Formal Methods for Software Development

Reasoning about Programs with Dynamic Logic

Wolfgang Ahrendt

13 October 2020

Symbolic Execution of Programs

Sequent calculus decomposes top-level operator in formula.
What is "top-level" in a sequential program `p; q; r;` ?

Symbolic Execution

- Follow the natural control flow when analysing a program
- Values of some variables unknown: symbolic state representation

Symbolic Execution of Programs

Sequent calculus decomposes top-level operator in formula.
What is “top-level” in a sequential program `p; q; r;` ?

Symbolic Execution

- Follow the natural control flow when analysing a program
- Values of some variables unknown: symbolic state representation

Example

Compute the final state after termination of

```
x=x+y; y=x-y; x=x-y;
```

Symbolic Execution of Programs Cont'd

Typical form of DL formulas in symbolic execution

$$\langle \texttt{stmt; } \mathit{rest} \rangle \phi \qquad [\texttt{stmt; } \mathit{rest}]\phi$$

- Rules symbolically execute *first* statement ("active statement")
- Repeated application of such rules corresponds to symbolic program execution

Symbolic Execution of Programs Cont'd

Typical form of DL formulas in symbolic execution

$$\langle \texttt{stmt; } \mathit{rest} \rangle \phi \qquad [\texttt{stmt; } \mathit{rest}] \phi$$

- Rules symbolically execute *first* statement ("active statement")
- Repeated application of such rules corresponds to symbolic program execution

Example (`symbolicExecution/simpleIf.key`, Demo, active statement only)

```
\programVariables {
 int x; int y; boolean b;
}
\problem {
 \<{ if (b) { x = 1; } else { x = 2; } y = 3; }\> y > x
}
```

Symbolic Execution of Programs Cont'd

Symbolic execution of conditional

$$\text{if}\ \frac{\Gamma, \mathtt{b} = \mathsf{TRUE} \Longrightarrow \langle \mathtt{p};\ \ \mathit{rest} \rangle \phi, \Delta \qquad \Gamma, \mathtt{b} = \mathsf{FALSE} \Longrightarrow \langle \mathtt{q};\ \ \mathit{rest} \rangle \phi, \Delta}{\Gamma \Longrightarrow \langle \mathbf{if}\ \mathtt{(b)}\ \mathtt{\{}\ \mathtt{p}\ \mathtt{\}}\ \mathbf{else}\ \mathtt{\{}\ \mathtt{q}\ \mathtt{\}}\ \mathtt{;}\ \ \mathit{rest} \rangle \phi, \Delta}$$

Symbolic execution must consider all possible execution branches

Symbolic Execution of Programs Cont'd

Symbolic execution of conditional

$$\text{if}\ \frac{\Gamma, \mathtt{b} = \mathsf{TRUE} \Longrightarrow \langle \mathtt{p;}\ \ \mathit{rest}\rangle\phi, \Delta \qquad \Gamma, \mathtt{b} = \mathsf{FALSE} \Longrightarrow \langle \mathtt{q;}\ \ \mathit{rest}\rangle\phi, \Delta}{\Gamma \Longrightarrow \langle \textbf{if}\ \ \mathtt{(b)}\ \ \{\ \mathtt{p}\ \}\ \ \textbf{else}\ \ \{\ \mathtt{q}\ \}\ \ ;\ \ \mathit{rest}\rangle\phi, \Delta}$$

Symbolic execution must consider all possible execution branches

Symbolic execution of loops: unwind

$$\text{unwindLoop}\ \frac{\Gamma \Longrightarrow \langle \textbf{if}\ \ \mathtt{(b)}\ \ \{\ \mathtt{p;}\ \ \textbf{while}\ \ \mathtt{(b)}\ \ \mathtt{p}\ \};\ \ \mathit{rest}\rangle\phi, \Delta}{\Gamma \Longrightarrow \langle \textbf{while}\ \ \mathtt{(b)}\ \ \{\mathtt{p}\};\ \ \mathit{rest}\rangle\phi, \Delta}$$

Updates for KeY-Style Symbolic Execution

Needed: a Notation for Symbolic State Changes

- Symbolic execution should "walk" through program in natural forward direction
- Need succinct representation of state changes, effected by each symbolic execution step
- Want to simplify effects of program execution early
- Want to apply state changes late (to branching conditions and post condition)

Updates for KeY-Style Symbolic Execution

Needed: a Notation for Symbolic State Changes

- Symbolic execution should "walk" through program in natural forward direction
- Need succinct representation of state changes, effected by each symbolic execution step
- Want to simplify effects of program execution early
- Want to apply state changes late (to branching conditions and post condition)

We use dedicated notation for state changes: updates

Explicit State Updates

Definition (Syntax of Updates, Updated Terms/Formulas)

If v is program variable, t FOL term (of right type), t' any FOL term, and ϕ any DL formula, then

- $\{\mathrm{v} := t\}$ is an update
- $\{\mathrm{v} := t\}t'$ is DL term
- $\{\mathrm{v} := t\}\phi$ is DL formula

Definition (Semantics of Updates)

State $\mathcal{S}$ interprets program variables v with $\mathcal{I}_{\mathcal{S}}(v)$, β variable assignment for logical variables in t, define semantics ρ as:

$\rho_\beta(\{\mathrm{v} := t\})(\mathcal{S}) = \mathcal{S}'$ where $\mathcal{S}'$ identical to $\mathcal{S}$ except $\mathcal{I}_{\mathcal{S}'}(\mathrm{v}) = val_{\mathcal{S},\beta}(t)$

Explicit State Updates Cont'd

Facts about updates $\{\mathtt{v} := t\}$

- Update semantics similar to that of assignment
- Value of update also depends on $\mathcal{S}$ and logical variables in t, i.e., β
- Updates are not assignments: right-hand side is FOL term

  $\{\mathtt{x} := n\}\phi$ cannot be turned into assignment if n is a logical variable

  $\langle\mathtt{x=i++;}\rangle\phi$ cannot (immediately) be turned into update
- Updates are not equations: they change value of $\mathtt{v}$

Computing Effect of Updates (Automated)

Rewrite rules for update followed by ...

program variable	$\{\mathrm{x} := t\}\mathrm{x} \leadsto t$ $\{\mathrm{x} := t\}\mathrm{y} \leadsto \mathrm{y}$
logical variable	$\{\mathrm{x} := t\}w \leadsto w$
complex term	$\{\mathrm{x} := t\}f(t_1, \ldots, t_n) \leadsto f(\{\mathrm{x} := t\}t_1, \ldots, \{\mathrm{x} := t\}t_n)$
atomic formula	$\{\mathrm{x} := t\}p(t_1, \ldots, t_n) \leadsto p(\{\mathrm{x} := t\}t_1, \ldots, \{\mathrm{x} := t\}t_n)$
FOL formula	$\{\mathrm{x} := t\}(\phi \ \& \ \psi) \leadsto \{\mathrm{x} := t\}\phi \ \& \ \{\mathrm{x} := t\}\psi$ $\cdots$ $\{\mathrm{x} := t\}(\forall \tau\ y; \phi) \leadsto \forall \tau\ y; (\{\mathrm{x} := t\}\phi)$
program formula	No rewrite rule for $\{\mathrm{x} := t\}\langle \mathit{prog} \rangle \phi$

