Comment les échecs de preuve peuvent aider à la correction de spécifications erronées de Systèmes Multi-Agents

B Mermet, Gaële Simon

Comment les échecs de preuve peuvent aider à la correction de spécifications erronées de Systèmes Multi-Agents

Bruno Mermet - Gaël Simon

A. GDT4MAS

Un modèle formel (LTL et Premier Ordre) de SMA

- Modélisation de l'environnement
- Modélisation des types d'agents
- Modélisation des instances de types d'agents

Un système de preuve

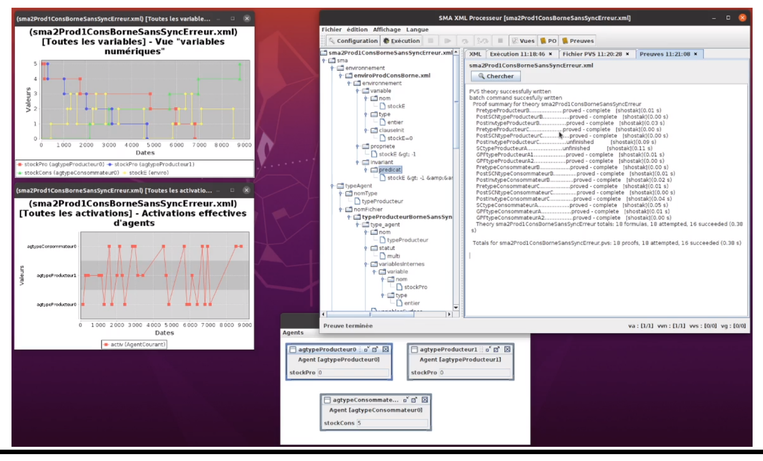
- Preuves de propriétés d'invariance
- Preuves de décompositions de buts en sous-buts
- des *schémas de preuve* pour traduire la spécification en *obligations de preuve*

Un modèle d'exécution

- Sémantique opérationnelle
- Équivalence prouvée entre la sémantique opérationnelle et le système de preuve

Un outil

- Génération des obligations de preuve
- Preuve automatique via un prouveur externe
- Exécution (différents modes) et visualisation



B. Échecs de preuve

Échec de preuve = théorème non prouvé

Causes

- théorème vrai mais non prouvable (incomplétude) ;
- limites du prouveur (GDT4MAS limite les risques) ;
- erreur dans la spécification.

Quelques types d'erreur

- Mauvais opérateur de décomposition de but en sous-buts
- Concurrence
- Mauvaise spécification d'un but
- Mauvais choix d'action

Premiers renseignements

- Obligations de preuve localisées
- $\Rightarrow$ échec d'une preuve localise l'origine du problème

C. Obligation de preuve

Une obligation de preuve (PO) est une formule de la forme $H(v) \rightarrow G(v)$ où :

- v désigne les variables pertinentes de l'agent et du système ;
- $H(v)$ sont les hypothèses de la PO ;
- $G(v)$ est le but de la PO.

Variables et PO

- Une variable x d'un agent est transformée en plusieurs variables (pour chaque instant considéré) dans une obligation de preuve (x_{-1}, x_0, etc.) ;
- Chaque terme d'une PO ne fait intervenir que des variables du même instant ou de 2 instants voisins.

Conditions nécessaires de preuve

L'une des conditions suivantes doit être vérifiée :

- Les hypothèses sont contradictoires ;
- Le but est une tautologie ;
- les hypothèses permettent d'établir une relation entre les différentes variables du but ;

D. Idée = Graphes de variables

Une obligation de preuve est spécifiée par :

- les variables v utilisées ;
- les termes apparaissant en hypothèse $H(v)$;
- le terme définissant son but $G(v)$;
- les variables v_g intervenant dans $G(v)$.

Graphe de variables associé à une PO

Graphe dont les nœuds sont les variables de la PO et dans lequel un arc entre 2 nœuds représente le fait que les 2 variables associées aux nœuds figurent dans un même terme des hypothèses $H(v)$.

