Une sémantique formelle pour les modèles Simulink®

Yann Duplouy

IRT SystemX et LSV, ENS Paris-Saclay

lundi 28 août 2017

ETR 2017
Session doctorants

Contexte : simulation pour la sécurité des véhicules autonomes

Thèse préparée au sein du **projet SVA** à l'**IRT SystemX**.

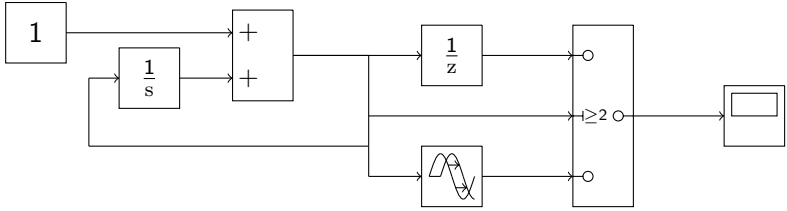
Objectif du projet : aider à la validation de la **fiabilité** des systèmes embarqués au sein des véhicules pour l'assistance aux conducteurs.

Problématique : Simulink est utilisé pour la conception de ces systèmes embarqués.

Objectif : Définir une sémantique formelle pour Simulink

- sémantique exacte ;
- sémantique approchée, dans le but de l'intégrer au *model-checker statistique* Cosmos.

SK-modèles



	 SineWave	 Add	 Integrator	 UnitDelay	 TrDelay	 Switch
Signaux d'entrée	0	2	1	1	1	3
Signaux de sortie	1	1	1	1	1	1
Discret ?	✗	✗	✗	✓	✗	✗
Immédiat ?	✓	✓	✗	✗	✗	✓
Retard infinitésimal ?	✓	✓	✓	✗	✗	✓
Paramètres	$\{f, A, \varphi\}$		$\{v_0\}$	$\{\delta, v_0\}$	$\{r, v_0\}$	$\{s, o\}$

Sémantique d'un modèle Simulink

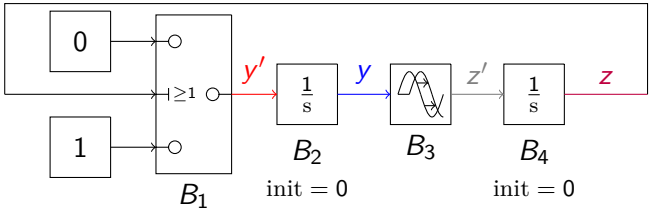
Objectif

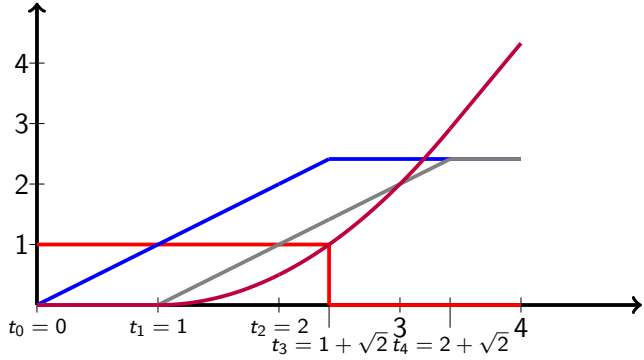
Pour $\mathcal{M}$ un SK-modèle sur $[t_{\text{init}}, t_{\text{end}}]$ l'intervalle de temps, déterminer une trajectoire : ensemble des valeurs de tous les signaux de sortie sur $[t_{\text{init}}, t_{\text{end}}]$.

Pour déterminer cette trajectoire :

- existence d'opérateurs discrets $\Rightarrow$ découpage en intervalles ;
- système d'équations différentielles sur chacun des intervalles.

Sémantique exacte d'un modèle Simulink





Unicité des trajectoires

Si un *SK*-modèle admet une trajectoire, alors cette trajectoire est unique.

Indécidabilité

Le problème de l'existence d'une trajectoire pour un *SK*-modèle est indécidable.

Sémantique exacte *versus* sémantique approchée

Problèmes de la sémantique exacte

- Le type réel ($\mathbb{R}$) n'est pas implémentable ;
- La sémantique dépend d'une infinité de valeurs sur les intervalles $[t_{\text{init}}, t_{\text{end}}]$;
- Dans le cas général, l'intégration requiert une méthode approchée.

