Semantics and Verification of Software

Winter Semester 2017/18

Lecture 14: Extension by Blocks and Procedures I (Operational Semantics)

Thomas Noll
Software Modeling and Verification Group
RWTH Aachen University

http://moves.rwth-aachen.de/teaching/ws-1718/sv-sw/

Software Modeling and Verification Chair

RWTH AACHEN UNIVERSITY

EvaSys | Vorlesung (dt./engl.)

RWTH Aachen | apl. Prof. Dr.rer.nat. Thomas Noll
WS17/18 | Concurrency Theory (17ws-38073)

RWTH AACHEN UNIVERSITY

Markieren Sie so: ☐☒☐☐☐ Verwenden Sie bitte einen Kugelschreiber, rote Farbe unbedingt vermeiden!
Mark: *Please use a black ballpoint pen. Do not use red ink!*
Korrektur: ☐■☐☒☐ Eintragungen außerhalb der makierten Felder fließen nicht in die Auswertung mit ein.
Correction: *Please observe the notes on the left when filling in the form in order to ensure optimal data collection.*

Liebe Studierende,
die RWTH Aachen hat das Ziel, Ihnen eine gute Lehre zu bieten. Dazu benötigen wir Ihre Mitarbeit und möchten Sie zu Ihrer Einschätzung zu der von Ihnen besuchten Veranstaltung befragen. Die Befragung und Auswertung erfüllen die datenschutzrechtlichen Bestimmungen; die Teilnahme ist anonym und freiwillig.
Die Lehrenden sind verpflichtet, die Ergebnisse aus der Studentischen Lehrveranstaltungsbewertung mit den Studierenden in der Veranstaltung zu besprechen. Sollte dies nicht der Fall sein, wenden Sie sich bitte an: lehre@rwth-aachen.de.
Dort wird Ihr Anliegen anonym behandelt.
Legende:
k.A. = keine Angabe

Dear Students,
RWTH Aachen University aims to offer high standard of teaching. To this end, we depend on your cooperation and your assessment of the course attended. The survey and evaluation are carried out in accordance with the legal regulations for data protection; participation is anonymous and voluntary.
Instructors are obliged to discuss the results of the student course evaluation with the students in the course. If this is not the case, please contact: lehre@rwth-aachen.de.
Your concern will be handled anonymously.

Explanation:
N/A = not applicable

1. Allgemein *General Information*

1.1 Geschlecht *Gender* ☐ weiblich *female* ☐ männlich *male* ☐ k.A. *N/A*

1.2 Nationalität *Nationality* ☐ deutsch (D) *German (D)* ☐ EU (ohne D) *EU (excl. D)* ☐ Non-EU

1.3 Derzeitiger Studiengang *Course Degree* ☐ Bachelor ☐ Master ☐ sonstiger *other*

1.4 Fachsemester *Core Semester* ☐ 1-2 ☐ 7-8 ☐ 3-4 ☐ >8 ☐ 5-6

1.5 Wie viel Zeit verwenden Sie derzeit pro Woche für die Vor- und Nachbereitung dieser Veranstaltung?
How much time do you currently spend on this course including preparation and follow up work?
☐ weniger als 1 Std. *less than 1 hr.* ☐ 1 bis 3 Std. *1 to 3 hrs.* ☐ 3 bis 5 Std. *3 to 5 hrs.*
☐ 5 bis 7 Std. *5 to 7 hrs.* ☐ 7 bis 9 Std. *7 to 9 hrs.* ☐ mehr als 9 Std. *more than 9 hrs.*

1.6 Die Veranstaltung interessiert mich. / *I find the course interesting.*
trifft zu *strongly agree* ☐ ☐ ☐ ☐ trifft nicht zu *strongly disagree* ☐ k.A. *N/A* ☐

2. Konzept der Vorlesung *Lecture Concept*

	trifft zu *strongly agree*				trifft nicht zu *strongly disagree*	k.A. *N/A*
2.1 Die Lernziele der Vorlesung sind definiert. *The learning goals of the lecture are defined.*	☐	☐	☐	☐	☐	☐
2.2 Die Vorlesung hat eine klar erkennbare Struktur. *The lecture is well structured.*	☐	☐	☐	☐	☐	☐
2.3 Die zur Verfügung gestellten Materialien sind hilfreich. *The materials provided are helpful.*	☐	☐	☐	☐	☐	☐
2.4 Die ausgewählten Beispiele sind hilfreich. *The examples chosen are helpful.*	☐	☐	☐	☐	☐	☐
2.5 Es werden Zusammenfassungen an sinnvollen Stellen gemacht. *Lecture material is summarized at appropriate intervals.*	☐	☐	☐	☐	☐	☐

