

Abstract State Machines



Angelo Gargantini

2024

Testing e verifica del sw

Scopo del Modulo

- Presentare
 - il formalismo delle Abstract State Machine (ASM)
 - e il metodo di sviluppo di sw complesso basato su di esse
- Imparare ad utilizzare i tools a supporto

- Materiale:
 - Queste slides
 - Dal sito principale:
 - <https://asmeta.github.io/>
- https://asmeta.github.io/material/AsmetaL_guide.pdf

ASMETA : ASm METAmodeling

- <https://asmeta.github.io/>
- Abstract State Machine Metamodel
 - tool set based on the Eclipse/EMF platform for MDE
- Model editing
 - and interchange format
- Validation
 - simulation
 - Scenario construction
 - model-based testing
- Verification
 - static analysis
 - model checking

Asmeta - Asmeta Tools x +

← → ↻ 🏠 <https://asmeta.github.io/download/index.html>

Asmeta

Overview

Asmeta toolset

- Editor
- Simulator
- Validator
- Animator
- Model checker
- Model advisor
- Visualizer
- Refinement prover
- Scenario refiner
- Asm2SMT
- Asm2C++

Papers

- Our papers
- Papers written by others

People

User documentation

- Documentation for users
- Asmeta language
- The Abstract State Machines Metamodel

Developer documentation

- Developer information
- Source repository

Web resources

Asmeta Tools

We have developed and are distributing the following (stable) tools

- **Asmee**: an editor for ASMs written in the AsmetaL language
- **AsmetaLc**: a compiler/parser for AsmetaL models
- **AsmetaS**: a simulator
- **AsmetaV**: a scenario-based validator
- **AsmetaA**: an execution animator
- **AsmetaSMV**: a model checker based on NuSMV
- **AsmetaMA**: a model advisor
- **AsmetaVis**: a graphical visualizer of AsmetaL models
- **AsmetaRefProver**: a prover of refinement correctness
- **Asm2SMT**: a translator from AsmetaL models to Yices logica
- **Asm2C++**: a code generator

Some tools are provided both as eclipse plugins and standalone jars :

Installing ASMETA in eclipse

Some ASMETA tools are integrated in eclipse. The update site is [http the update site:](http://asmeta.github.io/)

1. From your Eclipse menu select **Help Software Updates Find**
2. Check **Search for new features** and press **Next**.
3. Press **New Remote Site...** and enter <https://raw.githubusercontent.com/asmeta/asmeta.github.io/master/asmeta-update-site.xml>

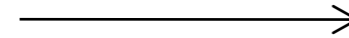
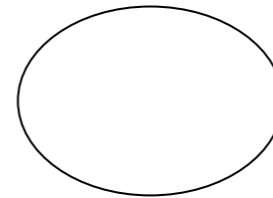
Idea guida

- ASM = FSM con stati generalizzati
- Le ASM rappresentano la forma matematica di Macchine Virtuali che estendono la nozione di Finite State Machine
 - Ground Model (descrizioni formali)
 - Raffinamenti (che non vedremo)
- Idee guida

Asm come estensione delle FSM

FSM

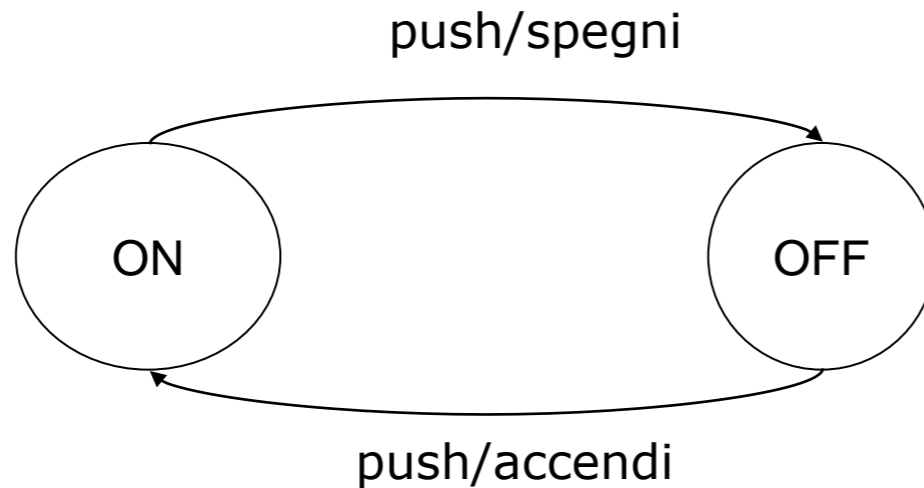
- Insieme (finito) di stati
- Collegati da transizioni
- Con condizioni e azioni sulle transizioni
 - Insieme finito di input e di azioni



cond/action

Esempio : interruttore di luce

- Un interruttore con un solo bottone che quando viene premuto (push) invia il comando alla lampada di accendersi o spegnersi



Due soli stati: On e Off
Un solo input push
Due output spegni e accendi

Macchina a Stati Finiti (1)

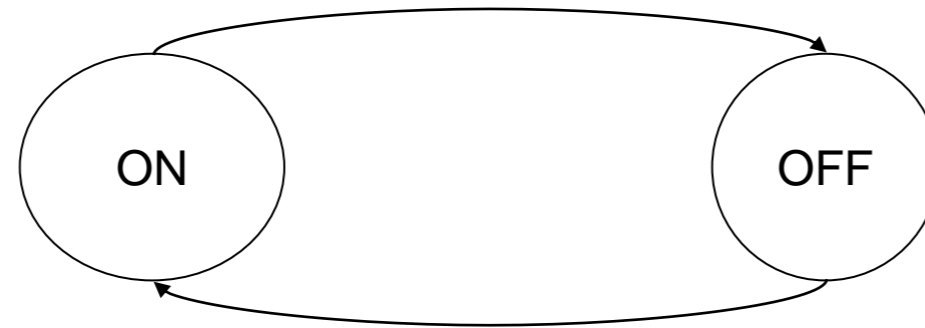
Una **macchina a stati finiti**, abbreviata FSM (Finite State Machine), è una notazione formale che permette la rappresentazione astratta del comportamento di un sistema

Le FSM hanno:

- una rigorosa definizione matematica
- una intuitiva rappresentazione grafica tramite **diagrammi di stato**

FSM: un primo esempio

Esempio: comportamento di una lampadina



- I **nodi** rappresentano gli stati del sistema
- Gli **archi** rappresentano il passaggio di stato

Estensioni di FSM

Altri modelli di macchine a stati finiti, arricchiti di ulteriori informazioni, tra cui:

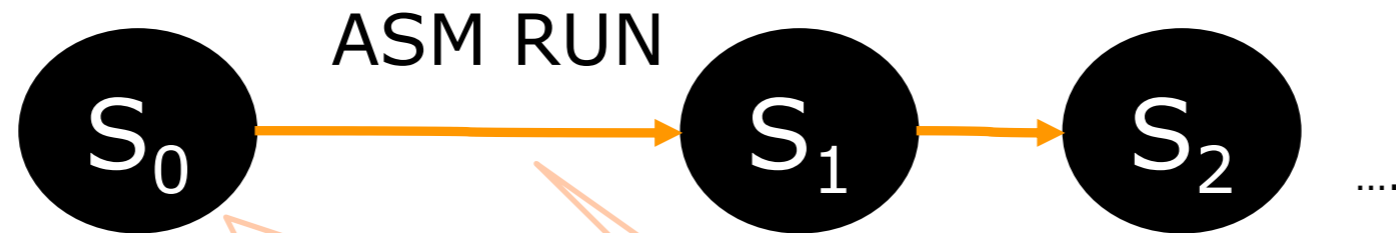
- **FSM con evento di output** (ad es. un'azione)
 - macchine di Mealy (output sulla transizione)
 - macchina di Moore (output nello stato)
- **FSM con variabili** (rappresentano la memoria interna della macchina)
- **le Statecharts di UML** dotate dei concetti di sottomacchina (modularità) e composizione sequenziale/parallela
- **le Abstract State Machines (ASM)** dotate dei concetti di sottomacchina, composizione sequenziale/parallela, e di **stato astratto**

Differenze FSM/ASM

- Le ASM sono analoghe alle FSM
- Le differenze riguardano
 - la concezione degli **stati**:
 - nelle FSM esiste un unico stato di controllo (ctl_state), che può assumere valori in un insieme finito
 - Nelle ASM lo stato è più complesso
 - le condizioni di input e le azioni di output
 - Nelle FSM alfabeto finito
 - Nelle ASM: input qualsiasi espressione, azioni generiche
 - che però stanno nello stato
 - la transizione dipende solo dallo stato corrente

Abstract State Machines

- ASMs are an extension of Finite State Machine
 - unstructured control states are replaced by states with arbitrary complex data.
 - Transition rules describe the change of state.



State: instantaneous configuration of the system and its environment
Monitored functions: inputs
Controlled functions: state + outputs

State transition: application of the rules to the previous state (update)

Modello computazionale - brief

ASM = Abstract State + *virtual* Machine

[Gurevich'95/'99]

Modello Computazionale

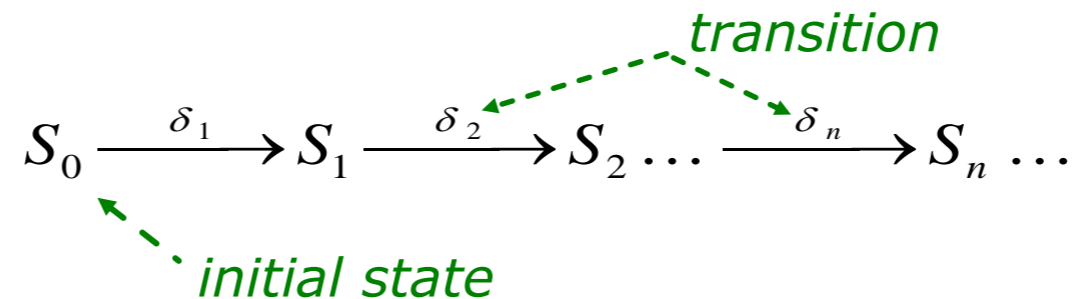
Vocabolario o segnatura

Stato: strutture del 1st ordine (domini, funzioni, predicati)

Azioni: transizioni di stato

if Cond then Updates

Computazione (una serie di *run* finite o infinite)



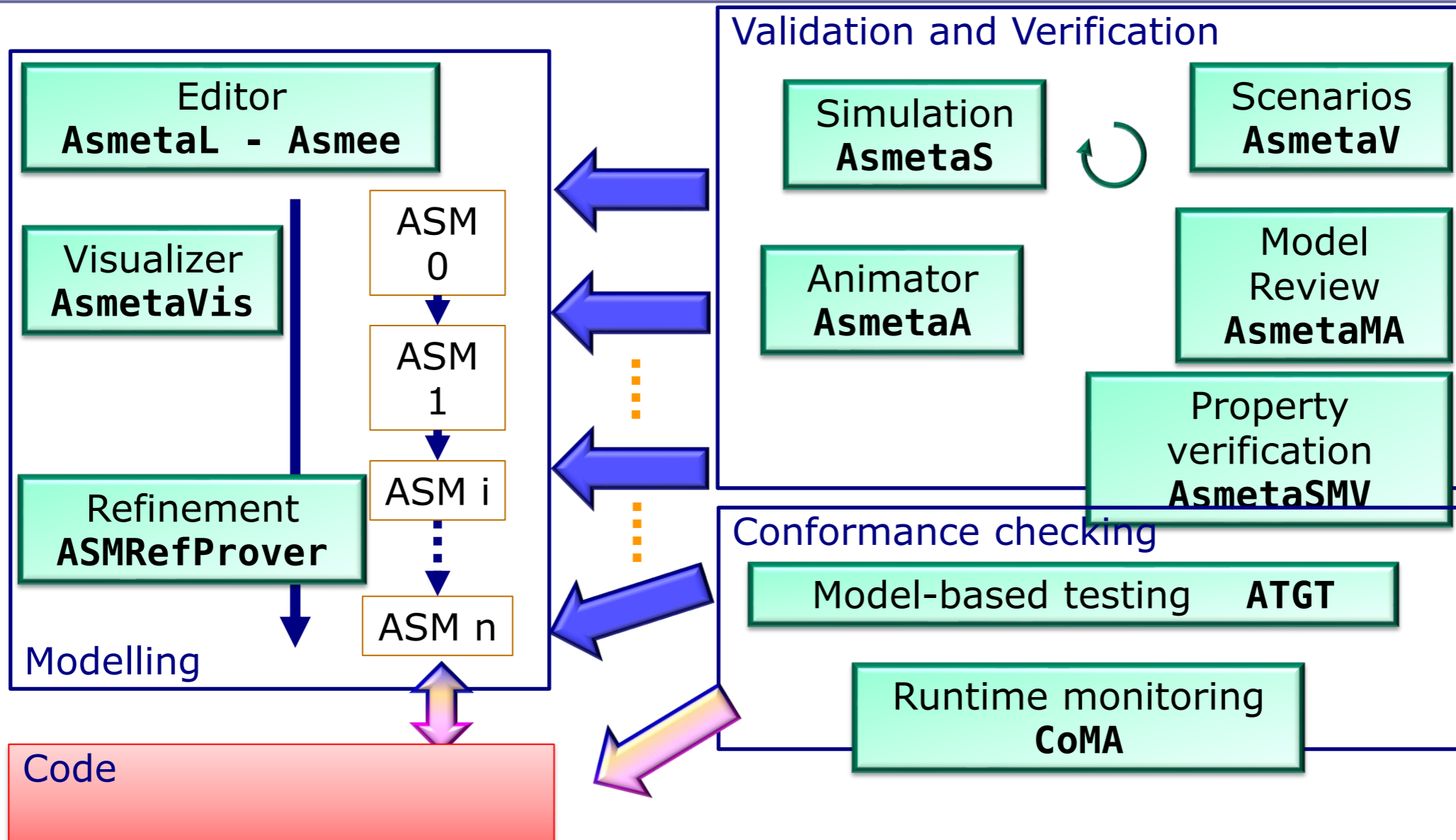
Programmi (istruzioni di aggiornamento) *Updates:*

