Decision Procedures in Verification

First-Order Logic (4)

3.12.2012

Viorica Sofronie-Stokkermans

e-mail: sofronie@uni-koblenz.de

Until now:

Syntax (one-sorted signatures vs. many-sorted signatures)

Semantics

Models, Validity, and Satisfiability

Entailment and Equivalence

Logical theories

Syntactic view: axioms $\mathcal{F}$ of (closed) first-order Σ-formulae.
$\mathrm{Mod}(\mathcal{F}) = \{\mathcal{A} \in \Sigma\text{-alg} \mid \mathcal{A} \models G, \text{ for all } G \text{ in } \mathcal{F}\}$

Semantic view: class $\mathcal{M}$ of Σ-algebras
$\mathrm{Th}(\mathcal{M}) = \{G \in F_\Sigma(X) \text{ closed} \mid \mathcal{M} \models G\}$

Algorithmic Problems; Decidability, Undecidability

Until now:

Methods for checking satisfiability: resolution

Normal Forms:

- Prenex Normal Form
- Skolemization
- Clausal Normal Form (Conjunctive Normal Form)

General resolution:

- Proposition resolution/resolution for ground clauses
- Lifting principle
- General resolution calculus (soundness and completeness)
- Unification
- Consequences:
  - Herbrand's theorem
  - The theorem of Löwenheim-Skolem
  - Compactness of predicate logic

Resolution for ground clauses

- Refinements with orderings and selection functions:

  Need: - well-founded ordering on ground atomic formulae/literals

  - selection function (for negative literals)

  $S : C \quad \mapsto \quad$ set of occurrences of *negative* literals in C

  Example of selection with selected literals indicated as $\boxed{X}$:

  $\boxed{\neg A} \vee \neg A \vee B$

  $\boxed{\neg B_0} \vee \boxed{\neg B_1} \vee A$

Ordered resolution with selection $Res^{\succ}_{S}$

Ordered resolution with selection

$$\frac{C \vee A \qquad D \vee \neg A}{C \vee D}$$

if

1. $A \succ C$;
2. nothing is selected in C by S;
3. $\neg A$ is selected in $D \vee \neg A$,
   or else nothing is selected in $D \vee \neg A$ and $\neg A \succeq \max(D)$.

Note: For positive literals, $A \succ C$ is the same as $A \succ \max(C)$.

Ordered factoring

$$\frac{C \vee A \vee A}{(C \vee A)}$$

if A is maximal in C and nothing is selected in C.

2.8 Ordered Resolution with Selection

Resolution Calculus $Res^{\succ}_{S}$

In the completeness proof, we talk about (strictly) maximal literals of *ground* clauses.

In the non-ground calculus, we have to consider those literals that correspond to (strictly) maximal literals of ground instances:

Let $\succ$ be a total and well-founded ordering on ground atoms. A literal L is called [strictly] maximal in a clause C if and only if there exists a ground substitution σ such that for all L' in C: $L\sigma \succeq L'\sigma$ [$L\sigma \succ L'\sigma$].

Example

Let $\Sigma = (\Omega, \Pi)$, with $\Omega = \{c/0, d/0\}$ and $\Pi = \{p/1, q/2\}$

Let $\succ$ be a total ordering on ground atoms such that

$$p(c) \succ q(c,c) \succ q(c,d) \succ q(d,c) \succ q(d,d) \succ p(d)$$

Consider the clause $C = p(x) \vee q(x,y)$.

- $p(x)$ is strictly maximal in C:
  There exists a ground substitution σ_1 with $\sigma_1(x) = c = \sigma_1(y)$ such that $\sigma_1(p(x)) = p(c) \succ q(c,c) \succ \sigma_1(q(x,y))$.
- $q(x,y)$ is strictly maximal in C:
  There exists a ground substitution σ_2 with $\sigma_2(x) = d = \sigma_2(y)$ such that $\sigma_2(q(x,y)) = q(d,d) \succ p(d) = \sigma_2(p(x))$.

