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 or Jahob.
The Key-Project

- Developed at University of Karlsruhe
- [http://www.key-project.org/](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

\[ \phi_1, \ldots, \phi_n \Rightarrow \psi_1, \ldots, \psi_m \]

where \( \phi_i, \psi_i \) are formulae.

The meaning of this formula is:

\[ \phi_1 \land \ldots \land \phi_n \rightarrow \psi_1 \lor \ldots \lor \psi_m \]

Why are sequents useful?

Simple syntax and nice calculus
Example for Sequents

\[ q = \frac{y}{x}, \quad r = y \% x \implies x = 0, \quad y = q \times x + r \]

It is logically equivalent to the formula:

\[ q = \frac{y}{x} \land r = y \% x \rightarrow x = 0 \lor y = q \times x + r \]

This is equivalent to the sequent

\[ \implies q = \frac{y}{x} \land r = y \% x \rightarrow x = 0 \lor y = q \times x + r \]

Another equivalent sequent is:

\[ x \neq 0, \quad q = \frac{y}{x}, \quad r = y \% x \implies y = q \times x + r \]
The Empty Sequent

What is the meaning of the following sequent?

\[ \Rightarrow \]

This is equivalent to

\[ \text{true} \Rightarrow \text{false} \]

which is \textit{false}. 
Sequent Calculus

To prove a goal (a formula) with sequent calculus:

- Start with the goal at the bottom
- Use rules to derive formulas, s.t.
  formulas are sufficient to prove the goal, formulas are simpler.
- A proof node can be closed if it holds trivially.
A Rule of Sequent Calculus

Rule impl-right: \[ \frac{\Gamma, \phi \implies \Delta, \psi}{\Gamma \implies \Delta, \phi \implies \psi} \]

This rule is sound:

\[ \Gamma \land \phi \implies \Delta \lor \psi \]

implies

\[ \Gamma \implies \Delta \lor (\phi \implies \psi) \]

Here \( \Delta \) and \( \Gamma \) stand for an arbitrary set of formulae. We abstract from order: rule is also applicable if \( \phi \implies \psi \) occur in the middle of the right-hand side, e.g.:

\[ \chi_1, \phi \implies \chi_2, \psi, \chi_3 \]

\[ \chi_1 \implies \chi_2, \phi \implies \psi, \chi_3 \]
A Sequent Calculus Proof

Axiom close: \( \Gamma, \phi \rightarrow \Delta, \phi \)

Rule impl-right:
\[
\frac{\Gamma \rightarrow \Delta, \phi \rightarrow \psi}{\Gamma \rightarrow \Delta, \phi \rightarrow \psi}
\]

Rule and-left:
\[
\frac{\Gamma, \phi, \psi \rightarrow \Delta}{\Gamma, \phi \land \psi \rightarrow \Delta}
\]

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

Let’s prove that \( \land \) commutes: \( \phi \land \psi \rightarrow \psi \land \phi \).

\[
\frac{\phi, \psi \rightarrow \psi}{\phi, \psi \rightarrow \psi \land \phi}
\]

close

\[
\frac{\phi, \psi \rightarrow \phi}{\phi, \psi \rightarrow \phi}
\]

close

\[
\frac{\phi \land \psi \rightarrow \psi \land \phi}{\phi \land \psi \rightarrow \psi \land \phi}
\]

impl-right

\[
\frac{\phi \land \psi \rightarrow \psi \land \phi}{\phi \land \psi \rightarrow \psi \land \phi}
\]

and-left

\[
\frac{\phi \land \psi \rightarrow \psi \land \phi}{\phi \land \psi \rightarrow \psi \land \phi}
\]

and-right
Sequent Calculus Logical Rules

- **close:** $\Gamma, \phi \Rightarrow \Delta, \phi$
- **false:** $\Gamma, \text{false} \Rightarrow \Delta$
- **not-left:**
  - $\Gamma \Rightarrow \Delta, \phi$
  - $\Gamma, \phi \Rightarrow \Delta$
- **and-left:**
  - $\Gamma, \phi \land \psi \Rightarrow \Delta$
  - $\Gamma \Rightarrow \Delta, \phi \land \psi$
- **or-left:**
  - $\Gamma, \phi \Rightarrow \Delta$
  - $\Gamma, \psi \Rightarrow \Delta$
  - $\Gamma \Rightarrow \Delta, \phi \lor \psi$
- **impl-left:**
  - $\Gamma \Rightarrow \Delta, \phi$
  - $\Gamma, \psi \Rightarrow \Delta$
  - $\Gamma \Rightarrow \Delta, \phi \rightarrow \psi$
- **true:** $\Gamma \Rightarrow \Delta, \text{true}$
- **not-right:**
  - $\Gamma \Rightarrow \Delta, \neg \phi$
- **and-right:**
  - $\Gamma \Rightarrow \Delta, \phi \land \psi$
- **or-right:**
  - $\Gamma \Rightarrow \Delta, \phi \lor \psi$
- **impl-right:**
  - $\Gamma, \phi \Rightarrow \Delta, \psi$
  - $\Gamma \Rightarrow \Delta, \phi \rightarrow \psi$
Sequent Calculus All-Quantifier