$f(t_1, t_2, \dots, t_n) := t_0$

Asmeta

- Useremo **Asmeta** come tool per le ASM:
- Ha un linguaggio/editor
 - AsmetaL
 - un ambiente eclipse (Asmee)
- Un simulatore e animatore
 - AsmetaS
- Un linguaggio per scenari (tipo test junit)
 - Avalla
- Un tool per l'analisi statica (tipo PMD)
 - asmetaMA
- Un tool per il model checking
 - AsmetaSMV

ASMETA framework



ASMETA tool set 1/2

- AsmM Abstract Syntax (ASM metamodel) un metamodello in EMF
- AsmM Concrete Syntax (AsmetaL)
 - La grammatica EBNF sviluppata con Sun/JavaCC
 - Una quick guide e esempi (rps_mono/ e rps_agents/) di specifiche ASM
- AsmM Standard Library
 - StandardLibrary.asm per domini/funzioni ASM predefinite

- **AsmetaLc** compiler per
 - processare specifiche **AsmetaL**
 - controllare la consistenza rispetto ai vincoli **AsmM-OCL**
 - generare la rappresentazione **XMI** (XML-based) corrispondente
 - Tradurle in istanze **AsmM** in oggetti Java usando le AsmM JMIs
- **AsmetaS** simulator
 - per simulare/eseguire una specifica ASM
 - un **interprete** che simula la specifica ASM come istanza di AsmM
- Un front-end grafico **ASMEE (ASM Eclipse Environment)**
 - **Eclipse plug-in** che fa da IDE per editare, manipolare, esportare nel formato XMI le spec. ASM usando i tool di cui sopra

Altri tools

- Validazione tramite scenari
 - Avalla
 - Scrive degli scenari tipo Junit
- Model advisor
 - Per trovare difetti (analisi statica)
- Animatore
 - Simulatore con UI
- Visualizzatore grafico di modelli
- Model checker
 - Basato su NuSMV
- Tests generator
 - ASM Tests Generation Tool (**ATGT**)

Sul linguaggio – AsmetaL

- The EBNF grammar for the AsmM textual notation.
- A quick guide of the concrete notation
- A more complete guide about the language
- several examples of ASM specs
 - Cerca sotto github la directory esempi
- The AsmM Standard Library A library of predefined ASM domains and functions: StandardLibrary.asm.(you need this)
- Anche il railroad:
 - <https://asmeta.github.io/material/AsmetaLRR.xhtml>

Standard Library

Operatori aritmetici

- +, -, *, /, %

Operatori relazionali

- =, !=, <, >, <=, >=

Operatori booleani

- not, and, or, implies, iff

Funzioni per insiemi e sequenze

- first(), tail(), union()

I domini standard: Naturali, Integer, ...

- La StandardLibrary.asm deve essere importata

StandardLibrary.asm

Come usare AsmetaS in riga di comando

Da linea di comando:

```
java -jar AsmetaS.jar <filename>
```

E' possibile specificare alcune opzioni per la terminazione della computazione, tra cui:

-n 3 per un numero fisso (ad es. 3) di passi

-n? per eseguire fino a che l'insieme degli aggiornamenti risulta vuoto

```
java -jar AsmetaS.jar -n 3 <filename.asm>
```

```
java -jar AsmetaS.jar -n? <filename.asm>
```

AsmetaS output

Il simulatore produce come output la traccia d'esecuzione della macchina.

L'output è disponibile all'utente in due forme:

- come **testo** non formattato inviato **sullo standard output**
- come **documento xml** memorizzato nel file ***log.xml*** residente nella directory di lavoro

Per cambiare stili di presentazione e media di memorizzazione, l'opzione `-log` consente di precisare un file `log4j` che sarà considerato dal simulatore in sostituzione di quello di default.

How to debug your ASM spec

- Il logger per il tracing dell'attività di parsing e la valutazione dei termini e delle regole
 - anche dall'interfaccia di Asmee
- può essere attivato cambiando le **proprietà di del file log4j:**

```
log4j.logger.org.asmeta.interpreter.ReflectiveVisitor=WARN
log4j.logger.org.asmeta.interpreter.TermEvaluator=DEBUG
log4j.logger.org.asmeta.interpreter.RuleEvaluator=OFF
log4j.logger.org.asmeta.interpreter.TermSubstitution=INFO
log4j.logger.org.asmeta.interpreter.RuleSubstitution=OFF
log4j.logger.org.asmeta.interpreter=OFF
```

AsmetaS modalità

Immettere valori per le funzioni monitorate:

Modalità Interattiva

- Per default, l'utente fornisce manualmente i valori quando vengono richiesti
- Modalità batch (valori letti da file)
- Specificando da linea di comando come ultimo argomento il pathname di un file d'ambiente `.env`, da dove i valori saranno letti

```
java -jar AsmetaS.jar <filename.asm>  
<fileambiente.env>
```


AsmetaS key features

□ Axiom checker

- Se un assioma viene violato, AsmetaS lancia l'eccezione `InvalidAxiomException` che tiene traccia dell'assioma violato

□ Consistent Updates checking

- In caso di update inconsistenti, AsmetaS lancia l'eccezione `UpdateClashException` che tiene traccia della coppia di locazioni oggetto dell'inconsistenza

□ Random simulation

- per mezzo di un *ambiente random* per le funzioni monitorate

□ Per maggiori info vedi scarica dal sito la guida:

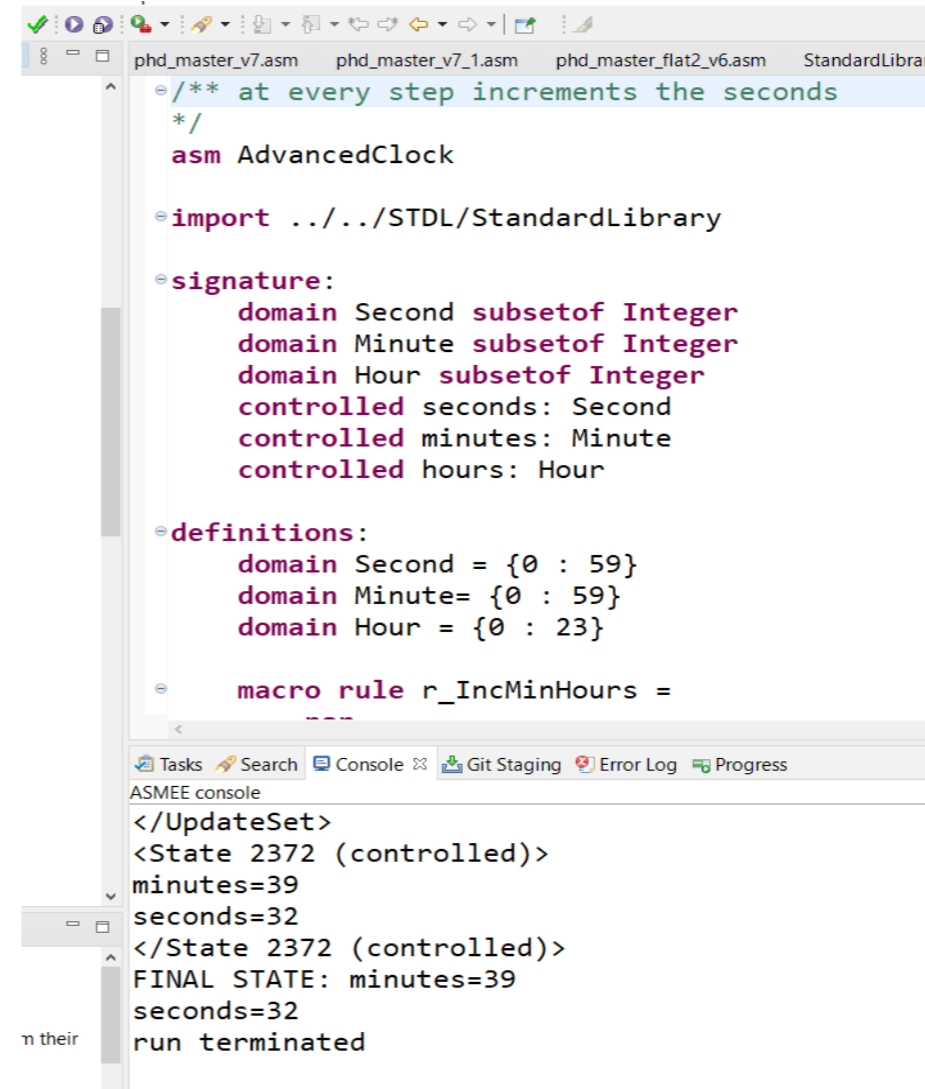
- https://raw.githubusercontent.com/asmeta/asmeta.github.io/master/src/material/AsmetaS_quickguide_it.pdf

Installing ASMETA in eclipse

- Eclipse plugin
- See instruction under **Installing ASMETA in eclipse**
- Open ASMETA....

A stand-alone version of Eclipse with all the of the ASMETA plugins is available

<https://github.com/asmeta/asmeta>



The screenshot shows the Eclipse IDE interface. The top part displays a code editor with the following ASMETA code:

```
phd_master_v7.asm phd_master_v7_1.asm phd_master_flat2_v6.asm StandardLibrar
=/** at every step increments the seconds
*/
asm AdvancedClock

import ../../STDL/StandardLibrary

signature:
  domain Second subsetof Integer
  domain Minute subsetof Integer
  domain Hour subsetof Integer
  controlled seconds: Second
  controlled minutes: Minute
  controlled hours: Hour

definitions:
  domain Second = {0 : 59}
  domain Minute = {0 : 59}
  domain Hour = {0 : 23}

macro rule r_IncMinHours =
  ...
```

The bottom part of the screenshot shows the ASMEE console output:


```
ASMEE console
</UpdateSet>
<State 2372 (controlled)>
minutes=39
seconds=32
</State 2372 (controlled)>
FINAL STATE: minutes=39
seconds=32
run terminated
```

L'IDE for ASMETA

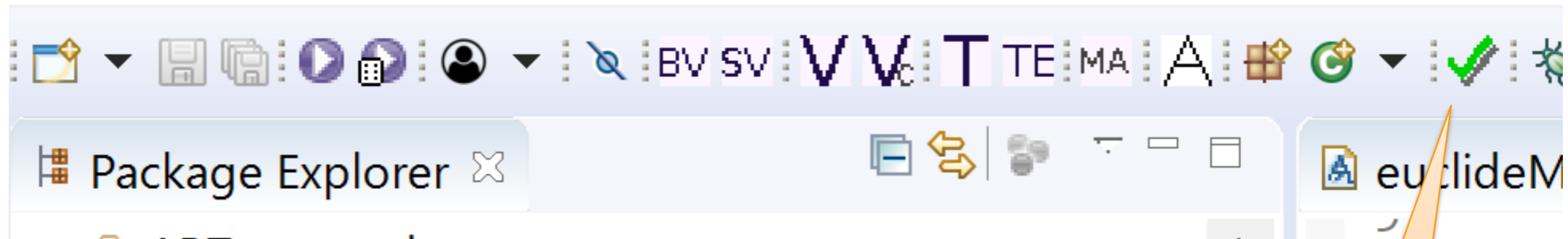
- Caratteristiche disponibili in ambiente Eclipse:
 - un wizard per **creare un nuovo file AsmetaL**:
 - **File->new File-> Other -> AmsetaL new File**
 - **synthax hightlighting**
 - I colori predefiniti possono anche essere modificati:
 - **Window -> Preferences -> Asmee**
- Azioni per simulare con AsmetaS un file AsmetaL:
 - **check** la tua specifica AsmetaL



Parse a model

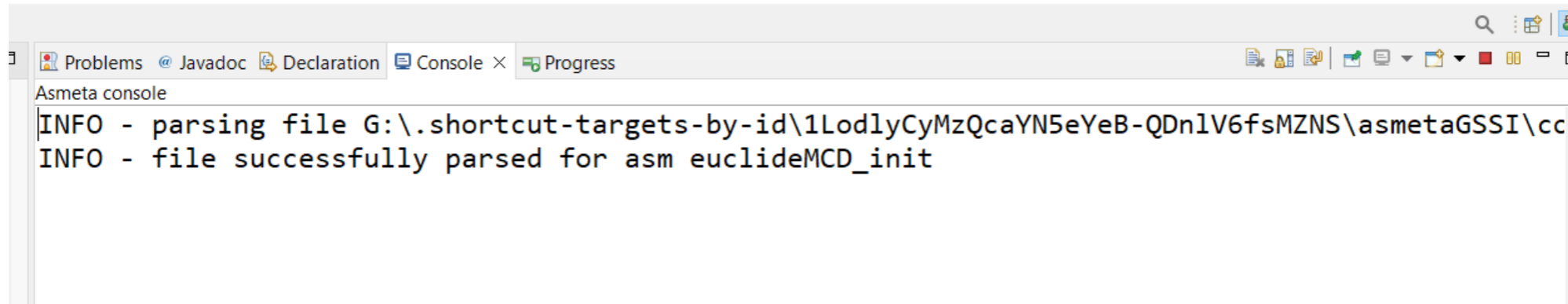
 eclipse-workspace - asmetacode/euclideMCD.asm - Eclipse IDE

