Méthodes formelles

Mohamed Tounsi

Faculté des Sciences Économiques et de Gestion de Sfax

Avril 2015

Le raffinement

Pourquoi le raffinement

- Une spécification peut regrouper des centaines (voir plus) de propriétés.
- Représenter toutes ces propriétés sous forme d'invariants d'une machine rendrais la spécification illisible et inutilisable.
- Les preuves de ces propriétés peuvent êtres non triviales.

Pourrait-on prouver les propriétés à différents niveaux d'abstractions, et réutiliser ces preuves ?

Le raffinement

Notion de raffinement

Raffinement

M' raffine M ($M' \sqsubseteq M$) : le comportement de M' "précise" celui de M. M' est appelée machine concrète et M machine abstraite.

Conséquences

- Le raffinement assure que chaque étape (M') préserve bien les propriétés de correction vis-à-vis de l'étape précédente (M).
- Le raffinement permet de construire progressivement et de manière incrémentale des programmes corrects à partir des spécifications abstraites.

Le Raffinement

Un exemple concret

Event a $\triangleq$
where
grd1 : $x < k$
then
act1 : $x := x + 1$

Event c $\triangleq$
where
grd1 : $y + z < k$
then
act1 : $y := y + 1$

$$R \triangleq x = y + z$$

Le Raffinement

Un exemple concret

Event a $\triangleq$
where
grd1 : $x < k$
then
act1 : $x := x + 1$

Event c $\triangleq$
where
grd1 : $y + z < k$
then
act1 : $y := y + 1$

$$R \triangleq x = y + z$$

- Renforcement de garde: x=y+z $\wedge$ y+z<k $\Rightarrow$ x<k
- Préservation de R: x=y+z $\Rightarrow$ (y+1)+z = x+1
- Dans la pratique, la relation de raffinement est un invariant de la machine concrète.

Le raffinement

Remarques

Utilisations de variables abstraites

Si un événement concret modifie une variable abstraite, la valeur de celle-ci doit être modifiée de la même manière que dans l'événement abstrait correspondant.

Les modifications de variables abstraites doivent rester les mêmes!

Nouveaux événements

Si un nouvel événement est introduit, alors cet événement doit raffiner l'événement "ne rien faire" (skip).

On ne change pas les valeurs des variables abstraites

Suppression de paramètre

Si un paramètre d'un événement est supprimé, un témoin de ce paramètre doit être fourni. Un témoin est une relation de raffinement locale.

Terminaison, variant et Deadlock Freeness en Event-B

Terminaison

Une machine termine si elle contient un événement qui décroit un variant *entier* quand il se déclenche.

Événement convergent

Un événement est convergent s'il décroît le variant.

Deadlock Freeness

Une machine "ne se bloque pas" si à tout moment un événement est exécutable. Si la disjonction des gardes des événements est un invariant (thèorème).

Les obligations de preuves (POs)

Définition

- Une PO est une proposition mathématique à démontrer pour prouver que les différents modules ainsi que le processus de spécification sont corrects.
- Formellement, elle est codée par un ensemble d'hypothèses et par une conclusion.
- La démonstration d'une PO nécessite obligatoirement la preuve de correction de sa conclusion eu égard à ses hypothèses.

Les POs dans Event-B

La méthode Event-B contient deux grandes classes de POs :

1. les POs du modèle.
2. les POs du raffinement.

Les obligations de preuves (POs)

les POs du modèle

La terminologie, utilisée dans cette section, est définie comme suit :

```
s : Eensembles et Constantes du contexte.
v : Variables d'état de la machine.
A(s) : Axiomes et théorèmes du contexte.
I(s, v) : Invariants et théorèmes de la machine.
x : Variables locales de l'événement.
G(x, s, v) : Gardes de l'événement.
PAA (x, s, v, v') : Prédicat avant-après de l'événement.
```

Les obligations de preuves (POs)

Préservation de l'invariant (INV)

Préservation de l'invariant

Un invariant est une propriété du système qui doit être toujours vraie. Concrètement, le système doit préserver cette propriété après tout déclenchent d'événement.