Substitution delayed until prog symbolically executed

Assignment Rule Using Updates

Symbolic execution of assignment using updates

$$\text{assign} \quad \frac{\Gamma \Longrightarrow \{\mathtt{x} := t\}\langle \mathit{rest} \rangle \phi, \Delta}{\Gamma \Longrightarrow \langle \mathtt{x}\ \mathtt{=}\ t\mathtt{;}\ \mathit{rest} \rangle \phi, \Delta}$$

- Works as long as t is 'simple' (has no side effects)
- For every built-in Java operation, we need a seperate rule (for `x = ` t_1`+`t_2 and `x = ` t_1`-`t_2 etc.)

Demo

`updates/assignmentToUpdate.key`

Parallel Updates

How to apply updates on updates?

Example

Symbolic execution of

```
t=x; x=y; y=t;
```

yields:

```
{t := x}{x := y}{y := t}
```

Need to compose three sequential state changes into a single one:

Parallel Updates

How to apply updates on updates?

Example

Symbolic execution of

```
t=x; x=y; y=t;
```

yields:

```
{t := x}{x := y}{y := t}
```

Need to compose three sequential state changes into a single one:
parallel updates

Parallel Updates Cont'd

Definition (Parallel Update)

A parallel update has the form $\{v_1 := r_1 || \cdots || v_n := r_n\}$, where each $\{v_i := r_i\}$ is simple update

- All r_i computed in old state before update is applied
- Updates of all program variables v_i executed simultaneously
- Upon conflict $v_i = v_j$, $r_i \neq r_j$ later update ($\max\{i, j\}$) wins

Parallel Updates Cont'd

Definition (Parallel Update)

A parallel update has the form $\{v_1 := r_1 || \cdots || v_n := r_n\}$, where each $\{v_i := r_i\}$ is simple update

- All r_i computed in old state before update is applied
- Updates of all program variables v_i executed simultaneously
- Upon conflict $v_i = v_j,\ r_i \neq r_j$ later update ($\max\{i, j\}$) wins

Definition (Parallelising Updates, Conflict Resolution)

$$\{v_1 := r_1\}\{v_2 := r_2\} \;=\; \{v_1 := r_1 || v_2 := \{v_1 := r_1\}r_2\}$$

Parallel Updates Cont'd

Definition (Parallel Update)

A parallel update has the form $\{v_1 := r_1 || \cdots || v_n := r_n\}$, where each $\{v_i := r_i\}$ is simple update

- All r_i computed in old state before update is applied
- Updates of all program variables v_i executed simultaneously
- Upon conflict $v_i = v_j,\ r_i \neq r_j$ later update $(\max\{i, j\})$ wins

Definition (Parallelising Updates, Conflict Resolution)

$$\{v_1 := r_1\}\{v_2 := r_2\} \;=\; \{v_1 := r_1 || v_2 := \{v_1 := r_1\}r_2\}$$

$$\{v_1 := r_1 || \cdots || v_n := r_n\}\mathtt{x} \;=\; \begin{cases} \mathtt{x} & \text{if } \mathtt{x} \notin \{v_1, \ldots, v_n\} \\ r_k & \text{if } \mathtt{x} = v_k,\ \mathtt{x} \notin \{v_{k+1}, \ldots, v_n\} \end{cases}$$

Symbolic Execution with Updates (by Example)

$\Longrightarrow$ `x` $<$ `y` `->` $\langle$`t=x; x=y; y=t;`$\rangle$ `y` $<$ `x`

Symbolic Execution with Updates (by Example)

$$\mathtt{x} < \mathtt{y} \implies \{\mathtt{t{:=}x}\}\langle\mathtt{x{=}y;\ y{=}t;}\rangle\, \mathtt{y} < \mathtt{x}$$

$$\vdots$$

$$\implies \mathtt{x} < \mathtt{y}\ \texttt{->}\ \langle\mathtt{t{=}x;\ x{=}y;\ y{=}t;}\rangle\, \mathtt{y} < \mathtt{x}$$

Symbolic Execution with Updates (by Example)

$$x < y \implies \{\texttt{t:=x}\}\{\texttt{x:=y}\}\langle\texttt{y=t;}\rangle\, y < x$$

$$\vdots$$

$$x < y \implies \{\texttt{t:=x}\}\langle\texttt{x=y; y=t;}\rangle\, y < x$$

$$\vdots$$

$$\implies x < y \texttt{ -> } \langle\texttt{t=x; x=y; y=t;}\rangle\, y < x$$

Symbolic Execution with Updates (by Example)

$$\mathtt{x} < \mathtt{y} \implies \{\mathtt{t{:=}x} \parallel \mathtt{x{:=}y}\}\{\mathtt{y{:=}t}\}\langle\rangle\ \mathtt{y} < \mathtt{x}$$

$$\vdots$$

$$\mathtt{x} < \mathtt{y} \implies \{\mathtt{t{:=}x}\}\{\mathtt{x{:=}y}\}\langle\mathtt{y=t;}\rangle\ \mathtt{y} < \mathtt{x}$$

$$\vdots$$

$$\mathtt{x} < \mathtt{y} \implies \{\mathtt{t{:=}x}\}\langle\mathtt{x=y;\ y=t;}\rangle\ \mathtt{y} < \mathtt{x}$$

$$\vdots$$

$$\implies \mathtt{x} < \mathtt{y}\ \mathtt{->}\ \langle\mathtt{t=x;\ x=y;\ y=t;}\rangle\ \mathtt{y} < \mathtt{x}$$

Symbolic Execution with Updates (by Example)

$$\mathtt{x} < \mathtt{y} \implies \{\mathtt{t:=x} \parallel \mathtt{x:=y} \parallel \mathtt{y:=x}\}\langle\rangle\ \mathtt{y} < \mathtt{x}$$

$$\vdots$$

$$\mathtt{x} < \mathtt{y} \implies \{\mathtt{t:=x} \parallel \mathtt{x:=y}\}\{\mathtt{y:=t}\}\langle\rangle\ \mathtt{y} < \mathtt{x}$$

$$\vdots$$

$$\mathtt{x} < \mathtt{y} \implies \{\mathtt{t:=x}\}\{\mathtt{x:=y}\}\langle\mathtt{y=t;}\rangle\ \mathtt{y} < \mathtt{x}$$

$$\vdots$$

$$\mathtt{x} < \mathtt{y} \implies \{\mathtt{t:=x}\}\langle\mathtt{x=y;\ y=t;}\rangle\ \mathtt{y} < \mathtt{x}$$

$$\vdots$$

$$\implies \mathtt{x} < \mathtt{y}\ \mathtt{->}\ \langle\mathtt{t=x;\ x=y;\ y=t;}\rangle\ \mathtt{y} < \mathtt{x}$$