File Edit Navigate Search Project AsmEE Run Asmeta Window Help



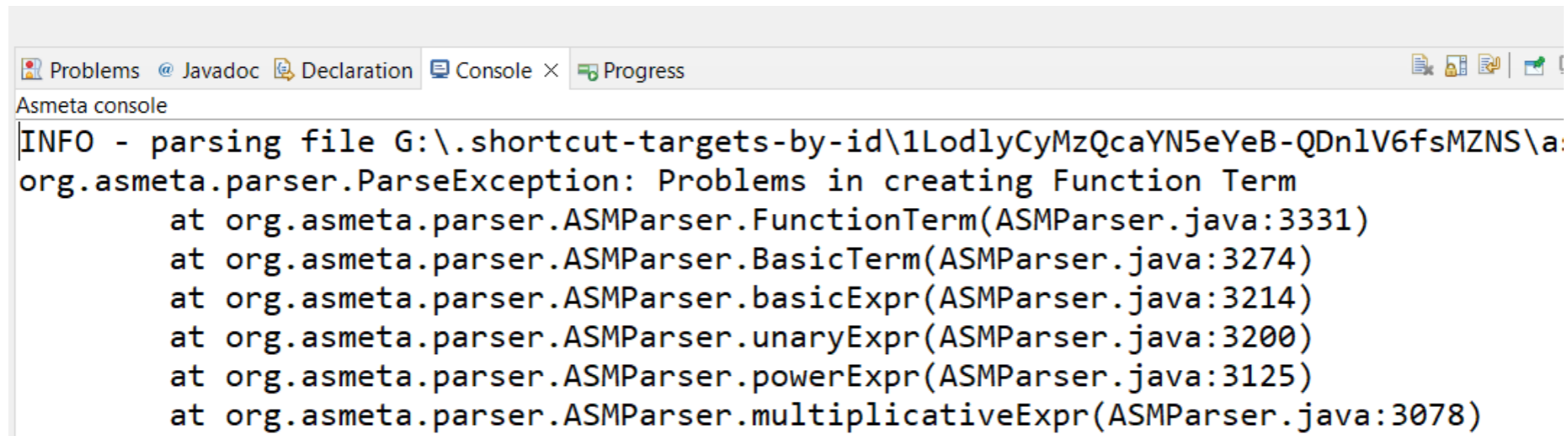
1. parser

AsmetaL Console





```
Asmeta console
INFO - parsing file G:\.shortcut-targets-by-id\1LodlyCyMzQcaYN5eYeB-QDn1V6fsMZNS\asmetaGSSI\cc
INFO - file successfully parsed for asm euclideMCD_init
```

❑ Errors as violation of OCL constraints



```
Asmeta console
INFO - parsing file G:\.shortcut-targets-by-id\1LodlyCyMzQcaYN5eYeB-QDn1V6fsMZNS\asmetaGSSI\cc
org.asmeta.parser.ParseException: Problems in creating Function Term
    at org.asmeta.parser.ASMParser.FunctionTerm(ASMParser.java:3331)
    at org.asmeta.parser.ASMParser.BasicTerm(ASMParser.java:3274)
    at org.asmeta.parser.ASMParser.basicExpr(ASMParser.java:3214)
    at org.asmeta.parser.ASMParser.unaryExpr(ASMParser.java:3200)
    at org.asmeta.parser.ASMParser.powerExpr(ASMParser.java:3125)
    at org.asmeta.parser.ASMParser.multiplicativeExpr(ASMParser.java:3078)
```

Simulazione in asmee

- Per simulare una ASM usa:
 - Simulazione interattiva (domanda gli input all'utente): 
 - Simulazione random (scegli valori a caso per input): 
- Puoi fermare la simulazione al verificarsi di due condizioni:

- Stop simulation if the update set is empty
- Stop simulation if the update set is trivial

Oppure usa



Noi useremo però l'animatore principalmente

Contribuire da sviluppatore

Progetto ospitato da github

- un repo con tutti i progetti eclipse
 - code/core il progetti principali

Altre tecnologie:

xtext, xtend ...

log4j for logging

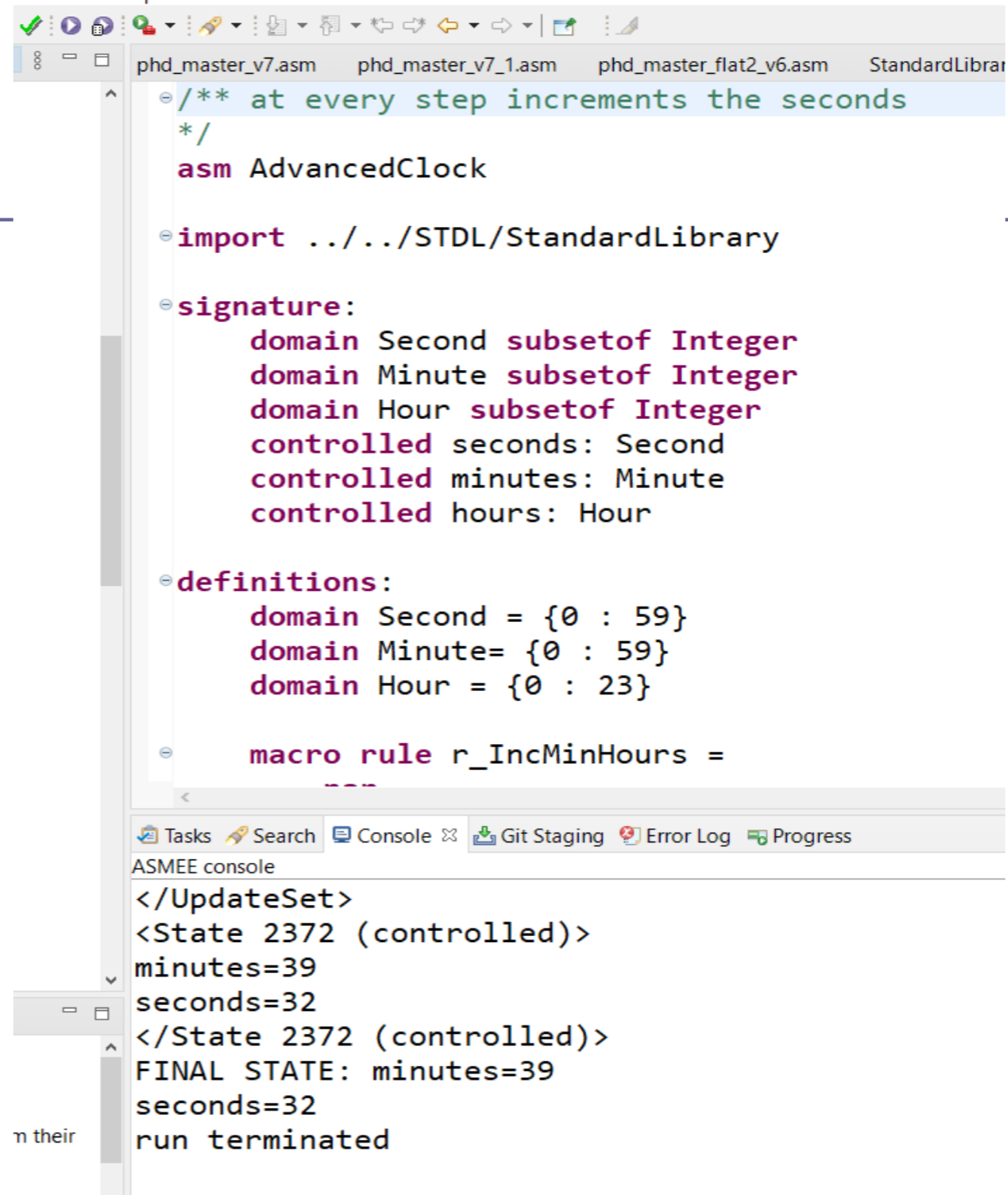
- Ogni utente può personalizzare il suo log (per scopi di debugging di specifiche ASM e per l'interprete)

JUnit per lo unit testing

CI con gitlab

L'IDE ASMEE

ASMETA
Eclipse
Environment



The screenshot shows the ASMEE IDE interface. The top part is a code editor with a file named `phd_master_v7.asm`. The code is as follows:

```
/** at every step increments the seconds
 */
asm AdvancedClock

import ../../STDL/StandardLibrary

signature:
  domain Second subsetof Integer
  domain Minute subsetof Integer
  domain Hour subsetof Integer
  controlled seconds: Second
  controlled minutes: Minute
  controlled hours: Hour

definitions:
  domain Second = {0 : 59}
  domain Minute = {0 : 59}
  domain Hour = {0 : 23}

macro rule r_IncMinHours =
```

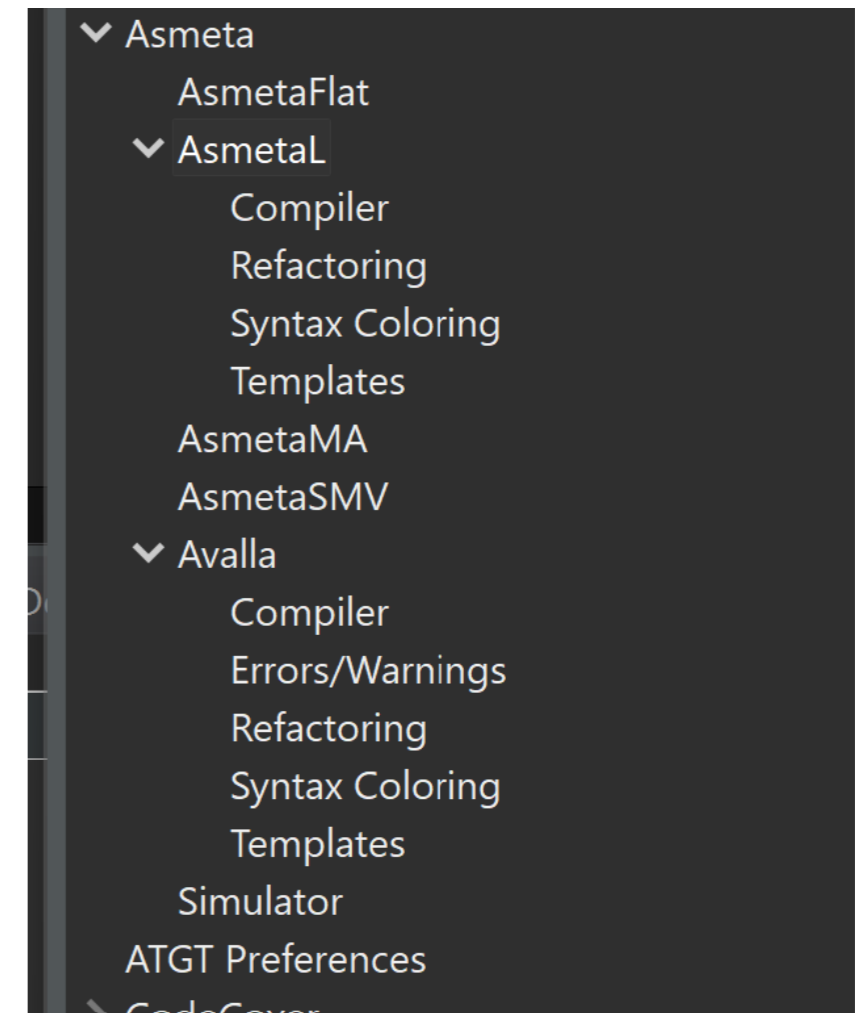
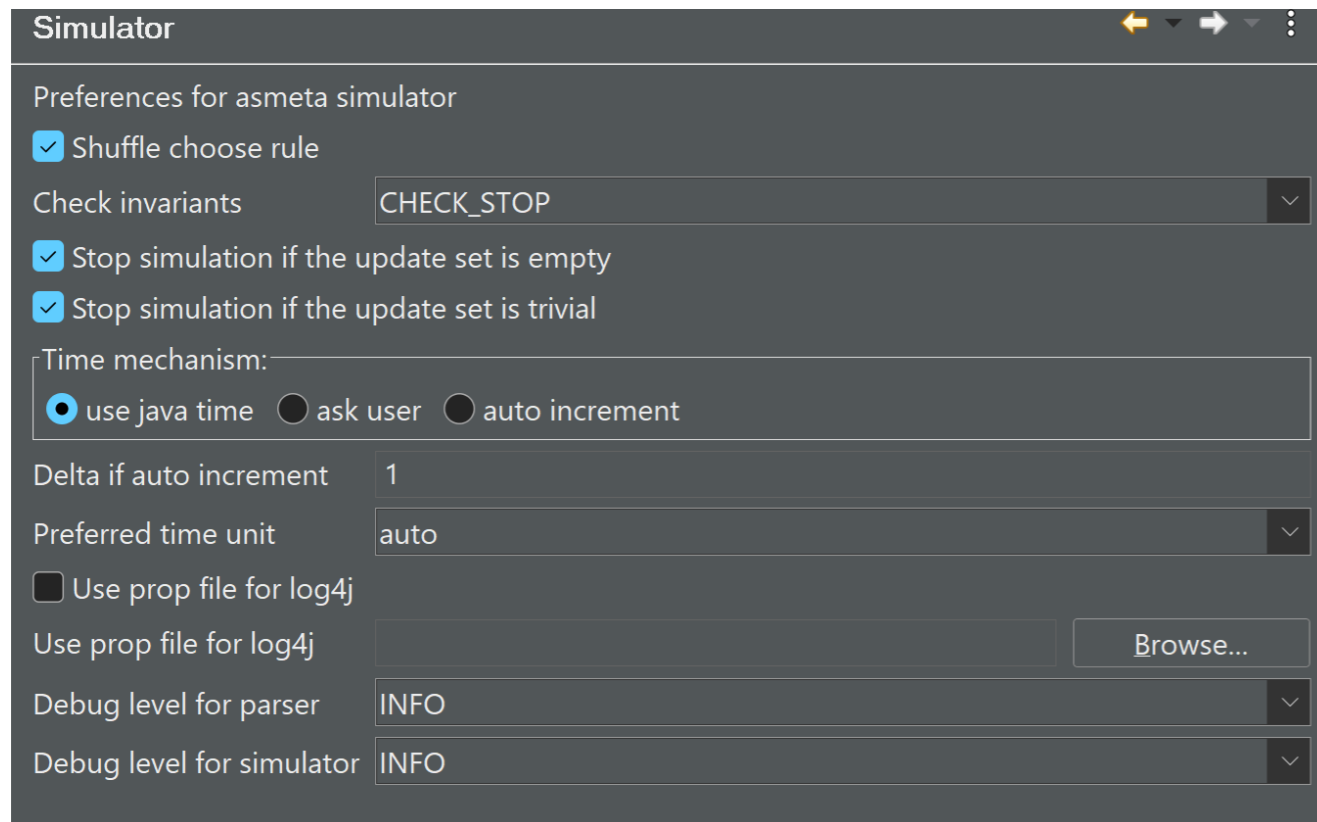
The bottom part of the IDE is a console window titled "ASMEE console". It displays the following output:

```
</UpdateSet>
<State 2372 (controlled)>
minutes=39
seconds=32
</State 2372 (controlled)>
FINAL STATE: minutes=39
seconds=32
run terminated
```

n their

Asmeta preferences

- ▣ Several preferences
- ▣ Like for the simulator:

