Decision Procedures in Verification

First-Order Logic (4)

5.12.2022

Viorica Sofronie-Stokkermans

e-mail: sofronie@uni-koblenz.de

Until now:

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

Semantics

Structures (also many-sorted)

Models, Validity, and Satisfiability

Entailment and Equivalence

Theories (Syntactic vs. Semantics view)

Normal Forms

Herbrand Interpretations

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

Tractable classes (Horn fragment, Local theories)

General Resolution

Resolution for General Clauses

General binary resolution *Res*:

$$\frac{C \vee A \qquad D \vee \neg B}{(C \vee D)\sigma} \quad \text{if } \sigma = \mathrm{mgu}(A, B) \qquad \text{[resolution]}$$

$$\frac{C \vee A \vee B}{(C \vee A)\sigma} \quad \text{if } \sigma = \mathrm{mgu}(A, B) \quad \text{[factorization]}$$

For inferences with more than one premise, we assume that the variables in the premises are (bijectively) renamed such that they become different to any variable in the other premises.
We do not formalize this. Which names one uses for variables is otherwise irrelevant.

Herbrand's Theorem

Lemma 2.33:

Let N be a set of Σ-clauses, let $\mathcal{A}$ be an interpretation.
Then $\mathcal{A} \models N$ implies $\mathcal{A} \models G_\Sigma(N)$.

Lemma 2.34:

Let N be a set of Σ-clauses, let $\mathcal{A}$ be a *Herbrand* interpretation.
Then $\mathcal{A} \models G_\Sigma(N)$ implies $\mathcal{A} \models N$.

Theorem 2.35 (Herbrand):

A set N of Σ-clauses is satisfiable if and only if it has a Herbrand model over Σ.

Consequences

Theorem 2.36 (Löwenheim–Skolem):
Let Σ be a countable signature and let S be a set of closed Σ-formulas. Then S is satisfiable iff S has a model over a countable universe.

Theorem (Refutational Completeness of General Resolution)
Let N be a set of general clauses where $Res(N) \subseteq N$. Then

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

Theorem 2.38 (Compactness Theorem for First-Order Logic):
Let Φ be a set of first-order formulas.
Φ is unsatisfiable $\Leftrightarrow$ some finite subset $\Psi \subseteq \Phi$ is unsatisfiable.

Compactness of Predicate Logic

Theorem 2.38 (Compactness Theorem for First-Order Logic):
Let Φ be a set of first-order formulas.
Φ is unsatisfiable $\Leftrightarrow$ some finite subset $\Psi \subseteq \Phi$ is unsatisfiable.

Proof:
The "$\Leftarrow$" part is trivial. For the "$\Rightarrow$" part let Φ be unsatisfiable and let N be the set of clauses obtained by Skolemization and CNF transformation of the formulas in Φ. Clearly $Res^*(N)$ is unsatisfiable. By Theorem 2.37, $\bot \in Res^*(N)$, and therefore $\bot \in Res^n(N)$ for some $n \in \mathbb{N}$. Consequently, $\bot$ has a finite resolution proof B of depth $\leq n$. Choose Ψ as the subset of formulas in Φ such that the corresponding clauses contain the assumptions (leaves) of B.

2.12 Ordered Resolution with Selection

Motivation: Search space for *Res* *very* large.

Ideas for improvement:

1. In the completeness proof (Model Existence Theorem 2.23) one only needs to resolve and factor maximal atoms
   $\Rightarrow$ if the calculus is restricted to inferences involving maximal atoms, the proof remains correct
   $\Rightarrow$ *order restrictions*

2. In the proof, it does not really matter with which negative literal an inference is performed
   $\Rightarrow$ choose a negative literal don't-care-nondeterministically
   $\Rightarrow$ *selection*

Selection Functions

A selection function is a mapping

$$S : C \quad \mapsto \quad \text{set of occurrences of } \textit{negative} \text{ literals in } C$$

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

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

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

Resolution Calculus $Res_S^{\succ}$

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: $L\sigma \succeq L'\sigma$ $[L\sigma \succ L'\sigma]$.

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 $\sigma = \text{mgu}(A, B)$ 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 $Res_S^{\succ}$

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

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

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 lifting lemma.

Craig Interpolation

Theorem: $Res_S^{\succ}$ is sound and refutationally complete.

A theoretical application of ordered resolution is Craig- Interpolation:

Theorem (Craig 57)

Let F and G be two propositional formulas such that $F \models G$.

Then there exists a formula H (called the interpolant for $F \models G$), such that H contains only propostional variables occurring both in F and in G, and such that $F \models H$ and $H \models G$.

