Formal Methods for Java
Lecture 12: Soundness of Sequent Calculus

Jochen Hoenicke

Software Engineering
Albert-Ludwigs-University Freiburg

June 12, 2017
Developed at University of Karlsruhe

http://www.key-project.org/

Interactive Theorem Prover

Theory specialized for Java(Card).

Can generate proof-obligations from JML specification.

Underlying theory: Sequent Calculus + Dynamic Logic

Proofs are given manually.
A sequent is a formula

$$\phi_1, \ldots, \phi_n \implies \psi_1, \ldots, \psi_m$$

where $\phi_i, \psi_i$ are formulae.

The meaning of this formula is:

$$\phi_1 \land \ldots \land \phi_n \rightarrow \psi_1 \lor \ldots \lor \psi_m$$
Sequent Calculus Logical Rules

**close:** \( \Gamma, \phi \Rightarrow \Delta, \phi \)

**false:** \( \Gamma, \text{false} \Rightarrow \Delta \)

**true:** \( \Gamma \Rightarrow \Delta, \text{true} \)

**not-left:** \( \frac{\Gamma \Rightarrow \Delta, \phi}{\Gamma, \neg \phi \Rightarrow \Delta} \)

**not-right:** \( \frac{\Gamma \Rightarrow \Delta, \neg \phi}{\Gamma \Rightarrow \Delta} \)

**and-left:** \( \frac{\Gamma, \phi, \psi \Rightarrow \Delta}{\Gamma, \phi \land \psi \Rightarrow \Delta} \)

**and-right:** \( \frac{\Gamma \Rightarrow \Delta, \phi \quad \Gamma \Rightarrow \Delta, \psi}{\Gamma \Rightarrow \Delta, \phi \land \psi} \)

**or-left:** \( \frac{\Gamma \Rightarrow \Delta, \phi \quad \Gamma, \psi \Rightarrow \Delta}{\Gamma, \phi \lor \psi \Rightarrow \Delta} \)

**or-right:** \( \frac{\Gamma \Rightarrow \Delta, \phi, \psi}{\Gamma \Rightarrow \Delta, \phi \lor \psi} \)

**impl-left:** \( \frac{\Gamma \Rightarrow \Delta, \phi \quad \Gamma, \psi \Rightarrow \Delta}{\Gamma, \phi \rightarrow \psi \Rightarrow \Delta} \)

**impl-right:** \( \frac{\Gamma, \phi \Rightarrow \Delta, \psi}{\Gamma \Rightarrow \Delta, \phi \rightarrow \psi} \)
The rules for the existential quantifier are dual:

**all-left:**
\[
\Gamma, \forall X \phi(X), \phi(t) \Rightarrow \Delta
\]
\[
\Rightarrow \Gamma, \forall X \phi(X) \Rightarrow \Delta
\]
where \( t \) is some arbitrary term.

**all-right:**
\[
\Gamma \Rightarrow \Delta, \phi(x_0)
\]
\[
\Rightarrow \Gamma \Rightarrow \Delta, \forall X \phi(X)
\]
where \( x_0 \) is a fresh identifier.

**exists-left:**
\[
\Gamma, \phi(x_0) \Rightarrow \Delta
\]
\[
\Rightarrow \Gamma, \exists X \phi(X) \Rightarrow \Delta
\]
where \( x_0 \) is a fresh identifier.

**exists-right:**
\[
\Gamma \Rightarrow \Delta, \exists X \phi(X), \phi(t)
\]
\[
\Rightarrow \Gamma \Rightarrow \Delta, \exists X \phi(X)
\]
where \( t \) is some arbitrary term.
Rules for equality

\[
\text{eq-close: } \Gamma \Rightarrow \Delta, \ t = t
\]

\[
\text{apply-eq: } \quad \frac{s = t, \Gamma[t/s] \Rightarrow \Delta[t/s]}{s = t, \Gamma \Rightarrow \Delta}
\]
The sequent calculus with the rules presented on the previous three slides is sound and complete.

- **Soundness**: Only true facts can be proven with the calculus.
- **Completeness**: Every true fact can be proven with the calculus.
A signature defines the constants, functions and predicates that can occur in a formula.

