Cours MCFSI

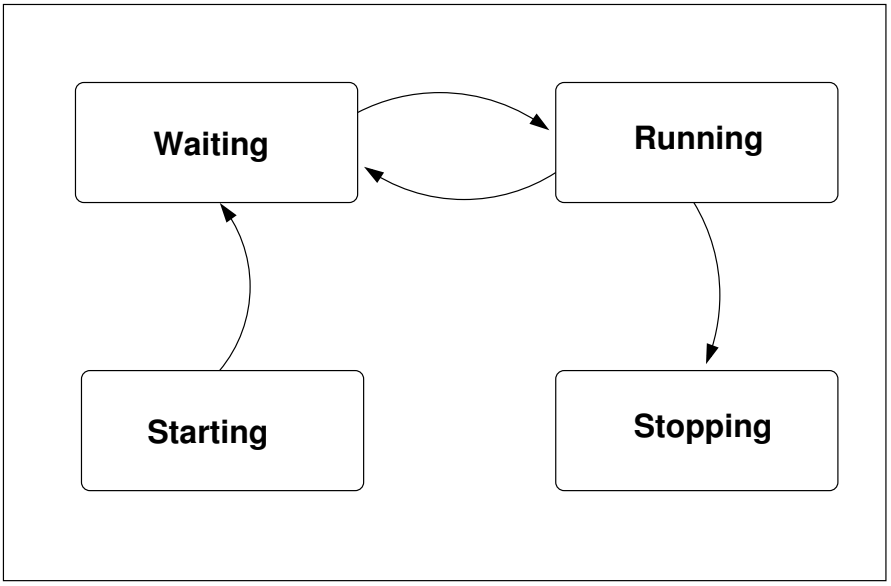
...

Spécifier un problème en Event-B

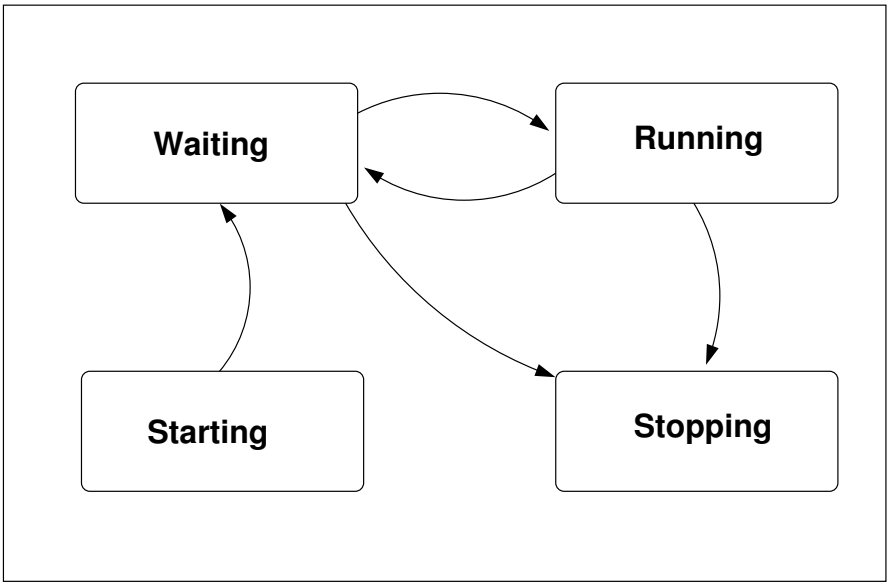
Dominique Méry

21 octobre 2024

Exercice 1 *mcfsi1-ex1-tut1.zip*
Traduire cette machine sous la forme d'une machine Event-B.



Exercice 2 *mcfsi1-ex2-tut1.zip*
Traduire cette machine sous la forme d'une machine Event-B.



Exercice 3 *(mcfsi1-simple)*
Soient deux ensembles A et B qui sont des parties de U.