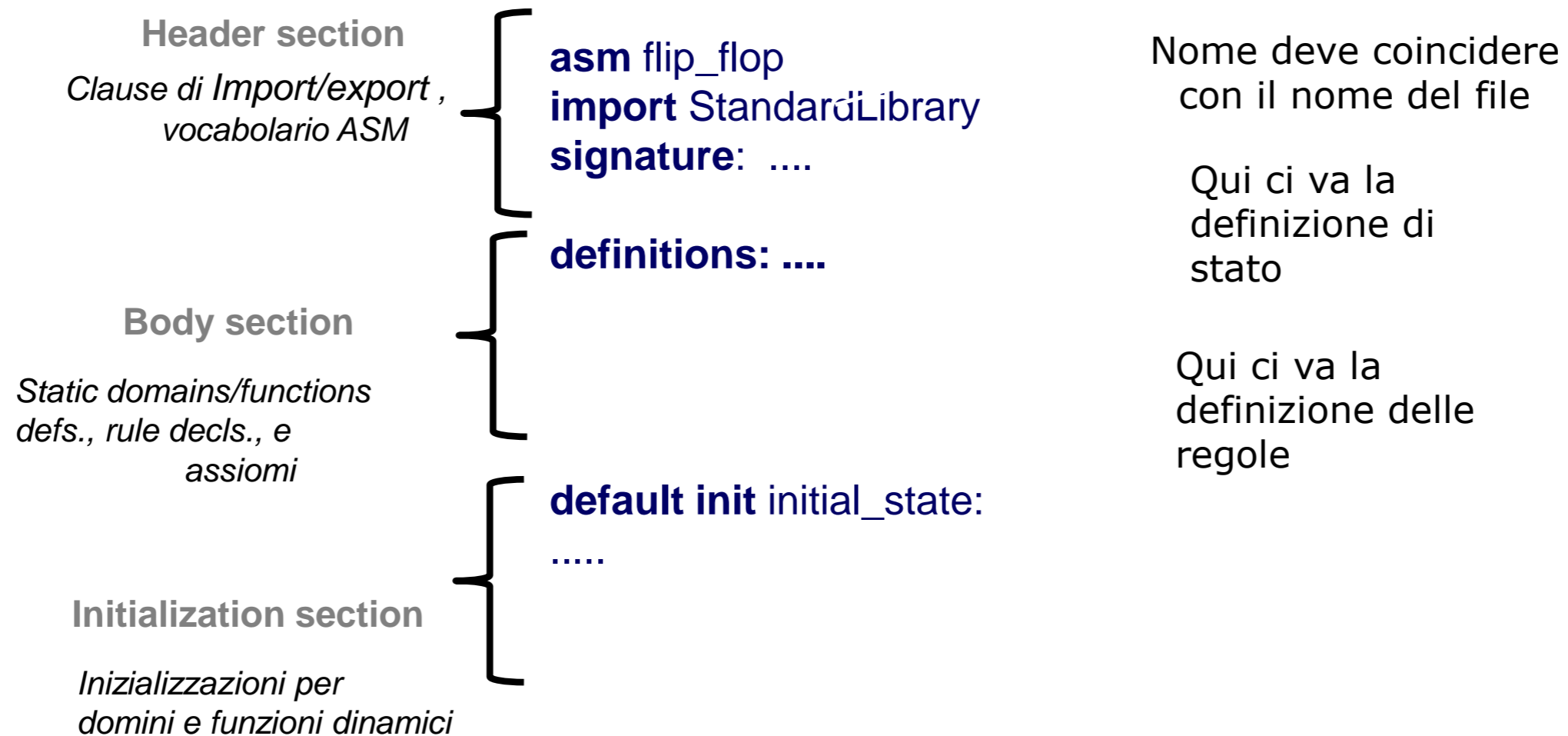


IL LINGUAGGIO ASMETAL

Il Linguaggio AsmetaL

- *Linguaggio strutturale*
 - costrutti per definire la struttura (scheletro) di una ASM mono-agente o sinc./asinc. multi-agente
- *Linguaggio delle definizioni*
 - costrutti per introdurre (dichiarare e definire) domini (*tipi del linguaggio*), funzioni (con domini e codomini), regole di transizione, e assiomi
- *Linguaggio dei termini*
 - **termini di base** come nella logica del primo ordine (costanti, variabili, termini funzionali $f(t_1, t_2, \dots, t_n)$)
 - **termini speciali** come tuple, collezioni (insiemi, sequenze, bag, mappe), ecc.
- *Linguaggio delle regole*
 - **regole di base** come skip, update, parallel block, ecc.
 - **turbo regole** come seq, iterate, turbo submachine call, ecc.

Struttura di una ASM in AsmetaL:



IL LINGUAGGIO DELLE DEFINIZIONI

Stato in ASM

- Nelle ASM lo stato è definito da un insieme di valori di qualsiasi tipo, memorizzate in apposite **locazioni**
 - come nella programmazione **le variabili**
 - In OO sono i **campi** dell'oggetto
- in ASM si chiamano **funzioni**
- distinguiamo **la cardinalità delle funzioni**
 - **Variabili e costanti (0-arie)** x, y, \dots
 - **Mappe/array/funzioni n-arie**
 - Es: $\text{name}(1), \text{name}(2), \dots$

Dinamiche/statiche

- Le **funzioni** possono essere dinamiche o statiche a seconda che il valore della funzione cambia o no da uno stato al successivo
 - Funzioni in senso matematico non informatico come "procedure"
 - Funzioni dinamiche: cambiano nel tempo
 - Funzioni statiche: la loro interpretazione rimane costante (come le funzioni in **scala**)
- Funzioni statiche di arità zero sono dette **costanti**
- Funzioni dinamiche di arità zero sono le comuni **variabili** dei linguaggi di programmazione
- Vedremo dopo come dichiarare le funzioni - **Domini**

Definizione dello stato

header è:

[**import** m1 [(id11,...,id1h1)] ...]

[**export** id1,...,ide] or

[**export** *]

signature :

[**dom_declarations**]

[**fun_declarations**]

import/export di simboli (id) di domini, funzioni (e loro domini e codomini), e regole da/verso altre ASM

Ricordare: la segnatura contiene dichiarazioni (non definizioni) di domini e funzioni!

DOMINI

ASM Domini

- I soliti domini predefiniti sono disponibili
 - Interi, String
 - Da importare dalla StandardLibrary
- L'utente può definirne altri
 - Da niente, come tipi astratti, come enumerativi
 - A partire da altri domini (strutturati)
 - Come alias ad esempio
 - ...

Il Linguaggio delle definizioni – type domain

- Caratterizzazione dei domini
- **type-domain**: caratterizzano il superuniverso
- **basic type-domains**: **Complex, Real, Integer, Natural, String, Char, Boolean, Rule**, e **Undef** definiti nella **standard library**!

basic domain Real

basic domain Integer

- Questi non devono essere definiti, ci sono già
- L'utente può definirne di suoi type domains
- NOTA: devono iniziare con la maiuscola!

ID_DOMAIN una stringa che inizia con una lettera maiuscola.

Esempi: **Integer** **X** **SetOfBags** **Person**

Il Linguaggio delle definizioni dei domini

- **abstract domain**: elementi di natura "astratta", non definiti se non attraverso funzioni definite su tale dominio

abstract domain D

dove D è il nome del type domain

Esempio: abstract domain Student

enum: enumerazioni,

- **enum domain D = { EL1 | ... | ELn }** oppure **{ EL1, ..., ELn }**
- dove D è il nome e EL1, ..., ELn le costanti dell'enumerazione
 - **ID_ENUM** una stringa di lunghezza ≥ 2 , fatta di sole lettere maiuscole.
Esempi: **ON** **OFF** **RED**
- ad esempio enum domain Color = {RED | GREEN | BLUE}

Domini Concreti

Dichiarazioni di **domini concreti** (`dom_declarations`)
user-defined e subset dei type-domain

[**dynamic**] **domain D subsetof td**

dove:

- D è il nome del dominio da dichiarare
- td è il type-domain di cui D è subset
- La parola chiave **dynamic** è opzionale e denota che l'insieme è *dinamico* (stesso concetto delle funzioni). Per default, un dominio è *statico* e va *definito* nella sezione **definitions**

Esempio:

signature:

domain State subsetof Integer

definitions:

domain State = {0,1}

*Basic domain
della standard library*



Caso di studio

- Proviamo a definire un orologio che:
 - Memorizza ora minuti e secondi (stato)
 - ad ogni passo incrementa secondi (e aggiorna lo stato in modo corretto)
 -
- Variante:
 - Ha un input che è il segnale, ed incrementa lo stato solo se il segnale è vero

Esempio - clock

- Un orologio che ad ogni passo se arriva un segnale avanza di un secondo

```
domain Second subsetof Integer  
domain Minute subsetof Integer  
domain Hour subsetof Integer
```

Domini Astratti e classi Java

- I domini astratti sostituiscono i costrutti come ADT (abstract data type) o le struct e le classi Java
- Esempio
- **Java:** `class Student{ ...}`
- **Asm:** abstract domain Student

Structured domain

structured: per costruire insiemi finiti, sequenze, bag, mappe, e tuple a partire da altri domini

Vedremo più avanti

Funzioni

FUNZIONI

Costanti

- Le costanti sono funzioni 0-arie statiche
- Sono simboli definiti una volta per tutte
- Per definizione, ogni vocabolario ASM contiene
 - le costanti **undef**,
 - **true, false**
 - I numeri sono costanti numeriche
 - 1,2, ...
- L'utente può aggiungerene di sue
- costante minimoVoto = 18 - vedremo come (static functions)
- Le stringhe sono costanti, esempio "pippo"

ASM Function Classification

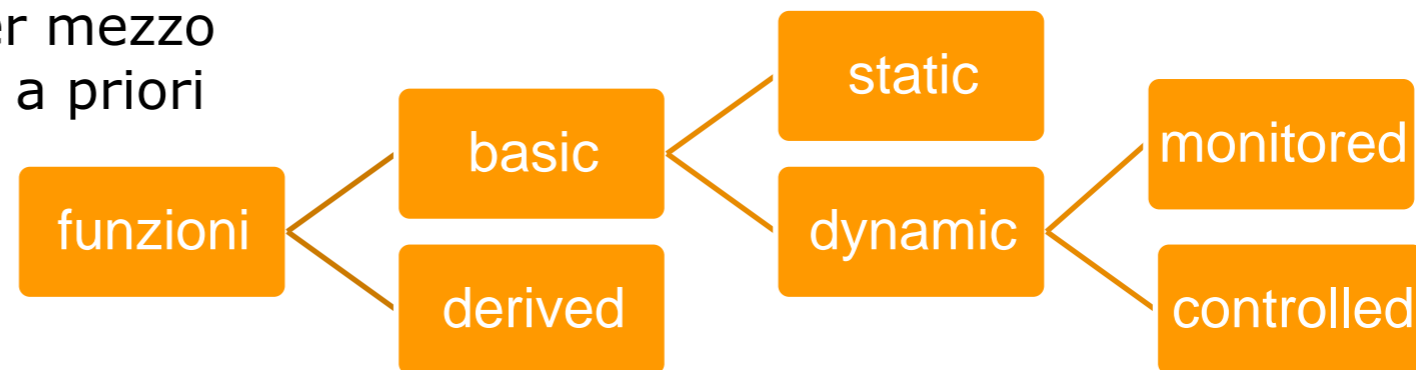
Le funzioni dinamiche unarie corrispondono alle variabili

Detta ***M*** l'ASM corrente e ***env*** l'ambiente di ***M***:

Dynamic: i valori dipendono dagli stati di ***M***

- **monitored:** lette (non aggiornate) da ***M***, scritte da ***env***
- **controlled:** lette e scritte da ***M***

Derived: valori computati da funzioni monitorate e funzioni statiche per mezzo di una "legge" o "schema" fissati a priori



Realizza l'incapsulamento/information hiding dei linguaggi OO

Funzioni **controlled** e **monitored**

- **Controlled:** rappresentano quelle che la macchina modifica
- **Monitored:** quelle modificati dall'ambiente esterno (in simulazione andranno domandate all'utente o lette da un file esterno)
- ASM: particolarmente adatte per sistemi reattivi

Definizione delle funzioni in AsmetaL

Dichiarazioni di funzioni 0-arie

Funzioni statiche	static f: C
Funzioni dinamiche	[dynamic] monitored f: C [dynamic] controlled f: C [dynamic] shared f: C [dynamic] out f: C [dynamic] local f: C

- . C è il codominio di f (f prende valori in C)
- . **ID_FUNCTION**
- . una stringa che inizia con una lettera minuscola diversa da "r_" e da "inv_". Esempi: **plus** **minus** **re**

Esempio - orologio

`monitored` signal:Boolean
`controlled` seconds:Second
`controlled` minutes:Minute
`controlled` hours:Hour

Funzioni statiche n-arie

- Le funzioni statiche sono definite tramite una legge fissa
- Esempio di funzioni statiche sono le usuali operazioni tra numeri
 - +., - , ...
 - Tra booleani AND, ...
 - Sono “standard”
- L'utente può definirne di sue
 - es.: $\max(n,m)$

Concetto di funzione dinamica n-aria

- Alcune funzioni n-arie possono cambiare “valori”
 - **Funzioni dinamiche n-arie**
- Per esprimere dal punto di vista informatico il concetto di funzione, possiamo pensarla come una tabella contenente valori
- Quando si parla di location si può pensare all'indicizzazione di una cella della tabella

Funzione dinamica n-aria

- Esempio
- voto: Studenti-> interi

Funzione:
Intera tabella

Studente	Voto
verdi	18
...	...
Rossi	30

locazione

Aggiorno la funzione, mediante aggiornamenti di locazioni,
Esempio: voto("Rossi") := 30

Asm funzioni vs campi Java

- Le funzioni asm sono simili ai campi Java
- Java:
 - `class Student{ String name...}`
- **Asm:**
 - abstract domain Student
 - controlled name: Student → String

Definizione delle funzioni in AsmetaL

Dichiarazioni di funzioni (`fun_declarations`)

