$$c \leq d \;\wedge\; d \leq c + \underbrace{\mathrm{car}(\mathrm{cons}(0, c))}_{c_1} \;\wedge\; P(\underbrace{\underbrace{h(c)}_{c_3} - \underbrace{h(d)}_{c_4}}_{c_2}) \;\wedge\; \neg P(\underbrace{\;0\;}_{c_5})$$

$\mathcal{R}$	$\mathcal{L}$	$\mathcal{E}$
$c \leq d$	$c_1 \approx \mathrm{car}(\mathrm{cons}(c_5, c))$	$P(c_2)$
$d \leq c + c_1$		$\neg P(c_5)$
$c_2 \approx c_3 - c_4$		$c_3 \approx h(c)$
$c_5 \approx 0$		$c_4 \approx h(d)$

Step 1: Purification

$$c \leq d \;\wedge\; d \leq c + \underbrace{\mathsf{car}(\mathsf{cons}(0, c))}_{c_1} \;\wedge\; P(\underbrace{\underbrace{h(c)}_{c_3} - \underbrace{h(d)}_{c_4}}_{c_2}) \;\wedge\; \neg P(\underbrace{0}_{c_5})$$

$\mathcal{R}$	$\mathcal{L}$	$\mathcal{E}$
$c \leq d$	$c_1 \approx \mathsf{car}(\mathsf{cons}(c_5, c))$	$P(c_2)$
$d \leq c + c_1$		$\neg P(c_5)$
$c_2 \approx c_3 - c_4$		$c_3 \approx h(c)$
$c_5 \approx 0$		$c_4 \approx h(d)$
satisfiable	satisfiable	satisfiable

Step 2: Propagation

$$c \leq d \;\wedge\; d \leq c + \underbrace{\mathrm{car}(\mathrm{cons}(0, c))}_{c_1} \;\wedge\; P(\underbrace{\underbrace{h(c)}_{c_3} - \underbrace{h(d)}_{c_4}}_{c_2}) \;\wedge\; \neg P(\underbrace{0}_{c_5})$$

$\mathcal{R}$	$\mathcal{L}$	$\mathcal{E}$
$c \leq d$	$c_1 \approx \mathrm{car}(\mathrm{cons}(c_5, c))$	$P(c_2)$
$d \leq c + c_1$		$\neg P(c_5)$
$c_2 \approx c_3 - c_4$		$c_3 \approx h(c)$
$c_5 \approx 0$		$c_4 \approx h(d)$

deduce and propagate equalities between constants entailed by components

Step 2: Propagation

$$c \leq d \;\wedge\; d \leq c + \underbrace{\text{car}(\text{cons}(0, c))}_{c_1} \;\wedge\; P(\underbrace{\underbrace{h(c)}_{c_3} - \underbrace{h(d)}_{c_4}}_{c_2}) \;\wedge\; \neg P(\underbrace{0}_{c_5})$$

$\mathcal{R}$	$\mathcal{L}$	$\mathcal{E}$
$c \leq d$	$c_1 \approx \text{car}(\text{cons}(c_5, c))$	$P(c_2)$
$d \leq c + c_1$		$\neg P(c_5)$
$c_2 \approx c_3 - c_4$		$c_3 \approx h(c)$
$c_5 \approx 0$		$c_4 \approx h(d)$

$$c_1 \approx c_5$$

Step 2: Propagation

$$c \leq d \;\wedge\; d \leq c + \underbrace{\mathrm{car}(\mathrm{cons}(0, c))}_{c_1} \;\wedge\; P(\underbrace{\underbrace{h(c)}_{c_3} - \underbrace{h(d)}_{c_4}}_{c_2}) \;\wedge\; \neg P(\underbrace{0}_{c_5})$$

$\mathcal{R}$	$\mathcal{L}$	$\mathcal{E}$
$c \leq d$	$c_1 \approx \mathrm{car}(\mathrm{cons}(c_5, c))$	$P(c_2)$
$d \leq c + c_1$		$\neg P(c_5)$
$c_2 \approx c_3 - c_4$		$c_3 \approx h(c)$
$c_5 \approx 0$		$c_4 \approx h(d)$
$c_1 \approx c_5$	$c_1 \approx c_5$	
$c \approx d$		

