Software Engineering using Formal Methods

Reasoning about Programs with Dynamic Logic

Wolfgang Ahrendt

6 October 2015

Part I

Where are we?

Where Are We?

before specification of JAVA programs with JML

now dynamic logic (DL) for resoning about JAVA programs

after that generating DL from JML+JAVA

+ verifying the resulting proof obligations

Motivation

Consider the method

```
public void doubleContent(int[] a) {
  int i = 0;
  while (i < a.length) {
    a[i] = a[i] * 2;
    i++;
  }
}
```

We want a logic/calculus allowing to express/prove properties like, e.g.:

If `a` $\neq$ `null`
then `doubleContent` terminates normally
and afterwards all elements of `a` are twice the old value

Motivation Cont'd

One such logic is dynamic logic (DL)

The above statement can be expressed in DL as follows:
(assuming a suitable signature)

$$
\begin{array}{l}
\quad \mathtt{a} \neq \mathtt{null} \\
\land\ \mathtt{a} \neq \mathtt{old\_a} \\
\land\ \forall \mathtt{int}\ \mathtt{i}; ((0 \leq \mathtt{i} \land \mathtt{i} < \mathtt{a.length}) \rightarrow \mathtt{a[i]} = \mathtt{old\_a[i]}) \\
\rightarrow \langle \mathtt{doubleContent(a);} \rangle \\
\quad \forall \mathtt{int}\ \mathtt{i}; ((0 \leq \mathtt{i} \land \mathtt{i} < \mathtt{a.length}) \rightarrow \mathtt{a[i]} = 2 * \mathtt{old\_a[i]})
\end{array}
$$

Observations

- DL combines first-order logic (FOL) with programs
- Theory of DL extends theory of FOL

Today

introducing dynamic logic for JAVA

- recap first-order logic (FOL)
- semantics of FOL
- dynamic logic = extending FOL with
  - dynamic interpretations
  - programs to describe state change

Repetition: First-Order Logic

Signature

A first-order signature Σ consists of

- a set T_Σ of type symbols
- a set F_Σ of function symbols
- a set P_Σ of predicate symbols

Type Declarations

- $\tau\ x$; 'variable x has type τ'
- $p(\tau_1, \ldots, \tau_r)$; 'predicate p has argument types $\tau_1, \ldots, \tau_r$'
- $\tau\ f(\tau_1, \ldots, \tau_r)$; 'function f has argument types $\tau_1, \ldots, \tau_r$ and result type τ'

Part II

First-Order Semantics

First-Order Semantics

From propositional to first-order semantics

- In prop. logic, an interpretation of variables with $\{T, F\}$ sufficed
- In first-order logic we must assign meaning to:
  - function symbols (incl. constants)
  - predicate symbols
- Respect typing: **int** `i`, `List l` must denote different elements

What we need (to interpret a first-order formula)

1. A collection of typed universes of elements
2. A mapping from variables to elements
3. For each function symbol, a mapping from arguments to results
4. For each predicate symbol, a set of argument tuples where that predicate holds

First-Order Domains/Universes

1. A collection of typed universes of elements

Definition (Universe/Domain)

A non-empty set $\mathcal{D}$ of elements is a universe or domain.
Each element of $\mathcal{D}$ has a fixed type given by $\delta : \mathcal{D} \rightarrow T_\Sigma$

- Notation for the domain elements of type $\tau \in T_\Sigma$:
  $\mathcal{D}^\tau = \{d \in \mathcal{D} \mid \delta(d) = \tau\}$
- Each type $\tau \in T_\Sigma$ must 'contain' at least one domain element:
  $\mathcal{D}^\tau \neq \emptyset$

First-Order States

3. For each function symbol, a mapping from arguments to results
4. For each predicate symbol, a set of argument tuples where that predicate holds

Definition (First-Order State)

Let $\mathcal{D}$ be a domain with typing function δ.