Funzioni statiche	<code>static f: [D ->] C</code>
Funzioni dinamiche	<code>[dynamic] monitored f: [D ->] C</code> <code>[dynamic] controlled f: [D ->] C</code> <code>[dynamic] shared f: [D ->] C</code> <code>[dynamic] out f: [D ->] C</code> <code>[dynamic] local f: [D ->] C</code>

- D e C sono risp. Il dominio ed il codominio di f
- D è opzionale; non va messo se f è 0-aria (cioè una variabile)

Definizione di funzioni – esempio 1

Dichiarazioni di funzioni (`fun_declarations`)

Esempi (Flip_Flop): **variabili**

dynamic controlled `ctl_state : State`

dynamic monitored `high : Boolean`

dynamic monitored `low : Boolean`

Costanti

static `value : Integer`

Altri esempi funzioni n-arie dinamiche (n = 1):

// una funzione che associa un intero ad ogni intero

controlled `votoByID: Integer -> Integer`

// una funzione che dice quali interi sono scelti

monitored `interoscelto: Integer -> Boolean`

demo

Definizione delle funzioni statiche

- Le funzioni statiche vanno prima dichiarate e poi definite
- Le costanti:
 - Va dato il loro valore
- Le variabili statiche di domini astratti rappresentano istanze predeterminate
 - Non vanno definite

```
static angelo: Student
```

Esempio Lift

- Lift: un sistema che gestisce più ascensori
- Ogni ascensore può avere due direzioni, e può essere ferma o in movimento, e può essere in un certo piano

```
abstract domain Lift
enum domain Direction = {UP | DOWN }
enum domain State = {MOVING | HALTED }
dynamic controlled direction : Lift -> Direction
dynamic controlled state : Lift -> State
dynamic controlled floor: Lift -> Floor
```

Esempio 2

signature:

abstract domain BancomatCard

enum domain Pressure_type = {TOO_LOW | NORMAL |HIGH}

monitored currCard: BancomatCard //n. della carta presente nel bancomat

controlled pressure : Pressure_type

Funzioni n-arie (statiche e dinamiche)

- Il dominio delle funzioni n-arie sono n domini
- In questo caso diciamo che il dominio è un prodotto di domini
- in asmetaL:

Prod (d1,d2,...,dn)

d1,...,dn sono i domini del prodotto cartesiano

Esempio:

// static: del massimo

static max: Prod(Integer,Integer) → Integer

// dinamica

controlled voto: Prod(Student,Class) → Integer

Altri domini strutturati

Altri **type-domain** (non dichiarati nella segnatura)

Sequenze	Seq (d) d è il dominio base delle possibili sequenze
Insiemi (dominio di insiemi)	Powerset (d) d è il dominio base dell'insieme delle parti (l'insieme di tutti i possibili insiemi di elementi di d)
	Bag (d) d è il dominio base dei possibili bag (borsa)
	Prod (d1,d2,...,dn) d1,...,dn sono i domini del prodotto cartesiano

Posso definire nuovi domini come strutturati.

Ad esempio: `domain IntList subsetof Seq(Integer)`

Esempi

Dichiarazioni di funzioni (`fun_declarations`) da più domini

```
// for every Lift gives if it is attracted in a directio  
monitored attracted: Prod(Dir, Lift) -> Boolean
```

```
//  
monitored f1: Seq(Integer) -> Boolean
```

```
monitored f2: Seq(Prod(Integer, Boolean))  
// es. f2=[(1,true),(5,false)]
```

```
controlled f3: Boolean -> Prod(Real,Real) //es. f3(true) = (3.0,4.5)
```

```
// given a set of Orders, return the quantity  
static totalQuantity: Powerset(Orders) -> Quantity  
// a constant list of integers  
static list:Seq(Integer) // es. list=[1,2,5,8]
```

Funzioni statiche n-arie

- **Le funzioni statiche n-arie servono per definire delle leggi per il calcolo**
- **Esempio: massimo tra due numeri**
 - `mymax: prod(Integer,Integer) -> Integer`
- Queste funzioni vanno definite prima di poter essere usate
- Psuedo:
 - `mymax(x,y) = if x > y then return x else return y`
- In AsmetaL dobbiamo definire la funzione con una espressione (termine)

DEFINIZIONI

Definizione di domini e funzioni

body è:

definitions :

domain D1 = Dterm1

...

function F1[(p11 in d11,...,p1k1 in d1k1)] = Fterm1

...

[rule_declarations]

[axiom_declarations]

Solo **domini concreti statici** possono essere definiti

Solo **funzioni statiche** possono essere definite

per una regola o assioma, dichiarazione e definizione sono la stessa cosa

Idem **le funzioni derivate**

TERMINI

AsmetaL termini

- In AsmetaL i termini o le espressioni sono del tutto simili alle espressioni dei linguaggi di programmazione
 - Funzioni e relazioni
 - Quelle dalle standard library
 - Es: $3 + 2$
 - $\text{exist } \$x \text{ in Student with voto}(\$x) > 10$
 - Introdotte dall'utente
 - Costanti

Variabili logiche

□ Il primo termine sono variabili logiche

Variabili logiche che non fanno parte dello stato

Si possono usare come termini

$\$v$

ID_VARIABLE logica una stringa che inizia con "\$".

Esempi $\$x$ $\$abc$ $\$pippo$

definitions :

function $F1[(p11 \text{ in } d11, \dots, p1k1 \text{ in } d1k1)] = Fterm1$

□ Esempio una funzione che resituisce se stessa

signature:

static itself : Integer \rightarrow Integer

definitions:

function itself($\$x$ in Integer) = $\$x$

Applicazione di funzioni

[**id .**] **f** [(**t1, ..., tn**)]

□ **dove:**

- **f** è il nome della funzione da applicare
- **(t1, ..., tn)** una tupla di termini
- **id** è il riferimento all'agente (se presente) che detiene la funzione **f**

□ Esempio funzione opposto

signature:

static opposto : Integer → Integer

definitions:

function opp(\$x in Integer) = minus(\$x)

Funzioni matematiche

- Nota: le funzioni matematiche possono essere usate normalmente:

definitions:

`function opp($x in Integer) = -$x`

...

- `max(2,3)`
- `abs(-4)`
- `abs(max(-2,-8))`
- `self.f(5)` o `f(self,5)`

Sequenze e insiemi

Sequence	$[t_1, \dots, t_n]$ con n termini della stessa natura $[]$ per la sequenza vuota
Set	$\{t_1, \dots, t_n\}$ con n termini della stessa natura $\{\}$ per l'insieme vuoto
Bag	$\langle t_1, \dots, t_n \rangle$ con n termini della stessa natura $\langle \rangle$ per il bag vuoto
Map	$\{t_1 \rightarrow s_1, \dots, t_n \rightarrow s_n\}$ con n termini della stessa natura, e S termini della stessa natura pure $\{- \rightarrow \}$ per la mappa vuota

Esempi

- Esempi di termini: sequence, set e bags
- **Set utili a definire concrete domains**

Sequence	<code>["hello","bye"]</code> <code>[[],[1,2]]</code> <code>[1:4] ≡ [1,2,3,4]</code>
Set	<code>{[],[1,2],[1]}</code> <code>{'a','b'}</code> <code>{1:2,0.5} ≡ {1.0,1.5,2.00}</code>
Bag	<code><1,2,1></code> <code><'a','b','a','b'></code> <code><1:10,2> ≡ <1,3,5,7,9></code>

if e let terms

IfTermC	if G then tthen [else telse] endif dove G è un termine booleano, tthen e telse sono termini della stessa natura
---------	--

Usato per definire un valore condizionale tipo operator ?: di Java

LetTerm	let(v1=t1,...,vn=tn)in tv1,...,vn endlet dove vi sono variabili logiche e t1,...,tn,tv1,...,vn sono termini
---------	--

Usato per introdurre nuove variabili „locali“. Queste variabili sono logiche nel senso che non fanno parte dello stato

Esempio temine condizionale e let

```
if $x>0 then 1
else if $x=0 then 0
           else 5
           endif
endif
----
(2x) * (2x)
let ( $double_x = $x+$x )
      in $double_x * $double_x
endlet
```

Comprehension Term

- Se si vogliono definire liste, insiemi... condizionati

variabile

Domini

guardia/condizione

termine

list	$[v_1 \text{ in } S_1, \dots, v_n \text{ in } S_n \mid G_{v_1, \dots, v_n} : t_{v_1, \dots, v_n}]$
set	$\{v_1 \text{ in } D_1, \dots, v_n \text{ in } D_n \mid G_{v_1, \dots, v_n} : t_{v_1, \dots, v_n}\}$
	$\langle v_1 \text{ in } B_1, \dots, v_n \text{ in } B_n \mid G_{v_1, \dots, v_n} : t_{v_1, \dots, v_n} \rangle$
	$\{v_1 \text{ in } D_1, \dots, v_n \text{ in } D_n \mid G_{v_1, \dots, v_n} : t_{v_1, \dots, v_n} \rightarrow s_{v_1, \dots, v_n}\}$

Esempi

La lista con i numeri pari da 1 a 100

```
[ $x in [0..2*$n-1] | $x mod 2=0 : g($x)]
```

```
{ $x in {0..$n} : 2+$x }
```

```
domain Primi100 = {1:100}
```

```
domain Primi100Doppi = { $x in {1:100} : 2 * $x }
```

```
domain Pari100 = { $x in {1:100} | mod($x,2) = 0 : $x }
```

```
function listapari = [ $x in [0:100] | mod($x,2) = 0 : $x ]
```

...

Exists/forall term

- Termini che controllano una condizione su un insieme
- resituiscono true false

Exist Term	(exist v1 in D1,...,vn in Dn with Gv1,...,vn)
ExistUnique Term	(exist unique v1 in D1,...,vn in Dn with Gv1,...,vn)
Forall Term	(forall v1 in D1,...,vn in Dn with Gv1,...,vn)

(exist \$x in {2,5,7} with \$x=2)

(exist unique \$x in X with \$x=0)

Esercizio: funzion che dato un insieme di interi e un intero dice se quel valore è più grande di ogni elemento

Caso di studio - clock

- Definizione dei domini:

`definitions:`

`domain Second={0:59}`

`domain Minute={0:59}`

`domain Hour={0:59}`

REGOLE/TRANSIZIONI DI STATO

ASM transitions

- In matematica le *algebre sono statiche* : non cambiano col passare del tempo.
- In Informatica, gli *stati sono dinamici* : evolvono essendo aggiornati durante le computazioni.
- **Aggiornare stati astratti** (*abstract states*) significa cambiare l'interpretazione delle (o solo di alcune) funzioni della segnatura della macchina.

ASM transitions

- Il modo in cui una macchina ASM aggiorna il proprio stato è descritto da **regole di transizione (transitions rules)** di una certa "forma"
- L'insieme delle regole di transizione di una ASM definiscono la sintassi di un **programma ASM**
- Le *regole di transizione di una ASM sono espressioni sintattiche generate come segue* attraverso l'uso di **costruttori di regole**

Regole

Dichiarazioni (definizioni) di regole (`rule_declarations`)

[macro] rule ID_RULE [(x1 in D1, ..., xn in Dn)] =
rule

Esempio:

ID_RULE = r_Fsm

ID_RULE

una stringa che inizia con "r_".

Esempi: **r_SetMyPerson** **r_update**

rule r_Fsm(\$i in State, \$cond in Boolean, \$rule in Rule, \$j in State) =

```
if ctl_state=$i and $cond
then par $rule
      ctl_state := $j
endpar
endif
```

rule: una regola condizionale

Il Linguaggio Strutturale – main rule

main rule è:

main rule $R = \text{rule}$

R è il nome della main rule

la main rule è sempre una (macro-)regola **chiusa**, cioè senza parametri

rule è proprio il corpo della regola di transizione

Se l'ASM è multi-agent, la main rule deve far partire in parallelo i programmi degli agenti

I programmi degli agenti sono specificati nello stato iniziale (vedi **initialization**)

Skip

- *Skip Rule:*
skip
Significato: non fare niente

Update rule

Update Rule: per aggiornare lo stato della macchina

$f(t_1, \dots, t_n) := t$

dove:

- f è un nome di funzione **dinamica** n -aria di Σ
- t_1, \dots, t_n e s sono termini di Σ
- t è un termine (un valore)

Significato: Nello stato successivo, il valore di f per gli argomenti t_1, \dots, t_n è aggiornato a t . Se f è 0-aria, cioè una variabile, l'aggiornamento ha la forma $c := s$

$f(t_1, \dots, t_n)$

viene detta locazione L

Update rule

Update Rule: aggiornamenti di locazioni

$L := t$

dove t è un termine e L (detta **locazione**) è o un termine funzionale $f(t_1, \dots, t_n)$ con f dinamica e non monitorata, o è una variabile

Significato: Nello stato successivo, la locazione L prende **valore t**

Esempio:

Output := 1

voto(rossi) := 30

Nota: il risultato dell'update si vede solo dopo che sono applicati, cioè nello stato successivo

Esempio - demo

Location Update

- Let $f(a_1, \dots, a_n)$ be a model function
- The pair $\text{loc}=(f, (a_1, \dots, a_n))$ is called *location*
 - memory unit: it saves the value of $f(a_1, \dots, a_n)$ in a given state
- Location *update is the pair:*
$$(\text{loc}, b) = ((f, (a_1, \dots, a_n)), b)$$
 - Firing a location update *means*: update the f interpretation on the arguments a_1, \dots, a_n to value b
- An *update set* is a set of location updates

Conditional Rule

- Serve per condizionare una certa azione:
 - ▣ **if cond then R1 [else R2] endif**
- Dove cond è una condizione booleana, R1 e R2 sono due regole

BlockRule

Per eseguire regole in parallelo

par R1 R2 ... Rn endpar

dove R_1, R_2, \dots, R_n sono regole da eseguire in parallelo

Esempio

Par

a(\$y) := 8

foo := 10

...

