Tutorial Modelling Software-based Systems
...
Tutorial 3 : Developing systems by refinement
Dominique Méry
26 septembre 2025

Exercice 1 *ggx1-tut3*
We consider the following Event-B machine and the machine is parametrized by the assertion $I(x)$ which is the invariant. The questions will consider several cases for the invariant $I(x)$.

MACHINE QUESTION
VARIABLES
x
INVARIANTS
$I(x)$
EVENTS
EVENT *INITIALISATION*
BEGIN
$act1 : x := -12$
END
EVENT *evt1*
WHEN
$grd1 : x \geq -6$
THEN
$act1 : x := x+1$
END
END

EVENT *evt2*
WHEN
$grd1 : x \leq -1$
$grd2 : x \geq -37$
THEN
$act1$: $x := x-1$
END
EVENT *evt3*
WHEN
$grd1 : x \leq -2$
$grd2 : x \geq -4$
THEN
$act1$: $x := x-1$
END
EVENT *evt4*
WHEN
$grd1 : x \leq -15$
THEN
$act1$: $x := x+1$
END
END

We consider several cases for defining the invariant and we have to consider the correctness of the proposed invariant. For every question, you should check that the assertion is either an invariant or a theorem or neither an ibvariant nor a theorem.
You can use the Rodin platform or you can use a formal justification.

Question 1.1

$$inv1 : x \in \mathbb{Z}$$
$$inv3 : x \leq -10$$

Question 1.2

$$inv1 : x \in \mathbb{Z}$$
$$inv3 : x \leq -1$$

Question 1.3

$$inv1 : x \in \mathbb{Z}$$
$$inv3 : x \leq -12$$
$$inv3 : x \geq -38$$

Question 1.4 *Propose an invariant $I(x)$ which is exactly characterizing the set of reachable states of the machine QUESTION or equivalently , the strongest invariant for the machine QUESTION. Explain why it is the strongest invariant of the machine QUESTION. The property to be the strongest invariant means that if $J(x)$ is another invariant, then $I(x) \Rightarrow J(x)$.*

Question 1.5 *In the last question, you derive an invariant $I(x)$ but now you should prove or disprove that the model QUESTION is deadlock-free.*

Exercice 2 *ggx2-tut3*
We consider the general problem of access control with the administration of access rights.

1. *Model the access control problem in the case of the access of persons in buildings. We assume that the rights are given and are not modified.*
2. *Model the access control problem by adding specific actions for administrating access rights.*