s c c h

software competence center hagenberg

Improving the Understandability of Formal Specifications

An Experience Report

Felix Kossak, Atif Mashkoor,
Verena Geist, Christa Illibauer

+43 7236 3343 811
felix.kossak@scch.at
www.scch.at

SCCH is an initiative of

JOHANNES KEPLER UNIVERSITY LINZ | JKU

SCCH is located in

softwarepark hagenberg

Contents

- Motivation
- Specific Suggestions
- Conclusion

Motivation

- Rigorous methods improve software quality
- But they are hard to sell
  - Stakeholders of a specification: domain experts, managers, lawyers, developers, ...
  - A specification is part of a contract
  - The first project phase is slower
  - It takes longer until something “can be seen”
- Key Problems:
  - Notation
  - Style

Suggestions

- Notation: Abstract State Machines
- Style:
  - Top-down
  - Identifiers
  - Bracketing
  - Keywords
  - Structure of expressions
  - Set expressions
- Flexibility

Identifiers

scch
software competence center
hagenberg

```
rule ConsumeOneToken(in, i) =
    choose t in toksInSFForInst(in, i) do
        remove t from toksInSF(in)


rule ConsumeOneToken(incomingSequenceFlow,
       instance) =
    choose token in tokensInSequenceFlowForInstance(
           incomingSequenceFlow, instance) do
        remove token from tokensInSequenceFlow(
           incomingSequenceFlow)
```

Bracketing

s c c h
software competence center
hagenberg

```
rule FlowNodeBehaviour(flowNode) =
    if eventCondition(flowNode)
        and controlCondition(flowNode)
        and dataCondition(flowNode)
        and resourceCondition(flowNode) then
      DataOperation(flowNode)
      ControlOperation(flowNode)
      EventOperation(flowNode)
      ResourceOperation(flowNode)
```

Bracketing (2)

scch
software competence center
hagenberg

```
rule FlowNodeBehaviour(flowNode) =
    if eventCondition(flowNode)
          and controlCondition(flowNode)
          and dataCondition(flowNode)
          and resourceCondition(flowNode) then
    parallelblock
      DataOperation(flowNode)
      ControlOperation(flowNode)
      EventOperation(flowNode)
      ResourceOperation(flowNode)
    endparallelblock
```

Bracketing (3)

scch
software competence center
hagenberg

```
rule FlowNodeBehaviour(flowNode) =
    if eventCondition(flowNode)
          and controlCondition(flowNode)
          and dataCondition(flowNode)
          and resourceCondition(flowNode) then
    do in parallel
       DataOperation(flowNode)
       ControlOperation(flowNode)
       EventOperation(flowNode)
       ResourceOperation(flowNode)
```

Keywords and Structure

scch
software competence center
hagenberg

- **forall** token **do** instanceOfToken(token) := instance
  forall token instanceOfToken(token) = instance

→ **foreach** token **do** ...
  foreach token **holds** ...

→ **forsome** token **holds** ...

➢ **do** completionQuantity(flowNode) **times**
  ProduceToken(...)

Set Expressions

{ node **|** node **ϵ** eventGateTargetNodes(...) **and** ... **}**

The set containing each node **for which holds**
node **is in** eventGateTargetNodes(...) **and** ...

?

Set Expressions (2)

scch
software competence center
hagenberg

```
{ instanceOfToken(token) |
    forsome sequenceFlow ϵ incomingSequenceFlows(
        flowNode) holds
      token ϵ sequenceFlow }


{ instance |
  forsome token holds
     forsome sequenceFlow ϵ incomingSequenceFlows(
         flowNode) holds
       token ϵ sequenceFlow and
       instanceOfToken(token) = instance
}
```

Conclusion

- Rigorous methods can and should be used in all kinds of software projects
- Rigorous methods can and should be made more generally understandable
- Rigorous methods can be introduced “gently”

Regio 13
Impulse für OÖ
Regionale Wettbewerbsfähigkeit OÖ 2007–2013

LAND
OBERÖSTERREICH