$$\frac{A(s) \quad I(s,v) \quad G(x,s,v) \quad PAA(x,s,v,v')}{I(s,v')}$$

Les obligations de preuves (POs)

Faisabilité des événements (FIS)

Faisabilité des événements

Une machine Event-B doit assurer que chaque substitution généralisée non-déterministe soit faisable. Autrement dit, si la garde de l'événement est vraie, alors l'action doit être réalisable.

$$
\begin{array}{l}
A(s) \\
I(s,v) \\
G(x,s,v) \\
- - - - - - - - - - - - - - - \\
\exists v' \cdot PAA(x,s,v,v')
\end{array}
$$

Les obligations de preuves (POs)

les POs du raffinement

Lors d'un raffinement, il est indisponible de vérifier que la machine concrète ne se contredit dans aucun cas avec l'abstraite. Dans cette optique, plusieurs obligations de preuve doivent être générées et déchargées pour valider la correction du raffinement.

```
w : Variables concretes de la machine.
J(s,v,w) : Invariants et Théorèmes concrets de la machine.
y : Variables locales de l'événement concret.
H(y, s, w) : Gardes de l'événement concret.
BA1(v, v') : Actions de l'événement abstrait.
BA2(w, w') : Actions de l'événement concret.
n(s, v) : Variant (le cas d'un entier naturel).
t(s, c, v) : Variant (le cas d'un ensemble).
W(x, y, s, w) : Témoins (witness) de l'événement concret.
```

Les obligations de preuves (POs)

Renforcement de la garde (GRD)

Principe

Le renforcement de la garde s'inscrit dans le cadre de la préservation de l'état abstrait par l'événement concret. Cette PO veille à ce que les gardes d'un événement concret renforcent correctement les gardes abstraites.

$$
\begin{array}{l}
A(s) \\
I(s,v) \\
J(s,v,w) \\
H(y,s,w) \\
W(x,y,s,w) \\
\hline
g(x,s,v)
\end{array}
$$

Les obligations de preuves (POs)

Simulation des actions (SIM)

Principe

Un événement concret doit garantir une simulation correcte des actions pour assurer la préservation de l'état abstrait. Cette PO doit garantir que lorsqu'un événement concret est "exécuté", alors ses actions ne doivent pas être contradictoires avec ceux de l'événement abstrait.

$$\frac{\begin{array}{l} A(s) \\ I(s,v) \\ J(s,c,w) \\ H(y,s,w) \\ W1(x,y,s,w) \\ W2(y,v',s,w) \\ BA2(w,w',...) \end{array}}{BA1(v,v',...)}$$

Les obligations de preuves (POs)

Correction des événements convergents

Principe

La définition d'un variant génère deux obligations de preuve : la première obligation assure que chaque événement convergent décroît le variant (si le variant est une mesure numérique), ou le diminue (si le variant est un ensemble). La deuxième obligation veille à ce que le variant proposé soit un entier positif.

$A(s)$ $I(s,v)$ $J(s,v,w)$ $G(x,s,w)$ $PAA(x,s,w,w')$ – – – – – – – – – – – – $n(s,w') < n(s,w)$	$A(s)$ $I(s,v)$ $J(s,v,w)$ $G(x,s,v)$ $PAA(x,s,w,w')$ – – – – – – – – – – – – $t(s,w') \subset t(s,w)$	 $A(s)$ $I(s,v)$ $J(s,v,w)$ $G(x,s,v)$ – – – – – – – – – – – $n(s,v) \in \mathbb{N}$

Les obligations de preuves (POs)

Correction des témoins (WFIS)

Principe

Un raffinement d'un événement indéterministe peut remplacer les variables abstraites par d'autres plus concrètes. Ainsi, il est indispensable de définir des témoins pour prouver la correction de l'événement. Les témoins sont des prédicats qui permettent de définir les variables locales abstraites en fonction des concrètes. Souvent, un témoin est formellement spécifié par une simple égalité.

$$
\begin{array}{l}
A(s) \\
I(s,v) \\
J(s,v,w) \\
H(y,s,w) \\
\hline
\exists x \cdot W(x,y,s,w)
\end{array}
$$