Symbolic Execution with Updates (by Example)

$$\mathtt{x} < \mathtt{y} \implies \{\mathtt{x:=y} \parallel \mathtt{y:=x}\}\langle\rangle\, \mathtt{y} < \mathtt{x}$$

$$\vdots$$

$$\mathtt{x} < \mathtt{y} \implies \{\mathtt{t:=x} \parallel \mathtt{x:=y} \parallel \mathtt{y:=x}\}\langle\rangle\, \mathtt{y} < \mathtt{x}$$

$$\vdots$$

$$\mathtt{x} < \mathtt{y} \implies \{\mathtt{t:=x} \parallel \mathtt{x:=y}\}\{\mathtt{y:=t}\}\langle\rangle\, \mathtt{y} < \mathtt{x}$$

$$\vdots$$

$$\mathtt{x} < \mathtt{y} \implies \{\mathtt{t:=x}\}\{\mathtt{x:=y}\}\langle\mathtt{y=t;}\rangle\, \mathtt{y} < \mathtt{x}$$

$$\vdots$$

$$\mathtt{x} < \mathtt{y} \implies \{\mathtt{t:=x}\}\langle\mathtt{x=y;\ y=t;}\rangle\, \mathtt{y} < \mathtt{x}$$

$$\vdots$$

$$\implies \mathtt{x} < \mathtt{y} \;\texttt{->}\; \langle\mathtt{t=x;\ x=y;\ y=t;}\rangle\, \mathtt{y} < \mathtt{x}$$

Symbolic Execution with Updates (by Example)

$$\mathtt{x} < \mathtt{y} \implies \mathtt{x} < \mathtt{y}$$

$$\vdots$$

$$\mathtt{x} < \mathtt{y} \implies \{\mathtt{x:=y} \parallel \mathtt{y:=x}\}\langle\rangle\, \mathtt{y} < \mathtt{x}$$

$$\vdots$$

$$\mathtt{x} < \mathtt{y} \implies \{\mathtt{t:=x} \parallel \mathtt{x:=y} \parallel \mathtt{y:=x}\}\langle\rangle\, \mathtt{y} < \mathtt{x}$$

$$\vdots$$

$$\mathtt{x} < \mathtt{y} \implies \{\mathtt{t:=x} \parallel \mathtt{x:=y}\}\{\mathtt{y:=t}\}\langle\rangle\, \mathtt{y} < \mathtt{x}$$

$$\vdots$$

$$\mathtt{x} < \mathtt{y} \implies \{\mathtt{t:=x}\}\{\mathtt{x:=y}\}\langle\mathtt{y=t;}\rangle\, \mathtt{y} < \mathtt{x}$$

$$\vdots$$

$$\mathtt{x} < \mathtt{y} \implies \{\mathtt{t:=x}\}\langle\mathtt{x=y;\ y=t;}\rangle\, \mathtt{y} < \mathtt{x}$$

$$\vdots$$

$$\implies \mathtt{x} < \mathtt{y} \texttt{ -> } \langle\mathtt{t=x;\ x=y;\ y=t;}\rangle\, \mathtt{y} < \mathtt{x}$$

Parallel Updates Cont'd

Demo

`updates/swap1.key`

Parallel Updates Cont'd

Example

symbolic execution of `x=x+y; y=x-y; x=x-y;` gives

`({x := x+y}{y := x-y}){x := x-y}`

Parallel Updates Cont'd

Example

symbolic execution of `x=x+y; y=x-y; x=x-y;` gives

```
({x := x+y}{y := x-y}){x := x-y}
{x := x+y || y := (x+y)-y}{x := x-y}
```

Parallel Updates Cont'd

Example

symbolic execution of `x=x+y; y=x-y; x=x-y;` gives

```
({x := x+y}{y := x-y}){x := x-y}
{x := x+y || y := (x+y)-y}{x := x-y}
{x := x+y || y := (x+y)-y || x := (x+y)-((x+y)-y)}
```

Parallel Updates Cont'd

Example

symbolic execution of `x=x+y; y=x-y; x=x-y;` gives

```
({x := x+y}{y := x-y}){x := x-y}
{x := x+y || y := (x+y)-y}{x := x-y}
{x := x+y || y := (x+y)-y || x := (x+y)-((x+y)-y)}
{x := x+y || y := x || x := y}
```

Parallel Updates Cont'd

Example

symbolic execution of `x=x+y; y=x-y; x=x-y;` gives

```
({x := x+y}{y := x-y}){x := x-y}
{x := x+y || y := (x+y)-y}{x := x-y}
{x := x+y || y := (x+y)-y || x := (x+y)-((x+y)-y)}
{x := x+y || y := x || x := y}
{y := x || x := y}
```

In case of conflict, KeY only keeps winning update

Parallel Updates Cont'd

Example

symbolic execution of `x=x+y; y=x-y; x=x-y;` gives

```
({x := x+y}{y := x-y}){x := x-y}
{x := x+y || y := (x+y)-y}{x := x-y}
{x := x+y || y := (x+y)-y || x := (x+y)-((x+y)-y)}
{x := x+y || y := x || x := y}
{y := x || x := y}
```

In case of conflict, KeY only keeps winning update

Parallel updates store intermediate state of symbolic computation

Another use of Updates

If you would like to quantify over a program variable ...

Another use of Updates

If you would like to quantify over a program variable ...

Not allowed: $\forall \tau\ \mathtt{i}; \langle \ldots \mathtt{i} \ldots \rangle \phi$
(program variables $\cap$ logical variables $= \emptyset$)

Another use of Updates

If you would like to quantify over a program variable ...