2.6 Der Schwierigkeitsgrad ist ... *The degree of difficulty is ...* ☐ angemessen *appropriate* ☐ zu schwer *too difficult* ☐ zu leicht *too easy*

[Fortsetzung] [continued]

2.7 Ich bewerte das Konzept der Vorlesung mit ... *I would evaluate the lecture concept as ...* ☐ 1 - sehr gut *very good* ☐ 2 - gut *good* ☐ 3 - befriedigend *satisfactory* ☐ 4 - ausreichend *sufficient* ☐ 5 - mangelhaft *poor*

3. Vermittlung und Verhalten *Instruction and Behavior*

Die Dozentin/der Dozent ... *The lecturer ...*

	trifft zu *strongly agree*				trifft nicht zu *strongly disagree*	k.A. *N/A*
3.1 ... erklärt den Stoff verständlich. *... explains the subject matter clearly.*	☐	☐	☐	☐	☐	☐
3.2. ... geht auf Verständnisfragen ein. *... is willing to answer questions.*	☐	☐	☐	☐	☐	☐
3.3 ... berücksichtigt unterschiedliche Kenntnisstände der Studierenden. *... considers students' different levels of knowledge.*	☐	☐	☐	☐	☐	☐
3.4 ... schafft es, mich für den Vorlesungsstoff zu begeistern. / *... engages my interest in the topic.*	☐	☐	☐	☐	☐	☐
3.5 ... spricht angemessen laut und deutlich. *... speaks audibly and clearly.*	☐	☐	☐	☐	☐	☐
3.6 ... ist gut vorbereitet. / *... is well prepared.*	☐	☐	☐	☐	☐	☐
3.7 ... ist außerhalb der Vorlesung ansprechbar. *... is available outside of the lecture.*	☐	☐	☐	☐	☐	☐
3.8 ... setzt Medien ein, die zum Verständnis beitragen. *... uses media that contribute to students' understanding.*	☐	☐	☐	☐	☐	☐

3.9 Das Tempo ist ... The pace is … ☐ angemessen *appropriate* ☐ zu hoch *too fast* ☐ zu niedrig *too slow*

3.10 Ich gebe der Dozentin/dem Dozenten die Gesamtnote *I would evaluate the lecturer as ...* ☐ 1 - sehr gut *very good* ☐ 2 - gut *good* ☐ 3 - befriedigend *satisfactory* ☐ 4 - ausreichend *sufficient* ☐ 5 - mangelhaft *poor*

4. Rahmenbedingungen *General Conditions*

	trifft zu *strongly agree*				trifft nicht zu *strongly disagree*	k.A. *N/A*
4.1 Der zeitliche Rahmen der Vorlesung wird eingehalten. *The lecture begins and ends on time.*	☐	☐	☐	☐	☐	☐

4.2 Die Anzahl der Sitzplätze ist ... *The number of seats is ...* ☐ angemessen *appropriate* ☐ zu groß *too much* ☐ zu klein *too few*

4.3 Wie oft hat die Vorlesung an regulären Terminen gar nicht stattgefunden? (Vorlesungsfreie Tage sind nicht gemeint!)
How often was the lecture cancelled on regularly scheduled dates? (Lecture-free days are not included!)
☐ 0 x ☐ 1 x ☐ 2 x ☐ 3 x ☐ 4 x ☐ >4 x

4.4 Wie häufig wurde die Vorlesung nicht von der angegebenen Person gehalten?
How many times did you have a substitute teacher?
☐ 0 x ☐ 1 x ☐ 2 x ☐ 3 x ☐ 4 x ☐ >4 x

4.5 Falls sich die Dozentin/der Dozent vertreten lassen hat, war die Vertretung geeignet?
In the event of a substitute teacher, was the substitute suitable?
☐ ja *yes* ☐ nein *no* ☐ k.A. *N/A*

Blocks and Procedures

- Extension of WHILE by nested blocks with local variables and recursive procedures
- Simple memory model ($\Sigma := \{\sigma \mid \sigma : \mathit{Var} \to \mathbb{Z}\}$) not sufficient any more as variables can occur in several instances

$\Rightarrow$ Involves new semantic concepts:

- variable and procedure environments
- locations (memory addresses) and stores (memory states)

