PROGRAM YOUR OWN RV SYSTEM

an exercise in DSL design

Klaus Havelund
Jet Propulsion Laboratory, USA

Summer School on Cyber-Physical Systems

July 7-10, 2014

Jet Propulsion Laboratory
California Institute of Technology

NASA/JPL Laboratory
for Reliable Software

Definition of "Runtime Verification"

Definition (Runtime Verification)

Runtime Verification is the discipline of computer science dedicated to the analysis of system executions, including checking them against formalized specifications.

Definition of “Runtime Verification”

Definition (Runtime Verification)

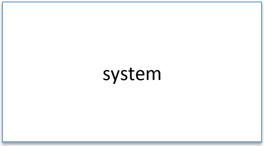
Runtime Verification is the discipline of computer science dedicated to the analysis of system executions, including checking them against formalized specifications.

Other variations:

- analysis with algorithms (no specs): data race and deadlock analysis
- specification learning
- trace visualization
- fault protection: changing behavior

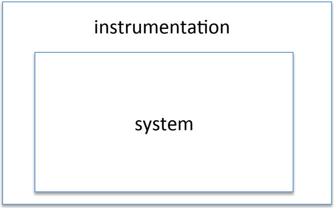
Runtime verification

- Start with a system to monitor.



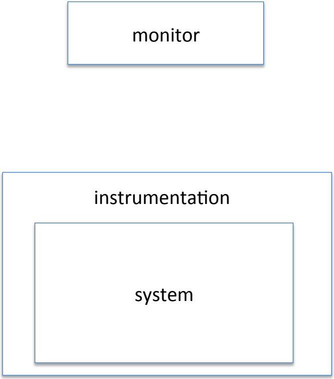
Runtime verification

- *Instrument* the system to record relevant events.



Runtime verification

- *Provide* a monitor.



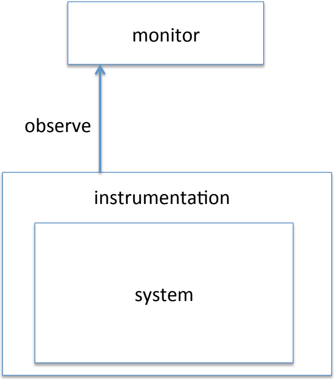
monitor

instrumentation

system

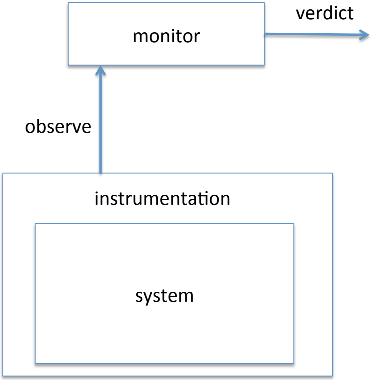
Runtime verification

- *Dispatch* each received event to the monitor.



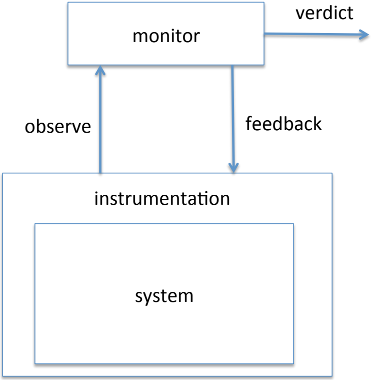
Runtime verification

- Compute a *verdict* for the trace received so far.



Runtime verification

- Possibly generate *feedback* to the system.



monitor

verdict

observe

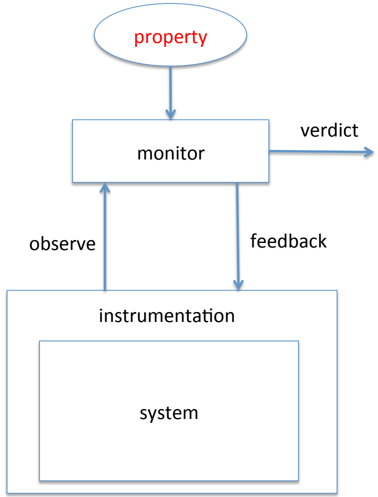
feedback

instrumentation

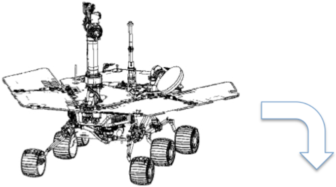
system

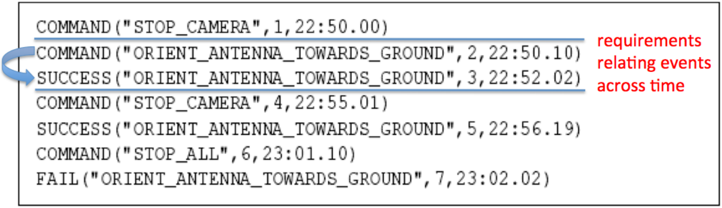
Runtime verification

- We might possibly have synthesized monitor from a *property*.



Trace evaluation





```
COMMAND("STOP_CAMERA",1,22:50.00)
COMMAND("ORIENT_ANTENNA_TOWARDS_GROUND",2,22:50.10)
SUCCESS("ORIENT_ANTENNA_TOWARDS_GROUND",3,22:52.02)
COMMAND("STOP_CAMERA",4,22:55.01)
SUCCESS("ORIENT_ANTENNA_TOWARDS_GROUND",5,22:56.19)
COMMAND("STOP_ALL",6,23:01.10)
FAIL("ORIENT_ANTENNA_TOWARDS_GROUND",7,23:02.02)
```

requirements relating events across time

Trace evaluation

- The type of events E
- A trace is a finite sequence of events: $Trace = E^*$
- A *property* ϕ denotes a *language* $\mathcal{L}(\phi) \subseteq Trace$:
- On the fly evaluation, say current trace is τ:

$\tau \in \mathcal{L}(\varphi)$	:	true	$\wedge$	no extension	can make it false
	:	true_{sofar}	$\wedge$	some extension	can make it false
$\tau \notin \mathcal{L}(\varphi)$	:	false	$\wedge$	no extension	can make it true
	:	false_{sofar}	$\wedge$	some extension	can make it true

How is the monitor specified?