For each f be declared as $\tau\ f(\tau_1, \ldots, \tau_r)$;

and each p be declared as $p(\tau_1, \ldots, \tau_r)$;

$\mathcal{I}(f)$ is a mapping $\mathcal{I}(f) : \mathcal{D}^{\tau_1} \times \cdots \times \mathcal{D}^{\tau_r} \rightarrow \mathcal{D}^{\tau}$

$\mathcal{I}(p)$ is a set $\mathcal{I}(p) \subseteq \mathcal{D}^{\tau_1} \times \cdots \times \mathcal{D}^{\tau_r}$

Then $\mathcal{S} = (\mathcal{D}, \delta, \mathcal{I})$ is a first-order state

First-Order States Cont'd

Example

Signature Σ: **int** `i`; **int** `j`; **int** `f(`**int**`)`; `Object obj`; `<(`**int**`,`**int**`)`;
$\mathcal{D} = \{17, 2, o\}$
The following $\mathcal{I}$ is a possible interpretation:

$$\mathcal{I}(i) = 17$$
$$\mathcal{I}(j) = 17$$
$$\mathcal{I}(\texttt{obj}) = o$$

$\mathcal{D}^{\textbf{int}}$	$\mathcal{I}(f)$
2	2
17	2

$\mathcal{D}^{\textbf{int}} \times \mathcal{D}^{\textbf{int}}$	in $\mathcal{I}(<)$?
$(2, 2)$	*no*
$(2, 17)$	*yes*
$(17, 2)$	*no*
$(17, 17)$	*no*

One of uncountably many possible first-order states!

Semantics of Reserved Signature Symbols

Definition

Reserved predicate symbol for equality: $=$

Interpretation is fixed as $\mathcal{I}(=) = \{(d, d) \mid d \in \mathcal{D}\}$

Exercise: write down all elements of the set $\mathcal{I}(=)$ for example domain

Signature Symbols vs. Domain Elements

- Domain elements different from the terms representing them
- First-order formulas and terms have no access to domain

Example

Signature Σ: `Object obj1, obj2;`
Domain: $\mathcal{D} = \{o\}$

In this state, necessarily $\mathcal{I}(\mathtt{obj1}) = \mathcal{I}(\mathtt{obj2}) = o$

Variable Assignments

2. A mapping from variables to domain elements

Definition (Variable Assignment)

A variable assignment β maps variables to domain elements.
It respects the variable type, i.e., if x has type τ then $\beta(x) \in \mathcal{D}^{\tau}$.

Semantic Evaluation of Terms

Given a first-order state $\mathcal{S}$ and a variable assignment β
it is possible to evaluate first-order terms under $\mathcal{S}$ and β

Definition (Valuation of Terms)

$val_{\mathcal{S},\beta}$: Term $\rightarrow \mathcal{D}$ such that $val_{\mathcal{S},\beta}(t) \in \mathcal{D}^{\tau}$ for $t \in \text{Term}_{\tau}$:

- $val_{\mathcal{S},\beta}(x) = \beta(x)$
- $val_{\mathcal{S},\beta}(f(t_1, \ldots, t_r)) = \mathcal{I}(f)(val_{\mathcal{S},\beta}(t_1), \ldots, val_{\mathcal{S},\beta}(t_r))$

Semantic Evaluation of Terms Cont'd

Example

Signature Σ: **int** `i`; **int** `j`; **int** `f(`**int**`)`;
$\mathcal{D} = \{17, 2, o\}$
Variables: `Object obj`; **int** `x`;

$\mathcal{I}(\mathtt{i}) = 17$
$\mathcal{I}(\mathtt{j}) = 17$

$\mathcal{D}^{\mathbf{int}}$	$\mathcal{I}(\mathtt{f})$
2	17
17	2

Var	β
`obj`	o
`x`	17

- $val_{\mathcal{S},\beta}(\mathtt{f(f(i))})$?
- $val_{\mathcal{S},\beta}(\mathtt{f(f(x))})$?
- $val_{\mathcal{S},\beta}(\mathtt{obj})$?

Preparing for Semantic Evaluation of Formulas

Definition (Modified Variable Assignment)

Let y be variable of type τ, β variable assignment, $d \in \mathcal{D}^\tau$:

$$\beta_y^d(x) := \begin{cases} \beta(x) & x \neq y \\ d & x = y \end{cases}$$

Needed for semantics of quantifiers.