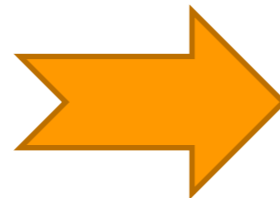
Simulazione

- Il modello di computazione è il seguente:
 1. Nello stato corrente valuta la main rule
 - E da quella le regole chiamate o interne alla main
 2. Valuta le regole che sono abilitate con i loro aggiornamenti
 3. Il valore delle monitorate è chiesto all'ambiente
 - Nel simulatore all'utente
 4. Applica tutti gli update in modo da avere lo stato successivo (nella parte controllata)

Modello computazionale

- **Ad ogni „passo“ (step) vengono lette le variabili monitorate dall'ambiente (chieste all'utente), viene eseguita la main rule e si produce un nuovo stato**
- **L'esecuzione della main rule può richiedere l'esecuzione delle sotto regole**
- **ATTENZIONE: gli update non sono immediati (tranne seq) ma sono fatti alla fine e visibili solo nel nuovo stato**

Stato corrente

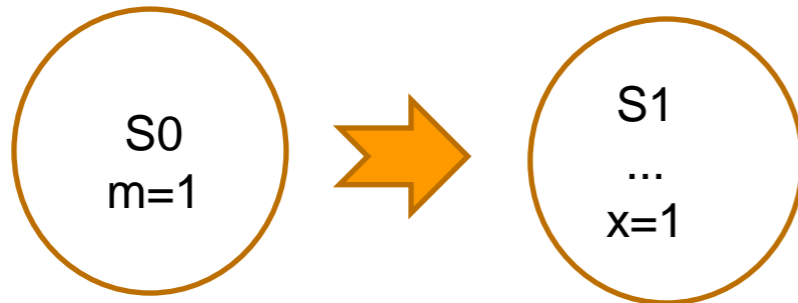


Prossimo stato

Esempio

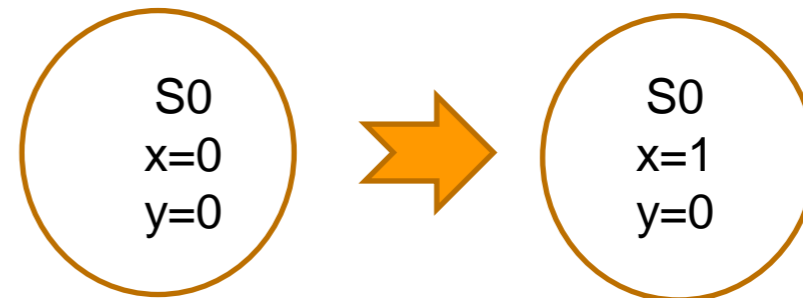
- **Le variabili controllate vengono aggiornate nel prossimo stato**

```
main rule r_main =  
  if m > 0 then  
    x := 1  
  endif
```



- La variabile x **non** viene aggiornata immediatamente

```
main rule r_main =  
  par  
    x := x + 1  
    y := x  
  endpar
```



AdvancedClock

AdvancedClock1

- *Un clock avanzato incrementa ad ogni passo i secondi (e se necessario i minuti e le ore)*

```
domain Second subsetof Integer
domain Second={0..59}
macro rule r_IncMinHours = par
main rule r_AdvancedClock =
par
  if seconds = 59 then r_IncMinHours[] endif
  seconds := (seconds+1) mod 60
endpar
```

AdvancedClock2

Le funzioni monitorate sono aggiornate dall'ambiente

L'ambiente può essere

- Un file
- Lo standard input

AdvancedClock2

- *Come AdvancedClock ma c'è una funzione monitorata signal che incrementa i secondi*

AdvancedClock2

- Monitorato:
 - segnale booleano
- Controllato:
 - Secondi, minuti ed ore
- Comportamento:
 - Se segnale è vero incrementa i secondi (e se necessario minuti e ore in modo corretto)

- Modifica di advancedClock1 ...

Strutturale: inizializzazione

Initialization è una sequenza di stati iniziali:

[**default**] **init** Id :

domain Dd1 = Dterm11

...

function Fd1[(p11 in d11,...,p1s1 in d1s1)] = Ftermd1

...

Uno stato iniziale deve essere denotato come *default*.

Solo **domini concreti dinamici** possono essere inizializzate

Solo **funzioni dinamiche**, non monitorate, possono essere inizializzate

Aggiornamenti Consistenti

- A causa del parallelismo (la regola Block e Forall), una regola di transizione può richiedere più volte l'aggiornamento di una stessa funzione per gli stessi argomenti
- si richiede in tal caso che tali aggiornamenti *siano consistenti*.

DEF: Un update set U è *consistente*, se vale:

if $(f, (a_1, \dots, a_n), b) \in U$ and $(f, (a_1, \dots, a_n), c) \in U$, then $b = c$

Nota che si potrebbero avere degli update inconsistenti:

par

X := 1

X := 2

endpar

Aggiornamenti Consistenti

- Se l'update set U è consistente, allora i suoi **aggiornamenti** possono essere effettivamente eseguiti (*fired*) in un dato stato. Il risultato è un nuovo stato (di arrivo) dove le **interpretazioni** dei nomi **delle funzioni dinamiche** sono cambiati secondo U .
- Le **interpretazioni** dei nomi **delle funzioni statiche** sono gli stessi dello stato precedente (di partenza).
- Le **interpretazioni** dei nomi **delle funzioni monitorate** sono date dall'ambiente esterno e possono dunque cambiare in maniera arbitraria.

Forall rule

Forallrule: per iterare una operazione sugli elementi di un insieme:

forall v_1 **in** D_1, \dots, v_n **in** D_n
with G_{v_1, \dots, v_n} **do** R_{v_1, \dots, v_n}

dove V_i sono variabili, D_i termini che rappresentano domini,
 G_{v_1, \dots, v_n} termine booleano che rappresenta la condizione, e
 R_{v_1, \dots, v_n} è una regola

Esempio:

forall \$s in Student with voto(\$s) = 10 do voto(\$s) := 20

Let rule

- Per introdurre variabili „locali“ usiamo il let

let ($v_1 = t_1, \dots, v_n = t_n$) **in**

R_{v_1, \dots, v_n}

endlet

- **dove** v_1, \dots, v_n **sono variabili (logiche),** t_1, \dots, t_n **sono termini,**
e R_{v_1, \dots, v_n} **è una regola**
- **Le variabili hanno valore solo per lo scope del let**

Macro call rule

Per chiamare un'altra regola

$r [t_1, \dots, t_n]$

dove r è il nome della regola e t_i sono termini che rappresentano gli effettivi argomenti passati

$r[]$

per chiamare una regola che è senza parametri

Esempio

rule $r_1 = \dots$

rule $r_2 = \text{if } c \text{ then } r_1[] \text{ endif}$

Nota: il passaggio dei parametri è per sostituzione. La macro viene espansa (come inline di C++)

Rule constructors macro

- Una *definizione di regola per un nome di regola* r di arietà n è un'espressione

$$r(x_1, \dots, x_n) = R$$

dove R è una regola di transizione.

In una call rule $r[t_1, \dots, t_n]$ le variabili x_i che occorrono nel corpo R della definizione di r vengono sostituite dai parametri t_i (*modularità*)

Choose rule

□ Per implementare delle scelte non deterministiche:

• *Choose Rule:*

choose x **with** φ **do** R

Significato: Esegui R per un x che soddisfa φ

Esempio:

```
choose i in Integer with i > 0 do x:= i*2
```

Illustrare il potere espressivo di “choose” e “forall”

Problema: ordinare un array a

Soluzioni possibili:

- usare una funzione statica, ad es. `qsort`

`a := qsort(a)`

- iterare localmente con swap:

```
choose i,j in dom(a) with (i < j & a(i) > a(j)) do
  par
    a(i) := a(j)
    a(j) := a(i)
  endpar
```

Nota! *Non occorrono variabili di appoggio per lo swap, perchè i nuovi valori degli aggiornamenti saranno disponibili solo nello stato successivo!*

Axioms

Dichiarazioni(definizioni) di assiomi (`axiom_declarations`)

invariant [ID] over id1,...,idn : term

- ID (opzionale) è il nome dell'assioma
- idi sono nomi di domini, funzioni* e regole (con nome) vincolati dall'assioma
- term è un termine che rappresenta l'espressione booleana del vincolo

*In caso di overloading di funzioni, occorre indicare anche il loro dominio, come in $f(D)$ (o $f()$ per funzioni 0-arie) con f nome di funzione e D nome del dominio di f .

ID_AXIOM

una stringa che inizia con "inv_". Esempio: `inv_I1`

Attenzione: prima del main e dopo le rule


Esempio: `axiom inv_neverBoth over high(), low(): not(high and low)`

simulator

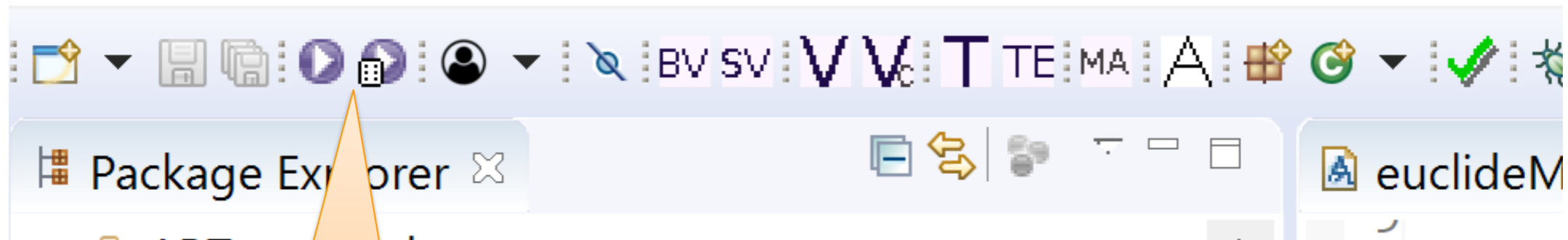


AsmataS

Launch the simulator

 eclipse-workspace - asmetacode/euclideMCD.asm - Eclipse IDE

File Edit Navigate Search Project AsmEE Run Asmeta Window Help



2. Execution
- Interactive
 - random

Simulation trace

```
INITIAL STATE:  
<UpdateSet - 0>  
numB=4  
</UpdateSet>  
<State 1 (controlled)>  
numA=6  
numB=4  
</State 1 (controlled)>  
<UpdateSet - 1>  
numA=2  
</UpdateSet>  
<State 2 (controlled)>  
numA=2  
numB=4  
</State 2 (controlled)>  
<UpdateSet - 2>  
numB=2  
</UpdateSet>
```

```
<State 3 (controlled)>  
numA=2  
numB=2  
</State 3 (controlled)>  
<UpdateSet - 3>  
</UpdateSet>  
<State 4 (controlled)>  
numA=2  
numB=2  
</State 4 (controlled)>  
FINAL STATE:  
numA=2  
numB=2  
run terminated
```

AsmetaS key features

- **Axiom checker**
to check model invariants
- **Consistent Updates checking**
to check for inconsistent updates
- **Random simulation**
random values for monitored functions
 - *Euclide model*

Consistent updates

□ Due to the parallel execution of rules, we require the resulting update set U to be consistent

□ definition:

if $((f, (a1, \dots, an)), b) \in U$ and $((f, (a1, \dots, an)), c) \in U$, the set U is *consistent*, if it is $b = c$

- otherwise, U is *inconsistent* and AsmetaS raises an exception `UpdateClashException` on the inconsistent update locations

Example on inconsistent updates

abstract domain **Orders**

enum domain **Status** = {PENDING | INVOICED | CANCEL}

static o1: Orders

static o2: Orders

static o3: Orders

controlled orderStatus: Orders -> Status

main rule **main** =

par

choose \$o in Orders with true do

orderStatus(\$o) := INVOICED

choose \$oo in Orders with true do

orderStatus(\$oo) := CANCEL

endpar

default init s0:

function orderStatus(\$o in Orders) = PENDING

Model invariants

- Constraints on functions and/or rules
- They must hold in any state
- They are declared in the declaration section by the keyword **invariant over**

invariant over `id_function, ..., id_rule : term`

- In case of invariant violation, AsmetaS raises an exception `InvalidAxiomException`

Simple example

```
asm axiom_example
import ../STDL/StandardLibrary
signature:
  dynamic controlled fooA: Integer
  dynamic controlled fooB: Integer
  dynamic monitored monA: Boolean
  dynamic monitored monB: Boolean
definitions:
  macro rule r_a =
    if(monA) then    fooA := fooA + 1
    endif
  macro rule r_b =
    if(monB) then    fooB := fooB + 1
    endif
invariant over fooA, fooB: fooA!=fooB
```

```
main rule r_main =
  par
    r_a[]
    r_b[]
  endpar
default init s0:
  function fooA = 1
  function fooB = 0
```

Invariant violation

```
Insert a boolean constant for monA:
true
Insert a boolean constant for monB:
true
<State 0 (monitored)>
monA=true
monB=true
</State 0 (monitored)>
<State 1 (controlled)>
fooA=2
fooB=1
</State 1 (controlled)>
Insert a boolean constant for monA:
false
Insert a boolean constant for monB:
true
<State 1 (monitored)>
monA=false
monB=true
</State 1 (monitored)>
<State 2 (controlled)>
fooA=2
fooB=2
</State 2 (controlled)>
<Invariant violation>
neq(fooA,fooB)
</Invariant violation>
Final state:
fooA=2
fooB=2
```

some runs can
violate the
invariant

Ferryman

```
asm ferrymanSimulator

import ../LIB/StandardLibrary

signature:
  enum domain Actors = {FERRYMAN | GOAT | CABBAGE
    | WOLF}
  enum domain Side = {LEFT | RIGHT}
  dynamic controlled position: Actors -> Side
  dynamic monitored carry: Actors
  derived oppositeSide: Side -> Side

definitions:

function oppositeSide($s in Side) =
  if($s = LEFT) then RIGHT
  else LEFT
  endif

rule r_carry($a in Actors) =
  if(position(FERRYMAN)=position($a)) then
  par
    position($a) := oppositeSide(position($a))
    position(FERRYMAN) :=
      oppositeSide(position(FERRYMAN))
  endpar
  endif
```