- Program (built-in algorithm focused on specific problem)
    - data race detection
    - deadlock detection
- Programming language
- Design by contract (pre/post conditions), JML for example
- Temporal formalism (expressing ordering of events)
    - state machines
    - regular expressions
    - grammars (context free languages)
    - linear temporal logic (past time, future time)
    - rule-based logics

Some instrumentation techniques

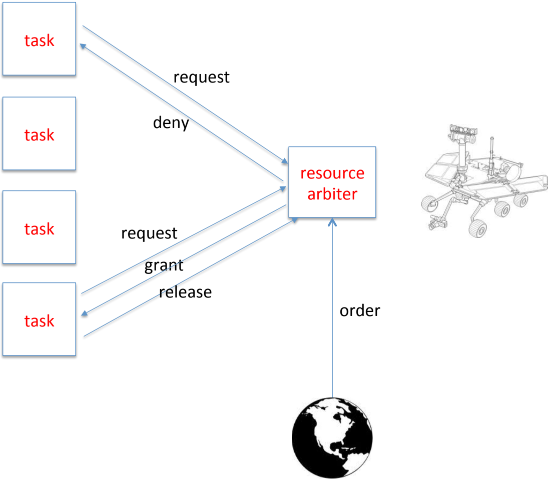
- Instrumentation of *byte/object code*
  - Valgrind (C) `http://valgrind.org`
  - BCEL (Java) `http://jakarta.apache.org/bcel`
- Instrumentation of *source code*
  - CIL (C) `http://sourceforge.net/projects/cil`
- Aspect-oriented programming (AOP):
  - AspectC (C) `https://sites.google.com/a/gapp.msrg.utoronto.ca/aspectc`
  - AspectC++ (C++) `http://www.aspectc.org`
  - AspectJ (Java) `http://www.eclipse.org/aspectj`

Data Automata

(Daut)

MSL

System architecture



task

task

task

task

request

deny

resource arbiter

request

grant

release

order

Resource allocation requirements

Requirement R_1

A grant of a resource to a task must be followed by a release of that resource by the same task, without another grant of that resource in between (to the same task or any other task).

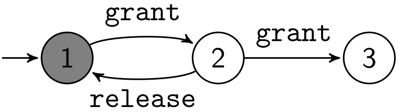
Requirement R_2

A resource cannot be released by a task, which has not been granted the resource.

A state machine

Requirement R_1

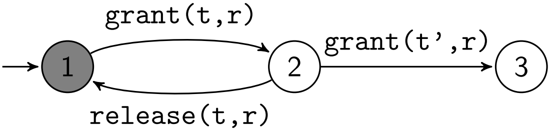
A grant of a resource to a task must be followed by a release of that resource by the same task, without another grant of that resource in between (to the same task or any other task).



A state machine with parameters

Requirement R_1

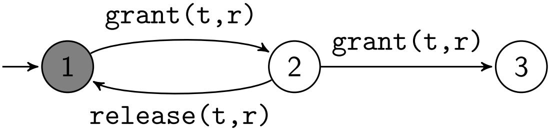
A grant of a resource to a task must be followed by a release of that resource by the same task, without another grant of that resource in between (to the same task or any other task).



A restriction in MOP

Requirement R_1

A grant of a resource to a task must be followed by a release of that resource by the same task, without another grant of that resource in between (**to the same task** or any other task).

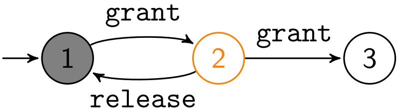


Consider trace

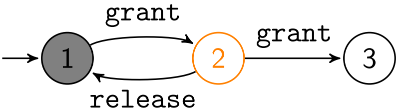
$$\langle grant(t_1, antenna), grant(t_2, motor_2), grant(t_3, motor_4)\rangle$$

MOP: monitor state is a map from parameters to states

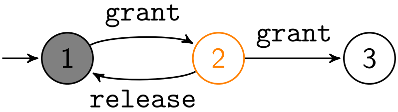
$(t_1, antenna) \mapsto$



$(t_2, motor_2) \mapsto$



$(t_3, motor_4) \mapsto$



DAUT: monitor state is a set of records

$$\{S2(t_1, antenna), S2(t_2, motor_2), S2(t_3, motor_4)\}$$

Design of a DSL

References

http://www.havelund.com

Monitoring with Data Automata Klaus Havelund. ISoLA 2014 – 6th International Symposium On Leveraging Applications of Formal Methods, Verification and Validation. Track: Statistical Model Checking, Past Present and Future. Organized by: K. Larsen and A. Legay. Editors: T. Margaria and B. Steffen. Springer, LNCS. Corfu, Greece, October 8-11, 2014.

Data Automata in Scala Klaus Havelund. TASE 2014 - The 8th International Symposium on Theoretical Aspects of Software Engineering, IEEE proceedings. Changsha, China, September 1-3, 2014.

Rule-based runtime verification revisited Klaus Havelund. Software Tools for Technology Transfer (STTT). Springer. April, 2014.

TraceContract: A Scala DSL for Trace Analysis Howard Barringer and Klaus Havelund. FM 2011 - 17th International Symposium on Formal Methods. Springer, LNCS 6664. Limerick, Ireland, June 20-24, 2011.

Data Automata

- as an **external** DSL
  1. small language with focused functionality
  2. specialized parser programmed using parser generator

Data Automata

- as an **external** DSL
  1. small language with focused functionality
  2. specialized parser programmed using parser generator
  3. advantages:
     1. complete control over language syntax
     2. analyzable

Data Automata

- as an **external** DSL
  1. small language with focused functionality
  2. specialized parser programmed using parser generator
  3. advantages:
     1. complete control over language syntax
     2. analyzable
- as an **internal** DSL
  1. API in SCALA
  2. using SCALA's infra-structure (compiler, IDEs, ...)

