Freinage ABS : validation avec un solveur de contraintes sur les flottants

Olivier Ponsini, Michel Rueher, Hélène Collavizza, Claude Michel

VACSIM - 16 et 17 avril 2013 - Brest

Fonction de Freinage ABS

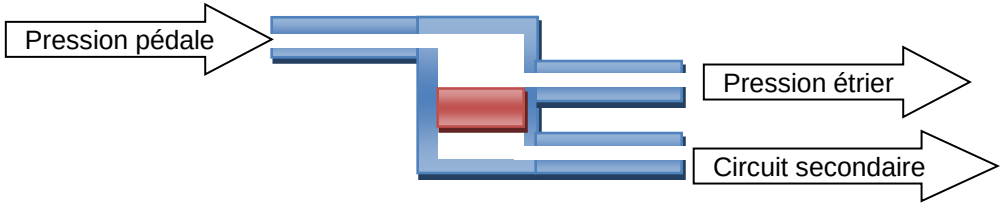
- Etude de cas fournie par Geensys / Dassault Systèmes
- Application temps-réel embarquée
- Programme C généré à partir d'un modèle Simulink
- Calculs sur les flottants et les entiers

ABS : Principe de fonctionnement

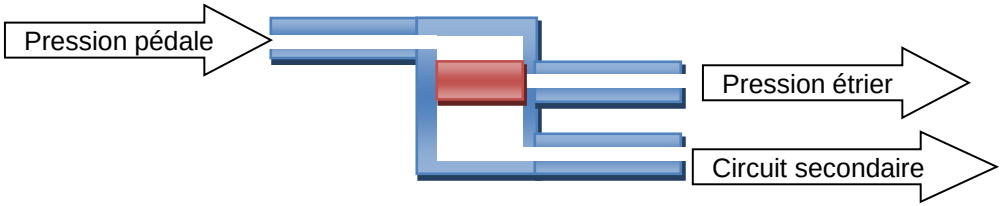
- Détection de la tendance à bloquer d'une roue
  - Taux de glissement : $t_g = 1 - \frac{V_{roue}}{V_{véhicule}}$
  - Taux optimal entre 30 % et 10 % selon le revêtement
- 3 modes possibles pour l'électrovanne
  - Mode passant
  - Mode maintien de pression
  - Mode diminution de pression