Not allowed: $\forall\,\tau\ \mathtt{i};\ \langle\ldots\mathtt{i}\ldots\rangle\phi$

(program variables $\cap$ logical variables $= \emptyset$)

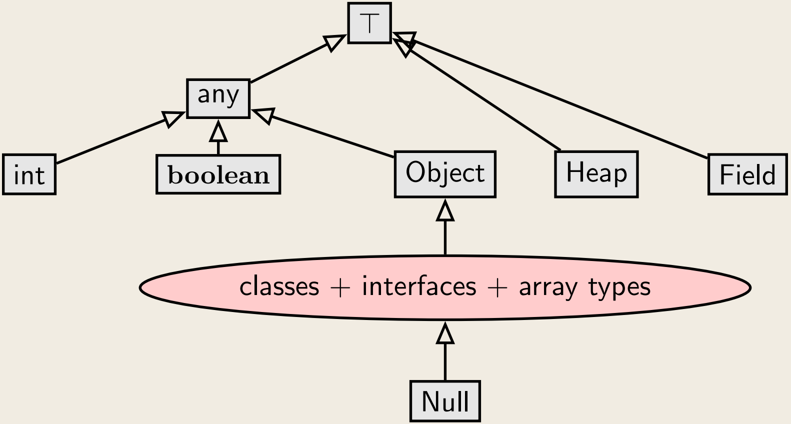
Instead

Quantify over value, and assign it to program variable:

$\forall\,\tau\ x;\ \{\mathtt{i} := x\}\langle\ldots\mathtt{i}\ldots\rangle\phi$

Modelling Java in FOL: Fixing a Type Hierarchy

Signature based on Java's type hierarchy



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

Modelling the Heap in FOL

The Java Heap

Objects are stored on (i.e., in) the heap.

- Status of heap changes during execution
- Each heap associates values to object/field pairs

Modelling the Heap in FOL

The Java Heap

Objects are stored on (i.e., in) the heap.

- Status of heap changes during execution
- Each heap associates values to object/field pairs

The Heap Model of KeY-DL

Each element of data type Heap represents a certain heap status.
Two functions involving heaps:

Modelling the Heap in FOL

The Java Heap

Objects are stored on (i.e., in) the heap.

- Status of heap changes during execution
- Each heap associates values to object/field pairs

The Heap Model of KeY-DL

Each element of data type Heap represents a certain heap status.
Two functions involving heaps:

- in F_{Σ}: Heap `store(`Heap, Object, Field, any`);`
  `store(`h, o, f, v`)` returns heap like h, but with v associated to $o.f$

Modelling the Heap in FOL

The Java Heap

Objects are stored on (i.e., in) the heap.

- Status of heap changes during execution
- Each heap associates values to object/field pairs

The Heap Model of KeY-DL

Each element of data type Heap represents a certain heap status.
Two functions involving heaps:

- in F_Σ: Heap `store`(Heap, Object, Field, any) ;
  `store`(h, o, f, v) returns heap like h, but with v associated to $o.f$
- in F_Σ: any `select`(Heap, Object, Field) ;
  `select`(h, o, f) returns value associated to $o.f$ in h

Modelling the Heap in FOL

Modelling instance fields

Person
int age int id
int setAge(int newAge) int getId()

- for each JAVA reference type C there is a type $C \in T_\Sigma$, for example, Person

Modelling the Heap in FOL

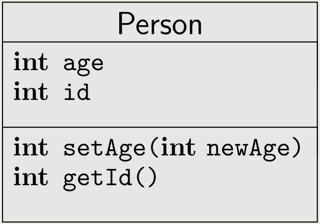
Modelling instance fields

Person
`int age` `int id`
`int setAge(int newAge)` `int getId()`

- for each JAVA reference type C there is a type $C \in T_\Sigma$, for example, Person
- for each field `f` there is a unique constant `f` of type Field, for example, `id`

Modelling the Heap in FOL

Modelling instance fields



- for each JAVA reference type C there is a type $C \in T_\Sigma$, for example, Person
- for each field `f` there is a unique constant `f` of type Field, for example, `id`
- domain of all Person objects: $\mathtt{D}^{\mathsf{Person}}$

Modelling the Heap in FOL

Modelling instance fields

```
Person
-----------------------------
int age
int id
-----------------------------
int setAge(int newAge)
int getId()
```

- for each JAVA reference type C there is a type C $\in T_\Sigma$, for example, Person
- for each field `f` there is a unique constant `f` of type Field, for example, `id`
- domain of all Person objects: $\mathtt{D}^{\mathsf{Person}}$
- heap maps pair (object, field) to value

Modelling the Heap in FOL

Modelling instance fields

```
Person
-----------------------------
int age
int id
-----------------------------
int setAge(int newAge)
int getId()
```

- for each JAVA reference type C there is a type $\mathsf{C} \in T_\Sigma$, for example, Person
- for each field `f` there is a unique constant `f` of type Field, for example, `id`
- domain of all Person objects: $\mathtt{D}^{\mathsf{Person}}$
- heap maps pair (object, field) to value

Reading Field `id` of Person `p`

FOL notation $\mathtt{select}(h, \mathtt{p}, \mathtt{id})$

Modelling the Heap in FOL

Modelling instance fields

Person
int age int id
int setAge(int newAge) int getId()

- for each JAVA reference type C there is a type $C \in T_\Sigma$, for example, Person
- for each field `f` there is a unique constant `f` of type Field, for example, `id`
- domain of all Person objects: $\mathtt{D}^{\text{Person}}$
- heap maps pair (object, field) to value

Reading Field `id` of Person `p`

FOL notation $\mathtt{select}(h, \mathtt{p}, \mathtt{id})$

KeY notation `p.id@`h (abbreviating $\mathtt{select}(h, \mathtt{p}, \mathtt{id})$)

Modelling the Heap in FOL

Modelling instance fields

Person
`int age` `int id`
`int setAge(int newAge)` `int getId()`

- for each JAVA reference type C there is a type $\mathsf{C} \in T_\Sigma$, for example, Person
- for each field `f` there is a unique constant `f` of type Field, for example, `id`
- domain of all Person objects: $\mathtt{D}^{\mathsf{Person}}$
- heap maps pair (object, field) to value

Reading Field `id` of Person `p`

FOL notation $\mathtt{select}(h, \mathtt{p}, \mathtt{id})$

KeY notation $\mathtt{p.id@}h$ (abbreviating $\mathtt{select}(h, \mathtt{p}, \mathtt{id})$)

$\mathtt{p.id}$ (abbreviating $\mathtt{select}(\mathtt{heap}, \mathtt{p}, \mathtt{id})$)[a]

---

[a] `heap` is special program variable for "current" heap; mostly implicit in $o.f$

Modelling the Heap in FOL

Modelling instance fields

Person
int age int id
int setAge(int newAge) int getId()

- for each JAVA reference type C there is a type $C \in T_\Sigma$, for example, Person
- for each field `f` there is a unique constant `f` of type Field, for example, `id`
- domain of all Person objects: $\mathtt{D}^{\text{Person}}$
- heap maps pair (object, field) to value

Writing to Field `id` of Person `p`

FOL notation $\mathtt{store}(h, \mathtt{p}, \mathtt{id}, 6238)$

Modelling the Heap in FOL

Modelling instance fields

Person
int age int id
int setAge(int newAge) int getId()

