B et le temps réel

étude de l'intégration du calcul des durées

Samuel Colin

Samuel.Colin@inrets.fr

INRETS/UVHC-LAMIH

Plan de la présentation

- Problématique temps-réel, exemples de formalismes
- Calcul des durées
- Exemples
- Validation par un outil de méta-modélisation
- Conclusion

Questions posées

- Limites de temps imposées : capteurs mis à jour sur une période donnée, actuateurs fonctionnant après un temps donné,. . .
- Fonctionnement pérenne : nécessité d'un formalisme pour la non-terminaison
- Ordonnancement : dans le cas de programmes concurrents avec exclusion mutuelle, le formalisme doit permettre d'éviter les interblocages

Exemples de langages

Lustre Expression de séquences

PC $= 0 \rightarrow$ pre C;

C $= if$ X $then$ (PC + 1) $else$ PC ;

Esterel Utilisation de signaux et d'instructions réactives

```
input A,B,R ;
output O ;
loop
   [ await A || await B ] ;
   emit O
each R
```

Quelques logiques temporelles

LTL :

- Opérateurs $f \wedge f, \neg f, f \mathcal{U} f, X f$
- Représentable par des automates

CTL :

- Opérateurs $f \wedge f, \neg f, \forall(f \mathcal{U} f), \forall(X f), \exists(f \mathcal{U} f), \exists(X f)$
- Quantification sur les chemins possibles
- Ni plus expressive, ni moins expressive que LTL

Logique d'intervalle :

- Logique propositionnelle ,$f \frown f$, ℓ
- Le pas de temps n'est pas discret si le domaine numérique ne l'est pas

Propriétés

LTL, CTL, dérivés :

- ➤ Temps logique
- ➤ Plus ou moins pertinent pour représenter des programmes

Logique d'intervalle :

- ➤ Le temps est représenté par des fenêtres
- ➤ Permet de représenter jusqu'à des traces d'exécution de programmes concurrents

Inconvénients :

- ➤ Indécidabilité
- ➤ Temps d'adaptation

Plan de la présentation

- ☑ Problématique temps-réel, exemples de formalismes

- ❒ Calcul des durées
- ❒ Exemples
- ❒ Validation par un outil de méta-modélisation
- ❒ Conclusion

Calcul des durées

- Calcul des prédicats : $\vee, \wedge, \neg, \Rightarrow, \forall$
- Logique d'intervalle : $\frown, \ell$
- Durée d'événements : $\int S$
- Événements : $0, 1, \neg S, S \vee S$
- Exemples :
  - $(\ell = 10)^\frown(\ell = 5)$
  - $\textbf{true}^\frown(\phi^\frown\textbf{true})$
  - $\int(\text{Gaz} \Rightarrow \text{Feu}) = \ell \wedge \ell > 0$

Propriétés et hypothèses

- Hérite des propriétés du calcul des prédicats, de la logique d'intervalle, et des inconvénients
- Permet de raisonner sur la durée d'événements et de leurs relations les uns aux autres
- Hypothèse de variabilité finie sur les fonctions numériques

Dérivés du calcul des durées

DC* Permet de découper un intervalle de temps en un nombre arbitraire de sous-intervalles (existence d'une sous-classe décidable)

WDC Permet de raisonner sur deux niveaux de temps

DC $_\infty$ Permet d'utiliser des intervalles de temps infinis

μ**HDC** Ordre supérieur, logique de voisinage, opérateur de point fixe

Plan de la présentation

- ☑ Problématique temps-réel, exemples de formalismes
- ☑ Calcul des durées
- ❒ Exemples
- ❒ Validation par un outil de méta-modélisation
- ❒ Conclusion

Exemple du container d'eau

Exemple du container d'eau

Besoin :

$$\Box\left(\int(\omega \leq SH) = \ell \wedge \int(\omega \geq SL) = \ell \wedge \ell > 0\right)$$

Implémentation :

while true **do**
    await $(\omega > CH \vee \omega < CL)$;
    if $\omega > CH$ **then** $valve :=$ *on* ; **await** $\omega \leq CH$
    else if $\omega < CL$ **then** $valve :=$ *off* ; **await** $\omega \geq CL$
        else skip fi fi
od

En B *classique*

- Utilisation d’une machine gérant le temps
- Utilisation de variables visibles partout
- Risques d’erreurs accrus
- Le modèle n’est plus soumis au temps, mais le manipule

En B *temps-réel*

- Utilisation de substitutions dédiées (délai et attente réactive)
- La modularité de B permet de modéliser les propriétés temporelles du système extérieur
- Abandon éventuel de l'hypothèse du vrai synchronisme
- Intérêt supplémentaire : la possibilité d'augmenter les instructions de B en rapport avec l'expressivité de sa sémantique

Plan de la présentation

- ☑ Problématique temps-réel, exemples de formalismes

- ☑ Calcul des durées
- ☑ Exemples
- ❒ Validation par un outil de méta-modélisation
- ❒ Conclusion

Problèmes de la validation

- Compatibilité avec le B *classique*
- Obligations de preuve supplémentaires
- Validation automatique : faire le moins possible confiance à l'humain
- Problèmes de la validation automatique :
  - Modélisation du calcul des durées
  - Modélisation de la sémantique de B

Un outil de validation : *Coq*

- Basé sur le **Calcul des Constructions Inductives** (théories des types) :
  - Isomorphisme de Curry-Howard
  - Raisonnement aux ordres supérieurs
  - Mécanisme de calcul
- Développé avec *Objective Caml*
- Version actuelle : 7.3
- Nombreuses librairies de théorèmes : entiers naturels, réels, ensembles, listes, relations, faits logiques,. . .

Plan de la présentation

- ☑ Problématique temps-réel, exemples de formalismes
- ☑ Calcul des durées
- ☑ Exemples
- ☑ Validation par un outil de méta-modélisation
- ❐ Conclusion

Conclusion

- Modélisation du calcul des durées
- Expression de la sémantique temporelle des substitutions B et modélisation
- Modélisation de l'intégration du calcul des durées à B
- Expression des obligations de preuve temporelle
- Développement d'un exemple d'utilisation
- Recherche des nouvelles possibilités apportées par cette nouvelle sémantique (concurrence, non-terminaison)