TP NUSMV – évaluation de propriétés CTL

Environnement
NuSMV est installé sur les machines de la salle SAR. Vous pouvez également le télécharger et l'installer à partir du site : nusmv.fbk.eu

On nomme NUSMV le point d'installation ; le tutoriel et le manuel utilisateur sont dans le répertoire ($NUSMV)/share/nusmv/doc .
Un ensemble d'exemples de systèmes modélisés et analysés sont dans le répertoire ($NUSMV)/share/nusmv/examples .

Exercice 1.
Construisez la structure de Kripke de la figure 1 et évaluez la validité des propriétés suivantes :

- Dans l'état E1, p est VRAIE et q est FAUSSE
- L'état E1 satisfait : EX(p)
- L'état E6 satisfait : EpUq
- Tous les états sauf E0 satisfont EpUq (en une seule formule)
- L'ensemble des états satisfaisant p et dont au moins un successeur satisfait p est exactement : {E1, E3, E4, E6}.

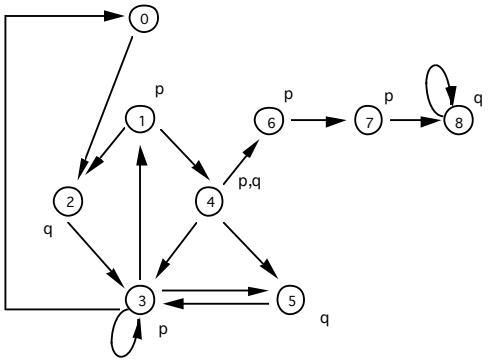

figure 1.

Exercice 2.
On considère deux processus concurrents asynchrones exécutant l'algorithme de synchronisation suivant, restreignant l'accès à une ressource critique. Les processus P et Q manipulent deux variables partagées `demP` et `demQ`, initialisées à `FAUX`.

```
processus P
   tant que VRAI faire
1      demP ← VRAI
2      tant que demQ=VRAI faire
3      finTq
4      <<SECTION CRITIQUE>>
5      demP ← FAUX
   finTq
```

```
processus Q
       tant que VRAI faire
1'             demQ ← VRAI
2'             tant que demP=VRAI faire
3'             finTq
4'             <<SECTION CRITIQUE>>
5'             demQ ← FAUX
       finTq
```

On souhaite vérifier les propriétés suivantes :

- P1 : l'exclusion mutuelle est garantie,
- P2 : tout processus demandant l'accès à la section critique finira (forcément) par l'obtenir,
- P3 : tout processus demandant l'accès à la section critique pourra l'obtenir,
- P4 : l'ordre d'accès à la section critique respecte l'ordre des demandes d'accès.

Proposez une modélisation de cet algorithme à partir de 2 processus concurrents (passez outre les mises en garde du tutoriel précisant qu'une telle modélisation est maintenant obsolète…). Avec ce formalisme des processus, la composition est asynchrone.

Décrivez les propriétés P1, P2, P3 et P4 en CTL et évaluez les sur le modèle. Qu'en concluez-vous ?

Proposez une correction de l'algorithme permettant d'éviter le blocage, et mieux encore, de satisfaire ces propriétés.

Exercice 3. Pour aller un peu plus loin : Synchronisation de feux de circulation (repris de T. Shiple 95)

On souhaite modéliser la synchronisation de deux feux de circulation régulant le flux de véhicules au croisement d'une route à grande circulation (appelée `highway`) et d'une route secondaire (appelée `smallway`). Le feu de la route à grande circulation est prioritaire sur celui de la route secondaire : le feu de la route secondaire ne passera au vert que s'il y a une voiture sur la route secondaire, et ce pour un temps borné.

Le système est modélisé par quatre automates synchrones, décrits ci-après :

- Un capteur placé au pied du feu de la route secondaire signale la présence de voiture sur cette route. C'est un automate à deux états, C_P (pour « car present ») et C_A (pour « car absent »), dont le changement d'état est indéterministe.
- Un temporisateur détermine les instants de changement de couleur des feux. Le temporisateur est déclenché par un signal `RESTART`. Le temporisateur peut être dans trois états : START (le décompte du temps à été déclenché), SHORT (la temporisation courte est atteinte), LONG (la temporisation longue est atteinte). A tout instant, le décompte du temps peut être réarmé par le signal `RESTART`.
- Le feu situé sur la route secondaire ; il peut être dans l'état GREEN, YELLOW ou RED. Ce feu peut réarmer le temporisateur lorsqu'il arrive dans l'état GREEN ou qu'il quitte l'état GREEN. Le passage de l'état YELLOW à l'état RED autorise le feu de la route principal à passer dans l'état GREEN.
- Le feu situé sur la route à grande circulation : il peut être dans l'état GREEN, YELLOW ou RED. Ce feu peut réarmer le temporisateur lorsqu'il arrive dans l'état GREEN ou qu'il quitte l'état GREEN. Le passage de l'état YELLOW à l'état RED autorise le feu de la route secondaire à passer dans l'état GREEN.