Craig Interpolation

Proof:

Translate F and $\neg G$ into CNF.

Let N and M, resp., denote the resulting clause set.

Choose an atom ordering $\succ$ for which the propositional variables that occur in F but not in G are maximal.

Saturate N into N^* wrt. $\mathrm{Res}_S^{\succ}$ with an empty selection function S.

Then saturate $N^* \cup M$ wrt. $\mathrm{Res}_S^{\succ}$ to derive $\bot$.

As N^* is already saturated, due to the ordering restrictions only inferences need to be considered where premises, if they are from N^*, only contain symbols that also occur in G.

The conjunction of these premises is an interpolant H.

The theorem also holds for first-order formulas. For universal formulas the above proof can be easily extended. In the general case, a proof based on resolution technology is more complicated because of Skolemization.

Applications of Craig Interpolation

Modular databases

Given: Two databases (different but possibly overlapping languages)

Task: Is the union of the two databases consistent? If not: locate error

Applications of Craig Interpolation

Modular databases

Given: Two databases (different but possibly overlapping languages)

Logical modeling: $F_1 \wedge F_2$

Task: Is the union of the two databases consistent? If not: locate error

$F_1 \wedge F_2 \models \perp$

Applications of Craig Interpolation

Modular databases

Given: Two databases (different but possibly overlapping languages)

Logical modeling: $F_1 \wedge F_2$

Task: Is the union of the two databases consistent? If not: locate error

$F_1 \wedge F_2 \models \perp$

$F_1 \models \neg F_2$ (assume we are in prop. logic)

Applications of Craig Interpolation

Modular databases

Given: Two databases (different but possibly overlapping languages)

Logical modeling: $F_1 \wedge F_2$

Task: Is the union of the two databases consistent? If not: locate error

$F_1 \wedge F_2 \models \perp$

$F_1 \models \neg F_2$ (assume we are in prop. logic)

Craig Interpolation (propositional case)

There exists I containing only propositional variables occurring in F_1 and F_2 such that:

$F_1 \models I$ and $I \models \neg F_2$

Applications of Craig Interpolation

Reasoning in combinations of theories

Given: Two theories (different but possibly overlapping languages) s.t. decision procedures for component theories for certain fragments exist

Task: Reason in the combination of the two theories

Question: Which information needs to be exchanged between provers?

Answer: Craig Interpolation

The case of two disjoint theories will be discussed later in this lecture

Applications of Craig Interpolation

Verification (programs or hardware)

Model programs as transition systems.

- Sets of states expressed as formulae
- Transitions expressed as formulae T

Question:
Can a state in a certain set of states E (error)
be reached from some state in a set I (initial) in k steps?

$\phi_I \wedge T_1 \wedge T_2 \wedge \cdots \wedge T_k \wedge \phi_E$

Applications of Craig Interpolation

Verification (programs or hardware)

Model programs as transition systems.

- Sets of states expressed as formulae
- Transitions expressed as formulae T

Question:

Can a state in a certain set of states E (error)
be reached from some state in a set I (initial) in k steps?

$$\underbrace{(\phi_I \wedge T_1)}_{F_1} \wedge \underbrace{(T_2 \wedge \cdots \wedge T_k \wedge \phi_E)}_{F_2}$$

Not reachable: $F_1 \wedge F_2 \models \perp$

Applications of Craig Interpolation

Verification (programs or hardware)

Model programs as transition systems.

- Sets of states expressed as formulae
- Transitions expressed as formulae T

Question:

Can a state in a certain set of states E (error)
be reached from some state in a set I (initial) in k steps?

$\underbrace{(\phi_I \wedge T_1)}_{F_1} \wedge \underbrace{(T_2 \wedge \cdots \wedge T_k \wedge \phi_E)}_{F_2}$ Not reachable: $F_1 \wedge F_2 \models \perp$

Interpolant: I overapproximates the set of successors of ϕ_I.

Goal

Goal: Make resolution efficient

Identify clauses which are not needed and can be discarded

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.

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 $C_1, \dots, C_n \in N$, $n \geq 0$, such that $C_i \prec C$ and $C_1, \dots, C_n \models C$.

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

Proof:

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

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

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 $C^i_1, \dots, C^i_{n_i} \in N$ such that $C^i_j \prec C_i$ and $C^i_1, \dots, C^i_{n_i} \models C_i$. We can replace C_i above with $C^i_1, \dots, C^i_{n_i}$. 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).

Some theorem provers for first-order logic

• SPASS	`http://www.spass-prover.org/`
• E	`http://www4.informatik.tu-muenchen.de/~schulz/E/E.html`
• Vampire	`http://www.vprover.org/`