- *Ecrire un modèle Event-B qui utilise deux variables v et w deux sous-ensembles de A et B*
- *Ajouter une fonction partielle de A dans B.*

— *Définir un événement e1 qui transfert un élément de A dans B s'il n'est pas dans A.*
— *Définir un événement e2 qui crée un lien entre un élément de A et un élément de B.*

Exercice 4 *(mcfsi1-variant)*
Un système permet de réaliser la somme de deux nombres x0 et y0 en ajoutant une unité à une variable z. Il comprend un événement incx2z qui décroit la valeur de x d'une unité et quio augmente la valeur de z de une unité et un événement incy2z qui décroît y d'une unité et qui augmente z d'une unité. Le processus global s'arrête quand les deux variables x et y sont nulles. Ecrire un modèle Event-B qui modélise ce système.

Exercice 5 *(mcfsi1-summation)*
Soit une suite de valeurs entières $v_1, \ldots, v_n$ où le nombre n est fixé. Ecrire une spécification événementielle décrivant le calcul de la somme des éléments de cette suite. Pour cela, vous devez décrire les données puis l'événement magique qui réalise ce calcul.

Exercice 6 *(mcsfi-ressources-pb1),*
Modéliser les problèmes suivants.

Question 6.1 *(mcsfi-ressources-pb1)*
On suppose disposer de ressources qui sont partagées par un ensemble de processus. Si un processus a besoin d'une ressource, il demande cette ressource et s'il n'a plus besoin de cette ressource, il la rend. Un processus peut utiliser plusieurs ressources à la fois mais une ressource ne peut pas être utilisée par deux processus à la fois.

Question 6.2 *(mcsfi-ressources-pb2)*
On suppose disposer de ressources qui sont partagées par un ensemble de processus. Si un processus a besoin d'une ressource, il demande cette ressource et s'il n'a plus besoin de cette ressource, il la rend. Un processus ne peut utiliser qu'une seule ressources à la fois et une ressource ne peut pas être utilisée par deux processus à la fois.

Exercice 7 *(mcfsi1-invariantssafety)*
Nous considérons le modèle suivant.

MACHINE $M1$
VARIABLES
x
INVARIANTS
...
EVENTS
EVENT *INITIALISATION*
BEGIN
$act1 : x := -10$
END
EVENT *evt1*
WHEN
$grd1 : x \geq -1$
THEN
$act1 : x := x+1$
END
EVENT *evt2*
WHEN
$grd1 : x \leq -1$
$grd2 : x \geq -44$
THEN
$act1 : x := x-1$
END
END

On considère plusieurs cas pour l'invariant.

Question 7.1 *(M1)*

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

Est-ce que toutes les conditions de vérification sont prouvées par le prouveur de l'application Rodin ? Expliquez clairement pourquoi elles sont prouvées ou non.

Question 7.2 *(M2)*

$inv1 : x \in \mathbb{Z}$
$inv3 : x \leq -3$

Est-ce que toutes les conditions de vérification sont prouvées par le prouveur de l'application Rodin ? Expliquez clairement pourquoi elles sont prouvées ou non.

Question 7.3 *(M3)*

$inv1 : x \in \mathbb{Z}$
$inv4 : -45 \leq x \wedge x \leq -10$

Est-ce que toutes les conditions de vérification sont prouvées par le prouveur de l'application Rodin ? Expliquez clairement pourquoi elles sont prouvées ou non.

Question 7.4 *(M4)*

$inv1 : x \in \mathbb{Z}$
$inv3 : x \leq -3$
$inv4 : -45 \leq x \wedge x \leq -10$
$inv2 : x \leq -1$

Est-ce que toutes les conditions de vérification sont prouvées par le prouveur de l'application Rodin ? Expliquez clairement pourquoi elles sont prouvées ou non.