- for each JAVA reference type C there is a type $C \in T_\Sigma$, for example, Person
- for each field `f` there is a unique constant `f` of type Field, for example, `id`
- domain of all Person objects: D^{Person}
- heap maps pair (object, field) to value

Writing to Field `id` of Person `p`

FOL notation $\mathtt{store}(h, \mathtt{p}, \mathtt{id}, 6238)$

KeY notation $h[\mathtt{p}.\mathtt{id} := 6238]$ (notation for `store`, not update)

The Algebra of Heaps

We do *not* formalise the *structure* (implementation) of heaps.
We formalise the *behaviour*, with an algebra of heap operations:

$$\mathtt{select}(\mathtt{store}(h, o, f, v), o, f) =$$

The Algebra of Heaps

We do *not* formalise the *structure* (implementation) of heaps.
We formalise the *behaviour*, with an algebra of heap operations:

$$\texttt{select}(\texttt{store}(h, o, f, v), o, f) = v$$

The Algebra of Heaps

We do *not* formalise the *structure* (implementation) of heaps.
We formalise the *behaviour*, with an algebra of heap operations:

$$\mathtt{select}(\mathtt{store}(h, o, f, v), o, f) = v$$

$$(o \neq o' \vee f \neq f') \;\rightarrow\; \mathtt{select}(\mathtt{store}(h, o, f, x), o', f') =$$

The Algebra of Heaps

We do *not* formalise the *structure* (implementation) of heaps.
We formalise the *behaviour*, with an algebra of heap operations:

$$\mathtt{select}(\mathtt{store}(h, o, f, v), o, f) = v$$

$$(o \neq o' \vee f \neq f') \;\rightarrow\; \mathtt{select}(\mathtt{store}(h, o, f, x), o', f') = \mathtt{select}(h, o', f')$$

The Algebra of Heaps

We do *not* formalise the *structure* (implementation) of heaps.
We formalise the *behaviour*, with an algebra of heap operations:

$$\texttt{select}(\texttt{store}(h, o, f, v), o, f) = v$$

$$(o \neq o' \vee f \neq f') \ \rightarrow \ \texttt{select}(\texttt{store}(h, o, f, x), o', f') = \texttt{select}(h, o', f')$$

Example

$\texttt{select}(\texttt{store}(h, \texttt{o}, \texttt{f}, 15), \texttt{o}, \texttt{f}) \leadsto 15$
$\texttt{select}(\texttt{store}(h, \texttt{o}, \texttt{f}, 15), \texttt{o}, \texttt{g}) \leadsto \texttt{select}(h, \texttt{o}, \texttt{g})$
$\texttt{select}(\texttt{store}(h, \texttt{o}, \texttt{f}, 15), \texttt{u}, \texttt{f}) \leadsto$
$\quad \text{if } (\texttt{o} = \texttt{u}) \text{ then } (15) \text{ else } (\texttt{select}(h, \texttt{u}, \texttt{f}))$

Pretty Printing

Shorthand Notations for Heap Operations

$\mathtt{o.f@h}$	is	$\mathtt{select}(\mathtt{h}, \mathtt{o}, \mathtt{f})$
$\mathtt{h}[\mathtt{o.f} := \mathtt{v}]$	is	$\mathtt{store}(\mathtt{h}, \mathtt{o}, \mathtt{f}, \mathtt{v})$

Pretty Printing

Shorthand Notations for Heap Operations

$\mathtt{o.f@h}$	is	$\mathtt{select}(\mathtt{h}, \mathtt{o}, \mathtt{f})$
$\mathtt{h}[\mathrm{o.f} := \mathrm{v}]$	is	$\mathtt{store}(\mathtt{h}, \mathtt{o}, \mathtt{f}, \mathtt{v})$

therefore:

$\mathtt{u.f@h}[\mathrm{o.f} := \mathrm{v}]$	is	$\mathtt{select}(\mathtt{store}(\mathtt{h}, \mathtt{o}, \mathtt{f}, \mathtt{v}), \mathtt{u}, \mathtt{f})$
$\mathtt{h}[\mathrm{o.f} := \mathrm{v}][\mathrm{o}'.\mathrm{f}' := \mathrm{v}']$	is	$\mathtt{store}(\mathtt{store}(\mathtt{h}, \mathtt{o}, \mathtt{f}, \mathtt{v}), \mathtt{o}', \mathtt{f}', \mathtt{v}')$

Pretty Printing

Shorthand Notations for Heap Operations

$\mathtt{o.f@h}$	is	$\mathtt{select}(\mathrm{h}, \mathrm{o}, \mathrm{f})$
$\mathrm{h}[\mathrm{o.f} := \mathrm{v}]$	is	$\mathtt{store}(\mathrm{h}, \mathrm{o}, \mathrm{f}, \mathrm{v})$

therefore:

$\mathrm{u.f@h}[\mathrm{o.f} := \mathrm{v}]$	is	$\mathtt{select}(\mathtt{store}(\mathrm{h}, \mathrm{o}, \mathrm{f}, \mathrm{v}), \mathrm{u}, \mathrm{f})$
$\mathrm{h}[\mathrm{o.f} := \mathrm{v}][\mathrm{o}'.\mathrm{f}' := \mathrm{v}']$	is	$\mathtt{store}(\mathtt{store}(\mathrm{h}, \mathrm{o}, \mathrm{f}, \mathrm{v}), \mathrm{o}', \mathrm{f}', \mathrm{v}')$

Very-Shorthand Notations for Current Heap

Current heap always in special variable $\mathtt{heap}$.

$\mathrm{o.f}$	is	$\mathtt{select}(\mathtt{heap}, \mathrm{o}, \mathrm{f})$
$\{\mathrm{o.f} := \mathrm{v}\}$	is update	$\{\mathtt{heap} := \mathtt{heap}[\mathrm{o.f} := \mathrm{v}]\}$

Modelling the Heap in FOL—The Full Story

Is formula $\texttt{select}(h, \texttt{p}, \texttt{id}) >= 0$ type-safe?

Modelling the Heap in FOL—The Full Story

Is formula $\texttt{select}(h, \texttt{p}, \texttt{id}) >= 0$ type-safe?

1. Return type is any—need to 'cast' to **int**
2. There can be many fields with name `id`

Modelling the Heap in FOL—The Full Story

Is formula $\texttt{select}(h, \mathrm{p}, \texttt{id}) >= 0$ type-safe?

1. Return type is any—need to 'cast' to **int**
2. There can be many fields with name `id`

Real Field Access

$\texttt{int::select}(h, \mathrm{p}, \mathsf{Person::}\texttt{\$id}) >= 0$ is type-safe

- `int::select` is a function name, not a cast
- can be understood *intuitively* as (**int**)`select`

Modelling the Heap in FOL—The Full Story

Is formula `select`$(h, \mathtt{p}, \mathtt{id}) >= 0$ type-safe?

