UNIVERSITÉ DE NANTES

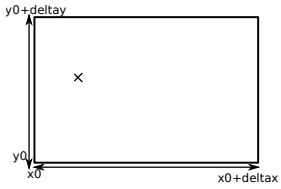
Master ALMA (M2)
Formal Software Engineering (FSE)
C. Attiogbé & Claude Jard - 2018/2019

Exercices

Exo 1 : positionnement d'un pointeur dans le plan

Soit à contrôler l'évolution des valeurs de deux variables xx, yy. Les valeurs sont entières. Elles peuvent représenter les coordonnées (x,y) d'une pointe traçante.

Chacune des deux variables évolue sur une plage δ à partir de sa valeur initiale ; par exemple les valeurs possibles de xx sont entre x_0 et $x_0 + \delta_x$; les valeurs possibles de yy sont entre y_0 et $y_0 + \delta_y$.



On veut écrire en B une machine abstraite GestPosition qui va proposer ses opérations à un programme de contrôle de la pointe traçante.

La machine abstraite GestPosition fournira les opérations suivantes :

— Changement de la valeur de xx ; on donne une nouvelle valeur nx en paramètre
— Changement de la valeur de yy ; on donne une nouvelle valeur ny en paramètre
— Incrémentation de la valeur de xx de px (un paramètre) ;
— Incrémentation de la valeur de yy de py ;
— Décrémentation de la valeur de xx de px ;
— Décrémentation de la valeur de yy de py ;
— Récupération de la valeur de xx ;
— Récupération de la valeur de yy ;
— Test si une valeur donnée ux est entre les bornes de xx ;
— Test si une valeur donnée uy est entre les bornes de yy ;

Q#1 Spécifiez une machine abstraite B (sans les opérations) pour décrire l'espace d'états correspondant à l'énoncé.

Q#2 Complétez la machine abstraite par la spécification des opérations qui sont décrites.

Exo 2 : modélisation d'un protocole de communication simplifié

Nous allons modéliser un protocole de communication dans lequel des processus échangent des messages via des canaux (abstraits). Nous distinguerons un canal de `sujets de discussion` et un canal de `commentaires` sur les sujets.

Un canal est vu à un instant donné comme un ensemble de messages. Sur cette base, on vous propose de modéliser un canal de `sujets de discussion` par une relation dont les éléments

sont des couples de numéros (identifiant les messages) et d'identifiants de sujets de discussion. Par exemple (1, sujetA), (3, sujetB), ... Un numéro identifie un seul sujet.

Des commentaires sont effectués (par des processus) sur des sujets issus du canal des `sujets de discussion`. Chaque commentaire est associé à un seul sujet.

Soit un canal abstrait (`commentaires`) représentant les commentaires effectués sur les sujets.

Il ne peut pas y avoir de commentaires sur un sujet qui n'est pas présent sur le canal des `sujets de discussion`.

Considérons un ensemble de processus ; quand un processus est dans le protocole de communication, il peut être dans l'état `actif` ou `inactif` mais pas simultanément. Chaque processus est identifié par un numéro unique.

Q#3 Analysez et modélisez ces données et propriétés en B (structurez avec les clauses SETS, VARIABLES, INVARIANT).

Q#4 En fonction de votre modèle, exprimez l'effet de la création d'un processus (le processus créé devient alors un des processus dans le protocole, il est par défaut inactif).

Q#5 Ecrivez une opération qui modélise l'activation d'un processus (le processus à activer existe, il devient actif).

Q#6 Ecrivez une opération qui modélise la désactivation d'un processus (le processus à désactiver existe).

Q#7 Ecrivez l'obligation de preuve de l'opération de désactivation d'un processus.

Q#8 Ecrivez une opération qui modélise la destruction d'un processus.

Plusieurs processus interragissent dans le protocole de communication ; dans la suite et pour simplifier, on considère que les identifiants des processus sont utilisés comme numéros des sujets de discussion qu'ils initient. Tous les processus ont accès aux canaux abstraits (`discussion`, `commentaires`) supports des discussions.