- Important: scope of variable and procedure identifiers

  static scoping: scope of identifier = declaration environment
  (also: “lexical” scoping; here)

  dynamic scoping: scope of identifier = calling environment
  (old Algol/Lisp dialects)

Static and Dynamic Scoping

Example 14.1

```
begin
  var x; var y;
  proc P is y := x end;
  x := 1;
  begin
    var x;
    x := 2;
    call P
  end
end
```

static scoping $\Rightarrow$ y = 1
dynamic scoping $\Rightarrow$ y = 2

Extending the Syntax

Syntactic categories:

Category	Domain	Meta variable
Procedure identifiers	$PVar = \{\mathtt{P}, \mathtt{Q}, \ldots\}$	P
Procedure declarations	$PDec$	p
Variable declarations	$VDec$	v
Commands (statements)	Cmd	c

Context-free grammar:

$$p ::= \mathtt{proc}\ P\ \mathtt{is}\ c\ \mathtt{end};p \mid \varepsilon \in PDec$$
$$v ::= \mathtt{var}\ x;v \mid \varepsilon \in VDec$$
$$c ::= \mathtt{skip} \mid x := a \mid c_1;c_2 \mid \mathtt{if}\ b\ \mathtt{then}\ c_1\ \mathtt{else}\ c_2\ \mathtt{end} \mid \mathtt{while}\ b\ \mathtt{do}\ c\ \mathtt{end} \mid \mathtt{call}\ P \mid \mathtt{begin}\ v\ p\ c\ \mathtt{end} \in Cmd$$

- All used variable/procedure identifiers have to be declared
- Identifiers declared within a block must be distinct

Locations and Stores

- So far: states $\Sigma = \{\sigma \mid \sigma : \mathit{Var} \to \mathbb{Z}\}$
- Now: explicit control over all (nested) instances of a variable:
  - variable environments

    $$\mathit{VEnv} := \{\rho \mid \rho : \mathit{Var} \dashrightarrow \mathit{Loc}\}$$

    (partial function to maintain declaredness information)
  - locations

    $$\mathit{Loc} := \mathbb{N}$$

  - stores

    $$\mathit{Sto} := \{\sigma \mid \sigma : \mathit{Loc} \dashrightarrow \mathbb{Z}\}$$

    (partial function to maintain allocation information)

$\Rightarrow$ Two-level access to a variable $x \in \mathit{Var}$:

1. determine current memory location of x:

   $$l := \rho(x)$$

2. reading/writing access to σ at location l

- Thus: previous state information represented as $\sigma \circ \rho$

Procedure Environments and Declarations

- Effect of procedure call determined by its body and variable and procedure environment of its declaration:

$$PEnv := \{\pi \mid \pi : PVar \dashrightarrow Cmd \times VEnv \times PEnv\}$$

  denotes the set of procedure environments

- Effect of declaration: update of environment (and store)

$$\begin{aligned} \mathrm{upd}_v[\![.]\!] &: VDec \times VEnv \times Sto \to VEnv \times Sto \\ \mathrm{upd}_v[\![\texttt{var } x\,; v]\!](\rho,\sigma) &:= \mathrm{upd}_v[\![v]\!](\rho[x \mapsto l_x], \sigma[l_x \mapsto 0]) \\ \mathrm{upd}_v[\![\varepsilon]\!](\rho,\sigma) &:= (\rho,\sigma) \\ \mathrm{upd}_p[\![.]\!] &: PDec \times VEnv \times PEnv \to PEnv \\ \mathrm{upd}_p[\![\texttt{proc } P \texttt{ is } c \texttt{ end}\,; p]\!](\rho,\pi) &:= \mathrm{upd}_p[\![p]\!](\rho, \pi[P \mapsto (c,\rho,\pi)]) \\ \mathrm{upd}_p[\![\varepsilon]\!](\rho,\pi) &:= \pi \end{aligned}$$

  where $l_x := \min\{l \in Loc \mid \sigma(l) = \bot\}$

Execution Relation I

Definition 14.2 (Execution relation)