Semantic Evaluation of Formulas

Definition (Valuation of Formulas)

$val_{\mathcal{S},\beta}(\phi)$ for $\phi \in For$

- $val_{\mathcal{S},\beta}(p(t_1,\ldots,t_r)) = T$ iff $(val_{\mathcal{S},\beta}(t_1),\ldots,val_{\mathcal{S},\beta}(t_r)) \in \mathcal{I}(p)$
- $val_{\mathcal{S},\beta}(\phi \wedge \psi) = T$ iff $val_{\mathcal{S},\beta}(\phi) = T$ and $val_{\mathcal{S},\beta}(\psi) = T$
- (also true, false, $\vee$, $\neg$, $\rightarrow$, $\leftrightarrow$ like valuation in propositional logic)
- $val_{\mathcal{S},\beta}(\forall\, \tau\; x;\, \phi) = T$ iff $val_{\mathcal{S},\beta_x^d}(\phi) = T$ for all $d \in \mathcal{D}^\tau$
- $val_{\mathcal{S},\beta}(\exists\, \tau\; x;\, \phi) = T$ iff $val_{\mathcal{S},\beta_x^d}(\phi) = T$ for at least one $d \in \mathcal{D}^\tau$

Semantic Evaluation of Formulas Cont'd

Example

Signature Σ: `int j; int f(int); Object obj; <(int,int);`

$\mathcal{D} = \{17,\ 2,\ o\}$, $\mathcal{D}^{\texttt{int}} = \{17,\ 2\}$, $\mathcal{D}^{\texttt{Object}} = \{o\}$

$\mathcal{I}(j) = 17$

$\mathcal{I}(\texttt{obj}) = o$

$\mathcal{D}^{\texttt{int}}$	$\mathcal{I}(f)$
2	2
17	2

$\mathcal{D}^{\texttt{int}} \times \mathcal{D}^{\texttt{int}}$	in $\mathcal{I}(<)$?
$(2,2)$	F
$(2,17)$	T
$(17,2)$	F
$(17,17)$	F

- $val_{\mathcal{S},\beta}(f(j) < j)$?
- $val_{\mathcal{S},\beta}(\exists\, \texttt{int}\ x;\ f(x) = x)$?
- $val_{\mathcal{S},\beta}(\forall\, \texttt{Object}\ o1;\ \forall\, \texttt{Object}\ o2;\ o1 = o2)$?

Semantic Notions

Definition (Truth, Satisfiability, Validity)

$val_{\mathcal{S},\beta}(\phi) = T$			$(\mathcal{S}, \beta$ **satisfies** $\phi)$
$\mathcal{S} \models \phi$	iff	for all β : $val_{\mathcal{S},\beta}(\phi) = T$	$(\phi$ is **true** in $\mathcal{S})$
$\mathrm{SAT}(\phi)$	iff	for some $\mathcal{S}$: $\mathcal{S} \models \phi$	$(\phi$ is **satisfiable**$)$
$\models \phi$	iff	for all $\mathcal{S}$: $\mathcal{S} \models \phi$	$(\phi$ is **valid**$)$

Example

- $f(j) < j$ is true in $\mathcal{S}$
- $\exists\,\mathbf{int}\ x;\ i = x$ is valid
- $\exists\,\mathbf{int}\ x;\ \neg(x = x)$ is not satisfiable

Part III

Towards Dynamic Logic

Towards Dynamic Logic

Reasoning about Java programs requires extensions of FOL

- JAVA type hierarchy
- JAVA program variables
- JAVA heap for reference types (next lecture)

Type Hierarchy

Definition (Type Hierarchy)

- T_Σ is set of types
- Subtype relation $\sqsubseteq \; \subseteq \; T_\Sigma \times T_\Sigma$ with top element $\top$
  - $\tau \sqsubseteq \top$ for all $\tau \in T_\Sigma$

Example (A Minimal Type Hierarchy)

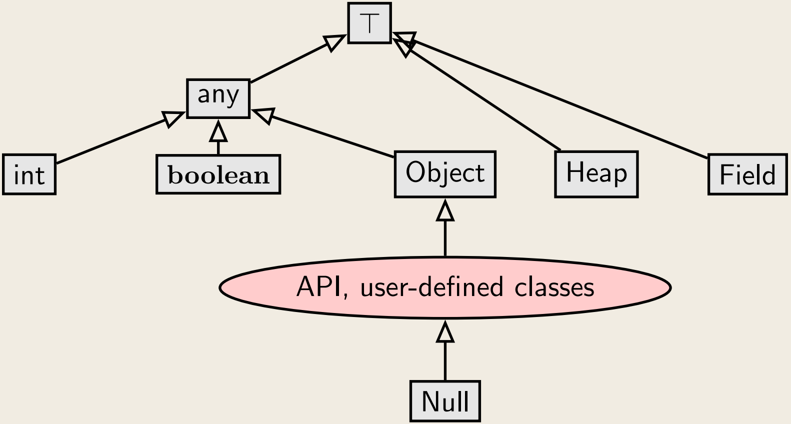
$T_\Sigma = \{\top\}$
All signature symbols have same type $\top$