Data Automata

- as an **external** DSL
  1. small language with focused functionality
  2. specialized parser programmed using parser generator
  3. advantages:
     1. complete control over language syntax
     2. analyzable
- as an **internal** DSL
  1. API in SCALA
  2. using SCALA's infra-structure (compiler, IDEs, ...)
  3. advantages:
     1. expressive, the programming language is never far away
     2. easier to develop/adapt (although, sometimes not)
     3. allows use of existing tools such as type checkers, IDEs, etc.

An external DSL

Recall the two resource allocation requirements

Requirement R_1

A grant of a resource to a task must be followed by a release of that resource by the same task, without another grant of that resource in between (to the same task or any other task).

Requirement R_2

A resource cannot be released by a task, which has not been granted the resource.

R_1 and R_2 as a state machine in DAUT

```
monitor R1R2 {
  init always Start {
    grant(t, r) → Granted(t,r)
    release(t, r) :: ¬Granted(t,r) → error
  }

  hot Granted(t,r) {
    release(t,r) → ok
    grant(_,r) → error
  }
}
```

top level abbreviation

```
monitor R1R2 {
  grant(t, r) → Granted(t,r)
  release (t, r) :: ¬Granted(t,r) → error

  hot Granted(t,r) {
    release (t,r) → ok
    grant(_,r) → error
  }
}
```

Requirement R_1

```
monitor R1 {
  grant(t,r) → hot {
    release (t,r) → ok
    grant(_,r) → error
  }
}
```

syntax

$\langle \mathit{Specification} \rangle ::= \langle \mathit{Monitor} \rangle *$

$\langle \mathit{Monitor} \rangle ::= \textbf{monitor}\ \langle \mathit{Id} \rangle\ `\{\text{'}\ \langle \mathit{Transition} \rangle *\ \langle \mathit{State} \rangle *\ `\}\text{'}$

$\langle \mathit{State} \rangle ::= \langle \mathit{Modifier} \rangle *\ \langle \mathit{Id} \rangle\ \lceil\ (\langle \mathit{Id} \rangle **)\ \rceil\ \lceil\ `\{\text{'}\ \langle \mathit{Transition} \rangle *\ `\}\text{'}\ \rceil$

$\langle \mathit{Modifier} \rangle ::= \textbf{init} \mid \textbf{hot} \mid \textbf{always}$

$\langle \mathit{Transition} \rangle ::= \langle \mathit{Pattern} \rangle\ `{:}{:}\text{'}\ \langle \mathit{Condition} \rangle\ `{\rightarrow}\text{'}\ \langle \mathit{Action} \rangle **$

$\langle \mathit{Pattern} \rangle ::= \langle \mathit{Id} \rangle\ `(\text{'}\langle \mathit{Id} \rangle **`)\text{'}$

$\langle \mathit{Condition} \rangle ::= \langle \mathit{Condition} \rangle\ `{\wedge}\text{'}\ \langle \mathit{Condition} \rangle$
$\quad \mid\ \langle \mathit{Condition} \rangle\ `{\vee}\text{'}\ \langle \mathit{Condition} \rangle$
$\quad \mid\ `{\neg}\text{'}\ \langle \mathit{Condition} \rangle$
$\quad \mid\ `(\text{'}\langle \mathit{Condition} \rangle`)\text{'}$
$\quad \mid\ \langle \mathit{Expression} \rangle\ \langle \mathit{relop} \rangle\ \langle \mathit{Expression} \rangle$
$\quad \mid\ \langle \mathit{Id} \rangle\ \lceil\ `(\text{'}\langle \mathit{Expression} \rangle **`)\text{'}\ \rceil$

$\langle \mathit{Action} \rangle ::= \textbf{ok}$
$\quad \mid\ \textbf{error}$
$\quad \mid\ \langle \mathit{Id} \rangle\ \lceil\ `(\text{'}\langle \mathit{Expression} \rangle **`)\text{'}\ \rceil$
$\quad \mid\ \textbf{if}\ `(\text{'}\ \langle \mathit{Condition} \rangle\ `)\text{'}\ \textbf{then}\ \langle \mathit{Action} \rangle\ \textbf{else}\ \langle \mathit{Action} \rangle$
$\quad \mid\ \langle \mathit{Modifier} \rangle *\ `\{\text{'}\ \langle \mathit{Transition} \rangle *\ `\}\text{'}$

Semantics

Basic concepts

- An environment: $env \in Env = Id \xrightarrow{m} V$

Basic concepts

- An environment: $env \in Env = Id \xrightarrow{m} V$
- An event: $e \in Event = Id \times V^*$

Basic concepts

- An environment: $env \in Env = Id \xrightarrow{m} V$
- An event: $e \in Event = Id \times V^*$
- We shall write an event $(id, \langle v_1, \ldots, v_n \rangle)$ as: $id(v_1, \ldots, v_n)$

Basic concepts

- An environment: $env \in Env = Id \xrightarrow{m} V$
- An event: $e \in Event = Id \times V^*$
- We shall write an event $(id, \langle v_1, \dots, v_n \rangle)$ as: $id(v_1, \dots, v_n)$
- A trace: $\sigma \in Trace = Event^*$

Basic concepts

- An environment: $env \in Env = Id \xrightarrow{m} V$
- An event: $e \in Event = Id \times V^*$
- We shall write an event $(id, \langle v_1, \ldots, v_n \rangle)$ as: $id(v_1, \ldots, v_n)$
- A trace: $\sigma \in Trace = Event^*$
- A particular state $s \in State = id(v_1, \ldots, v_n)$ represents an instantiation of the formal parameters