Step 2: Propagation

$$c \leq d \;\wedge\; d \leq c + \underbrace{\mathrm{car}(\mathrm{cons}(0, c))}_{c_1} \;\wedge\; P(\underbrace{\underbrace{h(c)}_{c_3} - \underbrace{h(d)}_{c_4}}_{c_2}) \;\wedge\; \neg P(\underbrace{0}_{c_5})$$

$\mathcal{R}$	$\mathcal{L}$	$\mathcal{E}$
$c \leq d$	$c_1 \approx \mathrm{car}(\mathrm{cons}(c_5, c))$	$P(c_2)$
$d \leq c + c_1$		$\neg P(c_5)$
$c_2 \approx c_3 - c_4$		$c_3 \approx h(c)$
$c_5 \approx 0$		$c_4 \approx h(d)$
$c_1 \approx c_5$	$c_1 \approx c_5$	$c \approx d$
$c \approx d$		$c_3 \approx c_4$

Step 2: Propagation

$$c \leq d \;\wedge\; d \leq c + \underbrace{\mathrm{car}(\mathrm{cons}(0, c))}_{c_1} \;\wedge\; P(\underbrace{\underbrace{h(c)}_{c_3} - \underbrace{h(d)}_{c_4}}_{c_2}) \;\wedge\; \neg P(\underbrace{0}_{c_5})$$

$\mathcal{R}$	$\mathcal{L}$	$\mathcal{E}$
$c \leq d$	$c_1 \approx \mathrm{car}(\mathrm{cons}(c_5, c))$	$P(c_2)$
$d \leq c + c_1$		$\neg P(c_5)$
$c_2 \approx c_3 - c_4$		$c_3 \approx h(c)$
$c_5 \approx 0$		$c_4 \approx h(d)$
$c_1 \approx c_5$	$c_1 \approx c_5$	$c \approx d$
$c \approx d$		$c_3 \approx c_4$
$c_2 \approx c_5$		$\bot$

The Nelson-Oppen algorithm

ϕ conjunction of literals

Step 1. Purification $\mathcal{T}_1 \cup \mathcal{T}_2 \cup \phi \mapsto (\mathcal{T}_1 \cup \phi_1) \cup (\mathcal{T}_2 \cup \phi_2)$:

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

Step 2. Propagation.

The decision procedure for ground satisfiability for $\mathcal{T}_1$ and $\mathcal{T}_2$ fairly exchange information concerning entailed unsatisfiability of constraints in the shared signature
i.e. clauses over the shared variables.

until an inconsistency is detected or a saturation state is reached.

The Nelson-Oppen algorithm

ϕ conjunction of literals

Step 1. Purification $\mathcal{T}_1 \cup \mathcal{T}_2 \cup \phi \mapsto (\mathcal{T}_1 \cup \phi_1) \cup (\mathcal{T}_2 \cup \phi_2)$:

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

> not problematic; requires linear time

Step 2. Propagation.

The decision procedure for ground satisfiability for $\mathcal{T}_1$ and $\mathcal{T}_2$ fairly exchange information concerning entailed unsatisfiability of constraints in the shared signature

i.e. clauses over the shared variables.

until an inconsistency is detected or a saturation state is reached.

> not problematic; termination guaranteed
> Sound: if inconsistency detected input unsatisfiable
> Complete: under additional assumptions

Implementation

ϕ conjunction of literals

Step 1. Purification: $\mathcal{T}_1 \cup \mathcal{T}_2 \cup \phi \mapsto (\mathcal{T}_1 \cup \phi_1) \cup (\mathcal{T}_2 \cup \phi_2)$,
where ϕ_i is a pure Σ_i-formula and $\phi_1 \wedge \phi_2$ is equisatisfiable with ϕ.