1. Return type is any—need to 'cast' to **int**
2. There can be many fields with name `id`

Real Field Access

$\mathtt{int::select}(h, \mathtt{p}, \mathrm{Person}::\$\mathtt{id}) >= 0$ is type-safe

- `int::select` is a function name, not a cast
- can be understood *intuitively* as (**int**)`select`

General

For each `T` typed field `f` of class `C`, F_Σ contains

- a constant declared as Field `C::$f`
- a function declared as `T` `T::select`(Heap, `C`, Field)

Modelling the Heap in FOL—The Full Story

Is formula `select`$(h, \mathtt{p}, \mathtt{id}) >= 0$ type-safe?

1. Return type is any—need to ‘cast’ to **int**
2. There can be many fields with name `id`

Real Field Access

$\mathtt{int::select}(h, \mathtt{p}, \mathsf{Person}::\$\mathtt{id}) >= 0$ is type-safe

- `int::select` is a function name, not a cast
- can be understood *intuitively* as (**int**)`select`

General

For each `T` typed field `f` of class `C`, F_Σ contains

- a constant declared as Field `C::$f`
- a function declared as `T` `T::select`(Heap, `C`, Field)

Everything blue is a function name

Field Update Assignment Rule

Changing the value of fields

How to (symbolically) execute assignment to field, e.g., `p.age=18;` ?

$$\text{assign}\ \frac{\Gamma \Longrightarrow \{\mathtt{o.f} := t\}\langle \mathit{rest}\rangle\phi, \Delta}{\Gamma \Longrightarrow \langle \mathtt{o.f\ =\ }t\mathtt{;}\ \mathit{rest}\rangle\phi, \Delta}$$

Admit on left-hand side of update JAVA location expressions

Field Update Assignment Rule

Changing the value of fields

How to (symbolically) execute assignment to field, e.g., `p.age=18;` ?

$$\text{assign}\ \frac{\Gamma \Longrightarrow \{\texttt{p.age} := 18\}\langle \mathit{rest} \rangle \phi, \Delta}{\Gamma \Longrightarrow \langle \texttt{p.age = 18;}\ \mathit{rest} \rangle \phi, \Delta}$$

Admit on left-hand side of update JAVA location expressions

Field Update Assignment Rule

Changing the value of fields

How to (symbolically) execute assignment to field, e.g., `p.age=18;` ?

$$\text{assign}\ \frac{\Gamma \Longrightarrow \{\mathtt{o.f} := t\}\langle \mathit{rest}\rangle\phi, \Delta}{\Gamma \Longrightarrow \langle \mathtt{o.f\ =\ }t\mathtt{;}\ \ \mathit{rest}\rangle\phi, \Delta}$$

Admit on left-hand side of update JAVA location expressions

But is this rule correct? See below.

Dynamic Logic: KeY input file

```
\javaSource "path to source code referenced in problem";

\programVariables { Person p; }

\problem {
        \<{   p.age = 18;  }\> p.age = 18
}
```

KeY reads in all source files and creates automatically
the necessary signature (types, program variables, field constants)

Dynamic Logic: KeY input file

```
\javaSource "path to source code referenced in problem";

\programVariables { Person p; }

\problem {
      \<{   p.age = 18;  }\> p.age = 18
}
```

KeY reads in all source files and creates automatically
the necessary signature (types, program variables, field constants)

Demo

`updates/firstAttributeExample.key`

Refined Semantics of Program Modalities

Does abrupt termination count as normal termination?

No! Need to distinguish normal and exceptional termination

Refined Semantics of Program Modalities

Does abrupt termination count as normal termination?
No! Need to distinguish normal and exceptional termination

- $\langle \mathtt{p} \rangle \phi$: $\mathtt{p}$ terminates normally and formula ϕ holds in final state (total correctness)

Refined Semantics of Program Modalities

Does abrupt termination count as normal termination?
No! Need to distinguish normal and exceptional termination

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

Refined Semantics of Program Modalities

Does abrupt termination count as normal termination?
No! Need to distinguish normal and exceptional termination

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

Abrupt termination on top-level counts as non-termination!

Example Reconsidered: Exception Handling

```
\javaSource "path to source code";

\programVariables {
   ...
}

\problem {
       p != null -> \<{   p.age = 18;  }\> p.age = 18
}
```

Only provable when no top-level exception thrown

Demo

`updates/secondAttributeExample.key`

The Self Reference

Modeling reference this

Special name for the object whose Java code is currently executed:

in JML: `Object` **this**;

in Java: `Object` **this**;

in KeY: `Object self;`

Default assumption in JML-KeY translation: $\texttt{self} \mathrel{!=} \textbf{null}$

Which Objects do Exist?

How to model object creation with **new** ?

Which Objects do Exist?

How to model object creation with **new** ?

Constant Domain Assumption

Assume that domain $\mathcal{D}$ is the same in all states $(\mathcal{D}, \delta, \mathcal{I}) \in \mathit{States}$

Consequence:
Quantifiers and modalities commute:

$$\models (\forall\ T\ x;\ [\mathrm{p}]\phi) \leftrightarrow [\mathrm{p}](\forall\ T\ x;\ \phi)$$

Object Creation (background; no need to remember this)

Realizing Constant Domain Assumption

- Implicitly declared field **boolean** `<created>` in class `Object`
- `<created>` has value **true** iff argument object has been created
- Object creation modeled as {`heap` := `create(heap, ob)`} for not (yet) created `ob` (essentially sets `<created>` field of `ob` to **true**)

Object Creation (background; no need to remember this)

Realizing Constant Domain Assumption

- Implicitly declared field **boolean** `<created>` in class `Object`
- `<created>` has value **true** iff argument object has been created
- Object creation modeled as $\{\texttt{heap} := \texttt{create(heap, ob)}\}$ for not (yet) created `ob` (essentially sets `<created>` field of `ob` to **true**)

$$\frac{\Gamma,\ \texttt{ob}.<\texttt{created}> = \texttt{FALSE} \Longrightarrow \{\texttt{heap}:=\texttt{create}(\texttt{heap},\texttt{ob})\}\{\texttt{o}:=\texttt{ob}\}\langle\texttt{o.<init>(}\mathit{param}\texttt{);}\ \omega\rangle\phi,\ \Delta}{\Gamma \Longrightarrow \langle\texttt{o} = \texttt{new T}(\mathit{param});\ \omega\rangle\phi, \Delta}$$

`ob` is a fresh program variable

Object Creation (background; no need to remember this)