Basic concepts

- An environment: $env \in Env = Id \xrightarrow{m} V$
- An event: $e \in Event = Id \times V^*$
- We shall write an event $(id, \langle v_1, \ldots, v_n \rangle)$ as: $id(v_1, \ldots, v_n)$
- A trace: $\sigma \in Trace = Event^*$
- A particular state $s \in State = id(v_1, \ldots, v_n)$ represents an instantiation of the formal parameters
- Environment of a state: $s.env = [id_1 \mapsto v_1, \ldots, id_n \mapsto v_n]$

Labeled Transition System

- $LTS = (Config, Event, \rightarrow, i, F)$.
    - $Config \subseteq State$
    - $Event$ is a set of parameterized events
    - $\rightarrow \subseteq Config \times (Event \times \mathbb{B}) \times Config$
    - $i \subseteq Config$ is the set of initial states
    - $F \subseteq Config$ is the set of final states
- Result of transitions will hence be pairs of the form $(flag, con) \in \mathbb{B} \times Config$
- $\perp$ indicates that an evaluation has failed

Semantics part 1/3

$$\boxed{\mathsf{E}}\ \frac{con, con \overset{e}{\hookrightarrow} b, con'}{con \xrightarrow{e,b} con'}$$

$$\boxed{\mathsf{E\text{-}ss_1}}\ \frac{}{con, \{\} \overset{e}{\hookrightarrow} (true, \{\})}$$

$$\boxed{\mathsf{E\text{-}ss_2}}\ \frac{\begin{array}{c} con, s \overset{e}{\longmapsto} res \\ con, ss \overset{e}{\hookrightarrow} res' \end{array}}{con, s \cup ss \overset{e}{\hookrightarrow} res \oplus res'}$$

Semantics part 2/3

$$\boxed{\text{E-s}_1}\ \frac{con, s.env, s.ts \overset{e}{\Longrightarrow} \bot}{con, s \overset{e}{\longmapsto} true, \{s\}}$$

$$\boxed{\text{E-s}_2}\ \frac{con, s.env, s.ts \overset{e}{\Longrightarrow} res}{con, s \overset{e}{\longmapsto} res}$$

$$\boxed{\text{E-ts}_1}\ \frac{}{con, env, Nil \overset{e}{\Longrightarrow} \bot}$$

$$\boxed{\text{E-ts}_2}\ \frac{\begin{array}{c} con, env, t \overset{e}{\rightharpoondown} res_\bot \\ con, env, ts \overset{e}{\Longrightarrow} res'_\bot \end{array}}{con, env, \langle t\rangle^\frown ts \overset{e}{\Longrightarrow} res_\bot \oplus_\bot res'_\bot}$$

Semantics part 3/3

$$\boxed{\text{E-t}_1}\ \frac{\begin{array}{c} t\ \textbf{is}\ `pat :: cond \to rhs' \\ [\![pat]\!]^P env\ \ e = \bot \end{array}}{con, env, t \overset{e}{\rightharpoondown} \bot}$$

$$\boxed{\text{E-t}_2}\ \frac{\begin{array}{c} t\ \textbf{is}\ `pat :: cond \to rhs' \\ [\![pat]\!]^P env\ \ e = env' \\ [\![cond]\!]^C con\ env' = false \end{array}}{con, env, t \overset{e}{\rightharpoondown} \bot}$$

$$\boxed{\text{E-t}_3}\ \frac{\begin{array}{c} t\ \textbf{is}\ `pat :: cond \to rhs' \\ [\![pat]\!]^P env\ \ e = env' \\ [\![cond]\!]^C con\ env' = true \\ [\![rhs]\!]^R con\ env' = res \end{array}}{con, env, t \overset{e}{\rightharpoondown} res}$$

Semantic functions

```
$[\![\_]\!]^P : Pattern \rightarrow Env \rightarrow Event \rightarrow Env_\perp$
$[\![pat]\!]^P env\ id(v_1, \ldots, v_n) =$
    case $pat$ of
        "_" $\Rightarrow env$
        $id(id_1, \ldots, id_n) \Rightarrow$
            let $env' = \{id_1 \mapsto v1, \ldots, id_n \mapsto v_n\}$ in
                if $(\forall id \in (dom(env) \cap dom(env')) \bullet env(id) = env'(id)))$
                    then $env \oplus env'$
                    else $\perp$
        $id'(\ldots)$ where $id \neq id' \Rightarrow \perp$  // event names do not match

$[\![\_]\!]^C : Cond \rightarrow Config \rightarrow Env \rightarrow \mathbb{B}$
$[\![cond]\!]^C con\ env =$
    case $cond$ of
        $id(exp_1, \ldots, exp_n) \Rightarrow id([\![exp_1]\!]env, \ldots, [\![exp_n]\!]env)) \in con$

$[\![\_]\!]^E : Exp \rightarrow Env \rightarrow \mathbb{B}$
```

Semantic functions

$$
\begin{array}{l}
[\![\_]\!]^R : Action^{**} \rightarrow Config \rightarrow Env \rightarrow Result \\
[\![act_1, \ldots, act_n]\!]^R con\ env = \\
\qquad \textbf{let} \\
\qquad\qquad results = \{[\![act_i]\!] con\ env \mid i \in 1..n\} \\
\qquad\qquad status = \bigwedge\{b \mid (b, con') \in results\} \\
\qquad\qquad con'' = \bigcup\{con' \mid (b, con') \in results\} \\
\qquad \textbf{in} \\
\qquad\qquad (status, con'')
\end{array}
$$

$$
\begin{array}{l}
[\![\_]\!]^A : Action \rightarrow Config \rightarrow Env \rightarrow Result \\
[\![act]\!]^A con\ env = \\
\qquad \textbf{case}\ act\ \textbf{of} \\
\qquad\qquad \textbf{ok} \Rightarrow (true, \{\}) \\
\qquad\qquad \textbf{error} \Rightarrow (false, \{\}) \\
\qquad\qquad id(exp_1, \ldots, exp_n) \Rightarrow (true, \{id([\![exp_1]\!]env, \ldots, [\![exp_n]\!]env)\}) \\
\qquad\qquad \textbf{if}\ (cond)\ \textbf{then}\ act_1\ \textbf{else}\ act_2 \Rightarrow \\
\qquad\qquad\qquad \textbf{if}\ ([\![cond]\!] con\ env) \textbf{then}\ [\![act_1]\!] con\ env\ \textbf{else}\ [\![act_2]\!] con\ env
\end{array}
$$