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

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

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

\(x_0\) is called a Skolem constant.
The rules for the existential quantifier are dual:

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

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

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

**exists-right:** \[ \frac{\Gamma \implies \Delta, \exists X \phi(X), \phi(t)}{\Gamma \implies \Delta, \exists X \phi(X)} \], where \( t \) is some arbitrary term.
Example: \((\forall X \phi(X)) \lor (\exists X \neg \phi(X))\)

**close:** \(\Gamma, \phi \Rightarrow \Delta, \phi\)  
**not-right:** \(\Gamma, \phi \Rightarrow \Delta\)  
**or-right:** \(\Gamma \Rightarrow \Delta, \phi \lor \psi\)

**all-right:** \(\Gamma \Rightarrow \Delta, \phi(x_0)\)  
\(\Gamma \Rightarrow \Delta, \forall X \phi(X)\), where \(x_0\) is a fresh identifier.

**exists-right:** \(\Gamma \Rightarrow \Delta, \exists X \phi(X), \phi(t)\)  
\(\Gamma \Rightarrow \Delta, \exists X \phi(X)\), where \(t\) is some arbitrary term.

Let’s prove \((\forall X \phi(X)) \lor (\exists X \neg \phi(X))\).

\[
\begin{align*}
\phi(x_0) & \Rightarrow \phi(x_0), \exists X \neg \phi(X) \\
\Rightarrow & \phi(x_0), \exists X \neg \phi(X), \neg \phi(x_0) \\
\Rightarrow & \phi(x_0), \exists X \neg \phi(X) \\
\Rightarrow & \forall X \phi(X), \exists X \neg \phi(X) \\
\Rightarrow & \forall X \phi(X) \lor \exists X \neg \phi(X)
\end{align*}
\]
Rules for equality

\[
\text{eq-close: } \Gamma \quad \Rightarrow \quad \Delta, \ t = t
\]

\[
\text{apply-eq: } \quad s = t, \ \Gamma[t/s] \quad \Rightarrow \quad \Delta[t/s] \quad s = t, \ \Gamma \quad \Rightarrow \quad \Delta
\]

These rules suffice to prove \( x = y \Rightarrow y = x \) and \( x = y, y = z \Rightarrow x = z \).
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.
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.
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 \( f/k \in \text{Func} \) of arity \( k \) a function

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

- and each predicate symbol \( p/k \in \text{Pred} \) of arity \( k \) a function

\[
\mathcal{I}(p) : \mathcal{D}^k \rightarrow \{\text{true}, \text{false}\}.
\]

The interpretation \( \mathcal{I}(c) \) of a constant \( c/0 \in \text{Func} \) 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 $\mathcal{M} = (D, \mathcal{I})$ 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 $\mathcal{M}[s] = \mathcal{M}[t]$.
- $\mathcal{M}[\phi \land \psi] = \begin{cases} \text{true} & \text{if } \mathcal{M}[\phi] = \text{true} \text{ and } \mathcal{M}[\psi] = \text{true}, \\ \text{false} & \text{otherwise.} \end{cases}$
- $\mathcal{M}[\phi \lor \psi]$, $\mathcal{M}[\phi \rightarrow \psi]$, and $\mathcal{M}[\neg \phi]$, analogously.
- $\mathcal{M}[\forall X \phi(X)] = \text{true}$, iff for all $d \in D$: $\mathcal{M}[x_0 := d][\phi(x_0)] = \text{true}$, where $x_0$ is a constant not occuring in $\phi$.
- $\mathcal{M}[\exists X \phi(X)] = \text{true}$, iff there is some $d \in D$ with $\mathcal{M}[x_0 := d][\phi(x_0)] = \text{true}$, where $x_0$ is a constant not occuring in $\phi$. 
Models and Tautologies

Definition (Model)

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

A sequent $\phi_1, \ldots, \phi_n \Rightarrow \psi_1, \ldots, \psi_m$ 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.