

Formal Methods for Java

Lecture 21: Sequent Calculus

Jochen Hoenicke



Software Engineering
Albert-Ludwigs-University Freiburg

January 18, 2013

Definition (Sequent)

A sequent is a formula

$$\phi_1, \dots, \phi_n \Longrightarrow \psi_1, \dots, \psi_m$$

where ϕ_i, ψ_i are formulae.

The meaning of this formula is:

$$\phi_1 \wedge \dots \wedge \phi_n \rightarrow \psi_1 \vee \dots \vee \psi_m$$

Sequent Calculus Logical Rules

close: $\Gamma, \phi \Longrightarrow \Delta, \phi$

false: $\Gamma, \mathbf{false} \Longrightarrow \Delta$

not-left:
$$\frac{\Gamma \Longrightarrow \Delta, \phi}{\Gamma, \neg\phi \Longrightarrow \Delta}$$

and-left:
$$\frac{\Gamma, \phi, \psi \Longrightarrow \Delta}{\Gamma, \phi \wedge \psi \Longrightarrow \Delta}$$

or-left:
$$\frac{\Gamma, \phi \Longrightarrow \Delta \quad \Gamma, \psi \Longrightarrow \Delta}{\Gamma, \phi \vee \psi \Longrightarrow \Delta}$$

impl-left:
$$\frac{\Gamma \Longrightarrow \Delta, \phi \quad \Gamma, \psi \Longrightarrow \Delta}{\Gamma, \phi \rightarrow \psi \Longrightarrow \Delta}$$

true: $\Gamma \Longrightarrow \Delta, \mathbf{true}$

not-right:
$$\frac{\Gamma, \phi \Longrightarrow \Delta}{\Gamma \Longrightarrow \Delta, \neg\phi}$$

and-right:
$$\frac{\Gamma \Longrightarrow \Delta, \phi \quad \Gamma \Longrightarrow \Delta, \psi}{\Gamma \Longrightarrow \Delta, \phi \wedge \psi}$$

or-right:
$$\frac{\Gamma \Longrightarrow \Delta, \phi, \psi}{\Gamma \Longrightarrow \Delta, \phi \vee \psi}$$

impl-right:
$$\frac{\Gamma, \phi \Longrightarrow \Delta, \psi}{\Gamma \Longrightarrow \Delta, \phi \rightarrow \psi}$$

Sequent Calculus Quantifier

The rules for the existential quantifier are dual:

all-left: $\frac{\Gamma, \forall X \phi(X), \phi(t) \Longrightarrow \Delta}{\Gamma, \forall X \phi(X) \Longrightarrow \Delta}$, where t is some arbitrary term.

all-right: $\frac{\Gamma \Longrightarrow \Delta, \phi(x_0)}{\Gamma \Longrightarrow \Delta, \forall X \phi(X)}$, where x_0 is a fresh identifier.

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

exists-right: $\frac{\Gamma \Longrightarrow \Delta, \exists X \phi(X), \phi(t)}{\Gamma \Longrightarrow \Delta, \exists X \phi(X)}$, where t is some arbitrary term.

Rules for equality

eq-close: $\Gamma \Longrightarrow \Delta, t = t$

apply-eq: ~~$\frac{s = t, \Gamma[t/s] \Longrightarrow \Delta[t/s]}{s = t, \Gamma \Longrightarrow \Delta}$~~ $\frac{s = t, \Gamma[t/X] \Longrightarrow \Delta[t/X]}{s = t, \Gamma[s/X] \Longrightarrow \Delta[s/X]}$

Example: Prove $c = f(c) \Longrightarrow c = f(f(c))$.

$$\frac{\frac{\frac{c = f(c) \Longrightarrow f(f(c)) = f(f(c))}{c = f(c) \Longrightarrow f(c) = f(f(c))}{c = f(c) \Longrightarrow c = f(f(c))} \text{ close-eq}}{\text{apply-eq } (\Delta : f(X) = f(f(c)))} \text{ apply-eq } (\Delta : X = f(f(c)))$$

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.

Definition (Signature)

A **signature** $Sig = (Func, Pred)$ is a tuple of sets of function and predicate symbols, where

- $f/k \in Func$ if f is a function symbol with k parameters,
- $p/k \in Pred$ if p is a predicate symbol with k parameters.

A constant $c/0 \in Func$ is a function without parameters. We assume there are infinitely many constants.

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 $f/k \in Func$ of arity k a function

$$\mathcal{I}(f) : \mathcal{D}^k \rightarrow \mathcal{D}$$

- and each predicate symbol $p/k \in Pred$ of arity k a function

$$\mathcal{I}(p) : \mathcal{D}^k \rightarrow \{\mathbf{true}, \mathbf{false}\}.$$

The interpretation $\mathcal{I}(c)$ of a constant $c/0 \in Func$ 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

$\mathcal{M}[[f(t_1, \dots, t_k)]] = \mathcal{I}(f)(\mathcal{M}[[t_1]], \dots, \mathcal{M}[[t_k]])$, in particular $\mathcal{M}[[c]] = \mathcal{I}(c)$.

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

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

Definition (Model)

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

A sequent $\phi_1, \dots, \phi_n \implies \psi_1, \dots, \psi_m$ is a **tautology**, if all structures are models of this sequent.

Definition (Soundness)

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

$$\models F_1 \text{ and } \dots \text{ and } \models F_n \text{ imply } \models G.$$

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. □

Soundness of impl-left

The rule

$$\frac{\Gamma \Longrightarrow \Delta, \phi \quad \Gamma, \psi \Longrightarrow \Delta}{\Gamma, \phi \rightarrow \psi \Longrightarrow \Delta}$$

is sound:

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

- If one of the formulas in Γ is **false** in \mathcal{M} , then F holds.
- Otherwise, from $\Gamma \Longrightarrow \Delta, \phi$ it follows that ϕ or a formula in Δ is **true**.
- If $\mathcal{M}[\phi] = \mathbf{true}$ and $\mathcal{M}[\psi] = \mathbf{false}$, then $\mathcal{M}[\phi \rightarrow \psi] = \mathbf{false}$. Hence, F holds.
- If $\mathcal{M}[\phi] = \mathbf{true}$ and $\mathcal{M}[\psi] = \mathbf{true}$, then $\Gamma, \psi \Longrightarrow \Delta$ implies that a formula in Δ is **true**.
- If a formula in Δ is **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 Γ nor Δ nor $\phi(X)$. 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 Γ is **false** in \mathcal{M} , then F holds.
- If $\mathcal{M}[\exists X \phi(X)] = \mathbf{false}$, then F holds.
- Otherwise, there is a $d \in \mathcal{D}$ such that $\mathcal{M}[x_0 := d][\phi(x_0)] = \mathbf{true}$.
- Also in $\mathcal{M}[x_0 := d]$, all formulas in Γ are **true**. Since $\Gamma, \phi(x_0) \implies \Delta$ is a tautology, some formula of Δ is **true** in $\mathcal{M}[x_0 := d]$.
- Since x_0 does not occur in Δ , the formula is also **true** in the structure \mathcal{M} . Therefore F holds in \mathcal{M} .