Semantic functions

$$
\begin{aligned}
&\mathit{res}_\perp \oplus_\perp \mathit{res}'_\perp = \\
&\qquad \textbf{case } (\mathit{res}_\perp, \mathit{res}'_\perp) \textbf{ of} \\
&\qquad\qquad (\perp, r) \Rightarrow r \\
&\qquad\qquad (r, \perp) \Rightarrow r \\
&\qquad\qquad (r_1, r_2) \Rightarrow r_1 \oplus r_2
\end{aligned}
$$

$$
\begin{aligned}
&(b_1, \mathit{con}_1) \oplus (b_2, \mathit{con}_2) = \\
&\qquad (b_1 \wedge b_2, \mathit{con}_1 \cup \mathit{con}_2)
\end{aligned}
$$

Summarized outcome

- *false* : if **error** reached, otherwise:
- *true* : if config contains no states
- *false sofar* : if config contains at least one non-final state
- *true sofar* : if config contains only final states, one or more

Implementation of external DSL

Scala is a high-level unifying language

- Object-oriented + functional programming features
- Strongly typed with type inference
- Script-like, semicolon inference
- Sets, list, maps, iterators, comprehensions
- Lots of libraries
- Compiles to JVM
- Lively growing community

Abstract syntax

```
case class Specification (automata: List[Automaton])
case class Automaton(name: Id, states: List[StateDef])

case class StateDef(
  modifiers: List[Modifier],
  name: Id,
  formals: List[Id],
  transitions: List[Transition])

case class Transition(
  pattern: Pattern,
  condition: Option[Condition],
  rhs: List[StateExp])

trait Pattern
case class FormalEvent(name: Id, formals: List[Id]) extends Pattern
case object Any extends Pattern
```

Abstract syntax

```
trait Condition
case class Relation(exp1: Exp, op: RelOp, exp2: Exp) extends Condition
case class StatePredicate(name: Id, exprs: List[Exp]) extends Condition
case class BinCond(cond1: Condition, op: BinCondOp, cond2: Condition)
  extends Condition
case class Negation(cond: Condition) extends Condition
case class ParenCond(cond: Condition) extends Condition

trait StateExp
case object ok extends StateExp
case object error extends StateExp
case class NewStateExp(name: Id, values: List[Exp]) extends StateExp
case class IfStateExp(
  cond: Condition, stateExp1: StateExp, stateExp2: StateExp) extends StateExp
case class InlinedStateExp(
  modifiers: List[Modifier], transitions : List[Transition]) extends StateExp
```

Parser

```
object Grammar extends JavaTokenParsers {
  def  specification  :  Parser[ Specification ]  =
    rep(automaton) ^^ {
      case automata ⇒transform( Specification (automata))
    }

  def automaton: Parser[Automaton] =
    "monitor" →ident ~ ("{" → rep( transition ) ~ rep( statedef ) ← "}") ^^
      {
        case name ~ ( transitions  ~  statedefs ) ⇒
          if  ( transitions .isEmpty)
            Automaton(name, statedefs)
          else  { // derived  form
            val   initialState   =
              StateDef( List ( init ,  always ),  "StartFromHere", Nil,  transitions )
            Automaton(name,  initialState  ::   statedefs )
          }
      }
```

Parser

```
  def statedef : Parser[StateDef] =
    rep(modifier) ~ ident ~ opt("(" → repsep(ident, ",") ← ")") ~
    opt("{" → rep( transition ) ← "}") ^^
      {
        case modifiers ~ name ~ formals ~ transitions ⇒
          StateDef(modifiers, name, toList(formals), toList( transitions ))
      }

  def transition : Parser[ Transition ] =
    pattern ~ opt("::" → condition) ~ ("->" →rep1sep(stateexp, ",")) ^^
      {
        case pat ~ cond ~ rhs ⇒
          Transition(pat, cond, rhs)
      }
  }
   ...
}
```

Interpreter interface

```
trait Monitor[Event] {
  def verify (event: Event)
  def end()
}
```

Preliminaries

```
object Preliminaries {
  type Id = String
  type Value = Any

  type Env = Map[Id, Value]

  def mkEnv(ids: List[Id], values: List[Value]): Env =
    (ids zip values).toMap
}
```

Interpreter

```
class Observer(fileName: String) {
  var monitors: List[Monitor[Event]] = Nil

  parse(fileName) match {
    case None ⇒ assert(false, "syntax error")
    case Some(spec @ Specification(automata)) ⇒
      for (automaton ∈ automata) {
        monitors ++= List(new MonitorImpl(automaton))
      }
  }

  def verify(event: Event) {
    monitors foreach (_.verify(event))
  }

  def end() {
    monitors foreach (_.end())
  }
}
```