Realizing Constant Domain Assumption

- Implicitly declared field **boolean** `<created>` in class `Object`
- `<created>` has value **true** iff argument object has been created
- Object creation modeled as $\{\texttt{heap} := \texttt{create(heap, ob)}\}$ for not (yet) created `ob` (essentially sets `<created>` field of `ob` to **true**)

$$\frac{\Gamma,\ \texttt{ob}.<\texttt{created}> = \texttt{FALSE} \Longrightarrow \{\texttt{heap}:=\texttt{create}(\texttt{heap},\texttt{ob})\}\{\texttt{o}:=\texttt{ob}\}\langle\texttt{o.<init>(}\mathit{param}\texttt{);}\ \omega\rangle\phi,\ \Delta}{\Gamma \Longrightarrow \langle\texttt{o} = \texttt{new T}(\mathit{param});\ \omega\rangle\phi, \Delta}$$

`ob` is a fresh program variable

Alternatives exisit in the literature. E.g.:
[Ahrendt, de Boer, Grabe, *Abstract Object Creation in Dynamic Logic – To Be or Not To Be Created*, Springer, LNCS 5850]

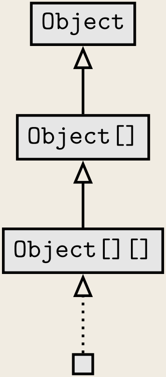
Dynamic Logic to (almost) full Java

KeY supports full sequential Java, with some limitations:

- Limited concurrency
- No generics
- No I/O
- No dynamic class loading or reflection
- Ongoing work to support floating point arithmetic
- API method calls: need either JML contract or implementation

Java Features in Dynamic Logic: Arrays

Arrays



- JAVA type hierarchy includes array types
- Types ordered according to JAVA subtyping rules
- Function $\texttt{arr} : \text{int} \to \text{Field}$ turns integer index into type Field (required in `store`).
- Store array elements on heap
- Value of `a[i]` in heap $\texttt{store}(\texttt{heap}, \texttt{a}, \texttt{arr}(\texttt{i}), 8)$ is 8
- Arrays `a` and `b` can refer to same object (aliasing)

Java Features in Dynamic Logic: Complex Expressions

Complex expressions with side effects

- JAVA expressions may have side effects, due to method calls, increment/decrement operators, nested assignments
- FOL terms have no side effect on the state

Example (Complex expression with side effects in Java)

`int i = 0; if ((i=2)>= 2) i++;` value of `i` ?

Complex Expressions Cont'd

Decomposition of complex terms by symbolic execution

Follow the rules laid down in JAVA Language Specification

Local code transformations

$$\text{evalOrderIteratedAssgnmt} \quad \frac{\Gamma \Longrightarrow \langle \texttt{y = t; x = y;}\ \omega\rangle\phi, \Delta}{\Gamma \Longrightarrow \langle \texttt{x = y = t;}\ \omega\rangle\phi, \Delta} \quad \texttt{t}\ \text{simple}$$

Temporary variables store result of evaluating subexpression

$$\text{ifEval} \quad \frac{\Gamma \Longrightarrow \langle \textbf{boolean}\ \texttt{v0; v0 = b; if (v0) p;}\ \omega\rangle\phi, \Delta}{\Gamma \Longrightarrow \langle \textbf{if}\ \texttt{(b) p;}\ \omega\rangle\phi, \Delta} \quad \texttt{b}\ \text{complex}$$

Java Features in Dynamic Logic: Abrupt Termination

Abrupt Termination: Exceptions and Jumps

Redirection of control flow via **return**, **break**, **continue**, exceptions

$$\langle \mathbf{try}\ \{\mathtt{p}\}\ \mathbf{catch}(\mathtt{T\ e})\ \{\mathtt{q}\}\ \mathbf{finally}\ \{\mathtt{r}\}\ \omega\rangle\phi$$

Java Features in Dynamic Logic: Abrupt Termination

Abrupt Termination: Exceptions and Jumps

Redirection of control flow via **return**, **break**, **continue**, exceptions

$$\langle \mathbf{try}\ \{\mathtt{p}\}\ \mathbf{catch}(\mathtt{T\ e})\ \{\mathtt{q}\}\ \mathbf{finally}\ \{\mathtt{r}\}\ \omega\rangle\phi$$

Rule tryThrow matches try–catch in pre-/postfix and active throw

$$\frac{\Longrightarrow \langle \mathrm{if}\,(\mathtt{e}\ \mathrm{instanceof}\ \mathtt{T})\{\mathrm{try}\{\mathtt{x=e;q}\}\mathrm{finally}\,\{\mathtt{r}\}\}\mathrm{else}\{\mathtt{r};\mathrm{throw}\ \mathtt{e};\}\ \omega\rangle\phi}{\Longrightarrow \langle \mathbf{try}\ \{\ \mathrm{throw}\ \mathtt{e};\ \mathtt{p}\}\ \mathbf{catch}(\mathtt{T\ x})\ \{\mathtt{q}\}\ \mathbf{finally}\ \{\mathtt{r}\}\ \omega\rangle\phi}$$

Java Features in Dynamic Logic: Abrupt Termination

Abrupt Termination: Exceptions and Jumps

Redirection of control flow via **return**, **break**, **continue**, exceptions

$$\langle \texttt{try}\ \{\texttt{p}\}\ \texttt{catch}(\texttt{T e})\ \{\texttt{q}\}\ \texttt{finally}\ \{\texttt{r}\}\ \omega\rangle\phi$$

Rule tryThrow matches try–catch in pre-/postfix and active throw

$$\frac{\Longrightarrow \langle \texttt{if (e instanceof T) \{try\{x=e;q\} finally \{r\}\} else\{r; throw e;\}}\ \omega\rangle\phi}{\Longrightarrow \langle \texttt{try \{ throw e; p\} catch(T x) \{q\} finally \{r\}}\ \omega\rangle\phi}$$

Demo

`exceptions/try-catch.key`

Java Features in Dynamic Logic: Null

Null pointer exceptions

There are no "exceptions" in FOL: $\mathcal{I}$ total on FSym

Need to model possibility that $\texttt{o} = \textbf{null}$ in $\texttt{o.a}$

Java Features in Dynamic Logic: Null

Null pointer exceptions

There are no "exceptions" in FOL: $\mathcal{I}$ total on FSym

Need to model possibility that $\mathtt{o} = \mathbf{null}$ in $\mathtt{o.a}$

- KeY branches over $\mathtt{o} = \mathbf{null}$ and $\mathtt{o} \neq \mathbf{null}$ upon each field access *within modalities*[a]