Step 2. Propagation: The decision procedure for ground satisfiability for $\mathcal{T}_1$ and $\mathcal{T}_2$ fairly exchange information concerning entailed unsatisfiability of constraints in the shared signature
i.e. clauses over the shared variables.

until an inconsistency is detected or a saturation state is reached.

How to implement Propagation?

Guessing: guess a maximal set of literals containing the shared variables; check it for $\mathcal{T}_i \cup \phi_i$ consistency.

Backtracking: identify disjunction of equalities between shared variables entailed by $\mathcal{T}_i \cup \phi_i$; make case split by adding some of these equalities to ϕ_1, ϕ_2. Repeat as long as possible.

The Nelson-Oppen algorithm

Termination: only finitely many shared variables to be identified

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

Completeness: Under additional hypotheses

Cause of incompleteness

There exist formulae satisfiable in finite models of bounded cardinality

Solution: Consider stably infinite theories.

$\mathcal{T}$ 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.

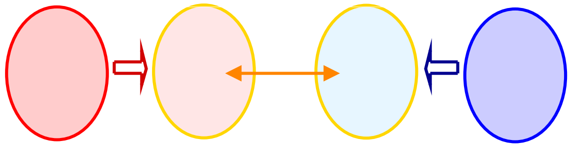
Completeness

Guessing version: C set of constants shared by ϕ_1, ϕ_2

R equiv. relation assoc. with partition of $C \mapsto ar(C, R) = \bigwedge_{R(c,d)} c \approx d \wedge \bigwedge_{\neg R(c,d)} c \not\approx d$

Lemma. Assume that there exists a partition of C s.t. $\phi_i \wedge ar(C, R)$ is $\mathcal{T}_i$-satisfiable. Then $\phi_1 \wedge \phi_2$ is $\mathcal{T}_1 \cup \mathcal{T}_2$-satisfiable.

Idea of proof: Let $\mathcal{A}_i \in \text{Mod}(\mathcal{T}_i)$ s.t. $\mathcal{A}_i \models \phi_i \wedge ar(C, R)$. Then $c_{A_1} = d_{A_1}$ iff $c_{A_2} = d_{A_2}$.
Let $i : \{c_{A_1} \mid c \in C\} \rightarrow \{c_{A_2} \mid c \in C\}$, $i(c_{A_1}) = c_{A_2}$ well-defined; bijection.
Stable infinity: can assume w.l.o.g. that $\mathcal{A}_1, \mathcal{A}_2$ have the same cardinality
Let $h : \mathcal{A}_1 \rightarrow \mathcal{A}_2$ bijection s.t. $h(c_{A_1}) = c_{A_2}$
Use h to transfer the Σ_1-structure on $\mathcal{A}_2$.



Theorem. If $\mathcal{T}_1, \mathcal{T}_2$ are both stably infinite and the shared signature is empty then the Nelson-Oppen procedure is sound, complete and terminating. Thus, it transfers decidability of ground satisfiability from $\mathcal{T}_1, \mathcal{T}_2$ to $\mathcal{T}_1 \cup \mathcal{T}_2$.

Complexity

Main sources of complexity:

(i) transformation of the formula in DNF

(ii) propagation

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

  (b) investigate different branches corresponding to disjunctions

Complexity

Main sources of complexity:

(i) transformation of the formula in DNF

(ii) propagation

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

$\mapsto$ No branching

Complexity

Main sources of complexity:

(i) transformation of the formula in DNF

(ii) propagation

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

$\mapsto$ No branching

Examples of convex theories:

- The theory of uninterpreted function symbols
- $LI(\mathbb{Q})$

Examples of theories which are not convex:

- $LI(\mathbb{Z})$

Complexity

Theorem. Let $\mathcal{T}_1$ and $\mathcal{T}_2$ be convex and stably infinite; $\Sigma_1 \cap \Sigma_2 = \emptyset$

If satisfiability of conjunctions of literals in $\mathcal{T}_i$ is in PTIME

Then satisfiability of conjunctions of literals in $\mathcal{T}_1 \cup \mathcal{T}_2$ is in PTIME

In general: non-deterministic procedure

Theorem. Let $\mathcal{T}_1$ and $\mathcal{T}_2$ be convex and stably infinite; $\Sigma_1 \cap \Sigma_2 = \emptyset$

If satisfiability of conjunctions of literals in $\mathcal{T}_i$ is in NP

Then satisfiability of conjunctions of literals in $\mathcal{T}_1 \cup \mathcal{T}_2$ is in NP

From conjunctions to arbitrary combinations

Until now:

check satisfiability for conjunctions of literals

Question:

how to check satisfiability of sets of clauses?

