Formal Methods for Java
Lecture 21: Sequent Calculus

Jochen Hoenicke

Software Engineering
Albert-Ludwigs-University Freiburg

January 18, 2013
Sequent Calculus

Definition (Sequent)

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:

\[ \phi_1 \land \ldots \land \phi_n \implies \psi_1 \lor \ldots \lor \psi_m \]
Sequent Calculus Logical Rules

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

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

\[
\text{not-left:} \quad \frac{\Gamma \implies \Delta, \phi}{\Gamma, \neg \phi \implies \Delta}
\]

\[
\text{and-left:} \quad \frac{\Gamma, \phi, \psi \implies \Delta}{\Gamma, \phi \land \psi \implies \Delta}
\]

\[
\text{or-left:} \quad \frac{\Gamma, \phi \implies \Delta \quad \Gamma, \psi \implies \Delta}{\Gamma, \phi \lor \psi \implies \Delta}
\]

\[
\text{impl-left:} \quad \frac{\Gamma \implies \Delta, \phi \quad \Gamma, \psi \implies \Delta}{\Gamma, \phi \to \psi \implies \Delta}
\]

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

\[
\text{not-right:} \quad \frac{\Gamma, \phi \implies \Delta}{\Gamma \implies \Delta, \neg \phi}
\]

\[
\text{and-right:} \quad \frac{\Gamma \implies \Delta, \phi \quad \Gamma \implies \Delta, \psi}{\Gamma \implies \Delta, \phi \land \psi}
\]

\[
\text{or-right:} \quad \frac{\Gamma \implies \Delta, \phi, \psi}{\Gamma \implies \Delta, \phi \lor \psi}
\]

\[
\text{impl-right:} \quad \frac{\Gamma, \phi \implies \Delta, \psi}{\Gamma \implies \Delta, \phi \to \psi}
\]
The rules for the existential quantifier are dual:

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

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

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

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

**eq-close:** \[ \Gamma \equiv \Delta, t = t \]

**apply-eq:**

\[ \begin{align*}
\frac{s = t, \Gamma[t/s] \Rightarrow \Delta[t/s]}{s = t, \Gamma \Rightarrow \Delta} & \quad \text{apply-eq (\Delta : f(X) = f(f(c)))} \\
\frac{s = t, \Gamma[t/X] \Rightarrow \Delta[t/X]}{s = t, \Gamma[s/X] \Rightarrow \Delta[s/X]} & \quad \text{apply-eq (\Delta : X = f(f(c)))}
\end{align*} \]

Example: Prove \( c = f(c) \Rightarrow c = f(f(c)) \).

\[ \begin{align*}
\frac{c = f(c) \Rightarrow f(f(c)) = f(f(c))}{c = f(c) \Rightarrow f(c) = f(f(c))} & \quad \text{close-eq} \\
\frac{c = f(c) \Rightarrow f(c) = f(f(c))}{c = f(c) \Rightarrow c = f(f(c))} & \quad \text{apply-eq (\Delta : X = f(f(c)))}
\end{align*} \]
Soundness and Completeness

Theorem (Soundness and Completeness)

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.
**Signature**

**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.
Definition (Structure)

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

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

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

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

Let $\mathcal{M} = (\mathcal{D}, I)$, $c$ a constant and $d \in \mathcal{D}$. With $\mathcal{M}[c := d]$ we denote the structure $(\mathcal{D}, I')$, where $I'(c) = d$ and $I'(f) = I(f)$ for all other function symbols $f$ and $I'(p) = I(p)$ 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 $\mathcal{M}[s] = \mathcal{M}[t]$.
- $\mathcal{M}[\phi \land \psi] = \begin{cases} 
\text{true} & \text{if } \mathcal{M}[\phi] = \text{true} \text{ and } \mathcal{M}[\psi] = \text{true}, \\
\text{false} & \text{otherwise}.
\end{cases}$
- $\mathcal{M}[\phi \lor \psi], \mathcal{M}[\phi \rightarrow \psi], \text{ and } \mathcal{M}[\neg \phi]$, 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 $\phi$. 

Jochen Hoenicke  (Software Engineering)
Models and Tautologies

Definition (Model)

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

A sequent \( \phi_1, \ldots, \phi_n \implies \psi_1, \ldots, \psi_m \) 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 \( \frac{F_1 \ldots F_n}{G} \) is sound, iff

\[ \models F_1 \text{ and } \ldots \text{ and } \models F_n \text{ imply } \models G. \]

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.
The rule

\[
\Gamma \Rightarrow \Delta, \phi \quad \Gamma, \psi \Rightarrow \Delta \\
\hline
\Gamma, \phi \rightarrow \psi \Rightarrow \Delta
\]

is sound:

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

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

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

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

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