Verification

Lecture 33

Martin Zimmermann

UNIVERSITÄT
DES
SAARLANDES

Plan for today

- Deductive verification
  - The Nelson-Oppen Method

Review: Decidability of first-order theories

Theory		**full**	**QFF**
T_E	Equality	no	yes
T_{PA}	Peano arithmetic	no	no
$T_{\mathbb{N}}$	Presburger arithmetic	yes	yes
$T_{\mathbb{Z}}$	integers	yes	yes
$T_{\mathbb{R}}$	reals	yes	yes
$T_{\mathbb{Q}}$	rationals	yes	yes
T_{cons}	lists	no	yes
T_{A}	arrays	no	yes
$T_{\mathsf{A}}^{=}$	arrays with extensionality	no	yes

What about `sorted`?

From the πVC tutorial:

```
predicate sorted(int[] arr, int low, int high) :=
(forall a,b.  ((low <= a && a <= b && b <= high) ->
               arr[a]<=arr[b]));
```

$$\forall a \forall b ((low \leq a \wedge a \leq b \wedge b \leq high) \rightarrow arr[a] \leq arr[b])$$

Neither a formula of $T_{\mathbb{Z}}$ nor a formula of T_{A}.

Combining Decision Procedures

Given

Theories T_i over signatures Σ_i
(constants, functions, predicates)
with corresponding decision procedures P_i for T_i-satisfiability.

Goal

Decide satisfiability of a sentence in theory $\bigcup_i T_i$.

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?

Combining Decision Procedures

Σ_1-theory T_1
$\boxed{P_1}$ for T_1-satisfiability

Σ_2-theory T_2
$\boxed{P_2}$ for T_2-satisfiability

?

$\boxed{P}$ for $(T_1 \cup T_2)$-satisfiability

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

Nelson-Oppen Combination Method (N-O Method)

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

Σ_1-theory T_1
stably infinite

$\boxed{P_1}$ for T_1-satisfiability
of quantifier-free Σ_1-formulae

Σ_2-theory T_2
stably infinite

$\boxed{P_2}$ for T_2-satisfiability
of quantifier-free Σ_2-formulae

$\boxed{P}$ for $(T_1 \cup T_2)$-satisfiability
of quantifier-free $(\Sigma_1 \cup \Sigma_2)$-formulae

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.,

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

   and both must contain the axioms of the theory of equality.
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 DNF and check each disjunct.

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
and that has a domain whose quotient by the interpretation of = is of infinite cardinality.

Example: Σ-theory T

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

Axioms

- $\forall x.\ x = a \ \vee \ x = b$
- and all axioms of the theory of equality

For every T-interpretation I, $|D_I|/\alpha_I(=) \leq 2$ (at most two elements).
Hence, T is not stably infinite.

All the other theories mentioned so far are stably infinite.

Example: Theory of partial orders

Σ-theory $T_{\preceq}$

$$\Sigma_{\preceq} : \ \{\preceq, \ =\}$$

where $\preceq$ is a binary predicate.

Axioms

1. $\forall x.\ x \preceq x$ ($\preceq$ reflexivity)
2. $\forall x, y.\ x \preceq y \ \wedge \ y \preceq x \ \rightarrow \ x = y$ ($\preceq$ antisymmetry)
3. $\forall x, y, z.\ x \preceq y \ \wedge \ y \preceq z \ \rightarrow \ x \preceq z$ ($\preceq$ transitivity)
4. the axioms of the theory of equality

We prove $T_{\preceq}$ is stably infinite.

Consider $T_{\preceq}$-satisfiable quantifier-free $\Sigma_{\preceq}$-formula F.
Consider arbitrary satisfying $T_{\preceq}$-interpretation $I : (D_I, \alpha_I)$,
where α_I maps $\preceq$ to $\leq_I$ and $=$ to $=_I$.

