Université de Sherbrooke, Département d'informatique

IGL501: IGL501 : Méthodes formelles en génie logiciel

Examen périodique Professeur : Marc Frappier,
Lundi 27 octobre 2008, 13h30 à 16h20, local D7-2011

Documentation permise. La correction est, entre autres, basée sur le fait que chacune de vos réponses soit *claire*, c'est-à-dire lisible et compréhensible pour le lecteur; *précise*, c'est-à-dire exacte et sans erreur; *concise*, c'est-à-dire qu'il n'y ait pas d'élément superflu; complète, c'est-à-dire que tous les éléments requis sont présents.

1. (50 pts) Spécifiez avec Event-B un système de réservation de salle. Spécifiez seulement les évènements suivants.

   - reserver($p : PERSONNE,\ s : SALLE,\ d : \mathbb{N},\ f : \mathbb{N}, n : \mathbb{N}$): permet à la personne p de réserver la salle s; la réservation débute au temps d et termine au temps f; le numéro de cette réservation est n
   - annuler($p : PERSONNE,\ n : \mathbb{N}$): permet à la personne p d'annuler la réservation n.

   Prenez en compte les contraintes suivantes:

   (a) Une personne ne peut pas annuler les réservations crées par d'autres personnes.
   (b) Une salle ne peut être réservée par deux personnes en même temps.
   (c) Une personne ne peut réserver deux salles pour des périodes qui se chevauchent.
   (d) Les numéros de réservation sont uniques.
   (e) Les personnes et les salles sont des constantes du système.

   Solution:

   MACHINE reservation

   VARIABLES

   $reservation, personne, salle, debut, fin$

   INVARIANT

   $reservation \subseteq \mathbb{N}$
   $personne \in reservation \rightarrow PERSONNE$
   $salle \in reservation \rightarrow SALLE$
   $debut \in reservation \rightarrow \mathbb{N}$
   $fin \in reservation \rightarrow \mathbb{N}$
   $\forall\, r \cdot r \in reservation \Rightarrow debut(r) < fin(r)$
   $\forall\, r_1, r_2 \cdot$
   $\quad r_1 \neq r_2 \land r_1 \in reservation \land r_2 \in reservation \land salle(r_1) = salle(r_2)$
   $\quad \Rightarrow$
   $\quad (fin(r_1) \leq debut(r_2) \lor fin(r_2) \leq debut(r_1))$
   $\forall\, r_1, r_2 \cdot$

$r_1 \neq r_2 \wedge r_1 \in reservation \wedge r_2 \in reservation \wedge personne(r_1) = personne(r_2)$
$\Rightarrow$
$(fin(r_1) \leq debut(r_2) \vee fin(r_2) \leq debut(r_1))$

EVENTS

INITIALISATION

$reservation := \emptyset$
$personne := \emptyset$
$salle := \emptyset$
$debut := \emptyset$
$fin := \emptyset$

reserver $\triangleq$

ANY
p, s, d, f, n
WHERE
$p \in PERSONNE$
$s \in SALLE$
$d \in \mathbb{N}$
$f \in \mathbb{N}$
$n \in \mathbb{N} - reservation$
$d < f$
$\forall r \cdot$
$r \in reservation \wedge salle(r) = s$
$\Rightarrow$
$(fin(r) \leq d \vee f \leq debut(r))$
$\forall r \cdot$
$r \in reservation \wedge personne(r) = p$
$\Rightarrow$
$(fin(r) \leq d \vee f \leq debut(r))$
THEN
$reservation := reservation \cup \{n\}$
$personne(n) := p$
$salle(n) := s$
$debut(n) := d$
$fin(n) := f$
END
annuler $\triangleq$

ANY
p, s, d, f, n
WHERE
$p \in PERSONNE$
$n \in reservation$

$personne(n) = p$

THEN

$reservation := reservation - \{n\}$

$personne(n) := \{n\} \lhd p$

$salle(n) := \{n\} \lhd s$

$debut(n) := \{n\} \lhd d$

$fin(n) := \{n\} \lhd f$

END

2. (20 pts) Prouvez que l'évènement e_1 préserve les invariants ci-dessous. Utilisez les règles d'inférence du livre Event-B. Si la preuve échoue, modifiez la garde pour la renforcer juste assez pour compléter la preuve. Pour raccourcir les preuves, on suppose pour les étapes de simplification arithmétique que $a \in \mathbb{N}, b \in \mathbb{N}, c \in \mathbb{N}, x \in \mathbb{N}$.