ABS : Modes de l'électrovanne

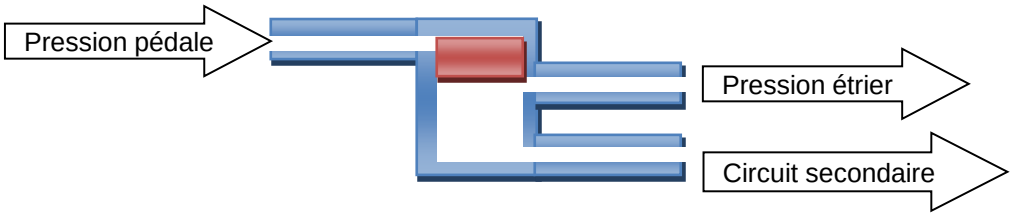
- Mode passant



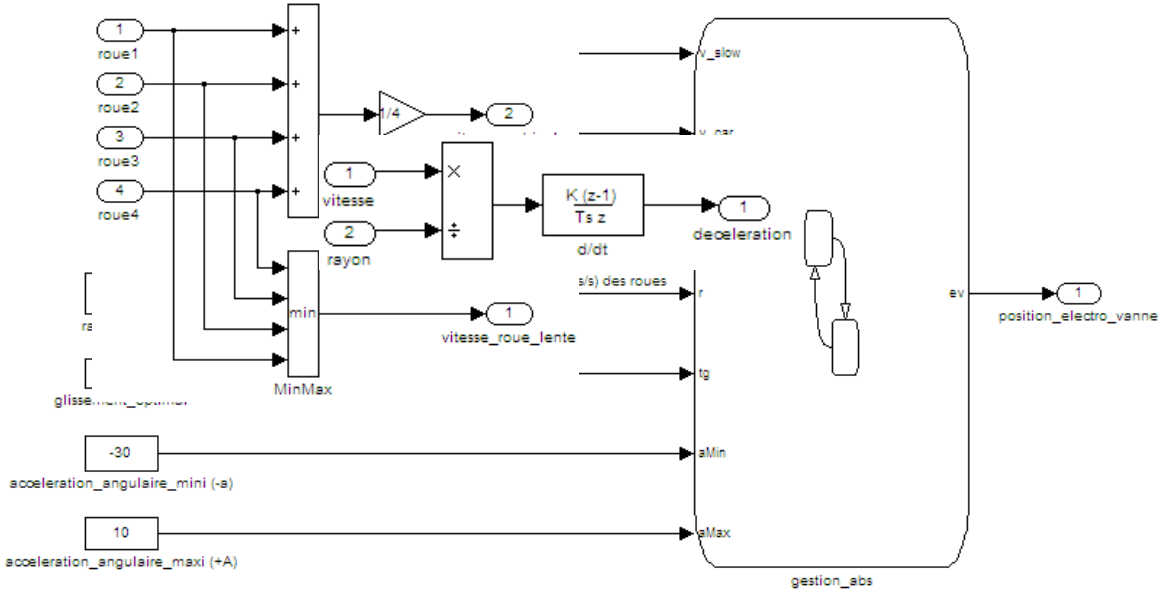
- Mode maintien de pression



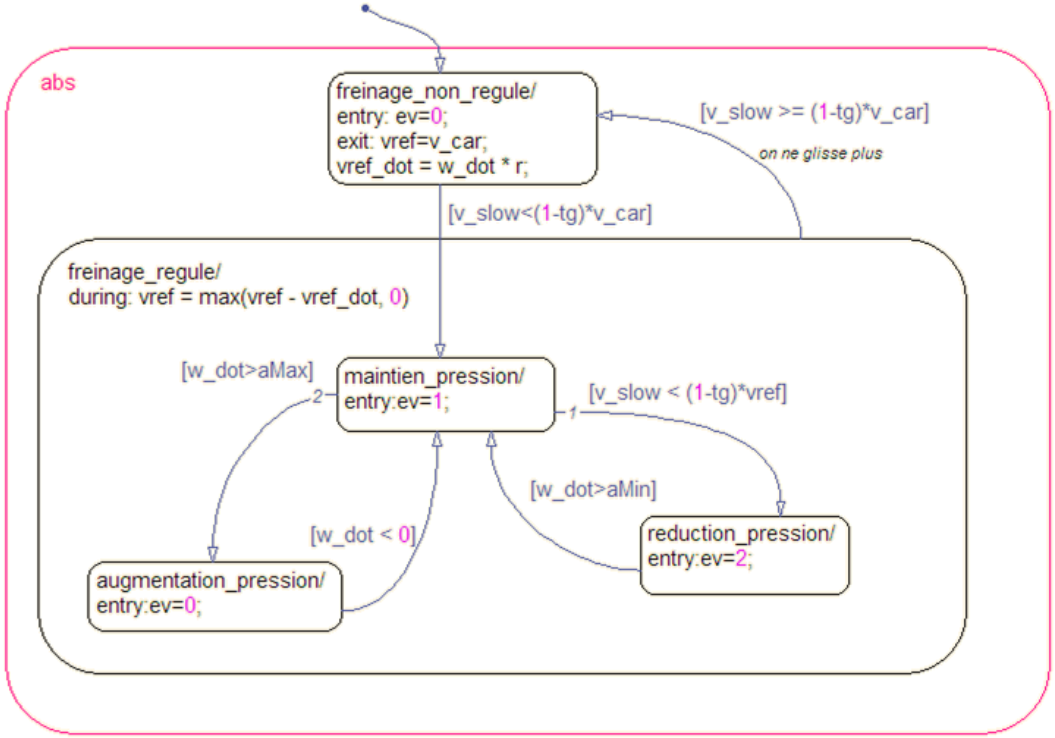
- Mode diminution de pression



ABS : Modèle Simulink



ABS : Diagramme d'états



ABS : Spécification

- 2 propriétés
  1. Le passage en mode régulé se fait dès que le taux de glissement est supérieur à 20 %
  2. Tant qu'une des roues est bloquée l'électrovanne doit être en position 2
     a. Dès qu'une des roues est bloquée l'électrovanne doit être en position 2
     b. Des roues bloquées à deux instants consécutifs entraînent que l'électrovanne doit être en position 2
- Pas de modèle du comportement du véhicule
  - Vitesse des roues comprise entre 0 et 50 $m.s^{-1}$

RAICP : Validation de programmes avec flottants

- Vérification de modèle bornée (*bounded model-checking*)
  - Dépliage de la boucle temps-réel