Example (Type Hierarchy for Java)

(see next slide)

Modelling Java in FOL: Fixing a Type Hierarchy

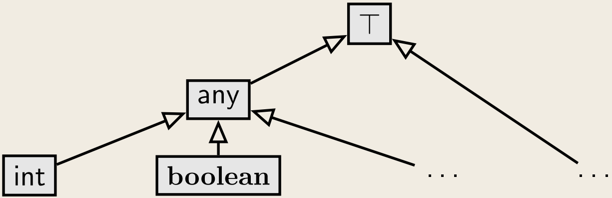
Signature based on Java's type hierarchy



Each interface and class in API and in target program becomes type with appropriate subtype relation

Subset of Types

Signature based on Java's type hierarchy



int and **boolean** are the only types for today
Class, interface types, etc., in next lecture

Modelling Dynamic Properties

Only static properties expressable in typed FOL, e.g.,

- Values of fields in a certain range
- Property (invariant) of a subclass implies property of a superclass

Considers only one program state at a time

Goal: Express behavior of a program, e.g.:

> If method `setAge` is called on an object *o* of type `Person`
> and the method argument `newAge` is positive
> then afterwards field `age` has same value as `newAge`

Requirements

Requirements for a logic to reason about programs

- can relate different program states, i.e., before and after execution, within a single formula
- program variables are represented by constant symbols that depend on current program state

Dynamic Logic meets the above requirements

Dynamic Logic

(Java) Dynamic Logic

Typed FOL

- $+$ programs $\mathtt{p}$
- $+$ modalities $\langle \mathtt{p} \rangle \phi$, $[\mathtt{p}]\phi$ ($\mathtt{p}$ program, ϕ DL formula)
- $+ \ldots$ (later)

An Example

$$\mathtt{i} > 5 \ \rightarrow \ [\mathtt{i = i + 10;}]\mathtt{i} > 15$$

Meaning?

If program variable `i` is greater than 5 in current state, then after executing the Java statement "`i = i + 10;`", `i` is greater than 15

Program Variables

Dynamic Logic = Typed FOL + ...

$$\mathtt{i} > 5 \rightarrow [\mathtt{i = i + 10;}]\mathtt{i} > 15$$

Program variable `i` refers to different values before and after execution

- Program variables such as `i` are state-dependent constant symbols
- Value of state-dependent symbols changeable by a program

Three words one meaning: state-dependent, non-rigid, flexible

Rigid versus Flexible Symbols

Signature of program logic defined as in FOL, but in addition, there are program variables

Rigid versus Flexible

- Rigid symbols, meaning insensitive to program states
  - First-order variables (aka logical variables)
  - Built-in functions and predicates such as `0,1,...,+,*,...,<,...`
- Non-rigid (or flexible) symbols, meaning depends on state. Capture side effects on state during program execution
  - Program variables are flexible

Any term containing at least one flexible symbol is called flexible

Signature of Dynamic Logic

Definition (Dynamic Logic Signature)

$\Sigma = (P_\Sigma, F_\Sigma, PV_\Sigma, \alpha_\Sigma), \quad F_\Sigma \cap PV_\Sigma = \emptyset$

(Rigid) Predicate Symbols $P_\Sigma = \{>, >=, \ldots\}$
(Rigid) Function Symbols $F_\Sigma = \{+, -, *, 0, 1, \ldots\}$
Non-rigid Program variables e.g. $PV_\Sigma = \{\mathtt{i}, \mathtt{j}, \mathtt{ready}, \ldots\}$

Standard typing of JAVA symbols: **boolean** `TRUE`; `<(`**int**`,`**int**`)`; ...

Dynamic Logic Signature - KeY input file

```
\sorts {
 // only additional sorts (int, boolean, any predefined)
}
\functions {
 // only additional rigid functions
 // (arithmetic functions like +,- etc., predefined)
}
\predicates {  /* same as for functions */  }

\programVariables { // non-rigid
   int i, j;
   boolean ready;
}
```

Empty sections can be left out

Again: Two Kinds of Variables

Rigid:

Definition (First-Order/Logical Variables)

Typed logical variables (rigid), declared locally in quantifiers as `T x;`
They may not occur in programs!

