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`.

The KeY-Project

- 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.

Definition (Sequent)

A sequent is a formula

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

where ϕ_i, ψ_i are formulae.
The meaning of this formula is:

$$\phi_1 \land \ldots \land \phi_n \to \psi_1 \lor \ldots \lor \psi_m$$

Why are sequents useful?

Simple syntax and nice calculus

Example for Sequents

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

It is logically equivalent to the formula:

$$q = y/x \land r = y\%x \rightarrow x = 0 \lor y = q * x + r$$

This is equivalent to the sequent

$$\Longrightarrow q = y/x \land r = y\%x \rightarrow x = 0 \lor y = q * x + r$$

Another equivalent sequent is:

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

The Empty Sequent

What is the meaning of the following sequent?

$$\Longrightarrow$$

This is equivalent to

$$\textbf{true} \Longrightarrow \textbf{false}$$

which is **false**.

A Rule of Sequent Calculus

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

This rule is sound:

$$\Gamma \land \phi \to \Delta \lor \psi$$

implies

$$\Gamma \to \Delta \lor (\phi \to \psi)$$

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

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

A Sequent Calculus Proof

Axiom close: $\Gamma, \phi \Longrightarrow \Delta, \phi$ Rule impl-right: $\dfrac{\Gamma, \phi \Longrightarrow \Delta, \psi}{\Gamma \Longrightarrow \Delta, \phi \rightarrow \psi}$

Rule and-left: $\dfrac{\Gamma, \phi, \psi \Longrightarrow \Delta}{\Gamma, \phi \land \psi \Longrightarrow \Delta}$ Rule and-right: $\dfrac{\Gamma \Longrightarrow \Delta, \phi \quad \Gamma \Longrightarrow \Delta, \psi}{\Gamma \Longrightarrow \Delta, \phi \land \psi}$

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

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\phi, \psi \Longrightarrow \psi}\text{ close} \quad \dfrac{}{\phi, \psi \Longrightarrow \phi}\text{ close}}{\phi, \psi \Longrightarrow \psi \land \phi}\text{ and-right}}{\phi \land \psi \Longrightarrow \psi \land \phi}\text{ and-left}}{\Longrightarrow \phi \land \psi \rightarrow \psi \land \phi}\text{ impl-right}$$

Sequent Calculus Logical Rules

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

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

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

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

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

and-left: $\dfrac{\Gamma, \phi, \psi \Longrightarrow \Delta}{\Gamma, \phi \land \psi \Longrightarrow \Delta}$

and-right: $\dfrac{\Gamma \Longrightarrow \Delta, \phi \quad \Gamma \Longrightarrow \Delta, \psi}{\Gamma \Longrightarrow \Delta, \phi \land \psi}$

or-left: $\dfrac{\Gamma, \phi \Longrightarrow \Delta \quad \Gamma, \psi \Longrightarrow \Delta}{\Gamma, \phi \lor \psi \Longrightarrow \Delta}$

or-right: $\dfrac{\Gamma \Longrightarrow \Delta, \phi, \psi}{\Gamma \Longrightarrow \Delta, \phi \lor \psi}$

impl-left: $\dfrac{\Gamma \Longrightarrow \Delta, \phi \quad \Gamma, \psi \Longrightarrow \Delta}{\Gamma, \phi \to \psi \Longrightarrow \Delta}$

impl-right: $\dfrac{\Gamma, \phi \Longrightarrow \Delta, \psi}{\Gamma \Longrightarrow \Delta, \phi \to \psi}$

Sequent Calculus All-Quantifier

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

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

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

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

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

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

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

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

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

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

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

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

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

Rules for equality

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

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

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

$$\cfrac{\cfrac{}{x = y \Longrightarrow x = x}\ \text{eq-close}}{x = y \Longrightarrow y = x}\ \text{apply-eq}$$

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

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.

Additional Rules

The calculus presented so far is already complete.

These rules are not necessary but can shorten proofs:

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

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