Overview

Satisfiability w.r.t. theories

- Propositional logic
  - resolution
  - DPLL
- First-order logic
  - resolution

- Ground formulae
  - conjunctions of literals: specialized methods
  - clauses: DPLL(T) ⇐ TODAY
- Formulae with quantifiers
  - reduction to SAT for ground formulae instantiation ⇐ NEXT WEEK (situations when sound and complete)
  - resolution (mod T)

3.6 The $DPLL(\mathcal{T})$ algorithm

Reminder: Propositional SAT

The DPLL algorithm

A succinct formulation

State: $M||F$,

where:

- M partial assignment (sequence of literals),

  some literals are annotated (L^d: decision literal)

- F clause set.

A succinct formulation

UnitPropagation

$M||F, C \vee L \Rightarrow M, L||F, C \vee L$ if $M \models \neg C$, and L undef. in M

Decide

$M||F \Rightarrow M, L^d||F$ if L or $\neg L$ occurs in F, L undef. in M

Fail

$M||F, C \Rightarrow$ Fail if $M \models \neg C$, M contains no decision literals

Backjump

$M, L^d, N||F \Rightarrow M, L'||F$ if $\begin{cases} \text{there is some clause } C \vee L' \text{ s.t.:} \\ F \models C \vee L', M \models \neg C, \\ L' \text{ undefined in } M \\ L' \text{ or } \neg L' \text{ occurs in } F. \end{cases}$

Example

Assignment:	Clause set:	
$\emptyset$	$\|\|\neg P_1 \lor P_2, \neg P_3 \lor P_4, \neg P_5 \lor \neg P_6, P_6 \lor \neg P_5 \lor \neg P_2$	$\Rightarrow$ (Decide)
P_1^d	$\|\|\neg P_1 \lor P_2, \neg P_3 \lor P_4, \neg P_5 \lor \neg P_6, P_6 \lor \neg P_5 \lor \neg P_2$	$\Rightarrow$ (UnitProp)
$P_1^d P_2$	$\|\|\neg P_1 \lor P_2, \neg P_3 \lor P_4, \neg P_5 \lor \neg P_6, P_6 \lor \neg P_5 \lor \neg P_2$	$\Rightarrow$ (Decide)
$P_1^d P_2 P_3^d$	$\|\|\neg P_1 \lor P_2, \neg P_3 \lor P_4, \neg P_5 \lor \neg P_6, P_6 \lor \neg P_5 \lor \neg P_2$	$\Rightarrow$ (UnitProp)
$P_1^d P_2 P_3^d P_4$	$\|\|\neg P_1 \lor P_2, \neg P_3 \lor P_4, \neg P_5 \lor \neg P_6, P_6 \lor \neg P_5 \lor \neg P_2$	$\Rightarrow$ (Decide)
$P_1^d P_2 P_3^d P_4 P_5^d$	$\|\|\neg P_1 \lor P_2, \neg P_3 \lor P_4, \neg P_5 \lor \neg P_6, P_6 \lor \neg P_5 \lor \neg P_2$	$\Rightarrow$ (UnitProp)
$P_1^d P_2 P_3^d P_4 P_5^d \neg P_6$	$\|\|\neg P_1 \lor P_2, \neg P_3 \lor P_4, \neg P_5 \lor \neg P_6, P_6 \lor \neg P_5 \lor \neg P_2$	$\Rightarrow$ (Backtrack)
$P_1^d P_2 P_3^d P_4 \neg P_5$	$\|\|\neg P_1 \lor P_2, \neg P_3 \lor P_4, \neg P_5 \lor \neg P_6, P_6 \lor \neg P_5 \lor \neg P_2$	

DPLL with learning

The DPLL system with learning consists of the four transition rules of the Basic DPLL system, plus the following two additional rules:

Learn

$M||F \Rightarrow M||F, C$ if all atoms of C occur in F and $F \models C$

Forget

$M||F, C \Rightarrow M||F$ if $F \models C$

In these two rules, the clause C is said to be learned and forgotten, respectively.