Non-rigid:

Program Variables

- Are not FO variables
- Cannot be quantified
- May occur in programs (and formulas)

Dynamic Logic Programs

Dynamic Logic = Typed FOL + programs ...

Programs here: any legal sequence of JAVA statements.

Example

Signature for FSym_f: `int r; int i; int n;`

Signature for FSym_r: `int 0; int +(int,int); int -(int,int);`

Signature for PSym_r: `<(int,int);`

```
i=0;
r=0;
while (i<n) {
  i=i+1;
  r=r+i;
}
r=r+r-n;
```

Which value does the program compute in `r`?

Relating Program States: Modalities

DL extends FOL with two additional (mix-fix) operators:

- $\langle \mathrm{p} \rangle \phi$ (diamond)
- $[p]\phi$ (box)

with p a program, ϕ another DL formula

Intuitive Meaning

- $\langle \mathrm{p} \rangle \phi$: p terminates and formula ϕ holds in final state (total correctness)
- $[p]\phi$: If p terminates then formula ϕ holds in final state (partial correctness)

> Attention: JAVA programs are deterministic, i.e., if a JAVA program terminates then exactly one state is reached from a given initial state.

Dynamic Logic - Examples

Let `i`, `j`, `old_i`, `old_j` denote program variables.
Give the meaning in natural language:

1. $\mathtt{i} = \mathtt{old\_i} \rightarrow \langle \mathtt{i = i + 1;} \rangle \mathtt{i} > \mathtt{old\_i}$

   If `i = i + 1;` is executed in a state where `i` and `old_i` have the same value, then the program terminates and in its final state the value of `i` is greater than the value of `old_i` .

2. $\mathtt{i} = \mathtt{old\_i} \rightarrow [\mathtt{while(true)}\{\mathtt{i = old\_i - 1;}\}]\mathtt{i} > \mathtt{old\_i}$

   If the program is executed in a state where `i` and `old_i` have the same value and if the program terminates then in its final state the value of `i` is greater than the value of `old_i`.

3. $\forall x. \; (\langle prog_1 \rangle \; \mathtt{i} = x \;\leftrightarrow\; \langle prog_2 \rangle \; \mathtt{i} = x \;)$

   $prog_1$ and $prog_2$ are equivalent concerning termination and the final value of `i`.

Dynamic Logic: KeY Input File

```
\programVariables {  // Declares global program variables
  int i;
  int old_i;
}


\problem {  // The problem to verify is stated here
        i = old_i -> \<{   i = i + 1;  }\> i > old_i
}
```

Visibility

- Program variables declared globally can be accessed anywhere
- Program variables declared inside a modality such as "$pre \rightarrow \langle$`int j; p`$\rangle post$" only visible in `p`

Dynamic Logic Formulas

Definition (Dynamic Logic Formulas (DL Formulas))

- Each FOL formula is a DL formula
- If p is a program and ϕ a DL formula then $\left\{ \begin{matrix} \langle \mathrm{p} \rangle \phi \\ [\mathrm{p}]\phi \end{matrix} \right\}$ is a DL formula
- DL formulas closed under FOL quantifiers and connectives

- Program variables are flexible constants: never bound in quantifiers
- Program variables need not be declared or initialized in program
- Programs contain no logical variables
- Modalities can be arbitrarily nested, e.g., $\langle \mathrm{p} \rangle [\mathrm{q}] \phi$

Dynamic Logic Formulas Cont'd

Example (Well-formed? If yes, under which signature?)

- $\forall\, \mathbf{int}\ y; (((\langle \texttt{x = 2;} \rangle \texttt{x} = y) \leftrightarrow (\langle \texttt{x = 1; x++;} \rangle \texttt{x} = y))$

  Well-formed if FSym_f contains $\mathbf{int}\ \texttt{x;}$

- $\exists\, \mathbf{int}\ x; [x = 1;](x = 1)$

  Not well-formed, because logical variable occurs in program

- $\langle \texttt{x = 1;} \rangle ([\mathbf{while}\ (\mathbf{true})\ \{\}]\mathbf{false})$

  Well-formed if PV_Σ contains $\mathbf{int}\ \texttt{x;}$

  program formulas can be nested

Dynamic Logic Semantics: States

First-order state can be considered as program state

- Interpretation of (non-rigid) program variables can vary from state to state
- Interpretation of rigid symbols is the same in all states
  (e.g., built-in functions and predicates)

Program states as first-order states

We identify first-order state $\mathcal{S} = (\mathcal{D}, \delta, \mathcal{I})$ with program state.

