Modelling with Event-B

Dominique Méry
LORIA & Telecom Nancy
Université de Lorraine
https://members.loria.fr/Mery
dominique-dot-mery-at-loria-dot-fr

March 3, 2025

1 Event-B Models for Correct-by-ConstructIon Sequential Algorithms

1.1 Computing the sum of elements of a vector.

Rodin Archive for the algorithm computing the sum of elements of a vector.

- Rodin Archive for the algorithm computing the sum of elements of a vector in pdf

1.2 Incrementing a positive value

Rodin archive for the algorithm *incrementing a positive value.*

Rodin archive for the algorithm *incrementing a positive value. in pdf*

1.3 Maximum of two integer values

Rodin archive for the algorithm *maximum of two integer values*

Rodin archive for the algorithm *maximum of two integer values*

Here's an example of using the lstlisting environment from the listings package:

```
import numpy as np

def incmatrix(genl1,genl2):
    m = len(genl1)
    n = len(genl2)
    M = None #to become the incidence matrix
    VT = np.zeros((n*m,1), int)  #dummy variable

    #compute the bitwise xor matrix
    M1 = bitxormatrix(genl1)
```

```
---------- MODULE TLASAFETY  ---------
EXTENDS Integers, Naturals, TLAPS
------------------------------
VARIABLES x
------------------------------
a ==  x \geq 0 /\ x' = x +1
------------------------------
Init == x=-1
Next == a  \/ x'=x
------------------------------
Spec == Init /\ [] [Next]_<<x>>
------------------------------
Typing ==  x \in Int
Safe1 == x = -1
Safe2 ==  x \leq 0
InductiveInvariant == Typing /\ Safe1
i == InductiveInvariant
------------------------------
THEOREM InitProperty == Init => InductiveInvariant
<1>SUFFICES ASSUME Init
PROVE  InductiveInvariant
OBVIOUS
<1>1. x=-1 BY  DEF Init
<1>2. QED
BY <1>1, SMT DEFS InductiveInvariant,Init, Safe1, Typing


==================
```

```
machine ex1spec sees ex1domain

variables x done

invariants
@inv1 x : Z & done : BOOL
  @inv2 done = TRUE  => x = x0 + 1

events
  event INITIALISATION
    then
  @act1 done:=FALSE
      @act2 x:=x0
  end

  event evt1
    where
      @grd1 done=FALSE
    then
      @act1 x := x0+1
      @act2 done:=TRUE
  end
end
```

1.4 List of square of natural values until a given number

Rodin archive for the algorithm *list of square of natural values until a given number*

Rodin archive for the algorithm *list of square of natural values until a given number* in pdf

Rodin archive for the algorithm *computing the power 2 of a natural number with only additions.* in pdf

Rodin archive for the algorithm *computing the power 12 of a natural number with only additions.* in pdf