# Formal Methods for Java

## Lecture 22: Completeness of Sequent Calculus

Jochen Hoenicke

Software Engineering
Albert-Ludwigs-University Freiburg

January 22, 2013

# Sequent Calculus

## Definition (Sequent)

A sequent is a formula

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

where $\phi_i, \psi_i$ are formulae.
The meaning of this formula is:

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

# Sequent Calculus Logical Rules

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

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

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

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

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

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

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

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

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

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

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

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

exists-left: $\dfrac{\Gamma, \phi(x_0) \Longrightarrow \Delta}{\Gamma, \exists X\ \phi(X) \Longrightarrow \Delta}$, 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.

# Completeness of Sequent Calculus (without Equality)

For completeness we assume we have finitely many functions and predicate symbols and countably infinitely many constants. This ensures that the set of formulas and terms are also countably infinite.

**Theorem (Completeness without Equality)**

*If a sequent $F$ without equalities is a tautology, it can be proven.*

Proof by contraposition: Assume $F$ is not provable, show that there is a model for which $F$ does not hold.

# Proof of Completeness without Equality

Let $\Gamma_0 \Longrightarrow \Delta_0$ be an unprovable sequent.

We apply in each path of the proof tree each applicable rule on each applicable subformula in a fair manner (e.g. round robin).
For the rules exists-right and all-left we chose a term in a fair manner, s.t. every term is eventually applied (possible since the set of terms is enumerable)
There are two cases

- At some point no rule is applicable, we have an open goal with no applicable rule.
- The proof tree is infinite and there is an infinite sub-path (König's Lemma).

In both cases, there is a path, where every rule that is infinitely often applicable is infinitely often applied. Since no rule can become unapplicable by applying another rule, every applicable rule is eventually applied. Moreover, every applicable all-left or exists-right rule is on every term eventually applied.

# Proof of Completeness (cont)

There are two cases

- At some point no rule is applicable, we have an open goal with no applicable rule.
- The proof tree is infinite and there is an infinite sub-path (König's Lemma).

In both cases we have a maximal open path in the sub-tree.

$$\begin{array}{c} \vdots \\ \Gamma_{i+1} \Longrightarrow \Delta_{i+1} \\ \Gamma_i \Longrightarrow \Delta_i \\ \vdots \\ \Gamma_0 \Longrightarrow \Delta_0 \end{array}$$

Define $\Gamma = \bigcup_i \Gamma_i$, $\Delta = \bigcup_i \Delta_i$.

# Proof of Completeness (continued)

The algorithm creates a sequence of unprovable sequents $\Gamma_i \Longrightarrow \Delta_i$,

Set $\Gamma := \bigcup_i \Gamma_i$ and $\Delta := \bigcup_i \Delta_i$. These are closed with respect to applications of the sequent calculus rules, e.g.,

- if $\neg\phi \in \Gamma$ then $\phi \in \Delta$,
- if $\phi \to \psi \in \Gamma$ then $\psi \in \Gamma$ or $\phi \in \Delta$,
- if $\forall X.\phi(X) \in \Gamma$ then $\phi(t) \in \Gamma$ for all terms $t$.

Note that although $\Gamma_i$ and $\Delta_i$ are finite for all $i$, $\Gamma$ and $\Delta$ can be infinite (if all-left or exists-right is applicable).
We define $H := \{\phi \mid \phi \in \Gamma\} \cup \{\neg\phi \mid \phi \in \Delta\}$.
Then $H$ is a Hintikka set (exercise).

# Hintikka set

We distinguish four kinds of formulas:

| $\alpha$ | $\alpha_1$ | $\alpha_2$ | $\beta$ | $\beta_1$ | $\beta_2$ |
|---|---|---|---|---|---|
| $\phi \wedge \psi$ | $\phi$ | $\psi$ | $\phi \vee \psi$ | $\phi$ | $\psi$ |
| $\neg(\phi \vee \psi)$ | $\neg\phi$ | $\neg\psi$ | $\neg(\phi \wedge \psi)$ | $\neg\phi$ | $\neg\psi$ |
| $\neg(\phi \rightarrow \psi)$ | $\phi$ | $\neg\psi$ | $(\phi \rightarrow \psi)$ | $\neg\phi$ | $\psi$ |
| $\neg\neg\phi$ | $\phi$ | $\phi$ | | | |

| $\gamma$ | $\gamma_1(X)$ | $\delta$ | $\delta_1(X)$ |
|---|---|---|---|
| $\forall X \phi(X)$ | $\phi(X)$ | $\exists X \phi(X)$ | $\phi(X)$ |
| $\neg\exists X \phi(X)$ | $\neg\phi(X)$ | $\neg\forall X \phi(X)$ | $\neg\phi(X)$ |

A set $H$ of formulas is a Hintikka set, iff

- For every atomic formula $\phi$, not both formulas $\phi, \neg\phi$ are in $H$.
- If $\alpha \in H$, then $\alpha_1 \in H$ and $\alpha_2 \in H$.
- If $\beta \in H$, then $\beta_1 \in H$ or $\beta_2 \in H$.
- If $\gamma \in H$, then for all terms $t$, $\gamma_1(t) \in H$.
- If $\delta \in H$, then for at least one term $t$, $\delta_1(t) \in H$.