For $c \in \mathit{Cmd}$, $\sigma, \sigma' \in \mathit{Sto}$, $\rho \in \mathit{VEnv}$, and $\pi \in \mathit{PEnv}$, the execution relation $(\rho, \pi) \vdash \langle c, \sigma \rangle \to \sigma'$ ("in environment (ρ, π), statement c transforms store σ into σ'") is defined by the following rules:

$$\text{(skip)}\ \frac{}{(\rho, \pi) \vdash \langle \texttt{skip}, \sigma \rangle \to \sigma}$$

$$\text{(asgn)}\ \frac{\langle a, \sigma \circ \rho \rangle \to z}{(\rho, \pi) \vdash \langle x := a, \sigma \rangle \to \sigma[\rho(x) \mapsto z]}$$

$$\text{(seq)}\ \frac{(\rho, \pi) \vdash \langle c_1, \sigma \rangle \to \sigma' \qquad (\rho, \pi) \vdash \langle c_2, \sigma' \rangle \to \sigma''}{(\rho, \pi) \vdash \langle c_1 ; c_2, \sigma \rangle \to \sigma''}$$

$$\text{(if-t)}\ \frac{\langle b, \sigma \circ \rho \rangle \to \text{true} \qquad (\rho, \pi) \vdash \langle c_1, \sigma \rangle \to \sigma'}{(\rho, \pi) \vdash \langle \texttt{if}\ b\ \texttt{then}\ c_1\ \texttt{else}\ c_2\ \texttt{end}, \sigma \rangle \to \sigma'}$$

Execution Relation II

Definition 14.2 (Execution relation; continued)

$$\text{(if-f)}\ \frac{\langle b, \sigma \circ \rho\rangle \to \text{false} \quad (\rho,\pi) \vdash \langle c_2, \sigma\rangle \to \sigma'}{(\rho,\pi) \vdash \langle \texttt{if}\ b\ \texttt{then}\ c_1\ \texttt{else}\ c_2\ \texttt{end}, \sigma\rangle \to \sigma'}$$

$$\text{(wh-f)}\ \frac{\langle b, \sigma \circ \rho\rangle \to \text{false}}{(\rho,\pi) \vdash \langle \texttt{while}\ b\ \texttt{do}\ c\ \texttt{end}, \sigma\rangle \to \sigma}$$

$$\text{(wh-t)}\ \frac{\langle b, \sigma \circ \rho\rangle \to \text{true} \quad (\rho,\pi) \vdash \langle c, \sigma\rangle \to \sigma' \quad (\rho,\pi) \vdash \langle \texttt{while}\ b\ \texttt{do}\ c\ \texttt{end}, \sigma'\rangle \to \sigma''}{(\rho,\pi) \vdash \langle \texttt{while}\ b\ \texttt{do}\ c\ \texttt{end}, \sigma\rangle \to \sigma''}$$

$$\text{(call)}\ \frac{(\rho', \pi'[P \mapsto (c, \rho', \pi')]) \vdash \langle c, \sigma\rangle \to \sigma'}{(\rho,\pi) \vdash \langle \texttt{call}\ P, \sigma\rangle \to \sigma'} \qquad \text{if } \pi(P) = (c, \rho', \pi')$$

$$\text{(block)}\ \frac{\text{upd}_v[\![v]\!](\rho,\sigma) = (\rho',\sigma') \quad \text{upd}_p[\![p]\!](\rho',\pi) = \pi' \quad (\rho',\pi') \vdash \langle c, \sigma'\rangle \to \sigma''}{(\rho,\pi) \vdash \langle \texttt{begin}\ v\ p\ c\ \texttt{end}, \sigma\rangle \to \sigma''}$$

Execution Relation III

Remarks about rules (call) and (block):

- Static scoping is modelled in (call) by using the environments ρ' and π' (as determined in (block)) from the declaration site of procedure P (and not ρ and π from the calling site)
- In (call), the procedure environment associated with procedure P is extended by a P-entry to handle recursive calls of P:

$$\pi'[P \mapsto (c, \rho', \pi')]$$

Execution Relation IV

Example 14.3

```
begin
  var x; var y;                                                  } v
  proc F is
    begin
      var z;
      z:=x;
      if z=1 then skip                                           }
             else x:=x-1; call F; y:=z*y end                     } c2   } c1   } cF   } p   } c
    end
  end;
  x:=2; y:=1; call F                                             } c0
end
```

Let $\sigma_\emptyset(l) = \rho_\emptyset(x) = \pi_\emptyset(P) = \bot$ for all $l \in Loc, x \in Var, P \in PVar$

Notation: $\sigma_{ijkl} \Leftrightarrow \sigma(0) = i, \sigma(1) = j, \sigma(2) = k, \sigma(3) = l$

Derivation tree for $(\rho_\emptyset, \pi_\emptyset) \vdash \langle c, \sigma_\emptyset \rangle \to \sigma_{1221}$: on the board