- Combinaison Interprétation Abstraite et Programmation par Contraintes
- Solveur correct sur les flottants
- Heuristique d'exploration des chemins exécutables
  - Graphe de flot de contrôle (CFG)
- Recherche d'une solution à la négation d'une assertion
  - Filtrage
  - Recherche exhaustive (produit un contre-exemple)

RAICP : ABS de série ?

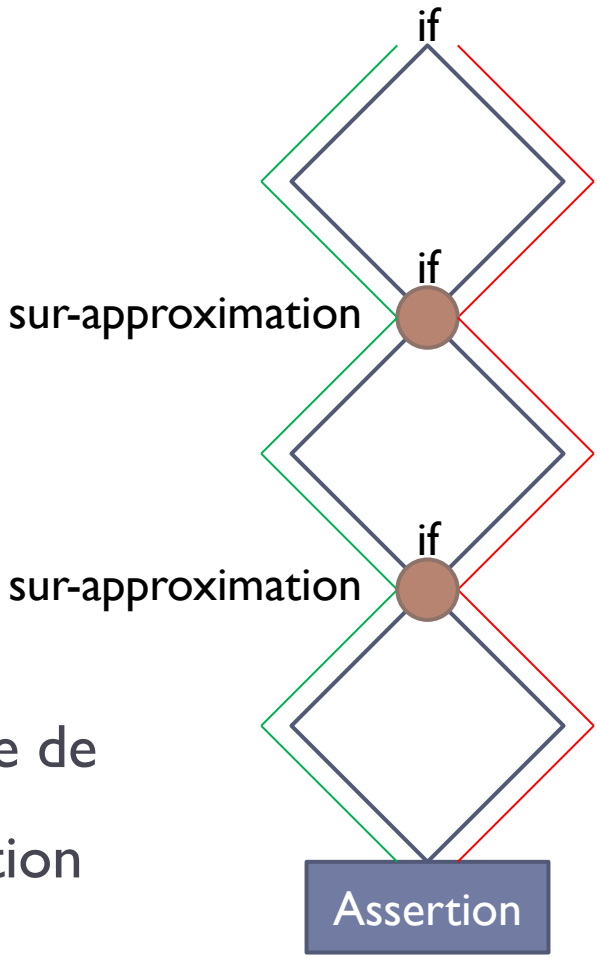
- Améliorations de la méthode et du prototype
  - Simplification symbolique
  - Heuristique incrémentale de recherche de contre-exemples
  - Combinaison avec un solveur sur les entiers
  - Gestion mémoire

RAICP : Simplification symbolique

- Problème
  - $a \in [0.0, 40.0], b \in [0.0, 40.0]$ $\quad\quad$ $a \geq b \wedge b < a$
  - Filtrage du solveur flottant énumère environ 2^62 valeurs
  - 150 siècles au rythme de 100 gigaFLOPS
- Solution
  - Module de simplification symbolique
    - Manipulations syntaxiques
  - Limites de l'arithmétique flottante