Resolution Calculus $Res_S^{\succ}$

Let $\succ$ be an atom ordering and S a selection function.

$$\frac{C \vee A \qquad \neg B \vee D}{(C \vee D)\sigma}$$ [ordered resolution with selection]

if $\sigma = \mathrm{mgu}(A, B)$ and

(i) $A\sigma$ strictly maximal wrt. $C\sigma$;

(ii) nothing is selected in C by S;

(iii) either $\neg B$ is selected,
or else nothing is selected in $\neg B \vee D$ and $\neg B\sigma$ is maximal in $D\sigma$.

Resolution Calculus $Res_S^{\succ}$

$$\frac{C \vee A \vee B}{(C \vee A)\sigma}$$ [ordered factoring]

if $\sigma = \mathrm{mgu}(A, B)$ and $A\sigma$ is maximal in $C\sigma$ and nothing is selected in C.

Example

Let $\Sigma = (\Omega, \Pi)$, with $\Omega = \{c/0, d/0\}$ and $\Pi = \{p/1, q/2\}$

Let $\succ$ be a total ordering on ground atoms such that

$$p(c) \succ q(c,c) \succ q(c,d) \succ q(d,c) \succ q(d,d) \succ p(d)$$

Consider the clauses $C = p(x) \vee q(x,y), \quad C_1 = \neg p(z), \quad C_2 = \neg q(z,u)$

- $p(x)$ and $q(x,y)$ are both strictly maximal in C.

The following inferences are possible:

$$\frac{p(x) \vee q(x,y) \qquad \neg p(z)}{q(z,y)} \qquad \frac{p(x) \vee q(x,y) \qquad \neg q(z,u)}{p(z)}$$

Soundness and Refutational Completeness

Theorem 2.39:

Let $\succ$ be an atom ordering and S a selection function such that $Res_S^{\succ}(N) \subseteq N$. Then

$$N \models \bot \Leftrightarrow \bot \in N$$

Proof:

The "$\Leftarrow$" part is trivial. For the "$\Rightarrow$" part consider first the propositional level: Construct a candidate model I_N as for unrestricted resolution, except that clauses C in N that have selected literals are not productive, even when they are false in I_C and when their maximal atom occurs only once and positively.

The result for general clauses follows using the same argument as in the completeness proof for "usual" resolution.

Redundancy

So far: local restrictions of the resolution inference rules using orderings and selection functions.

Is it also possible to delete clauses altogether?
Under which circumstances are clauses unnecessary?
(Conjecture: e. g., if they are tautologies or if they are subsumed by other clauses.)

Intuition: If a clause is guaranteed to be neither a minimal counterexample nor productive, then we do not need it.

Construction of Candidate Models Formally

Let $N, \succ$ be given.

- Order N increasing w.r.t. the extension of $\succ$ to clauses.
- Define sets I_C and Δ_C for all ground clauses C over the given signature inductively over $\succ$:

$$I_C := \bigcup_{C \succ D} \Delta_D$$

$$\Delta_C := \begin{cases} \{A\}, & \text{if } C \in N,\ C = C' \vee A,\ A \succ C',\ I_C \not\models C \\ & \text{and nothing is selected in } C \\ \emptyset, & \text{otherwise} \end{cases}$$

  We say that C produces A, if $\Delta_C = \{A\}$.

The candidate model for N (wrt. $\succ$) is given as $I_N^{\succ} := \bigcup_C \Delta_C$.

(We write I_N for $I_N^{\succ}$ if $\succ$ is irrelevant or known from the context.)

