INP ENSEEIHT

Département Sciences du Numériques
Parcours "Systèmes Logiciels"
3ème Année. 2020-2021

Développement formel de systèmes complexes

19 Mars 2021.

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. Une obligation de preuve déchargée (prouvée), peut-elle être considérée comme un théorème ?

B. Expliquer pourquoi les obligations de preuve peuvent-elles être générées automatiquement ?

C. Quel mécanisme de preuve est associé à la preuve d'un invariant ?

D. Une machine décrit des invariants et des théorèmes. Tout deux décrivent des propriéts de la machines. Pourquoi théorèmes et invariants ont-ils été différenciés ?

E. Lorsqu'un variant est introduit, il doit décroitre grâce aux évènements dit "convergents". Quelles propriétés peut-on garantir grâce à la présence d'un variant décroissant ?

F. Le raffinement établit une relation de simulation entre deux machines. Expliquer le rôle de la relation de simulation ?

Il est demandé de répondre en quelques lignes seulement.

Pour les parties 2 et 3, si vous souhaitez introduire des précisions, veuillez les décrire dans votre copie.

Partie 2. Une machine Event-B

On veut spécifier un système de réservation. Les passagers appartiennent à un ensemble passagers $PASSAGERS$ défini dans un contexte $TICKETS\_RESERVATIONS$. Un second ensemble $VILLES$ est défini, il caractérise les ville origine et destination d'un billet. Le contexte suivant est défini.

CONTEXT
$TICKETS\_RESERVATIONS$
SETS
$PASSAGERS$
$VILLES$
END

L'objectif du modèle consiste à définir un système de réservation de billets d'avion avec possibilité de réserver ou d'annuler un voyage. La machine Event-B *Voyage* ci-dessous décrit ce modèle.

Un ensemble de *passagers* est défini dans la clause VARIABLES de cette machine. Il est possible d'obtenir le prix d'un billet, l'âge d'un passager ainsi que l'origine et la destination d'un passager par les applications *prix*, *age*, *origine* et *destination* également définies dans la clause VARIABLES de cette machine.

À l'initialisation, les ensembles *passagers*, *age*, *prix*, *origine* et *destination* sont vides.

MACHINE
Voyage
SEES
$TICKETS\_RESERVATIONS$
VARIABLES
$passagers, age, prix, origine, destination$
INVARIANT
INV1 : $passagers \subseteq PASSAGERS$
INV2 : $age \in passagers \longrightarrow NAT$
INV3 : $prix \in passagers \longrightarrow NAT$
INV4 : $origine \in passagers \longrightarrow VILLES$
INV5 : $destination \in passagers \longrightarrow VILLES$
...
INITIALISATION
$passagers, age, prix, origine, destination := \emptyset$
EVENTS
Réserver_billet = ...

Annuler_billet = ...

Les évènements suivants sont introduits.
— Réserver_billet permettent de réserver un billet pour un passager donné
— Annuler_billet pour annuler le billet d'un passager ayant déjà réservé un billet.

Questions

2.1. Compléter la machine abstraite Voyage en écrivant un invariant INV6 qui indique que l'origine et la destination d'un billet donné ne sont pas identiques.

2.2. Compléter la machine abstraite Voyage en exprimant la spécification formelle des 2 évènements Réserver_billet et Annuler_billet.
Vous veillerez à respecter les invariants de ce modèle.

2.3. Ecrire l'obligation de preuve associée à l'invariant proposé en question 2.1. pour l'évènement Réserver_billet.

2.4. Ecrire les obligations de preuve associées aux invariants INV1 et INV2 pour l'évènement Annuler_billet.

2.5. Justifier, en quelques lignes ou par une démonstration, la correction de l'évènement Réserver_billet par rapport à l'invariant proposé en question 2.1.

Partie 3. Un raffinement Event-B

La machine ci-dessous décrit le squelette du raffinement demandé

MACHINE
Voyage_Ref
REFINES
Voyage
SEES
TICKETS_RESERVATIONS
VARIABLES
passagers, age, prix, origine, destination
INVARIANT
...
INITIALISATION
passengers, age, prix, origine, destination := ∅
EVENTS
Réserver_billet_Jeune =
REFINES **Réserver_billet**
...

Échange_Billet = ...

Nous introduisons la possibilité de réserver un billet à l'aide des évènements suivants
— *Réserver_billet_Jeune* pour réserver un billet pour un jeune (âge entre 12 et 25 ans)
— *Échange_Billet* qui permet à un passager donné, ayant réservé un billet, de pouvoir échanger son billet. Dans ce cas, seule la destination peut changer.

Questions

3.1. Décrire un invariant qui indique que le prix de tout billet réservé par un passager "jeune" (âge entre 12 et 25 ans) ne dépasse pas 300 le billet.

3.2. Quel évènement est raffiné par l'évènement Échange_Billet ?

3.3. Compléter le raffinement ci-dessous en décrivant les évènements *Réserver_billet_Jeune* et *Échange_Billet*.
Il est inutile de recopier les variables, invariant, initialisation, événements qui ne changent pas par rapport à la machine Voyage

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