# Construction a Counter-Structure

**Lemma**

*For every Hintikka set $H$ there is a structure $\mathcal{M}$ with $\mathcal{M}[\![\phi]\!] = \mathbf{true}$ for all $\phi \in H$.*

Proof: As domain $\mathcal{D}$ choose the set of terms. The interpretation $\mathcal{I}$ is defined as follows:

$$\begin{aligned} \mathcal{I}(c) &= c \\ \mathcal{I}(f)(t_1, \ldots, t_k) &= f(t_1, \ldots, t_k) \\ \mathcal{I}(p)(t_1, \ldots, t_k) &= \mathbf{true}, \text{ iff } p(t_1, \ldots, t_k) \in H \end{aligned}$$

Show by induction over the terms $t$: $\mathcal{M}[\![t]\!] = t$.
Then one can show by induction over the number of logical operators in $\phi$:

$$\text{If } \phi \in H \text{ then } \mathcal{M}[\![\phi]\!] = \mathbf{true} \qquad \text{and} \qquad \text{if } \neg\phi \in H \text{ then } \mathcal{M}[\![\phi]\!] = \mathbf{false}$$

# Counter-Structure (cont.)

Show by induction over over the number of logical operators in $\phi$:

If $\phi \in H$ then $\mathcal{M}[\![\phi]\!] = \textbf{true}$ and if $\neg\phi \in H$ then $\mathcal{M}[\![\phi]\!] = \textbf{false}$.

Base Case: $\phi = p(t_1, \ldots, t_k)$: If $\phi \in H$, then by definition
$\mathcal{M}[\![\phi]\!] = \mathcal{I}(p)(\mathcal{M}[\![t_1]\!], \ldots, \mathcal{M}[\![t_k]\!]) = \mathcal{I}(p)(t_1, \ldots, t_k) = \textbf{true}$.
If $\neg\phi \in H$, then $\phi \notin H$. Hence,
$\mathcal{M}[\![\phi]\!] = \mathcal{I}(p)(\mathcal{M}[\![t_1]\!], \ldots, \mathcal{M}[\![t_k]\!]) = \mathcal{I}(p)(t_1, \ldots, t_k) = \textbf{false}$.

Induction Step: Assume the hypothesis holds for $\phi, \psi$. Show that it holds for $\neg\phi, \phi \wedge \psi, \phi \vee \psi, \phi \rightarrow \psi, \exists X.\phi(X), \forall X.\phi(X)$.

$\neg\phi$: If $\neg\phi \in H$, then by induction hypothesis, $M[\![\phi]\!] = \textbf{false}$. Hence,
$\mathcal{M}[\![\neg\phi]\!] = \textbf{true}$.
If $\neg\neg\phi \in H$, then since $H$ is a Hintikka set, $\phi \in H$. By induction hypothesis, $\mathcal{M}[\![\phi]\!] = \textbf{true}$. Hence, $\mathcal{M}[\![\neg\phi]\!] = \textbf{false}$.

# Proof of Completeness (Conclusion)

We started with an unprovable sequent $\Gamma_0 \Longrightarrow \Delta_0$.
We constructed $\Gamma \supseteq \Gamma_0$ and $\Delta \supseteq \Delta_0$. This lead to a Hintikka set $H$ with $\phi \in H$ for $\phi \in \Gamma$ and $\neg\phi \in H$ for $\phi \in \Delta$.
We constructed a structure $\mathcal{M}$ with

$$\text{If } \phi \in H \text{ then } \mathcal{M}[\![\phi]\!] = \textbf{true} \qquad \text{and} \qquad \text{if } \neg\phi \in H \text{ then } \mathcal{M}[\![\phi]\!] = \textbf{false}$$

This structure $\mathcal{M}$ is not a model for $\Gamma \Longrightarrow \Delta$. Thus,

$$\mathcal{M} \not\models \Gamma_0 \Longrightarrow \Delta_0$$

Hence, every unprovable sequent is not a tautology.
In other words, every tautology can be proven.

# Additional Rules

The calculus presented so far is already complete.

These rules are not necessary but can shorten proofs:

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

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

# The KeY-Project

- Theorem Prover
- Developed at University of Karlsruhe
- `http://www.key-project.org/`.

- Theory specialized for Java(Card).
- Can generate proof-obligations from JML specification.
- Underlying theory: Sequent Calculus + Dynamic Logic

# Dynamic Logic

Dynamic logic extends predicate logic by

- $[\alpha]\phi$
- $\langle\alpha\rangle\phi$

where $\alpha$ is a program and $\phi$ a sub-formula.

The meaning is as follows:

- $[\alpha]\phi$: after all terminating runs of program $\alpha$ formula $\phi$ holds.
- $\langle\alpha\rangle\phi$: after some terminating run of program $\alpha$ formula $\phi$ holds.

# Comparison with Hoare Logic

The sequent $\phi \Longrightarrow [\alpha]\psi$ corresponds to partial correctness of the Hoare formula:

$$\{\phi\}\alpha\{\psi\}$$

If $\alpha$ is deterministic, $\phi \Longrightarrow \langle\alpha\rangle\psi$ corresponds to total correctness.