INP ENSEEIHT

3A SN SIL 2021-2022

Développement Formel de Systèmes

18 Janvier 2022

Durée 1h30

Documents autorisés

Partie 1. Questions de cours

La méthode Event-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 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 propriétés de la machines. Qu'est-ce qui les différencie ?

E. Qu'est-ce qu'un variant ? Quel type de propriété permet-il d'établir ? Vous donnerez précisément les caractéristiques du variant.

F. Le raffinement établit une relation de simulation entre deux systèmes états-transitions associés à deux machines. Expliquer le rôle de la relation de simulation ?

Il est demandé de répondre en quelques lignes seulement.

Pour les parties 2, 3 et 4, si vous souhaitez introduire des précisions, veuillez les décrire dans votre copie.

Partie 2. Une machine Event-B

On désire modéliser, à l'aide d'Event-B, un système ferroviaire simple comprenant une gare avec plusieurs voies et plusieurs trains. Un train en circulation peut entrer en gare, et dans ce cas il occupe une voie. Chaque voie de la gare peut contenir **au plus un** train. Un train en gare peut la quitter, et dans ce cas il transite par un tronçon appelé *sortie*, avant de rejoindre le réseau de circulation en dehors de la gare. **Au plus un** train peut occuper ce tronçon de sortie.

Le contexte Ferroviaire0Ctx ci-dessous définit les éléments nécessaires à la modélisation de notre problème.

CONTEXT Ferroviaire0Ctx
SETS
  $TRAINS$
  $VOIES$
AXIOMS
  axm1 : finite($TRAINS$)

La machine Event-B Ferroviaire0 ci-dessous décrit le système ferroviaire. L'état du système est modélisé par trois variables :

- *circulation* représente les trains en circulation hors de la gare,
- *voies* modélise les trains arrêtés dans la gare, et associe à chacun d'entre eux une voie,
- et finalement, *sortie* modélise le tronçon en sortie de la gare, auquel sont connectées chacune des voies, et qui mène au réseau de circulation normal.

Notez qu'à l'état initial, tous les trains sont en circulation, aucun n'est en gare.

MACHINE Ferroviaire0
SEES Ferroviaire0Ctx
VARIABLES
  circulation
  voies
  sortie
INVARIANTS
  inv1 : $circulation \subseteq TRAINS$
  inv2 : $sortie \subseteq TRAINS$
  inv3 : $voies \in TRAINS \leftrightarrow VOIES$
EVENTS
  INITIALISATION
  THEN
    act1 : $circulation := TRAINS$
    act2 : $sortie := \emptyset$
    act3 : $voies := \emptyset$
  END

  Arriver ...
  Partir ...
  Circuler ...

En plus de l'initialisation, nous introduisons les événements suivants :

- **Arriver** modélise l'entrée en gare : un train en circulation se voit affecter une voie libre
- **Partir** modélise la sortie de gare : un train arrêté sur une voie démarre et rentre dans le tronçon de sortie, si ce dernier est libre
- **Circuler** modélise le retour en circulation : le train sur le tronçon de sortie rejoint le réseau ferré, hors de l'administration de la gare

Questions

1.1. Compléter la machine abstraite Ferroviaire0 avec les invariants suivants :
  - inv4 : le tronçon de sortie ne peut pas contenir plus d'un train à la fois.
  - inv5 : un train ne peut pas être simultanément en circulation, sur une voie et en sortie.
  - inv6 : chaque voie contient **au plus un** train à la fois.

1.2. Compléter la machine abstraite Ferroviaire0 en exprimant la spécification formelle des 3 événements **Arriver**, **Partir** et **Circuler**.
Vous veillerez à respecter l'invariant dans cette spécification.

1.3. Écrire l'obligation de preuve d'invariant associée à l'événement **Arriver** pour l'invariant inv6 écrit dans la question 1.1.

1.4. Justifier, en quelques lignes ou par une démonstration, la correction de l'événement **Arriver** vis-à-vis de l'invariant inv6 écrit dans la question 1.1.

