Département SN – 3ème Année. 2019-2020

Développements formels de systèmes complexes

16 Janvier 2020.

Durée 1h30

Documents autorisés

Partie 1. Questions de cours

La méthode B propose de décrire des spécifications de systèmes comprenant des variables, des invariants, une initialisation des variables ainsi que des évènements.

A. Qu'est-ce qu'une obligation de preuve ?

B. Comment ces obligations de preuve sont-elles générées ?

C. Quel est le rôle de l'invariant dans la spécification de propriétés de systèmes ?

D. Le maintien des invariants par l'évènement d'initialisation et par chaque évènement d'une machine permet de garantir le maintien de cet invariant pour tous les comportements décrits par cette machine. Expliquer pourquoi.

E. Lorsqu'un variant est introduit, il doit décroitre grâce aux évènements dit "convergents". Quelles sont les obligations de preuve du variant associées à ces évènements ?

Il est demandé de répondre en quelques lignes seulement.

Partie 2. Une machine Event-B

On veut spécifier un système de gestion d'employés. Les employés appartiennent à un ensemble d'employés $EMPLOYES$ (type) définis dans un contexte $Emp\_Definitions$ comme suit.

CONTEXT
$Emp\_Definitions$
SETS
$EMPLOYES$
END

Un ensemble d'employés *employes* est défini dans l'état (clause *variables*) de ce système. Il est possible d'obtenir le salaire et l'âge d'un employé par les applications *salaire* et *age* également définies dans l'état (clause *variables*) de ce système.

Les évènements suivants sont introduits.

— embaucher est un évènement qui crée un nouvel employé d'âge supérieur à 18 et de salaire 10 000. Cet employé fait partie de l'ensemble des employés lorsqu'il est embauché ;
— augmenter_salaire : a pour effet d'ajouter une valeur de salaire au salaire d'un employé.

À l'initialisation, l'ensemble des employés noté *employes* est vide.

MACHINE
$Travail$
SEES
$Emp\_Definitions$
VARIABLES
$employes, salaire, age$
INVARIANT
INV1 : $employes \subseteq EMPLOYES$
INV2 : $age \in employes \longrightarrow NAT$
INV3 : $salaire \in employes \longrightarrow NAT$
...
INITIALISATION
$employes, age, salaire := \emptyset$
EVENTS
$embaucher = \ldots$

$augmenter\_salaire = \ldots$

Questions

1.1. Compléter la machine abstraite B Travail en écrivant un invariant inv4 qui indique que l'âge de tout employé est compris entre 18 et 65 et que le salaire de tout employé est supérieur à 10 000.

1.2. Compléter la machine abstraite B Travail en exprimant la spécification formelle des évènements embaucher, et augmenter_salaire. Vous veillerez à respecter l'invariant dans cette spécification.

1.3. Ecrire les deux obligations de preuve d'invariants associées aux évènements embaucher et augmenter_salaire.

1.4. Justifier, en quelques lignes ou par une démonstration, la correction des évènements définis en question 1.2 par rapport à l'invariant proposé en question 1.1.

Partie 3. Un raffinement Event-B

On souhaite prendre en compte l'ancienneté d'un employé pour les augmentations de salaires et le départ à la retraite. Pour cela, on se propose de définir une machine de raffinement Travail_Ref de la machine abstraite Travail en

— supposant que le maximum d'employés dans cette entreprise est de 50.
— introduisant une nouvelle variable d'état anciennete qui associe l'ancienneté (en nombre d'années travaillées) à chaque employé. L'ancienneté d'un employé nouvellement embauché vaut 0. L'ancienneté ne peut pas dépasser 45

— définissant un événement augmenter_anciennete qui augmente d'une année l'ancienneté de chaque employé
— définissant un évènement retraite qui retire un employé de l'ensemble des employés embauchés lorsque l'ancienneté est égale ou dépasse 42 ans ou que l'âge dépasse 65 ans
— raffinant les évènements de la machine travail sachant que le salaire d'un employé est augmenté, d'un montant positif, seulement tous les 5 ans
— supposant qu'un employé embauché ne quitte son emploi qu'en partant à la retraite.

Ce raffinement correspond à la machine donnée ci-dessous.

MACHINE
$Travail\_Ref$
REFINES
$Travail$
SEES
$Emp\_Definitions$
VARIABLES
$employes, salaire, age,$ **anciennete**
INVARIANT
INV1 : $employes \subseteq EMPLOYES$
INV2 : $age \in employes \longrightarrow NAT$
INV3 : $salaire \in employes \longrightarrow NAT$
...
INITIALISATION
$employes, age, salaire,$ **anciennete** $:= \emptyset$
EVENTS
$embaucher =$
refines embaucher
...

$augmenter\_salaire =$
refines augmenter_salaire
...

augmenter_anciennete = ...

retraite = ...

Questions

2.1. Compléter les invariants de la machine Travail_Ref en prenant en compte les exigences décrites ci-dessus

2.2. Compléter les définitions des 4 évènements de la machine de raffinement Travail_Ref

2.3. Donner l'obligation de preuve de correction du raffinement de l'évènement augmenter_salaire

2.4. Le raffinement obtenu est-il correct ? Justifier votre réponse.