Automates et Vérification Formelle

Séance pratique : Passage à Niveau

Introduction

Le but de l'exercice est de modéliser un passage à niveau (l'intersection d'une voie ferrée et d'une voie de circulation automobile).

Les éléments (template UPPAAL) suivants sont attendus :

- Train : un train ;
- Warnings : des signaux d'avertissement ;
- Gate : une barrière ;
- Control : l'automate de control.

Le scénario nominal :

1. Le train est détecté en approche (état Far)
2. En réponse, les signaux sont activés
3. Le train est proche (état Close)
4. En réponse, la barrière est abaissée
5. Le train passe (état Passing)
6. En réponse, les signaux sont désactivés
7. Le train est passé (état Gone)
8. En réponse, la barrière est relevée

Les propriétés que le modèle devra vérifier portent sur

- l'absence de « deadlock » ;
- la sécurité (signaux activés et barrière abaissée quand il faut) ;
- la disponibilité (signaux désactivés et barrière relevée après passage).

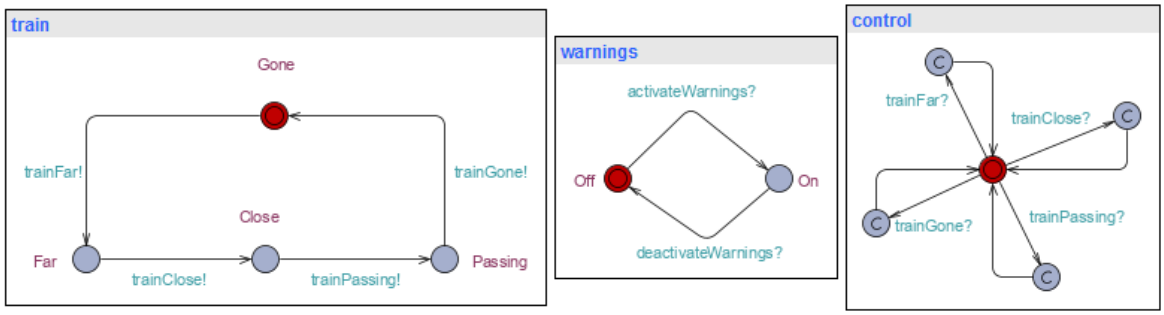
Hypothèses simplificatrices :

- Les règles de circulation sont respectées par les automobiles ;
- Pas de pannes ;
- Un seul train ;
- Les entrées et les sorties du contrôleur sont instantanés ;
- Le temps d'exécution du contrôleur est négligeable.

Des aspects liés au temps seront détaillés par la suite.

Etape 1 : « warnings »

On se limite ici au train, signaux et contrôle (pas de barrière) :



E1.Q1 : Reproduisez les automates ci-dessus avec UPPAAL.

E1.Q2 : Vérifiez l'absence de « deadlock » (P1).

E1.Q3 : Ajoutez une propriété vérifiant que les signaux sont actifs lorsque le train est « Close » (P2) ; constatez que la propriété n'est pas vérifiée.

E1.Q4 : Corrigez le modèle en conséquence (synchronisez « warnings » et « control »).

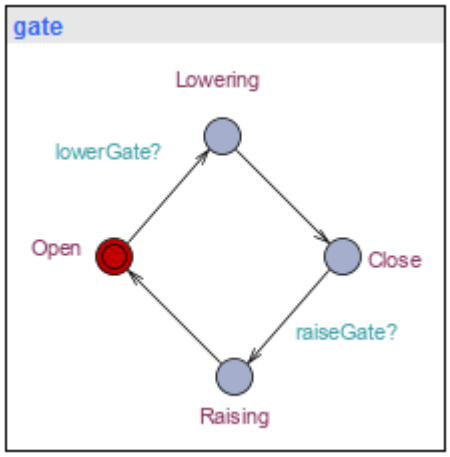
E1.Q5 : Ajoutez une propriété assurant que les signaux ne sont pas actifs lorsque le train est « Gone » (P3). Corrigez votre modèle si besoin pour que cette propriété passe.

Sauvegardez votre modèle sous le nom « PaN_step1 ».

Etape 2 : « Gate »

Sauvegardez votre modèle sous le nom « PaN_step2 ».

Au contraire des signaux, abaisser et relever la barrière peut prendre du « temps ». Pas d'aspects temporisés lors de cette étape mais on veut tout de même capturer les états intermédiaires.



E2.Q1 : Ajoutez le template ce-dessus à votre modèle.

E2.Q2 : Ajoutez une propriété vérifiant que la barrière est baissée lorsque le train est « Passing » (P4) ; constatez que la propriété n'est pas vérifiée.

E2.Q3 : Corrigez votre modèle pour que P4 passe. Certains états du template « Gate » devront être marqués « committed », lesquels et pourquoi ?

E2.Q4 : Ajoutez une propriété assurant que la barrière est ouverte lorsque le train est « Far » (P5).

Sauvegardez votre modèle (« PaN_step2 »).

Etape 3 : Temporisé

Sauvegardez votre modèle sous le nom « PaN_step3 ».

E3.Q1 : Déclarez une horloge « cTrain » et ajoutez gardes/invariants/reset au template « Train » pour assurer les contraintes suivantes :

- Le train reste dans l'état « Gone » au minimum 50 unités de temps et au maximum 100 unités de temps ;
- Le train reste dans chacun des états « Far », « Close » et « Passing » au minimum 5 unités de temps et au maximum 10 unités de temps.

E3.Q2 : De manière similaire, déclarez une horloge « cGate » et temporisez l'automate de la barrière (n'oubliez pas d'enlever les mentions « committed »). Proposez deux jeux de contraintes (pour la barrière), l'un assure que P4 est vérifiée, l'autre non.

E3.Q3 : Ajoutez une nouvelle propriété (P6) vérifiant que si la barrière se baisse elle finit éventuellement par être de nouveau ouverte.

Sauvegardez votre modèle (« PaN_step3 »).

Passage à Niveau : Réponses écrites

Note : Un étudiant par groupe me transmet vos modèles (« PaN_step1 », « PaN_step2 » et « PaN_step3 ») avant la fin de la séance (n'oubliez pas de préciser les autres membres de votre groupe). Pour rappel, mon adresse : luka.le_roux@ensta-bretagne.fr

Nom/Prénom des étudiants dans le groupe **:**

P1 :

P2 :

P3 :

P4 :

P5 :

P6 :

E2.Q3 « Lesquels et pourquoi ? » **:**

E3.Q2, dessinez les deux automates de la barrière avec leurs contraintes temporisées **:**

Vos commentaires (optionnels) **:**