Exercice 8 Question 8.1 *On suppose que les variables sont x, t et que $x \in \mathbb{Z}$ et $t \in 1..K \to \mathbb{Z}$. K est une constante entière strictement plus grande que 15.*
Ecrire un événement E2 qui modélise la transformation décrite comme suit :

Quand l'événement E2 est observé, la variable x est égale au produit des valeurs de t avant l'observation et la valeur de t n'est pas modifiée. On suppose que l'expression $\prod_{i=a}^{b} f(i)$ désigne le produit des éléments du tableau $f \in u..v \to \mathbb{Z}$ avec $a, b \in u..v$ et $a \leq b$.

Question 8.2 *. Soit un tableau $t \in 1..n \to \mathbb{N}$ dont la dimension est $n \in \mathbb{N}$ différent de 0. On suppose que m et i sont deux variables entières.*
Ecrire un événement E3 qui modélise l'affectation à la variable m d'une valeur plus grande que 57 et plus petite que 151 stockée dans le tableau t et qui affecte à i la valeur de l'indice où est stockée cette valeur dans le tableau t. Il est possible que plusieurs valeurs conviennent et il faut en choisir une qui convient.

Question 8.3 *On se donne un graphe $G = (N, R)$ où N est un ensemble fini de nœuds et R est une relation binaire sur N ($R \subseteq N \times N$). On suppose que CR est la fermeture ou clôture transitive de R ($CR \subseteq N \times N$, $CR; R \subseteq CR$ et $R \subseteq CR$).*
Soit une variable sol ($sol \in \mathbb{B}ool$). On se donne deux sommets a et b distincts. Ecrire un événement E4 affectant à sol la valeur vraie s'il existe un chemin de a vers b selon R et faux sinon.

Exercice 9 *mcfsi1-ex9.zip*
Soit la machine suivante.

MACHINE QUESTION
VARIABLES
x
INVARIANTS
$I(x)$
EVENTS
EVENT *INITIALISATION*
BEGIN
$act1 : x := -23$
END
EVENT *evt1*
WHEN
$grd1 : x \in 12..45$
THEN
$act1 : x := x+789$
END
END

EVENT *evt2*
WHEN
$grd1 : x \leq -12$
THEN
$act1 : x := x+2$
END
EVENT *evt3*
WHEN
$grd1 : x > -25$
THEN
$act1 : x := x-1$
END
END

On rappelle que une propriété $I(x)$ est inductivement invariante si $Init(x) \Rightarrow I(x)$ et pour tout événement e, $I(x) \wedge BA(e)\S x, x') \Rightarrow I(x')$. $BA(e)(x, x')$ désigne la relation before-after nde l'événement e.
On rappelle qu'une propriété $J(x)$ est simplement invariante, si $J(x)$ est vraie pour tous les états du système.

Question 9.1 *Ecrire la définition $BA(e)(x, x')$ pour les événements evt1, evt2, evt3.*

Nous allons étudier des solutions pour $I(x)$. Pour chaque question, vous devez préciser si l'assertion est inductivement invariante ou simplement invariante.

Question 9.2
$inv1 : x \in \mathbb{Z}$
$inv12 : x \in -25..-5$

Question 9.3
$inv1 : x \in \mathbb{Z}$
$inv12 : x \in -25..-17$

Question 9.4
$inv1 : x \in \mathbb{Z}$
$inv12 : x \in -30..0$

Question 9.5
$inv1 : x \in \mathbb{Z}$
$inv12 : x \in -25..-10$

Question 9.6
$inv1 : x \in \mathbb{Z}$
$inv12 : x \in -24..-10$

Exercice 10 *ex8-tut1.zip*
A semaphore s is a shared variable accessible by two operations : $P(s)$ and $V(s$. Informally, we can describe the effect of these two operations as follows :

— *$P(s)$ is testing if the value of s is greater than 0 and is not equal to 0. Il the value of s is 0, the process which is executing $P(s)$ is inserted in a queue.*

— $V(s)$ *is increasing the value of* s *by one, if the queue is non empty. If the queue is non empty, the first waiting process of the queue is awaken and becomes a lively process.*

Using the Event B modelling features, describe a system using the primitives.