Spécification erronnée

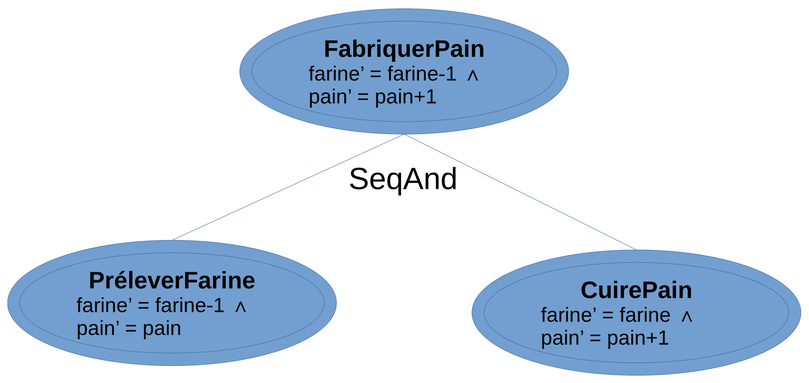
Dans le graphe de variables, il n'existe pas de chemin entre les variables v_g du but.

E. Exemple

La sandwicherie

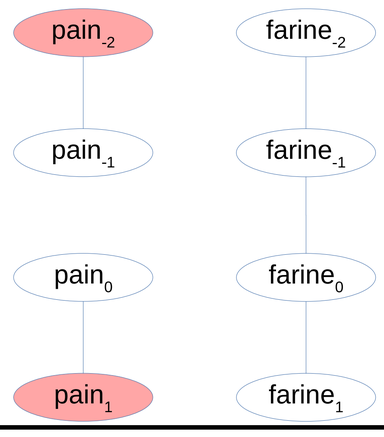
- des agents, les *boulangers*, fabriquent (et rendent disponibles) une baguette à partir d'une livre de farine ;
- des agents, les *cuisiniers*, utilisent une baguette disponible pour fabriquer un sandwitch ;
- les étagères permettent de stocker jusqu'à 20 pains en attente d'être utilisés.

Comportement du boulanger



Obligation de preuve de la décompostion du but racine

$farine_{-2} > 0 \wedge pain_{-2} < 2 \wedge farine_{-2} > -1 \wedge$
$pain_{-2} > -1 \wedge pain_{-2} < 3 \wedge$
$farine_{-1} = farine_{-2} - 1 \wedge pain_{-1} = pain_{-2} \wedge$
$farine_{-1} = farine_0 \wedge farine_{-1} > -1 \wedge$
$pain_{-1} > -1 \wedge pain_{-1} < 3 \wedge farine_0 > -1 \wedge$
$pain_0 > -1 \wedge pain_0 < 3 \wedge pain_1 = pain_0 + 1 \wedge$
$farine_1 = farine_0 \wedge farine_0 > -1 \wedge pain_0 > -1 \wedge$
$pain_0 < 3 \wedge farine_1 > -1 \wedge pain_1 > -1 \wedge pain_1 < 3$
$\rightarrow$
$pain_1 = pain_{-2} + 1$



F. Analyse des types d'erreur

Des cas discrimants

- problème de concurrence : arc manquant entre 2 nœuds correspondant à la même variable à 2 instants de part et d'autre d'un opérateur ;
- manque de condition de préservation : arc manquant entre 2 nœuds correspondant à la même variable à 2 instants de part et d'autre d'un but ;
- comportement incomplet : arc manquant entre 2 nœuds correspondant à la même variable à 2 instants de part et d'autre d'un but, non corrigé par l'ajout d'une condition de préservation.

Des cas "invisibles"

- Condition de satisfaction erronée ;
- Contexte déclencheur sous-spécifié ;
- Mauvais opérateur de décomposition.

Perspectives

- Discriminer les cas invisibles sur les graphes de variables ;
- Améliorer l'outil pour proposer des corrections automatiques lorsque c'est possible.