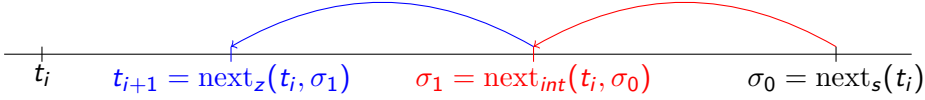
Défis de la sémantique approchée

- Le calcul du prochain pas de temps doit prendre en compte les changements discrets
  (induits par des blocs Switch, Relay et Stateflow) ;
- L'intégration dépend du choix d'une méthode avec pas fixe ou variable ;
- L'évaluation des blocs avec retard (comme Transport Delay) nécessite une interpolation sur les valeurs mémorisées.

Sémantique approchée

Principe général

1. construction *itérative* des instants d'échantillonnage $(t_i)_{i \in I}$:
   - contraintes statiques (next_s),
   - contraintes liées à l'intégration,
   - recherche des franchissement de seuils, à ε_V près.
2. calcul des valeurs des signaux correspondants ;
3. calcul sur $]t_{i+1}, t_{i+1} + \varepsilon_{\mathbb{T}}]$ des valeurs de signaux pour déterminer les modes.



Sémantique approchée

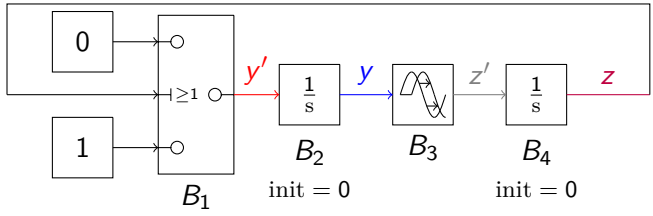
Principe général

1. construction *itérative* des instants d'échantillonnage $(t_i)_{i \in I}$:
   - contraintes statiques (next_s),
   - contraintes liées à l'intégration,
   - recherche des franchissement de seuils, à ε_V près.
2. calcul des valeurs des signaux correspondants ;
3. calcul sur $]t_{i+1}, t_{i+1} + \varepsilon_{\mathbb{T}}]$ des valeurs de signaux pour déterminer les modes.

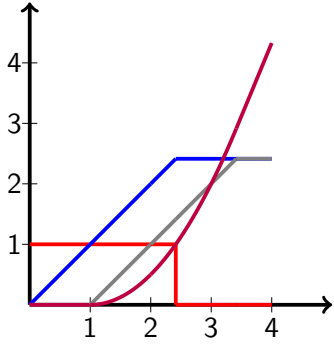
Conjecture

Pour tout ε, il existe $\varepsilon_{\mathbb{T}}$ et ε_V tels que la sémantique approchée approxime la sémantique exacte à ε près.

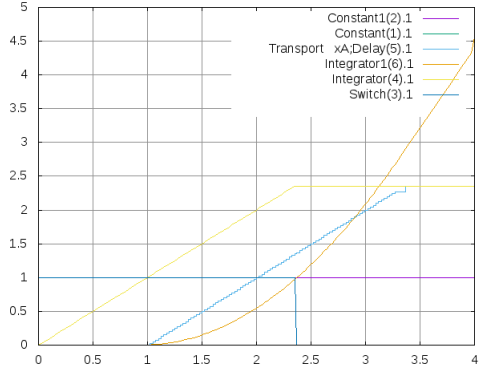
Illustration



Sémantique exacte



Sémantique approchée (via Cosmos)



Conclusions et perspectives

Contributions

- Définition d'une syntaxe et de sémantiques des *SK*-modèles ;
- Développement de Cosmos : intégration d'une sémantique approchée de Simulink.

Perspectives

- Intégration à compléter pour définir un formalisme multi-modèles entre réseaux de Petri et Simulink dans Cosmos ;
- Valider cette implémentation par des cas d'études :
  - Utilisant les contrôleurs fournis, en Simulink, par le projet ;
  - Étendant les comportements des véhicules dans les réseaux de Petri.

Merci de votre attention