Interpreter

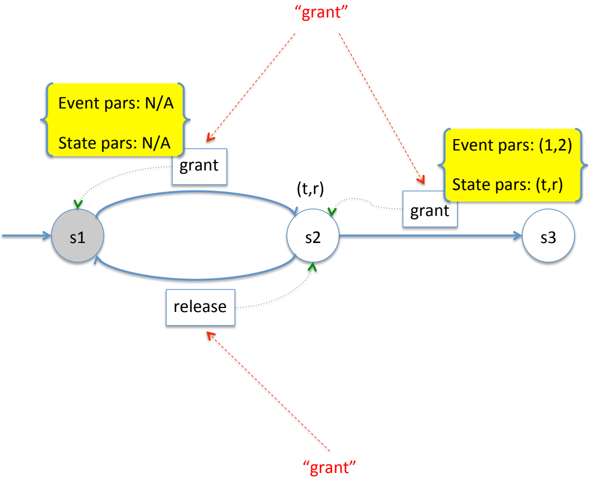
```
class MonitorImpl(automaton: Automaton) extends Monitor[Event] {
  case class State(name: Id, values: List[Value]) {
    var env: Env = null
  }

  type Config = Set[State]
  type Result = (Boolean, Config)

  var currentConfig: Config = initialConfig(automaton)

  def verify(event: Event) {
    val (status, con) = eval(currentConfig)(event)
    if (!status) println("*** error")
    currentConfig = con
  }
  ...
}
```

Interpreter

```
def evalTransition(con: Config, env: Env, transition: Transition)
                  (event: Event): Option[Result] =
{
  val Transition(pat, cond, rhs) = transition
  val optEnv = evalPat(pat)(env, event)
  optEnv match {
    case None ⇒None
    case Some(env_) ⇒
      if (evalCond(cond)(con, env_))
        Some(evalRight(rhs)(con, env_))
      else
        None
  }
}
```

Optimization with indexing

State nodes and event nodes



Indexed monitor

```
class MonitorImpl(automaton: Automaton) {
  val config = new Config(automaton)
   ...
  def verify(event: Event) {
    var statesToRem: Set[State] = {}
    var statesToAdd: Set[State] = {}
    for (state ∈ config.getStates(event)) {
      val (rem, add) = execute(state, event)
      statesToRem ++= rem
      statesToAdd ++= add
    }
    statesToRem foreach config.removeState
    statesToAdd foreach config.addState
  }
}
```

Indexed monitor

```
class Config(automaton: Automaton) {
  var stateNodes: Map[String, StateNode] = Map()
  var eventNodes: Map[String, List[EventNode]] = Map()
   ...
  def getStates(event: Event): Set[State] = {
    val (eventName, values) = event
    var result : Set[State] = Set()
    eventNodes.get(eventName) match {
      case None ⇒
      case Some(eventNodeList) ⇒
        for (eventNode ∈ eventNodeList) {
          result ++= eventNode.getRelevantStates(event)
        }
    }
     result
  }
}
```

Indexed monitor

```
case class EventNode(stateNode: StateNode,
  eventIds: List[Int], stateIds: List[String]) {
  ...
  def getRelevantStates(event: Event): Set[State] = {
    val (_, values) = event
    stateNode.get(
      stateIds,
      for (eventId ∈ eventIds) yield values(eventId)
    )
  }
}
```

Indexed monitor

```
case class StateNode(stateName: String, paramIdList: List[String]) {
  var index: Map[List[String], Map[List[Value], Set[State]]] = Map()
   ...
  def get(paramIdList: List[String], valueList : List[Value]): Set[State] =
  {
    index(paramIdList).get( valueList ) match {
      case None ⇒ emptySet
      case Some(stateSet) ⇒  stateSet
    }
  }
}
```

Another example

```
monitor R3 {
  grant(t, r) → Granted(t,r)

  hot Granted(t,r) {
    release (t,r) → ok
    cancel(r) → ok
  }
}
```

Indexing for this example

Suppose we observe the events:

$$\langle \mathit{grant}(t_1, a), \mathit{grant}(t_2, a) \rangle$$

Index after this trace:

$$\begin{array}{lcl} \langle t, r \rangle & \mapsto & [\ \langle t_1, a \rangle \mapsto \{\mathit{Granted}(t_1, a)\},\ \langle t_2, a \rangle \mapsto \{\mathit{Granted}(t_2, a)\}\ ] \\ \langle r \rangle & \mapsto & [\ \langle a \rangle \mapsto \{\mathit{Granted}(t_1, a), \mathit{Granted}(t_2, a)\}\ ] \end{array}$$

An internal DSL

Event type modeled in internal DSL

```
trait Event
case class grant(task: String, resource: String) extends Event
case class release(task: String, resource: String) extends Event
```

Properties modeled in internal DSL

```
class R1R2 extends Monitor[Event] {
  Always {
    case grant(t, r) ⇒ Granted(t, r)
    case release(t, r) if !Granted(t, r) ⇒ error
  }

  case class Granted(t: String, r: String) extends state{
    Watch {
      case release(‘t‘, ‘r‘) ⇒ ok
      case grant(_, ‘r‘) ⇒ error
    }
  }
}
```

Properties modeled in internal DSL

```
class R1 extends Monitor[Event] {
  Always {
    case grant(t, r) ⇒ hot {
      case release(‘t‘, ‘r‘) ⇒ ok
      case grant(_, ‘r‘) ⇒ error
    }
  }
}
```

Properties modeled in internal DSL

```
object Main {
  def main(args: Array[String]) {
    val obs = new R1R2

    obs.verify(grant("t1", "A"))
    obs.verify(grant("t2", "A"))
    obs.verify(release("t2", "A"))
    obs.verify(release("t1", "B"))
    obs.end()
  }
}
```

amazon.com

S. Hallé and R. Villemaire,
"Runtime enforcement of web service message contracts with data",
IEEE Transactions on Services Computing, vol. 5, no. 2, 2012. –
formalized in $\mathrm{LTL\text{-}FO}^{+}$.