**Definition (Signature)**

A signature \( \text{Sig} = (\text{Func}, \text{Pred}) \) is a tuple of sets of function and predicate symbols, where

- \( f/k \in \text{Func} \) if \( f \) is a function symbol with \( k \) parameters,
- \( p/k \in \text{Pred} \) if \( p \) is a predicate symbol with \( k \) parameters.

A constant \( c/0 \in \text{Func} \) is a function without parameters. We assume there are infinitely many constants.
Structures

A structure gives a meaning to the constants, functions and predicates.

**Definition (Structure)**

A structure \( \mathcal{M} \) is a tuple \((\mathcal{D}, \mathcal{I})\). The domain \( \mathcal{D} \) is an arbitrary non-empty set. The interpretation \( \mathcal{I} \) assigns to

- each function symbol \( f/k \in \text{Func} \) of arity \( k \) a function
  \[
  \mathcal{I}(f) : \mathcal{D}^k \to \mathcal{D}
  \]

- and each predicate symbol \( p/k \in \text{Pred} \) of arity \( k \) a function
  \[
  \mathcal{I}(p) : \mathcal{D}^k \to \{\text{true, false}\}.
  \]

The interpretation \( \mathcal{I}(c) \) of a constant \( c/0 \in \text{Func} \) is an element of \( \mathcal{D} \).

Let \( \mathcal{M} = (\mathcal{D}, \mathcal{I}) \), \( c \) a constant and \( d \in \mathcal{D} \). With \( \mathcal{M}[c := d] \) we denote the structure \((\mathcal{D}, \mathcal{I}')\), where \( \mathcal{I}'(c) = d \) and \( \mathcal{I}'(f) = \mathcal{I}(f) \) for all other function symbols \( f \) and \( \mathcal{I}'(p) = \mathcal{I}(p) \) for all predicate symbols \( p \).
Semantics of Terms and Formulas

Let $\mathcal{M} = (\mathcal{D}, \mathcal{I})$ be a structure.

The semantics $\mathcal{M}[t]$ of a term $t$ is defined inductively by

$$\mathcal{M}[f(t_1, \ldots, t_k)] = \mathcal{I}(f)(\mathcal{M}[t_1], \ldots, \mathcal{M}[t_k]),$$

in particular $\mathcal{M}[c] = \mathcal{I}(c)$.

The semantics of formula $\phi$, $\mathcal{M}[\phi] \in \{\text{true}, \text{false}\}$, is defined by

- $\mathcal{M}[p(t_1, \ldots, t_k)] = \mathcal{I}(p)(\mathcal{M}[t_1], \ldots, \mathcal{M}[t_k])$.
- $\mathcal{M}[s = t] = \text{true}$, iff $\mathcal{M}[s] = \mathcal{M}[t]$.
- $\mathcal{M}[\phi \land \psi] = \begin{cases} \text{true} & \text{if } \mathcal{M}[\phi] = \text{true} \text{ and } \mathcal{M}[\psi] = \text{true}, \\ \text{false} & \text{otherwise.} \end{cases}$
- $\mathcal{M}[\phi \lor \psi], \mathcal{M}[\phi \to \psi], \text{ and } \mathcal{M}[\neg \phi]$, analogously.
- $\mathcal{M}[\forall X \phi(X)] = \text{true}$, iff for all $d \in \mathcal{D}$: $\mathcal{M}[x_0 := d][\phi(x_0)] = \text{true}$, where $x_0$ is a constant not occurring in $\phi$.
- $\mathcal{M}[\exists X \phi(X)] = \text{true}$, iff there is some $d \in \mathcal{D}$ with $\mathcal{M}[x_0 := d][\phi(x_0)] = \text{true}$, where $x_0$ is a constant not occurring in $\phi$. 
Models and Tautologies

Definition (Model)

A structure $\mathcal{M}$ is a model of a sequent $\phi_1, \ldots, \phi_n \Rightarrow \psi_1, \ldots, \psi_m$ if $\mathcal{M}[\phi_i] = \text{false}$ for some $1 \leq i \leq n$, or if $\mathcal{M}[\psi_j] = \text{true}$ for some $1 \leq j \leq m$. We say that the sequent holds in $\mathcal{M}$.