- Let $A = \{1_0, a_1, a_2, \ldots\}$ be any infinite set disjoint from D_I
- Construct new interpretation $J : (D_J, \alpha_J)$
  - $D_J = D_I \cup A$
  - $\alpha_J = \{\preceq \mapsto \leq_J, = \mapsto =_J\}$, where for $a, b \in D_J$,
    $a \leq_J b$ iff one of the following cases holds:
    - $a, b \in D_I$ and $a \leq_I b$, or
    - $a, b \in A$, $a = a_i$, $b = a_j$ and $i \leq j$.

  and $a =_J b$ iff $a, b \in D_I$ and $a =_I b$

J is $T_{\preceq}$-interpretation satisfying F with infinite quotient of domain under interpretation of $=$ (all elements in A are pairwise unequal).
Hence, $T_{\preceq}$ is 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

Phase 1: Variable Abstraction

- Given conjunction F in theory $T_1 \cup T_2$.
- Convert to conjunction $F_1 \wedge F_2$ s.t.
  - F_i in theory T_i
  - $F_1 \wedge F_2$ satisfiable iff F satisfiable.

Phase 2: Check

- If there is some set S of equalities and disequalities between the shared variables of F_1 and F_2
  $\text{shared}(F_1, F_2) = \text{free}(F_1) \cap \text{free}(F_2)$
  s.t. $S \wedge F_i$ are T_i-satisfiable for all i,
  then F is **satisfiable**.
- Otherwise, **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

Σ_1-formula F_1 and Σ_2-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.

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

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 $\mathrm{hd}(t) \in \Sigma_j$,

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

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

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

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

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

(4) if $\mathrm{hd}(s) \in \Sigma_i$ and $\mathrm{hd}(t) \in \Sigma_j$,

$$F[s \neq t] \quad \Rightarrow \quad F[w_1 \neq w_2] \ \wedge \ w_1 = s \ \wedge \ w_2 = t$$

where w, w_1, and w_2 are fresh variables.

Phase 2: Guess and Check

- Phase 1 separated $(\Sigma_1 \cup \Sigma_2)$-formula F into two formulae:
  Σ_1-formula F_1 and Σ_2-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:
  $$\alpha(V, E) : \bigwedge_{u,v \,\in\, V.\ uEv} u = v \ \wedge \bigwedge_{u,v \,\in\, V.\ \neg(uEv)} u \neq v$$

Then,
the original formula F is $(T_1 \cup T_2)$-satisfiable iff
there exists an equivalence relation E of 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.

Practical Efficiency

Phase 2 was formulated as “guess and check”:
First, guess an equivalence relation E,
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
Phase 1 as before
Phase 2 asks the decision procedures P_1 and P_2 to propagate new equalities.

Convex Theories

$\boxed{\text{Equality propagation is a decision procedure for convex theories.}}$

Def. A Σ-theory T is convex iff

for every quantifier-free conjunction Σ-formula F

and for every disjunction $\bigvee_{i=1}^{n}(u_i = v_i)$

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

then $F \vDash u_i = v_i$, for some $i \in \{1, \ldots, n\}$

Convex Theories

- $T_E, T_{\mathbb{R}}, T_{\mathbb{Q}}, T_{\text{cons}}$ are convex
- $T_{\mathbb{Z}}, T_{\mathsf{A}}$ are not convex

Example: $T_{\mathbb{Z}}$ is not convex

Consider quantifier-free conjunction

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

Then

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

but

$$F \ \not\models \ z = u$$

$$F \ \not\models \ z = v$$

Example:

The theory of arrays T_A is not convex.
Consider the quantifier-free conjunctive Σ_A-formula

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

Then

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

but

$$\begin{array}{l} F \not\Rightarrow i = j \\ F \not\Rightarrow a[j] = v \; . \end{array}$$

What if T is Not Convex?

Case split when:

$$\Gamma \models \bigvee_{i=1}^{n} (u_i = v_i)$$

but

$$\Gamma \not\models u_i = v_i \qquad \text{for all } i = 1, \ldots, n$$

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