Partie 3. Un raffinement Event-B

On souhaite prendre en compte la notion de temps dans le système de gestion de trains. On propose pour cela de raffiner Ferroviaire0 avec une nouvelle machine, Ferroviaire1, dont le squelette est donné ci-dessous.

```
MACHINE Ferroviaire1 REFINES Ferroviaire0
VARIABLES
  circulation
  voies
  sortie
  horloge
  departs
INVARIANTS
  inv1 : horloge ∈ ℕ
  inv2 : departs ∈ TRAINS ⇸ ℕ
  inv3 : dom(departs) = dom(voies)
EVENTS
  INVARIANTS extended
  THEN
    act4 : horloge :∈ ℕ
    act5 : departs := ∅
  END

  Arriver ...
  Partir ...
  Circuler ...

  Tick ...
  THEN
    act1 : horloge := horloge + 1
  END
```

Chaque train qui arrive en gare renseigne son heure de *départ* (située dans le futur). Le système garde trace du passage du temps, modélisé par la variable *horloge* et l'événement **Tick** qui la fait progresser, et s'assure que chaque train parte *au minimum après que son heure de départ soit dépassée.*
Si plusieurs trains sont autorisés à partir, celui qui part en premier est choisi de manière non-déterministe.

Questions

2.1. Quel évènement est raffiné par l'évènement **Tick** ?

2.2. Compléter le raffinement ci-dessus en donnant la définition de **Arriver** et **Partir** pour qu'ils prennent en compte le système de temps et d'horaire de départ décrit plus haut.

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

Partie 4. Encore du raffinement

On souhaite maintenant préciser le fonctionnement de notre système en introduisant deux types de voies : les voies *normales* (pour les trains types TER) et les voies *grandes vitesses* (pour les TGV).
Dans un premier temps, on introduit le contexte Ferroviaire2Ctx ci-dessous.

```
CONTEXT Ferroviaire2Ctx EXTENDS Ferroviaire0Ctx
CONSTANTS
  VOIES_NORMALES
  VOIES_TGV
AXIOMS
  axm1 : partition(VOIES, VOIES_NORMALES, VOIES_TGV)
END
```

On désire maintenant capturer ce nouveau fonctionnement en raffinant la machine Ferroviaire1 obtenue dans la partie précédente. La spécification de cette machine Ferroviaire2 est la suivante :

FUN1. Le type d'un train (normal ou grande vitesse) est connu à l'entrée en gare.

FUN2 Le type d'un train détermine sur quel type de voie il s'engage. Un train normal ne peut pas occuper une voie grande vitesse, et inversement.

FUN3 L'horaire de départ d'un TGV entré en gare est toujours égal à son horaire d'arrivée plus 10.

ENV1 Le type des trains (normal ou grande vitesse) n'est pas pris en compte lorsque les trains sont en circulation.

Questions

3.1. On se propose de raffiner en faisant disparaître la variable *voies* au profit de deux variables, *voies_normales* et *voies_tgv*. Quelle expression relie ces trois variables ? En déduire l'invariant de collage pour cette troisième machine.

3.2. Ébaucher le raffinement Ferroviaire2 de la machine Ferroviaire1, implémentant la spécification donnée ci-dessus. Vous veillerez à donner :
- (toutes) les variables de la machine Ferroviaire2
- les invariants de la machine Ferroviaire2 (inutile de réécrire ceux des machines précédentes)
- les nouveaux événements de la machine Ferroviaire2, et/ou les événements raffinés *qui ont changé*

3.3. Justifiez la correction de ce raffinement.

3.4. On désire étudier la propriété suivante :

« Tous les trains du système finissent par quitter la gare »

De quelle type de propriété s'agit-il ? Comment pourrait-on la démontrer ? Il n'est pas demandé de mettre en place la solution ; cependant, vous prendrez soin d'expliquer précisément les détails de cette solution et les mécanismes formels mis en jeu.