Un processus actif peut initier (créer) une discussion à tout moment en donnant le sujet de discussion ; l'identifiant du processus et le sujet apparaissent alors sur le canal des `sujets de discussion`.

Une discussion est vue comme un sujet initié par un processus, et un ensemble de commentaires effectués sur ce sujet par d'autres processus actifs.

Lorsqu'une discussion est initiée, on dit qu'elle est active ; elle peut alors être rejointe par divers autres processus qui deviennent alors des processus participants. Les processus participants actifs font des commentaires sur les sujets de discussion présents sur le canal.

Une discussion peut disparaître à tout moment, sur la demande de destruction d'un processus qui l'a créé.

Les processus inactifs ne peuvent ni initier des discussions ni participer aux discussions en cours.

Q#9 A partir de cette description, listez toutes les opérations élémentaires qui permettront de modéliser le reste du protocole et des interactions décrites.

Q#10 Complétez au besoin les hypothèses et argumentez.

Q#11 Proposez la modélisation de chacune des opérations listées ; vous indiquerez clairement vos hypothèses (commentez les opérations).

Exo 3 : modélisation d'une application de domotique

Une maison intelligente est équipée d'**objets ou dispositifs divers** dotés de logiciels assurant leur fonctionnement. Les objets peuvent être contrôlés à partir d'une interface de pilotage. Les objets sont classés en catégories : *mobile*, *fixe*. Typiquement nous avons : un dispositif d'alarme, des dispositifs d'ouverture-fermeture de volets et fenêtres, des robots électroménagers (des robots-aspirateurs, des robots assistants de cuisine, éplucheurs, repasseurs), etc. Ces robots cohabitent et peuvent coopérer pour certaines tâches.

On peut donner des ordres de fonctionnement ou d'arrêt aux objets ou dispositifs contrôlés. Plusieurs usagers d'une maison peuvent donner des ordres ; les ordres sont reçus et analysés par un logiciel global qui coordonne les actions des différents objets.

Vous devez contribuer à la modélisation, en utilisant la méthode formelle B, du logiciel nécessaire pour garantir un bon fonctionnement de la maison intelligente.

Le bon fonctionnement de la maison est garantie par le respect de **propriétés** ; par exemple :

— *quand l'alarme est en marche, les robots ne peuvent pas être activés.*

— *Les robots ne doivent pas se gêner dans leur position ou mouvement ; par exemple la prochaine position calculée doit être libre avant d'y déplacer un objet.*

Dans le temps imparti à cet exercice, on se limite à quelques attributs ou caractéristiques des objets contrôlés ; chaque objet mobile (tel un robot), a une position en x, y à un moment donné, et cela varie. Chaque objet peut être `actif`, `inactif` ou `invalide` lorsqu'il n'est plus en état de fonctionnement. Un objet peut être incompatible avec un ou plusieurs autres, donc ils ne peuvent pas être actifs en même temps.

1. Spécifiez en B une machine abstraite (ou plusieurs) permettant de modéliser les caractéristiques des objets contrôlés dans le logiciel décrit. Vous formaliserez aussi les propriétés énoncées ci-dessus, dans l'invariant de la machine.
2. donnez des obligations de preuve pour l'initialisation de votre machine.

En précisant vos hypothèses, écrivez quelques une des opérations élémentaires pour :

3. ajouter aux objets à contrôler un nouvel objet avec son attribut `fixe` ou `mobile` ; initialement un objet ajouté est `inactif`.
4. activer un objet mobile `obj`. Donnez les obligations de preuve de cohérence pour cette opération.
5. désactiver un objet `obj`.
6. activer le système d'alarme (objet fixe).
7. trouver quels sont tous les équipements actifs.
8. trouver quels sont les équipements connectés aux logiciels mais qui sont invalides.