Recall

Construction of I for the extended clause set:

	clauses C	I_C	Δ_C	Remarks
1	$\neg P_0$	$\emptyset$	$\emptyset$	
2	$P_0 \vee P_1$	$\emptyset$	$\{P_1\}$	
3	$P_1 \vee P_2$	$\{P_1\}$	$\emptyset$	
4	$\neg P_1 \vee P_2$	$\{P_1\}$	$\{P_2\}$	
9	$\neg P_1 \vee \neg P_1 \vee P_3 \vee P_0$	$\{P_1, P_2\}$	$\{P_3\}$	
8	$\neg P_1 \vee \neg P_1 \vee P_3 \vee P_3 \vee P_0$	$\{P_1, P_2, P_3\}$	$\emptyset$	true in $\mathcal{A}_C$
5	$\neg P_1 \vee P_4 \vee P_3 \vee P_0$	$\{P_1, P_2, P_3\}$	$\emptyset$	
6	$\neg P_1 \vee \neg P_4 \vee P_3$	$\{P_1, P_2, P_3\}$	$\emptyset$	true in $\mathcal{A}_C$
7	$\neg P_3 \vee P_5$	$\{P_1, P_2, P_3\}$	$\{P_5\}$	

The resulting $I = \{P_1, P_2, P_3, P_5\}$ is a model of the clause set.

A Formal Notion of Redundancy

Let N be a set of ground clauses and C a ground clause (not necessarily in N). C is called redundant w. r. t. N, if there exist $C_1, \ldots, C_n \in N$, $n \geq 0$, such that $C_i \prec C$ and $C_1, \ldots, C_n \models C$.

Redundancy for general clauses:
C is called redundant w. r. t. N, if all ground instances $C\sigma$ of C are redundant w. r. t. $G_\Sigma(N)$.

Intuition: Redundant clauses are neither minimal counterexamples nor productive.

Note: The same ordering $\succ$ is used for ordering restrictions and for redundancy (and for the completeness proof).

Examples of Redundancy

Proposition 2.40:

- C tautology (i.e., $\models C$) $\Rightarrow$ C redundant w. r. t. any set N.
- $C\sigma \subset D \Rightarrow D$ redundant w. r. t. $N \cup \{C\}$
- $C\sigma \subseteq D \Rightarrow D \vee \overline{L}\sigma$ redundant w. r. t. $N \cup \{C \vee L,\ D\}$

(Under certain conditions one may also use non-strict subsumption, but this requires a slightly more complicated definition of redundancy.)

Saturation up to Redundancy

N is called saturated up to redundancy (wrt. $Res_S^{\succ}$)

$$:\Leftrightarrow Res_S^{\succ}(N \setminus Red(N)) \subseteq N \cup Red(N)$$

Theorem 2.41:

Let N be saturated up to redundancy. Then

$$N \models \bot \Leftrightarrow \bot \in N$$

Saturation up to Redundancy

Proof (Sketch):
(i) Ground case:

- consider the construction of the candidate model $I_N^{\succ}$ for $Res_S^{\succ}$
- redundant clauses are not productive
- redundant clauses in N are not minimal counterexamples for $I_N^{\succ}$

The premises of "essential" inferences are either minimal counterexamples or productive.

(ii) Lifting: no additional problems over the proof of Theorem 2.39.

Monotonicity Properties of Redundancy

Theorem 2.42:

(i) $N \subseteq M \Rightarrow Red(N) \subseteq Red(M)$

(ii) $M \subseteq Red(N) \Rightarrow Red(N) \subseteq Red(N \setminus M)$

We conclude that redundancy is preserved when, during a theorem proving process, one adds (derives) new clauses or deletes redundant clauses.

Monotonicity Properties of Redundancy

Theorem 2.42:

(i) $N \subseteq M \Rightarrow Red(N) \subseteq Red(M)$

(ii) $M \subseteq Red(N) \Rightarrow Red(N) \subseteq Red(N \setminus M)$

Proof:

(i) Let $C \in red(N)$. Then there exist $C_1, \ldots, C_n \in N, n \geq 0$ such that $C_i \prec C$ for all $i = 1, \ldots, n$ and $C_1, \ldots, C_n \models C$.