Java Features in Dynamic Logic: Null

Null pointer exceptions

There are no "exceptions" in FOL: $\mathcal{I}$ total on FSym

Need to model possibility that $\mathtt{o} = \mathbf{null}$ in o.a

- KeY branches over $\mathtt{o} = \mathbf{null}$ and $\mathtt{o} \neq \mathbf{null}$ upon each field access *within modalities*[a]
- Thereby, o.a appears *outside modalities* mostly under assumption $\mathtt{o} \neq \mathbf{null}$

Java Features in Dynamic Logic: Null

Null pointer exceptions

There are no "exceptions" in FOL: $\mathcal{I}$ total on FSym

Need to model possibility that $\mathtt{o} = \mathbf{null}$ in o.a

- KeY branches over $\mathtt{o} = \mathbf{null}$ and $\mathtt{o} \neq \mathbf{null}$ upon each field access *within modalities*[a]
- Thereby, o.a appears *outside modalities* mostly under assumption $\mathtt{o} \neq \mathbf{null}$
- $\mathbf{null}$.a *outside modalities* has a value, which is unknown

Java Features in Dynamic Logic: Null

Null pointer exceptions

There are no "exceptions" in FOL: $\mathcal{I}$ total on FSym

Need to model possibility that $\mathtt{o} = \mathbf{null}$ in o.a

- KeY branches over $\mathtt{o} = \mathbf{null}$ and $\mathtt{o} \neq \mathbf{null}$ upon each field access *within modalities*[a]
- Thereby, o.a appears *outside modalities* mostly under assumption $\mathtt{o} \neq \mathbf{null}$
- **null**.a *outside modalities* has a value, which is unknown

[a] Can be changed with Taclet Option runtimeExceptions

Field Update Assignment Rule Revisited (A)

Changing the value of fields

How to (symbolically) execute assignment to field?

$$\frac{\Gamma, \qquad\qquad \Longrightarrow \{\texttt{o.f} := \texttt{e}\}\langle \quad \omega\rangle\phi, \Delta}{\Gamma \Longrightarrow \langle \quad \texttt{o.f} = \texttt{e};\, \omega\rangle\phi, \Delta}$$

Field Update Assignment Rule Revisited (A)

Changing the value of fields

How to (symbolically) execute assignment to field?

$$\frac{\Gamma, \mathtt{o} \neq \mathbf{null} \Longrightarrow \{\mathtt{o.f} := \mathtt{e}\}\langle \quad \omega\rangle\phi, \Delta}{\Gamma \Longrightarrow \langle \quad \mathtt{o.f} = \mathtt{e};\, \omega\rangle\phi, \Delta}$$

Field Update Assignment Rule Revisited (A)

Changing the value of fields

How to (symbolically) execute assignment to field?

$$\frac{\Gamma, \mathtt{o} = \mathbf{null} \Longrightarrow \qquad \begin{array}{c}\Gamma, \mathtt{o} \neq \mathbf{null} \Longrightarrow \{\mathtt{o.f} := \mathtt{e}\}\langle \quad \omega\rangle\phi, \Delta \\ \end{array} \qquad , \Delta}{\Gamma \Longrightarrow \langle \quad \mathtt{o.f} = \mathtt{e};\, \omega\rangle\phi, \Delta}$$

Field Update Assignment Rule Revisited (A)

Changing the value of fields

How to (symbolically) execute assignment to field?

$$\frac{\Gamma, \mathsf{o} \neq \mathtt{\textbf{null}} \Longrightarrow \{\mathsf{o.f} := \mathsf{e}\}\langle\ \ \omega\rangle\phi, \Delta \qquad \Gamma, \mathsf{o} = \mathtt{\textbf{null}} \Longrightarrow \langle\ \ \mathtt{\textbf{throw}}\ \mathtt{new\ NullPointerException();}\ \omega\rangle\phi, \Delta}{\Gamma \Longrightarrow \langle\ \ \mathsf{o.f} = \mathsf{e};\ \omega\rangle\phi, \Delta}$$

Field Update Assignment Rule Revisited (A)

Changing the value of fields

How to (symbolically) execute assignment to field?

$$\frac{\begin{array}{c}\Gamma, \mathsf{o} \neq \mathbf{null} \Longrightarrow \{\mathsf{o.f} := \mathsf{e}\}\langle\pi\ \omega\rangle\phi, \Delta \\ \Gamma, \mathsf{o} = \mathbf{null} \Longrightarrow \langle\pi\, \mathbf{throw}\ \texttt{new NullPointerException();}\ \omega\rangle\phi, \Delta\end{array}}{\Gamma \Longrightarrow \langle\pi\, \mathsf{o.f} = \mathsf{e};\, \omega\rangle\phi, \Delta}$$

π is the "inactive prefix", any number of opening try blocks: $(\mathbf{try}\{)^*$

Field Update Assignment Rule Revisited (B)

Changing the value of fields

How to (symbolically) execute assignment to field?

$$\frac{\Gamma \Longrightarrow \mathtt{o} = \mathbf{null}, \{\mathtt{o.f} := \mathtt{e}\}\langle\pi\ \omega\rangle\phi, \Delta \qquad \Gamma, \mathtt{o} = \mathbf{null} \Longrightarrow \langle\pi\, \mathbf{throw}\ \mathtt{new\ NullPointerException();}\ \omega\rangle\phi, \Delta}{\Gamma \Longrightarrow \langle\pi\, \mathtt{o.f} = \mathtt{e};\ \omega\rangle\phi, \Delta}$$

π is the "inactive prefix", any number of opening try blocks: $(\mathbf{try}\{)^*$

Revisit: Field Assignment Demo

```
\javaSource "path to source code referenced in problem";

\programVariables { Person p; }

\problem {
      \<{   p.age = 18;  }\> p.age = 18
}
```

Demo

updates/firstAttributeExample.key

Java Features in Dynamic Logic: Aliasing

Demo

`aliasing/attributeAlias1.key`

Java Features in Dynamic Logic: Aliasing

Demo

`aliasing/attributeAlias1.key`

Reference Aliasing

Alias resolution causes proof split

Summary

- Most JAVA features covered in KeY
- Degree of automation for loop-free programs is very high
- Handling of loops: last lecture

Literature for this Lecture

KeYbook *W. Ahrendt*, B. Beckert, R. Bubel, R. Hähnle, P. Schmitt, M. Ulbrich, editors.
Deductive Software Verification - The KeY Book
Vol 10001 of *LNCS*, Springer, 2016
(E-book at `link.springer.com`)

- B. Beckert, V. Klebanov, B. Weiß, Dynamic Logic for Java
  Chapter 3 in [KeYbook]
  on the surface only: Sections 3.1, 3.2, 3.4, 3.5.5, 3.5.6, 3.5.7, 3.6
- *W. Ahrendt*, S. Grebing, Using the KeY Prover
  Chapter 15 in [KeYbook]