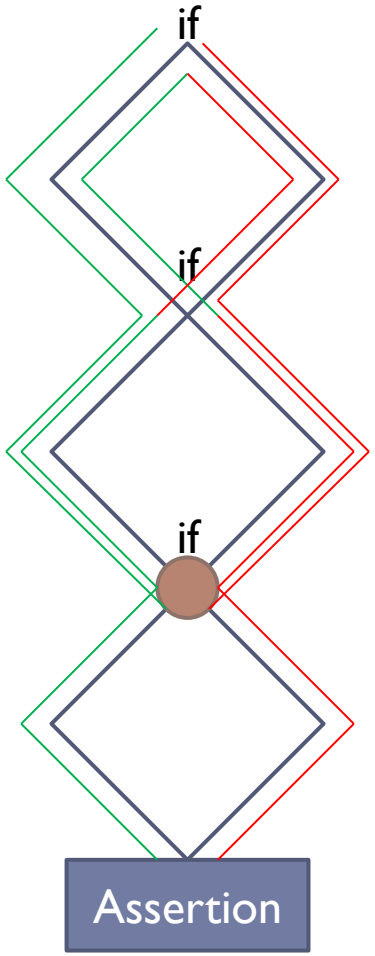
RAICP : Heuristique d'exploration

- Problème
  - Faux positifs
  - Absence de contre-exemple
- Solution
  - Améliorer la précision en diminuant les points de sur-approximation
  - Augmenter incrémentalement le nombre de nœuds de jonction avant sur-approximation



RAICP : Heuristique d'exploration

- Problème
  - Faux positifs
  - Absence de contre-exemple
- Solution
  - Améliorer la précision en diminuant les points de sur-approximation
  - Augmenter incrémentalement le nombre de nœuds de jonction avant fusion



RAICP : Solveurs flottant et entier

- Problème
  - Le solveur flottant… ne traite que les flottants
- Solution
  - Intégration d'un solveur sur les entiers
  - Communication via les domaines des variables partagées

RAICP : Gestion mémoire

- Problème
  - Taille du CFG (1000 dépliages : 75000 nœuds, 9000 variables)
  - Plusieurs solveurs en mémoire
  - Solveur flottant
    - 32 bits
    - Mémoire jamais libérée
  - Java
    - Machine virtuelle
    - Gestion du tas
- Solution
  - Optimisation mémoire de certains algorithmes
  - Améliorations du solveur flottant (version 64 bits avec libération de la mémoire)
  - Récupération de l'espace libre dans le tas de la machine virtuelle Java

Résultats : Propriété 1

Dépliages	CBMC		Fluctuat		RAICP	
	Validité	Temps (s)	Validité	Temps (s)	Validité	Temps (s)
1	valide	0.2	valide	0.1	valide	1.7
2	-	> 1h	?	0.2	valide	1.7
100	-	-	?	0.8	valide	14.6
1000	-	-	?	0.8	valide	351
2000	-	-	?	0.8	valide	1188
2500	-	-	?	0.8	valide	1802
3000	-	-	?	0.8	-	Mémoire

Résultats : Propriété 2

Propriété	Dépliages	CBMC		Fluctuat		RAICP	
		Validité	Temps (s)	Validité	Temps (s)	Validité	Temps (s)
P2a	1	valide	0.2	valide	0.1	valide	1.7
P2a	2	invalide	1.7	?	0.2	invalide	5.4
P2b	1	valide	0.3	valide	0.1	valide	1.7
P2b	2	invalide	1.8	?	0.2	invalide	6.7

Conclusion

- Etude de cas réel
  - Problème du passage à l'échelle
  - Améliorations du prototype
- Aspect contrôle-commande prépondérant
  - Limites de l'heuristique d'exploration du CFG actuelle