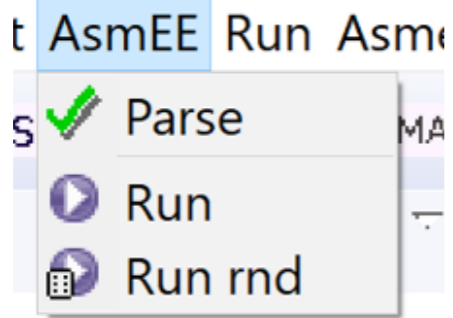
```
rule r_carry($a in Actors) =
  if(position(FERRYMAN)=position($a)) then
  par
    position($a) := oppositeSide(position($a))
    position(FERRYMAN) :=
      oppositeSide(position(FERRYMAN))
  endpar
  endif

//AsmetaL invariants
//Se capra (GOAT) e cavolo (CABBAGE) sono sulla
stessa sponda, allora deve esserci anche il FERRYMAN
invariant over position:
position(GOAT)=position(CABBAGE) implies
position(GOAT)=position(FERRYMAN)
//Se lupo (WOLF) e capra (GOAT) sono sulla stessa
sponda, allora deve esserci anche il FERRYMAN
invariant over position:
position(WOLF)=position(GOAT) implies
position(WOLF)=position(FERRYMAN)

main rule r_Main = r_carry[carry]

default init s0:
function position($a in Actors) = LEFT
```


Simulator options



The image shows the Eclipse Preferences dialog box, specifically the 'Asmee' section. The left sidebar lists various preference categories, with 'Asmeta' expanded to show 'Asmee', 'AsmetaMA', and 'AsmetaSMV'. The main area contains the following settings:

- Preferences for AsmEE**
- Keyword color**: Red color swatch
- Comment color**: Green color swatch
- Variables color**: Magenta color swatch
- Rule color**: Blue color swatch
- Shuffle choose rule
- Check invariants
- Stop simulation if the update set is empty
- Stop simulation if the update set is trivial
- Use prop file for log4j
- Use prop file for log4j**: [Empty text field] **Browse...**
- Debug level for parser**: INFO (dropdown)
- Debug level for simulator**: INFO (dropdown)

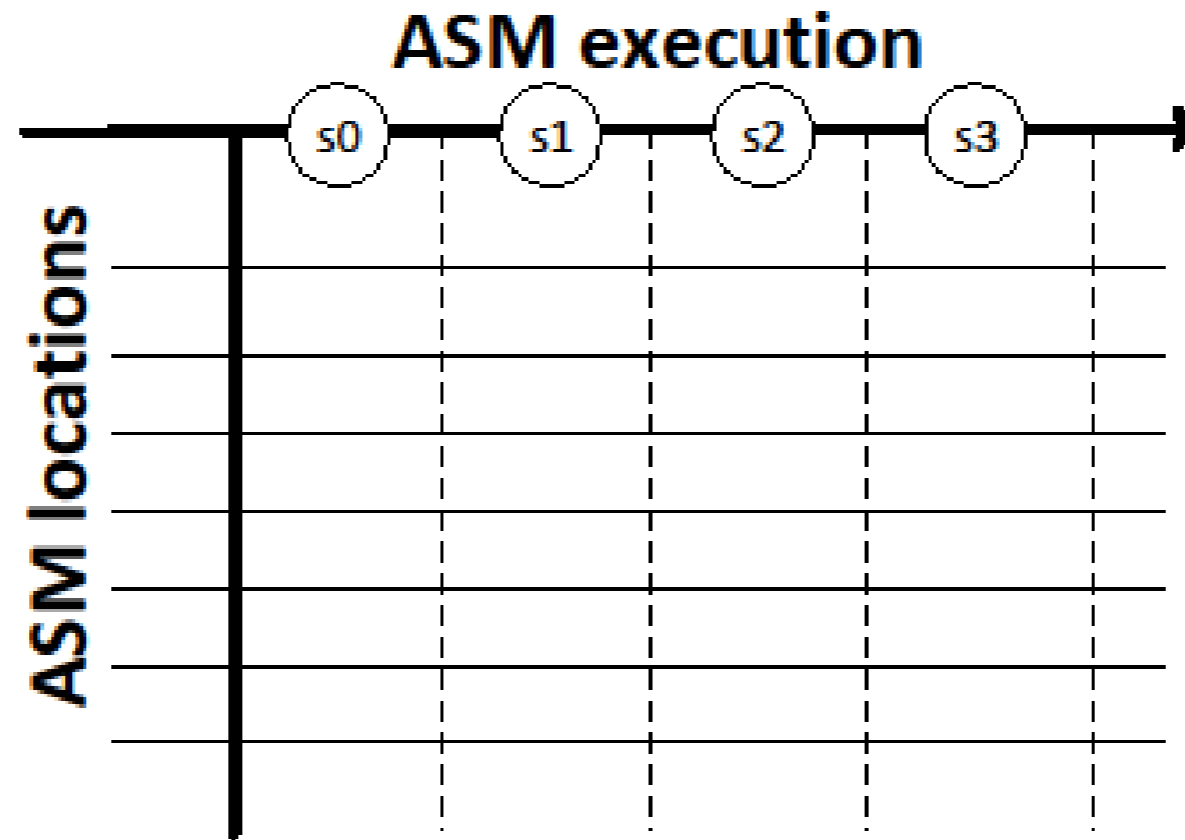
At the bottom of the dialog, there are buttons for 'Restore Defaults', 'Apply', 'Apply and Close', and 'Cancel'. The footer of the dialog reads 'Gargantini & Riccobene - ASMETA - GSSI July 2022'.

Examples


- Euclide MCD
- Ferryman
- Fattoriale
- Tic Tac Toe

ASMETA Animator

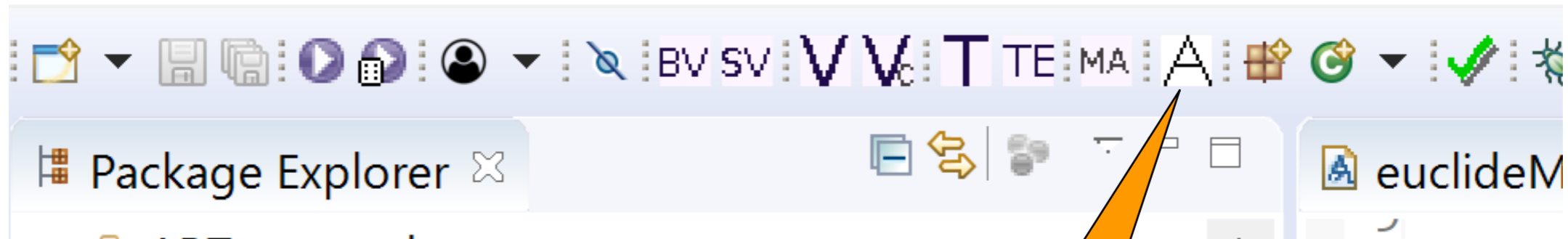
Graphical representation of a simulation



Launch the animator

 eclipse-workspace - asmetacode/euclideMCD.asm - Eclipse IDE

File Edit Navigate Search Project AsmEE Run Asmeta Window Help



animator

ASMETA Animator

The screenshot shows the ASMETA Animator interface. On the left, there are control buttons: "Do one interactive step" (highlighted with a blue box), "Do random step/s", a text input for "Insert random step number" containing "1", and a dropdown for "Invariant violation / exceptions". Below these are buttons for "Move Controlled Functions U", "Move Controlled Functions DO", "Move Monitored Functions U", "Move Monitored Functions DO", and "export to Avalla". The main area contains a table with columns "Type", "Functions", "State 0", and "State 1".

Type	Functions	State 0	State 1
<input type="checkbox"/> ^	M	numAinit	24
<input type="checkbox"/> ^	M	numBinit	18
<input type="checkbox"/> ^	C	numA	24 6
<input type="checkbox"/> ^	C	numB	18 18

```
<State 0 (monitored)>
numAinit=24
numBinit=18
</State 0 (monitored)>
<UpdateSet - 0>
numA=6
</UpdateSet>
<State 1 (controlled)>
numA=6
numB=18
</State 1 (controlled)>
```

Use of the Animator

- Animate an ASM execution
 - euclideMCD.asm
 - ferrymanSimulator.asm

visualizer



AsmataVis

P. Arcaini, S. Bonfanti, A. Gargantini, E. Riccobene.

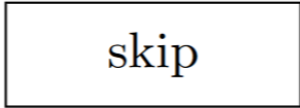
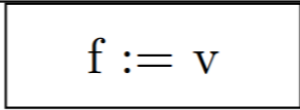


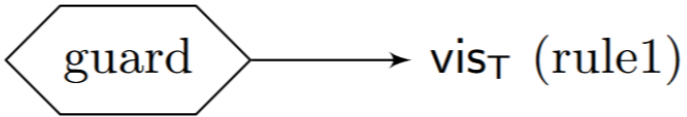
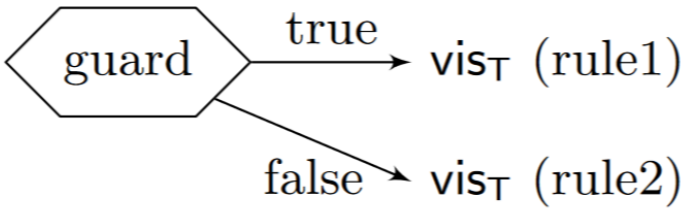
Visual notation and patterns for Abstract State Machines.

In Proc of Human-Oriented Formal Methods (HOFM 2016), 2016

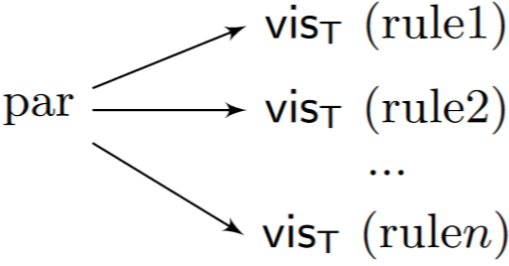
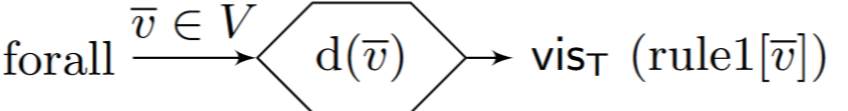
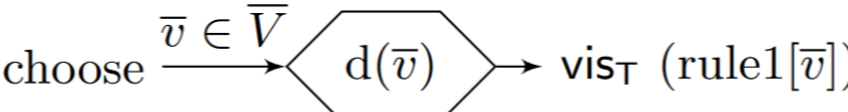
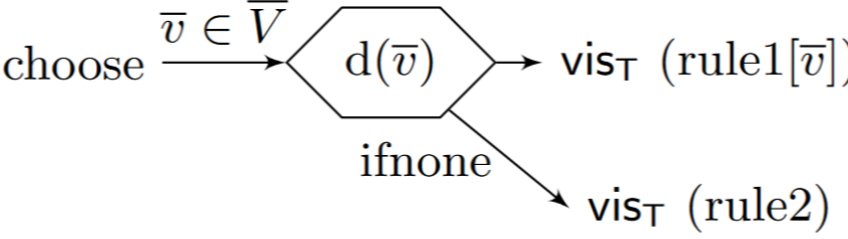
Model visualization

- Visualize a model in terms of a navigable forest of **tree structures**
- It applies:
 - **Structural patterns**
 - useful to visualize the model structure of a compact way
 - **Semantic patterns**
 - Useful when additional information on the machine workflow can be inferred from the model
 - It allows a model visualization in terms of final state machine when a *mode* function is defined and changes over states


Graphical notation

Rule	Visual tree	AsmetaL notation
Skip rule do nothing		skip
Update rule update f to v		$f := v$
Macro call rule		r_rule[]
invoke rule r_rule with arguments \bar{v} (if any)		r_rule[\bar{v}]
Conditional rule execute $rule1$ if $guard$ holds, otherwise execute $rule2$ (if given)	 	if guard then rule1 endif if guard then rule1 else rule2 endif

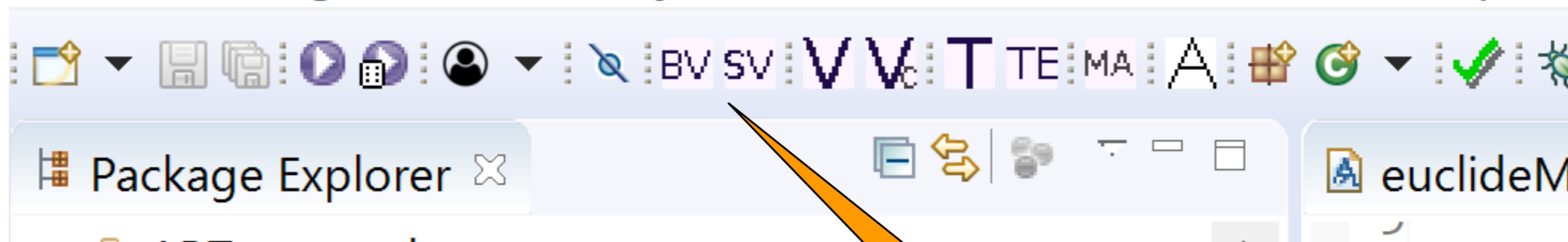
Graphical notation

<p>Block rule execute <i>rule1</i> ... <i>ru1en</i> in parallel</p>		<p>par rule1 rule2 ... ru1en endpar</p>
<p>forall rule execute <i>rule1</i> with all values $\bar{v} \in \bar{V}$ for which $d(\bar{v})$ holds</p>		<p>forall $\bar{v} \in \bar{V}$ with $d(\bar{v})$ do rule1[\bar{v}]</p>
<p>Choose rule execute <i>rule1</i> with a $\bar{v} \in \bar{V}$ for which $d(\bar{v})$ holds. If no such \bar{v} ex- ists, execute <i>rule2</i> (if given)</p>		<p>choose $\bar{v} \in \bar{V}$ with $d(\bar{v})$ do rule1[\bar{v}]</p>
<p>Let rule execute <i>rule1</i> substi- tuting \bar{t} for \bar{x}</p>		<p>let $(\bar{x} = \bar{t})$ in rule1[\bar{x}] endlet</p>