XML based client server communication

XML

client

server

Example of XML message

```
<CartAdd>
  <CartId>1</CartId>
  <Items>
    <Item>
      <ASIN>10</ASIN>
    </Item>
    <Item>
      <ASIN>20</ASIN>
    </Item>
  </Items>
</CartAdd>
```

Amazon E-Commerce Service

ItemSearch(txt)	→	search items on site
CartCreate(its)	→	create cart with items
CartCreateResponse(c)	←	get cart id back
CartGetResponse(c, its)	←	result of get query
CartAdd(c, its)	→	add items
CartRemove(c, its)	→	remove items
CartClear(c)	→	clear cart
CartDelete(c)	→	delete cart

Definition of events

```
case class Item(asin : String )

 trait Event
case class ItemSearch(text : String ) extends Event
case class CartCreate(items: List [Item]) extends Event
case class CartCreateResponse(id: Int ) extends Event
case class CartGetResponse(id: Int , items: List [Item]) extends Event
case class CartAdd(id: Int , items: List [Item]) extends Event
case class CartRemove(id:Int, items: List [Item]) extends Event
case class CartClear( id : Int ) extends Event
case class CartDelete( id : Int ) extends Event
```

From XML to objects

```
def xmlToObject(xml:scala.xml.Node):Event =
  xml match {
    case x @ <CartAdd>{ _* }</CartAdd> ⇒
      CartAdd(getId(x), getItems(x))
     ...
  }

def xmlStringToObject(msg:String):Event = {
  val xml = scala.xml.XML.loadString(msg)
  xmlToObject(xml)
}

def getId(xml:scala.xml.Node):Int =
  (xml \ "CartId").text.toInt

def getItems(xml:scala.xml.Node):List[Item] =
  (xml \ "Items" \ "Item" \ "ASIN").
     toList.map(i ⇒ Item(i.text))
```

Properties

- **Property 1** - *Until a cart is created, the only operation allowed is ItemSearch.*
- **Property 2** - *A client cannot remove something from a cart that has just been emptied.*
- **Property 3** - *A client cannot add the same item twice to the shopping cart.*
- **Property 4** - *A shopping cart created with an item should contain that item until it is deleted.*
- **Property 5** - *A client cannot add items to a non-existing cart.*

Properties formalized

```
class  Property1 extends Monitor[Event] {
  Unless  {
    case ItemSearch(_) ⇒ ok
    case _  ⇒ error
  } {
    case CartCreate(_) ⇒ ok
  }
}

class  Property2 extends Monitor[Event] {
  Always {
    case CartClear(c)  ⇒  unless  {
      case CartRemove(‘c‘,  _) ⇒  error
    } {
      case CartAdd(‘c‘,  _) ⇒ ok
    }
  }
}
```

```
class Property3 extends Monitor[Event] {
  Always {
    case CartCreate(items) ⇒ next {
      case CartCreateResponse(c) ⇒ always {
        case CartAdd(‘c‘, items_) ⇒ items disjointWith items_
      }
    }
  }
}

class Property4 extends Monitor[Event] {
  Always {
    case CartAdd(c, items) ⇒
      for (i ∈ items) yield unless {
        case CartGetResponse(‘c‘, items_) ⇒ items_ contains i
      } {
        case CartRemove(‘c‘, items_) if items_ contains i ⇒ ok
      }
  }
}
```

```
class Property5 extends Monitor[Event] {
  Always {
    case CartCreateResponse(c) ⇒ CartCreated(c)
    case CartAdd(c, _) if !CartCreated(c) ⇒ error
  }

  case class CartCreated(c: Int) extends state {
    Watch {
      case CartDelete(‘c‘) ⇒ ok
    }
  }
}
```

Recall property 3

- **Property 3** - *A client cannot add the same item twice to the shopping cart.*

Property 3 made less strict

```
class  Property3Liberalized  extends Monitor[Event] {
  Always {
    case CartCreate(items) ⇒ next {
      case CartCreateResponse(c) ⇒ CartCreated(c, items)
    }
  }

  case class CartCreated(id: Int, items: List[Item]) extends state {
    Watch {
      case CartAdd(‘id‘, items_) ⇒
        val newCart = CartCreated(id,items + items_)
        if (items disjointWith items_) newCart else error & newCart
      case CartRemove(‘id‘, items_) ⇒ CartCreated(id, items diff items_)
    }
  }
}
```

Property 4 formulated on XML messages directly

```
class Property4_XML extends Monitor[scala.xml.Elem] {
  Always {
    case add @ <CartAdd>{_∗}</CartAdd> ⇒
      val c = getId(add)
      val items = getItems(add)
      for (i ∈ items) yield
        unless {
          case res @ <CartGetResponse>{_∗}</CartGetResponse>
            if c == getId(res) ⇒ getItems(res) contains i
        } {
          case rem @ <CartRemove>{_∗}</CartRemove>
            if c == getId(rem) &&
             (getItems(rem) contains i) ⇒ ok
        }
  }
}
```

Creating and applying a monitor

```
class  Properties  extends Monitor[Event] {
  monitor(
    new Property1(), new Property2(), new Property3(),
    new Property4(), new Property5())
}

object Main {
  def main(args: Array[String]) {
    val m = new Properties
    val  file :  String  = "..."
    val xmlEvents = scala.xml.XML.loadFile( file )

    for  (elem ∈ xmlEvents \ "_") {
      m. verify (xmlToObject(elem))
    }
    m.end()
  }
}
```

Implementation

Implementation

```
class Monitor[E <: AnyRef] {
  val monitorName = this.getClass().getSimpleName()

  var states : Set[state] = Set()

  var monitors : List[Monitor[E]] = List()

  def monitor(monitors:Monitor[E]*) {
    this.monitors ++= monitors
  }

   ...

}
```

Implementation

```
type Transitions = PartialFunction[E, Set[state]]

def noTransitions : Transitions = {
  case _ if false ⇒ null
}

val emptySet : Set[state] = Set()
```

Implementation

```
class state {
  var transitions : Transitions = noTransitions
  var isFinal : Boolean = true

  def apply(event:E):Set[state] =
     if (transitions.isDefinedAt(event))
        transitions(event) else emptySet

  def Watch(ts: Transitions) {
     transitions = ts
  }

  def Always(ts: Transitions) {
     transitions = ts andThen (_ + this)
  }

  def Hot(ts: Transitions) {
    Watch(ts); isFinal = false
  }
```