We assumed that $N \subseteq M$, so we know that $C_1, \ldots, C_n \in M$. Thus: there exist $C_1, \ldots, C_n \in M, n \geq 0$ such that $C_i \prec C$ for all $i = 1, \ldots, n$ and $C_1, \ldots, C_n \models C$. Therefore, $C \in Red(M)$.

Monotonicity Properties of Redundancy

Theorem 2.42:

(i) $N \subseteq M \Rightarrow Red(N) \subseteq Red(M)$

(ii) $M \subseteq Red(N) \Rightarrow Red(N) \subseteq Red(N \setminus M)$

Proof (Idea):

(ii) Let $C \in Red(N)$. Then there exist $C_1, \ldots, C_n \in N, n \geq 0$ such that $C_i \prec C$ for all $i = 1, \ldots, n$ and $C_1, \ldots, C_n \models C$.

Case 1: For all i, $C_i \notin M$. Then $C \in Red(N \setminus M)$.

Case 2: For some i, $C_i \in M \subseteq Red(N)$. Then for every such index i there exist $C_1^i, \ldots, C_{n_i}^i \in N$ such that $C_j^i \prec C_i$ and $C_1^i, \ldots, C_{n_i}^i \models C_i$. We can replace C_i above with $C_1^i, \ldots, C_{n_i}^i$. We can iterate the procedure until none of the C_i's are in M (termination guaranteed by the fact that $\succ$ is well-founded).

Decidable subclasses of first-order logic

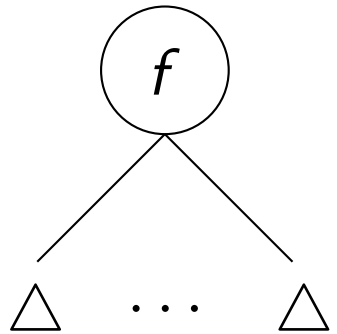
Herbrand Interpretations

Assume Ω contains at least one constant symbol.

A Herbrand interpretation (over Σ) is a Σ-algebra $\mathcal{A}$ such that

- $U_{\mathcal{A}} = \mathsf{T}_{\Sigma}$ (= the set of ground terms over Σ)
- $f_{\mathcal{A}} : (s_1, \ldots, s_n) \mapsto f(s_1, \ldots, s_n), \;\; f/n \in \Omega$

$$f_{\mathcal{A}}(\triangle, \ldots, \triangle) =$$



Herbrand Interpretations

In other words, *values are fixed* to be ground terms and *functions are fixed* to be the term constructors. Only predicate symbols $p/m \in \Pi$ may be freely interpreted as relations $p_{\mathcal{A}} \subseteq \mathsf{T}_{\Sigma}^{m}$.

Proposition 2.12

Every set of ground atoms I uniquely determines a Herbrand interpretation $\mathcal{A}$ via

$$(s_1, \ldots, s_n) \in p_{\mathcal{A}} \quad :\Leftrightarrow \quad p(s_1, \ldots, s_n) \in I$$

Thus we shall identify Herbrand interpretations (over Σ) with sets of Σ-ground atoms.

Herbrand Interpretations

Example: $\Sigma_{Pres} = (\{0/0, s/1, +/2\},\ \{</2, \leq/2\})$

$\mathbb{N}$ as Herbrand interpretation over Σ_{Pres}:

$$
\begin{aligned}
I = \{ \quad & 0 \leq 0,\ 0 \leq s(0),\ 0 \leq s(s(0)),\ \ldots, \\
& 0 + 0 \leq 0,\ 0 + 0 \leq s(0),\ \ldots, \\
& \ldots,\ (s(0) + 0) + s(0) \leq s(0) + (s(0) + s(0)) \\
& \ldots \\
& s(0) + 0 < s(0) + 0 + 0 + s(0) \\
& \ldots\}
\end{aligned}
$$

Existence of Herbrand Models

A Herbrand interpretation I is called a Herbrand model of F, if $I \models F$.