- Interpretation $\mathcal{I}$ only changes on program variables.
  $\Rightarrow$ only record values of variables $\in PV_\Sigma$
- Set of all states $\mathcal{S}$ is called *States*

Kripke Structure

Definition (Kripke Structure)

Kripke structure or Labelled transition system $K = (\mathit{States}, \rho)$

- States $\mathcal{S} = (\mathcal{D}, \delta, \mathcal{I}) \in \mathit{States}$
- Transition relation $\rho : \mathit{Program} \rightarrow (\mathit{States} \rightharpoonup \mathit{States})$

$$\rho(\mathrm{p})(\mathcal{S}_1) = \mathcal{S}_2$$

iff.

program p executed in state $\mathcal{S}_1$ terminates and its final state is $\mathcal{S}_2$, otherwise undefined.

- ρ is the semantics of programs $\in \mathit{Program}$
- $\rho(\mathrm{p})(\mathcal{S})$ can be undefined ('$\rightharpoonup$'):
  p may not terminate when started in $\mathcal{S}$
- Our programs are deterministic (unlike PROMELA):
  $\rho(\mathrm{p})$ is a function (at most one value)

Semantic Evaluation of Program Formulas

Definition (Validity Relation for Program Formulas)

- $\mathcal{S} \models \langle \mathrm{p} \rangle \phi$ iff $\rho(\mathrm{p})(\mathcal{S})$ is defined and $\rho(\mathrm{p})(\mathcal{S}) \models \phi$

  (p terminates and ϕ is true in the final state after execution)
- $s \models [\mathrm{p}]\phi$ iff $\rho(\mathrm{p})(\mathcal{S}) \models \phi$ whenever $\rho(\mathrm{p})(\mathcal{S})$ is defined

  (If p terminates then ϕ is true in the final state after execution)

A DL formula ϕ is valid iff $\mathcal{S} \models \phi$ for all states $\mathcal{S}$.

- Duality: $\langle \mathrm{p} \rangle \phi$ iff $\neg[\mathrm{p}]\neg\phi$
  Exercise: justify this with help of semantic definitions
- Implication: if $\langle \mathrm{p} \rangle \phi$ then $[\mathrm{p}]\phi$
  Total correctness implies partial correctness
  - converse is false
  - holds only for deterministic programs

More Examples

valid?
meaning?

Example

$\forall\, \tau\ y; ((\langle \mathrm{p} \rangle \mathrm{x} = y) \leftrightarrow (\langle \mathrm{q} \rangle \mathrm{x} = y))$

Not valid in general

Programs p and q behave equivalently on variable τ x

Example

$\exists\, \tau\ y; (\mathrm{x} = y \rightarrow \langle \mathrm{p} \rangle \mathbf{true})$

Not valid in general

Program p terminates if initial value of x is suitably chosen

Semantics of Programs

In labelled transition system $K = (\mathit{States}, \rho)$:
$\rho : \mathit{Program} \to (\mathit{States} \rightharpoonup \mathit{States})$ is semantics of programs $\mathtt{p} \in \mathit{Program}$

ρ defined recursively on programs

Example (Semantics of assignment)

States $\mathcal{S}$ interpret program variables $\mathtt{v}$ with $\mathcal{I}_{\mathcal{S}}(\mathtt{v})$

$\rho(\mathtt{x=t;})(\mathcal{S}) = \mathcal{S}'$ where $\mathcal{S}'$ identical to $\mathcal{S}$ except $\mathcal{I}_{\mathcal{S}'}(x) = \mathit{val}_{\mathcal{S}}(t)$

Very advanced task to define ρ for JAVA $\Rightarrow$ Not done in this course
Next lecture, we go directly to calculus for program formulas!

Literature for this Lecture

- W. Ahrendt, Using KeY Chapter 10 in [KeYbook]
- up-to-date alternative:
  W. Ahrendt, S. Grebing Using the KeY Prover
  to appear in the new KeY Book (see Google group)
- Dynamic Logic (Sections 3.1, 3.2, 3.4, 3.5, 3.6.1, 3.6.3, 3.6.4),
  Chapter 3 in [KeYbook]