Launch the visualizer

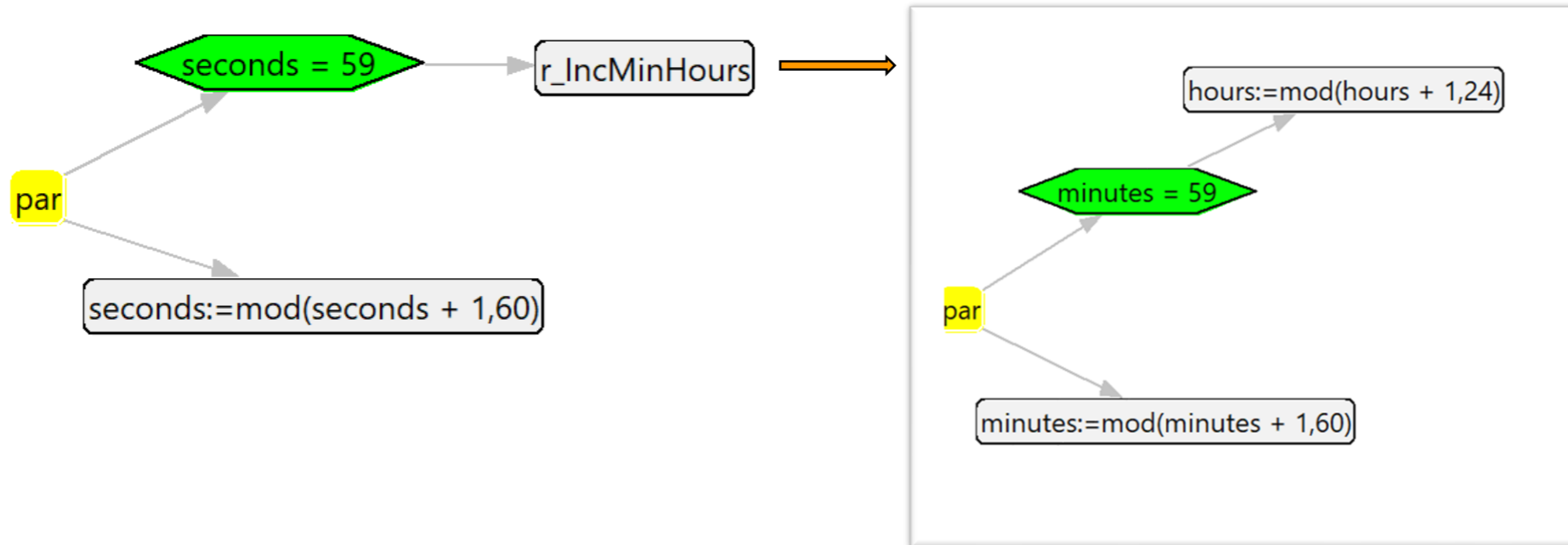
 eclipse-workspace - asmetacode/euclideMCD.asm - Eclipse IDE

File Edit Navigate Search Project AsmEE Run Asmeta Window Help

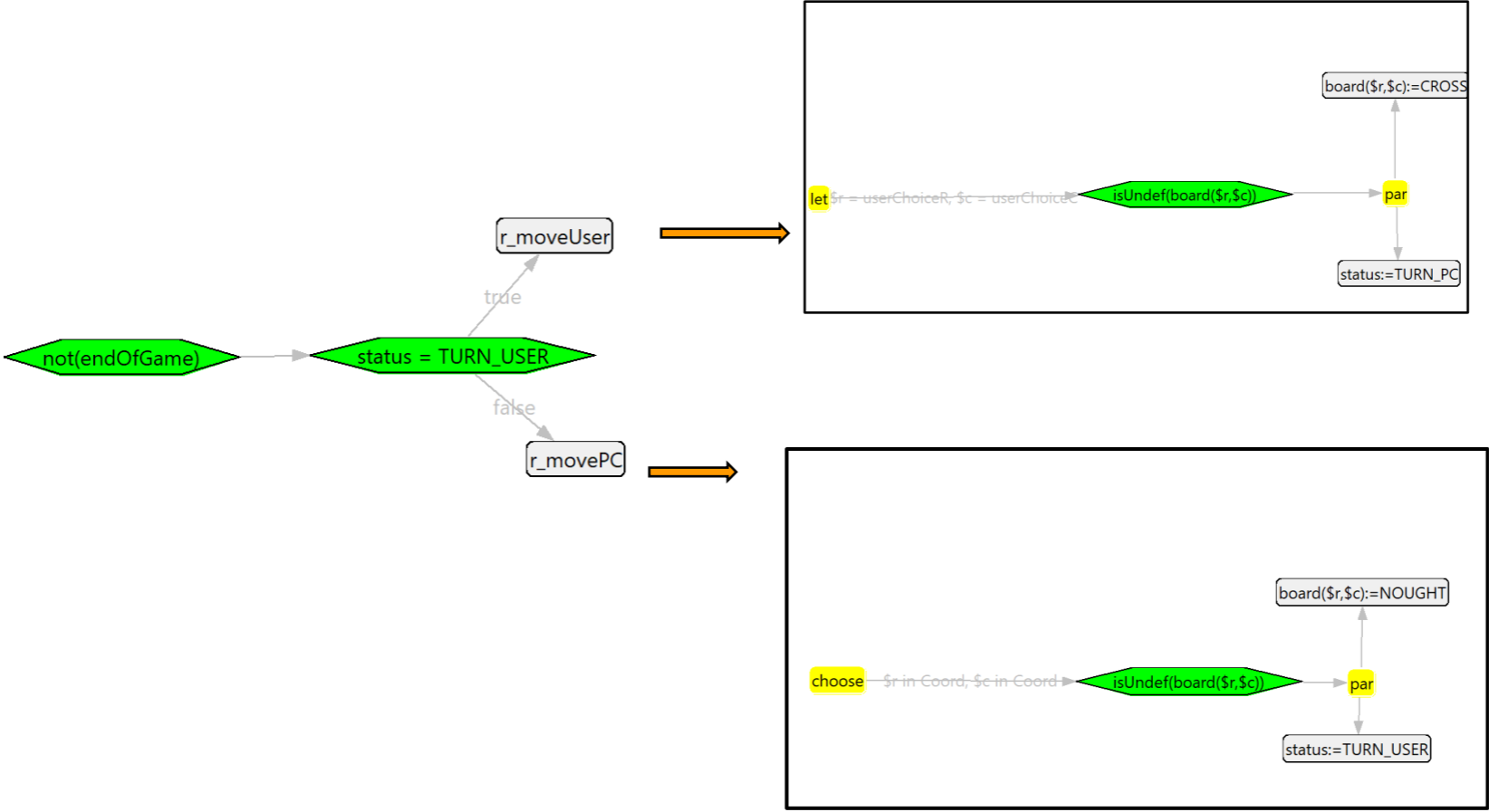


BV: basic
SV: semantic

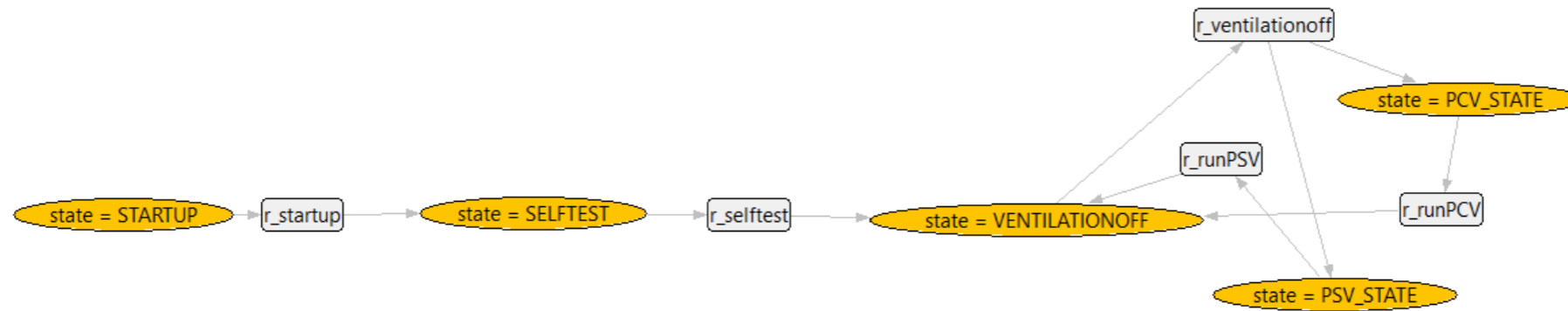
Advanced clock model



Tic Tac Toe visualization



Semantic model: MVM controller



```
...
main rule r_Main =
```

```
  par
```

```
    //transition from startup to selftest
```

```
    if state = STARTUP then
```

```
      r_startup[]
```

```
    endif
```

```
    //transition from selftest to ventilation off
```

```
    if state = SELFTEST then
```

```
      r_selftest[]
```

```
    endif
```

```
    //start ventilation, either pcv or psv
```

```
    if state = VENTILATIONOFF then
```

```
      r_ventilationoff[]
```

```
    endif
```

```
    //transition from PCV to ventilation off if requested
```

```
    if state = PCV_STATE then
```

```
      r_runPCV[]
```

```
    endif
```

```
    //transition from PSV to ventilation off if requested
```

```
    if state = PSV_STATE then
```

```
      r_runPSV[]
```

```
    endif
```

La tesi ASM

The ASM thesis is that any algorithm can be modeled at its natural abstraction level by an appropriate ASM. (Gurevich, 1985)

Sequential thesis:

Sequential ASMs capture sequential algorithms. (Gurevich, 2000)

Parallel thesis:

ASMs capture parallel algorithms. (Blass/Gurevich, 2003)

... ?

ASM Distribute (o multi-agenti)

- Agenti computazionali
- Stati globali condivisi tra gli agenti
- Movimenti concorrenti sincroni/asincroni

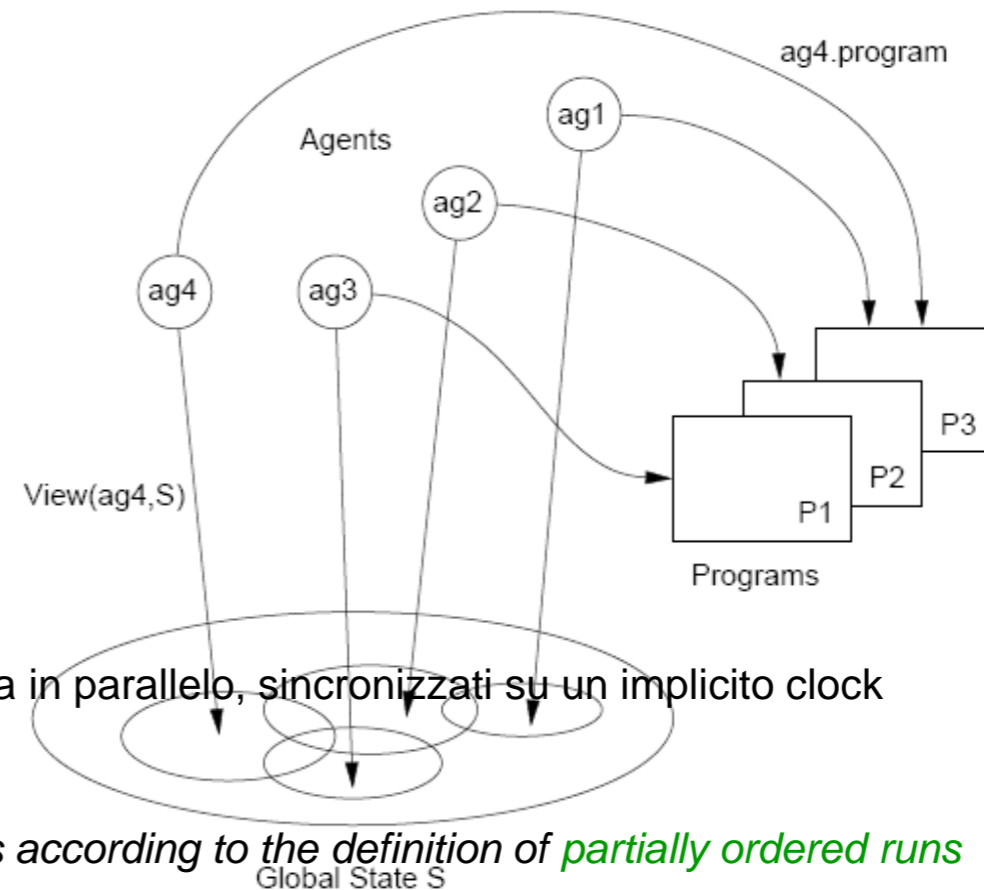
Una *sync/async ASM* è una famiglia di coppie $(a, ASM(a))$ di agenti $a \in Agent$

- (il dominio degli agenti)
- programmi ASM (a)
- di ASM di base (sequenziali)
- $f(self, x)$ per una $f : A \rightarrow B$,
- denota la *versione privata di $f(x)$*
- dell'agente corrente $self$.
- La dichiarazione di f diventa $f : Agent \times A \rightarrow B$

In una *sync ASM* gli agenti eseguono il loro programma in parallelo, sincronizzati su un implicito clock globale del sistema.

Asynchronous computation model (Gurevich, 1995)

*Semantic model resolves potential conflicts according to the definition of *partially ordered runs**



Riferimenti bibliografici

- **ASM Web Site** <http://www.eecs.umich.edu/gasm>
<http://www.di.unipi.it/~boerger>
- **Abstract State Machines Research Center**
<http://rotor.di.unipi.it/AsmCenter/Lists/AboutLinks/AllItems.aspx>
- **Libro ASM** E. Boerger and R. Staerk. *Abstract State Machines: A Method for High-Level System Design and Analysis*. Springer Verlag, 2003.
<http://www.di.unipi.it/AsmBook/>
- **ASM Survey** E. Börger High Level System Design and Analysis using ASMs LNCS Vol. 1012 (1999), pp. 1-43
- **ASM History** E. Börger The Origins and the Development of the ASM Method for High Level System Design and Analysis. J. Universal Computer Science 8 (1) 2002
- **Original ASM Definition** Y. Gurevich Evolving algebra 1993: Lipari guide. Specification and Validation Methods. (Ed.E. Börger) OUP 1995
- **Libro sul caso di studio Java-ASM** R. Stärk, J. Schmid, E. Börger. Java and the Java Virtual Machine: Definition, Verification, Validation. Springer-Verlag 2001.
<http://www.inf.ethz.ch/~jbook>