Theorem 2.13

Let N be a set of Σ-clauses.

$$\begin{array}{lcl} N \text{ satisfiable} & \Leftrightarrow & N \text{ has a Herbrand model (over } \Sigma) \\ & \Leftrightarrow & G_\Sigma(N) \text{ has a Herbrand model (over } \Sigma) \end{array}$$

where $G_\Sigma(N) = \{C\sigma \text{ ground clause} \mid C \in N,\ \sigma : X \to \mathrm{T}_\Sigma\}$ is the set of ground instances of N.

(Proof – completeness proof of resolution for first-order logic.)

Example of a G_Σ

For Σ_{Pres} one obtains for

$$C = (x < y) \vee (y \leq s(x))$$

the following ground instances:

$(0 < 0) \vee (0 \leq s(0))$
$(s(0) < 0) \vee (0 \leq s(s(0)))$
$\ldots$
$(s(0) + s(0) < s(0) + 0) \vee (s(0) + 0 \leq s(s(0) + s(0)))$
$\ldots$

Consequences of Herbrans's theorem

Decidability results.

- Formulae without function symbols and without equality

  The Bernays-Schönfinkel Class $\exists^*\forall^*$

The Bernays-Schönfinkel Class

$\Sigma = (\Omega, \Pi)$, Ω is a finite set of constants

The Bernays-Schönfinkel class consists only of sentences of the form

$$\exists x_1 \ldots \exists x_n \forall y_1 \ldots \forall y_m F(x_1, \ldots, x_n, y_1, \ldots, y_n)$$

The Bernays-Schönfinkel Class

$\Sigma = (\Omega, \Pi)$, Ω is a finite set of constants

The Bernays-Schönfinkel class consists only of sentences of the form

$$\exists x_1 \ldots \exists x_n \forall y_1 \ldots \forall y_m F(x_1, \ldots, x_n, y_1, \ldots, y_n)$$

Idea: CNF translation:

$$\begin{aligned}
&\exists \overline{x}_1 \forall \overline{y}_1 F_1 \wedge \ldots \exists \overline{x}_n \forall \overline{y}_n F_n \\
&\qquad \Rightarrow_P \exists \overline{x}_1 \ldots \exists \overline{x}_n \forall \overline{y}_1 \ldots \forall \overline{y}_n F(\overline{x}_1, \ldots, \overline{x}_n, \overline{y}_1, \ldots, \overline{y}_n) \\
&\qquad \Rightarrow_S \forall \overline{y}_1 \ldots \forall \overline{y}_m F(\overline{c}_1, \ldots, \overline{c}_n, \overline{y}_1, \ldots, \overline{y}_n) \\
&\qquad \Rightarrow_K \forall \overline{y}_1 \ldots \forall \overline{y}_m \bigwedge \bigvee L_i((\overline{c}_1, \ldots, \overline{c}_n, \overline{y}_1, \ldots, \overline{y}_n)
\end{aligned}$$

$\overline{c}_1, \ldots, \overline{c}_n$ are tuples of Skolem constants

The Bernays-Schönfinkel Class

$\Sigma = (\Omega, \Pi)$, Ω is a finite set of constants

The Bernays-Schönfinkel class consists only of sentences of the form

$$\exists x_1 \ldots \exists x_n \forall y_1 \ldots \forall y_m F(x_1, \ldots, x_n, y_1, \ldots, y_n)$$

Idea: CNF translation:

$$\exists \overline{x}_1 \forall \overline{y}_1 F_1 \wedge \ldots \exists \overline{x}_n \forall \overline{y}_n F_n$$
$$\Rightarrow_K^* \forall \overline{y}_1 \ldots \forall \overline{y}_m \bigwedge \bigvee L_i((\overline{c}_1, \ldots, \overline{c}_n, \overline{y}_1, \ldots, \overline{y}_n)$$

$\overline{c}_1, \ldots, \overline{c}_n$ are tuples of Skolem constants

The Herbrand Universe is finite $\mapsto$ decidability