A sequent $\phi_1, \ldots, \phi_n \Rightarrow \psi_1, \ldots, \psi_m$ is a tautology, if all structures are models of this sequent.
A calculus is sound, iff every formula \( F \) for which a proof exists is a tautology.

- We write \( \vdash F \) to indicate that a proof for \( F \) exists.
- We write \( \models F \) to indicate that \( F \) is a tautology.
Definition (Soundness of a rule)

A rule $\frac{F_1 \cdots F_n}{G}$ is sound, iff

$\models F_1$ and $\cdots$ and $\models F_n$ imply $\models G$.

An axiom $G$ is sound, iff $G$ is a tautology, i.e., $\models G$.

Lemma

A calculus is sound, if all of its rules and axioms are sound.

Proof.

By structural induction over the proof.
Soundness of impl-left

The rule

\[ \frac{\Gamma \implies \Delta, \phi \quad \Gamma, \psi \implies \Delta}{\Gamma, \phi \rightarrow \psi \implies \Delta} \]

is sound:
Assume \( \Gamma \implies \Delta, \phi \) and \( \Gamma, \psi \implies \Delta \) are tautologies and \( \mathcal{M} \) is an arbitrary structure. Prove that \( F := (\Gamma, \phi \rightarrow \psi \implies \Delta) \) holds in \( \mathcal{M} \).

- If one of the formulas in \( \Gamma \) is false in \( \mathcal{M} \), then \( F \) holds in \( \mathcal{M} \).
- Otherwise, from \( \Gamma \implies \Delta, \phi \) it follows that \( \phi \) or a formula in \( \Delta \) is true.
- If \( \mathcal{M}[\phi] = \text{true} \) and \( \mathcal{M}[\psi] = \text{false} \), then \( \mathcal{M}[\phi \rightarrow \psi] = \text{false} \). Hence, \( F \) holds in \( \mathcal{M} \).
- If \( \mathcal{M}[\phi] = \text{true} \) and \( \mathcal{M}[\psi] = \text{true} \), then \( \Gamma, \psi \implies \Delta \) implies that a formula in \( \Delta \) is true.
- If a formula in \( \Delta \) is true, \( F \) holds in \( \mathcal{M} \).
Soundness of exists-left

exists-left: \[
\frac{\Gamma, \phi(x_0) \implies \Delta}{\Gamma, \exists X \phi(X) \implies \Delta}, \text{ where } x_0 \text{ is a fresh identifier (constant)}.
\]

Assume \( \Gamma, \phi(x_0) \implies \Delta \) is a tautology, where \( x_0 \) does not occur in \( \Gamma \) nor \( \Delta \). Given an arbitrary structure \( \mathcal{M} \), prove that \( F := (\Gamma, \exists X \phi(X) \implies \Delta) \) holds in \( \mathcal{M} \).

- If one of the formulas in \( \Gamma \) is \textbf{false} in \( \mathcal{M} \), then \( F \) holds.
- If \( \mathcal{M}[\exists X \phi(X)] = \textbf{false} \), then \( F \) holds in \( \mathcal{M} \).
- Otherwise, there is a \( d \in \mathcal{D} \) such that \( \mathcal{M}[x_0 := d][\phi(x_0)] = \textbf{true} \).
- Also in \( \mathcal{M}[x_0 := d] \), all formulas in \( \Gamma \) are \textbf{true}. Since \( \Gamma, \phi(x_0) \implies \Delta \) is a tautology, some formula of \( \Delta \) is \textbf{true} in \( \mathcal{M}[x_0 := d] \).
- Since \( x_0 \) does not occur in \( \Delta \), the formula is also \textbf{true} in the structure \( \mathcal{M} \). Therefore \( F \) holds in \( \mathcal{M} \).
Completeness

Theorem (Completeness)

*If a sequent $F$ is a tautology, it can be proven.*

In this lecture we do not prove completeness.