INVARIANT

inv1 : $a + b = c$

inv2 : $a = 0 \vee b = 0$

$e_1 \triangleq$

WHEN

$b \neq 0$

THEN

$c := c + x$

$a := b + x$

$b := 0$

END

Solution: Preuve e_1/inv1/INV

$a + b = c$

$a = 0 \vee b = 0$

$b \neq 0$

$\vdash$

$b + x + 0 = c + x$

ARI,OR_L cas 1,MON : $a = 0$

$a + b = c$

$a = 0$

$\vdash$

$b + x = c + x$

EQ_LR

$0 + b = c$

$\vdash$

$b + x = c + x$

ARI

$b = c$
$\vdash$
$b + x = c + x$

EQ_LR

$b = c$
$\vdash$
$c + x = c + x$

MON,EQL

fin OR_L cas 1
OR_L cas 2 : $b = 0$

$a + b = c$
$b = 0$
$b \neq 0$
$\vdash$
$b + x = c + x$

MON

$b = 0$
$b \neq 0$
$\vdash$
$b + x = c + x$

NOT_L

$b = 0$
$\vdash$
$b = 0$
HYP

Preuve e_1/inv2/INV

$a + b = c$
$a = 0 \vee b = 0$
$b \neq 0$
$\vdash$
$b + x = 0 \vee 0 = 0$

MON

$\vdash$

$b + x = 0 \lor 0 = 0$

OR_R1

$\vdash$
$0 = 0$

EQL

3. (10 pts) Prouvez que l'évènement e_1 de la question 2 ne diverge pas. **Solution:**

   Variant est simplement b.

   Preuve e_1/WFD_REF1

   $b \in \mathbb{N}$
   $a + b = c$
   $a = 0 \lor b = 0$
   $b \neq 0$
   $\vdash$
   $b \in \mathbb{N}$

   MON,P1

   Preuve e_1/WFD_REF2

   $b \in \mathbb{N}$
   $a + b = c$
   $a = 0 \lor b = 0$
   $b \neq 0$
   $\vdash$
   $0 < b$

   MON,P3

4. (10 pts) Prouvez que l'évènement e_1 de la question 2 et l'évènement e_2 ci-dessous, lorsque considérés comme des évènements de la même specification, ne bloquent pas (*deadlock freedom* règle DLF). Les invariants sont ceux de la question 2. Si la preuve échoue, choisissez un des invariants suivants à ajouter et complétez la preuve. Notez bien que vous n'avez pas à prouver la préservation de l'invariant que vous ajoutez.

   inv3 $c > 0$

   inv4 $a = b$

   $e_2 \triangleq$
   WHEN
   $\quad a \neq 0$

THEN
$c := c + x$
$b := a + x$
$a := 0$
END

Solution: Preuve e_1, e_2/DLF. La preuve échoue; on choisit $c > 0$.

$a + b = c$
$a = 0 \vee b = 0$
$c > 0$
$\vdash$
$b \neq 0 \vee a \neq 0$

NEG

$a + b = c$
$a = 0 \vee b = 0$
$c > 0$
$b = 0$
$\vdash$
$a \neq 0$

NOT_R cas 1 avec Q quelconque.

$a + b = c$
$a = 0 \vee b = 0$
$c > 0$
$b = 0$
$a = 0$
$\vdash$
Q

MON,EQ_LR,EQ_LR

$0 + 0 = c$
$c > 0$
$b = 0$
$a = 0$
$\vdash$
Q

ARI,MON

$0 = c$
$c > 0$
$\vdash$
Q

EQ_LR, MON, CNTR

$0 = c$
$0 > 0$
$\vdash$
Q
NOT_R cas 2 : preuve identique, avec $\neg Q$.

5. (10 pts) On vous propose un raffinement pour un évènement e_3. Sans nécessairement faire la preuve, indiquez s'il y a bien raffinement et expliquez pourquoi. Le symbole k est une constante: $k \in \mathbb{N}$ et $k > 0$.

Version abstraite	Version concrète
VARIABLES d, e INVARIANT $d \in \mathbb{N}$ $e \in \mathbb{N}$ $e_3 \triangleq$ WHEN $d > 0$ THEN $d :\mid d' \in e..e + k$ END	VARIABLES f, g INVARIANT $f \in \mathbb{N}$ $g \in \mathbb{N}$ $f = 2 * d$ $g = 2 * e$ $e_3 \triangleq$ WHEN $f > 0$ THEN $f :\mid f' \in g..g + k$ END

Solution: Il n'y a pas de raffinement. Voici un contre-exemple. Une exécution concrète possible est $f = 1, g = 0, f' = 1, g' = g$. Il n'y a pas d'exécution correspondante dans la machine abstraite, Par l'invariant $f' = 2 * d'$, on a $d' = 0.5$ pour $f' = 1$, ce qui n'est pas un naturel.