

Formal Methods for Java

Lecture 11: Sequent Calculus

Jochen Hoenicke



Software Engineering
Albert-Ludwigs-University Freiburg

November 30, 2011

Runtime vs. Static Checking

Runtime Checking

- finds bugs at run-time,
- tests for violation during execution,
- can check most of the JML,
- is done by `jmlrac`.

Static Checking

- finds bugs at compile-time,
- proves that there is no violation,
- can check only parts of the JML,
- is done by `ESC/Java`.

- 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.

Sequent Calculus

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:

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

Why are sequents useful?

Simple syntax and nice calculus

Example for Sequents

$$q = y/x, r = y \% x \implies x = 0, y = q * x + r$$

It is logically equivalent to the formula:

$$q = y/x \wedge r = y \% x \rightarrow x = 0 \vee y = q * x + r$$

This is equivalent to the sequent

$$\implies q = y/x \wedge r = y \% x \rightarrow x = 0 \vee y = q * x + r$$

Another equivalent sequent is:

$$x \neq 0, q = y/x, r = y \% x \implies y = q * x + r$$

The Empty Sequent

What is the meaning of the following sequent?

\Rightarrow

This is equivalent to

true \Rightarrow false

which is **false**.

A Rule of Sequent Calculus

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

This rule is sound:

$$\Gamma \wedge \phi \rightarrow \Delta \vee \psi$$

implies

$$\Gamma \rightarrow \Delta \vee (\phi \rightarrow \psi)$$

Here Δ and Γ stand for an arbitrary set of formulae. We abstract from order: rule is also applicable if $\phi \rightarrow \psi$ occur in the middle of the right-hand side, e.g.:

$$\frac{\chi_1, \phi \Longrightarrow \chi_2, \psi, \chi_3}{\chi_1 \Longrightarrow \chi_2, \phi \rightarrow \psi, \chi_3}$$

A Sequent Calculus Proof

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

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

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

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

Let's prove that \wedge commutes: $\phi \wedge \psi \rightarrow \psi \wedge \phi$.

$$\frac{\frac{\frac{\overline{\phi, \psi \Longrightarrow \psi}}{\text{close}} \quad \frac{\overline{\phi, \psi \Longrightarrow \phi}}{\text{close}}}{\text{and-right}} \quad \frac{\phi, \psi \Longrightarrow \psi \wedge \phi}{\text{and-left}}}{\frac{\phi \wedge \psi \Longrightarrow \psi \wedge \phi}{\text{impl-right}}} \Longrightarrow \phi \wedge \psi \rightarrow \psi \wedge \phi$$

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 All-Quantifier

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.

This is sound because $\forall X \phi(X)$ implies $\phi(t)$.

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

x_0 is called a Skolem constant.

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.

Example: $(\forall X \phi(X)) \vee (\exists X \neg \phi(X))$

close: $\Gamma, \phi \Longrightarrow \Delta, \phi$ not-right: $\frac{\Gamma, \phi \Longrightarrow \Delta}{\Gamma \Longrightarrow \Delta, \neg \phi}$ or-right: $\frac{\Gamma \Longrightarrow \Delta, \phi, \psi}{\Gamma \Longrightarrow \Delta, \phi \vee \psi}$

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

Let's prove $(\forall X \phi(X)) \vee (\exists X \neg \phi(X))$.

$$\frac{\frac{\frac{\frac{\frac{\frac{\overline{\phi(x_0) \Longrightarrow \phi(x_0), \exists X \neg \phi(X)}}{\Longrightarrow \phi(x_0), \exists X \neg \phi(X), \neg \phi(x_0)}}{\Longrightarrow \phi(x_0), \exists X \neg \phi(X)}}{\Longrightarrow \forall X \phi(X), \exists X \neg \phi(X)}}{\Longrightarrow \forall X \phi(X) \vee \exists X \neg \phi(X)}}{\text{close}}}{\text{not-right}}}{\text{exists-right}}}{\text{all-right}}}{\text{or-right}}$$

Rules for equality

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

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

These rules suffice to prove $x = y \Longrightarrow y = x$ and $x = y, y = z \Longrightarrow x = z$.

$$\frac{\overline{x = y \Longrightarrow x = x} \text{ eq-close}}{x = y \Longrightarrow y = x} \text{ apply-eq}$$
$$\frac{\overline{x = y, y = z \Longrightarrow y = z} \text{ close}}{x = y, y = z \Longrightarrow x = z} \text{ apply-eq}$$

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.

Additional Rules

The calculus presented so far is already complete.

These rules are not necessary but can shorten proofs:

$$\text{cut: } \frac{\Gamma, \phi \Longrightarrow \Delta \quad \Gamma \Longrightarrow \Delta, \phi}{\Gamma \Longrightarrow \Delta}$$

$$\text{known-left: } \frac{\Gamma \Longrightarrow \Delta}{\Gamma, \phi \Longrightarrow \Delta}$$

$$\text{known-right: } \frac{\Gamma \Longrightarrow \Delta}{\Gamma \Longrightarrow \Delta, \phi}$$