SAT Modulo Theories (SMT)

Some problems are more naturally expressed in richer logics than just propositional logic, e.g:

- Software/Hardware verification needs reasoning about equality, arithmetic, data structures, ...

SMT consists of deciding the satisfiability of a ground 1st-order formula with respect to a background theory T

Example 1: $\mathcal{T}$ is Equality with Uninterpreted Functions (UIF):

$$f(g(a)) \not\approx f(c) \;\vee\; g(a) \approx d, \quad g(a) \approx c, \quad c \not\approx d$$

Example 2: for combined theories:

$$A \approx \mathrm{write}(B, a+1, 4), \qquad \mathrm{read}(A, b+3) \approx 2 \;\vee\; f(a-1) \not\approx f(b+1)$$

SAT Modulo Theories (SMT)

The "very eager" approach to SMT

Method:

– translate problem into equisatisfiable propositional formula;

– use off-the-shelf SAT solver

- Why "eager"?

  Search uses all theory information from the beginning

- Characteristics:

  + Can use best available SAT solver

  – Sophisticated encodings are needed for each theory

  – Sometimes translation and/or solving too slow

Main Challenge for alternative approaches is to combine:

- DPLL-based techniques for handling the boolean structure

- Efficient theory solvers for conjunctions of $\mathcal{T}$-literals

SAT Modulo Theories (SMT)

"Lazy" approaches to SMT: Idea

Example: consider $\mathcal{T} = UIF$ and the following set of clauses:

$$\underbrace{f(g(a)) \not\approx f(c)}_{\neg P_1} \vee \underbrace{g(a) \approx d}_{P_2}, \quad \underbrace{g(a) \approx c}_{P_3}, \quad \underbrace{c \not\approx d}_{\neg P_4}$$

1. Send $\{\neg P_1 \vee P_2,\ P_3,\ \neg P_4\}$ to SAT solver

   SAT solver returns model $[\neg P_1, P_3, \neg P_4]$
   Theory solver says $\neg P_1 \wedge P_3 \wedge \neg P_4$ is $\mathcal{T}$-inconsistent

2. Send $\{\neg P_1 \vee P_2,\ P_3,\ \neg P_4,\ P_1 \vee \neg P_3 \vee P_4\}$ to SAT solver

   SAT solver returns model $[P_1, P_2, P_3, \neg P_4]$
   Theory solver says $P_1 \wedge P_2 \wedge P_3 \wedge \neg P_4$ is $\mathcal{T}$-inconsistent

3. Send $\{\neg P_1 \vee P_2, P_3, \neg P_4, P_1 \vee \neg P_3 \vee P_4, \neg P_1 \vee \neg P_2 \vee \neg P_3 \vee P_4\}$ to SAT solver

   SAT solver says UNSAT

SAT Modulo Theories (SMT)

Optimized lazy approach

LA	• Check T-consistency only of full propositional models
OLA	• Check T-consistency of partial assignment while being built
LA	• Given a T-inconsistent assignment M, add $\neg M$ as a clause
OLA	• Given a T-inconsistent assignment M, find an explanation (a small T-inconsistent subset of M) and add it as a clause
LA	• Upon a T-inconsistency, add clause and restart
OLA	• Upon a T-inconsistency, do conflict analysis of the explanation and Backjump

SAT Modulo Theories (SMT)

"Lazy" approaches to SMT

- Why "lazy"?

Theory information used only lazily, when checking $\mathcal{T}$-consistency of propositional models

- Characteristics:

  + Modular and flexible
  − Theory information does not guide the search (only validates a posteriori)

Tools: CVC-Lite, ICS, MathSAT, TSAT+, Verifun, ...