Implementation

```
  def Wnext(ts: Transitions ) {
    transitions  = ts orElse {
        case _ ⇒ ok
     }
  }

  def Next(ts : Transitions ) {
    Wnext(ts); isFinal = false
  }

  def Unless(ts1 : Transitions )(ts2 : Transitions ) {
    transitions  = ts2 orElse
      (ts1 andThen (_ + this))
  }

  def Until (ts1 : Transitions )(ts2 : Transitions ) {
    Unless(ts1 )(ts2 ); isFinal = false
  }
}
```

Implementation

```
case object ok extends state
case object error extends state

def error(msg:String): state = {
  println("\n*** " + msg + "\n")
  error
}
```

Implementation

```
def watch(ts: Transitions) = new state {Watch(ts)}
def always(ts: Transitions) = new state {Always(ts)}
def hot(ts: Transitions) = new state {Hot(ts)}
def wnext(ts: Transitions) = new state {Wnext(ts)}
def next(ts: Transitions) = new state {Next(ts)}

def unless(ts1: Transitions)(ts2: Transitions) =
  new state { Unless(ts1)(ts2) }

def until(ts1: Transitions)(ts2: Transitions) =
  new state { Until(ts1)(ts2) }
```

Implementation

```
def  initial (s: state) { states += s }

def Always(ts: Transitions) {  initial (always(ts)) }

def Unless(ts1: Transitions)(ts2: Transitions) {
   initial (unless(ts1)(ts2))
}

...
```

Implementation

```
implicit def stateAsBoolean(s: state ): Boolean =
  states contains s
```

Implementation

```
def stateExists(p: PartialFunction[state,Boolean]): Boolean = {
  states exists (p orElse { case _ => false })
}
```

Implementation

```
implicit def ss1(u:Unit):Set[state] = Set(ok)

implicit def ss2(b:Boolean):Set[state] = Set(if (b) ok else error)

implicit def ss3(s:state):Set[state] = Set(s)

implicit def ss4(ss:List[state]):Set[state] = ss.toSet

implicit def ss5(s1:state) = new {
  def &(s2:state):Set[state] = Set(s1, s2)
}

implicit def ss6(set:Set[state]) = new {
  def &(s:state):Set[state] = set + s
}
```

Implementation

```
var statesToRemove : Set[state] = Set()
var statesToAdd : Set[state] = Set()
```

Implementation

```
def verify (event:E) {
  for (sourceState ∈ states) {
    val targetStates = sourceState(event)
    if (! targetStates.isEmpty) {
      statesToRemove += sourceState
      for (targetState ∈ targetStates) {
        targetState match {
          case ‘error‘ ⇒ println ("*** " + monitorName + " error!")
          case ‘ok‘ ⇒
          case _ ⇒ statesToAdd += targetState
        }
      }
    }
  }
  states −−= statesToRemove; states ++= statesToAdd
  statesToRemove = emptySet; statesToAdd = emptySet
  for (monitor ∈ monitors) {monitor.verify (event)}
}
```

Implementation

```
def end() {
  val hotStates = states filter (!_.isFinal)
  if (!hotStates.isEmpty) {
    println ("hot " + monitorName + " states:")
    hotStates foreach println
  }
  for (monitor ∈ monitors) {
    monitor.end()
  }
}
```

Evaluation

Results

trace nr.	1	2	3	4	5	6	7
memory	1	1	5	30	100	500	5000
length	30,933	2,000,002	2,100,010	2,000,060	2,000,200	2,001,000	1,010,000
parsing	3 sec	45 sec	47 sec	46 sec	46 sec	46 sec	24 sec
LogFire	26 1:190	42 47:900	41 50:996	34 58:391	23 1:27:488	8 3:55:696	1 15:54:769
Rete/UL	38 816	109 18:428	75 28:141	41 48:524	14 2:26:983	4 8:25:867	0.4 43:33:366
Drools	10 3:97	8 4:1:758	9 3:47:535	9 3:34:648	8 4:14:497	7 4:36:608	3 5:4:505
Ruler	95 326	138 14:441	78 27:77	8 4:5:593	0.8 41:39:750	0.034 977:20:636	DNF
LogScope	17 1:842	15 2:11:908	7 4:54:605	2 21:42:389	0.4 76:17:341	0.09 369:25:312	0.01 2074:43:470
TrContract	48 645	69 28:851	37 57:428	6 5:58:497	0.9 36:29:594	0.036 919:5:134	DNF
Daut	49 631	84 23:847	86 24:338	89 22:432	90 22:298	86 23:287	80 12:612
Daut^{sos}	102 302	192 10:435	79 26:438	24 1:22:727	8 4:19:697	2 16:27:990	0.18 92:2:26
Daut^{int}	233 133	1715 1:166	770 2:729	373 5:368	195 10:236	54 36:929	5 3:6:560
Mop	595 52	1381 1:448	1559 347	1341 1:491	7143 280	7096 282	847 1:193

Conclusion

Conclusion

- We have seen the concept of data automata
- implemented as an external as well as an internal DSL
- internal DSL is simple but hard to optimize if shallow

Will programming and specification merge?

- Modern programming languages, such as Python, Scala, Fortress have many things in common with specification language such as VDM.
- I see a trend in this direction: specification and programming will merge.
- We see programming constructs such as:
  - functional programming combined with imperative programming
  - algebraic datatypes
  - sets, list and maps as built in data types with mathematic notation
  - predicate subtypes ($\mathbb{N} = \{i \in \mathbb{Z} \mid i \geqq 0\}$)
  - design by contract: pre/post conditions, invariants on state
  - session types
  - predicate logic, quantification over finite sets (as functions)
  - verification systems built around programming languages
  - meta programming for defining DSLs
  - integration of visualization and programming

The end