Les diagrammes des automates sont donnés sur la figure 2 (2.a à 2.d).

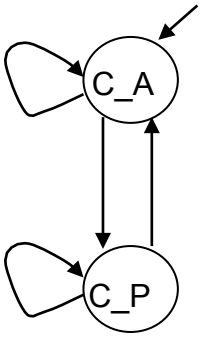

Figure 2.a : le capteur
(les transitions non étiquetées sont indéterministes)

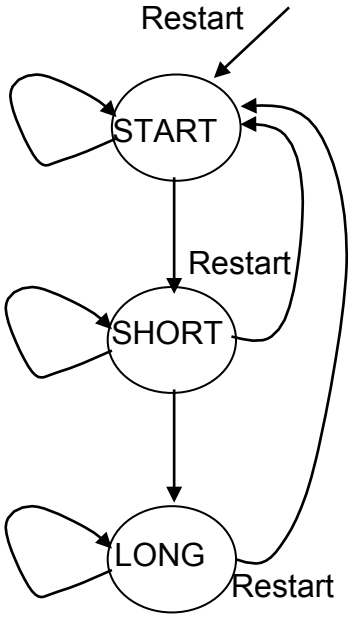

Figure 2.b Le temporisateur.
(les transitions non étiquetées sont indéterministes)

Les automates de contrôle des feux sont déterministes et couplés : le signal `Enable_hwy` est produit par le feu de la route secondaire, et apparaît comme une condition de franchissement sur l'automate du feu de la route principale. Symétriquement, le signal `Enable_small` est produit par le feu de la route principale et apparaît comme une condition de franchissement sur l'automate du feu de la route secondaire.

Sur l'automate du feu de la route secondaire, le signal `Enable_hwy` est positionné à VRAI lorsque l'automate franchit la transition menant de l'état YELLOW à l'état RED.
Sur l'automate de la route principale, le signal `Enable_small` est positionné à VRAI lorsque l'automate franchit la transition menant de l'état YELLOW à l'état RED.
Sur les automates contrôlant les feux, le signal `RESTART` est positionné quand l'un des deux automates passe de RED à GREEN ou de GREEN à YELLOW.

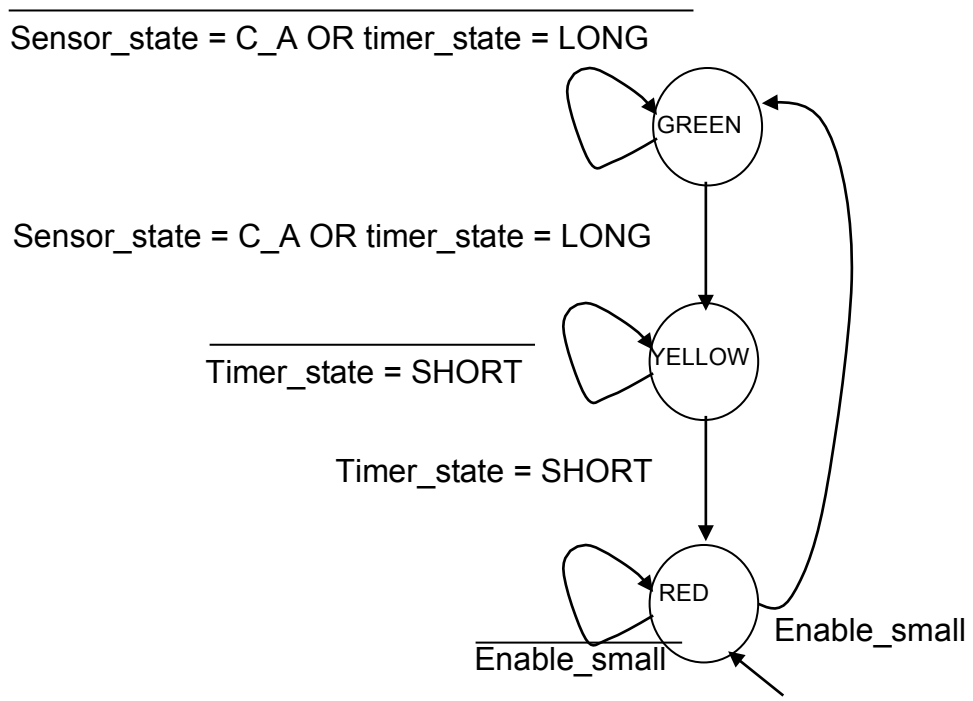

Figure 2.c. Le contrôle du feu de la route secondaire.
Ces transitions sont toutes déterministes.

Cet automate peut activer le signal `RESTART` du temporisateur et autoriser le passage au vert du feu de la route principale en positionnant le signal `Enable_hwy`.

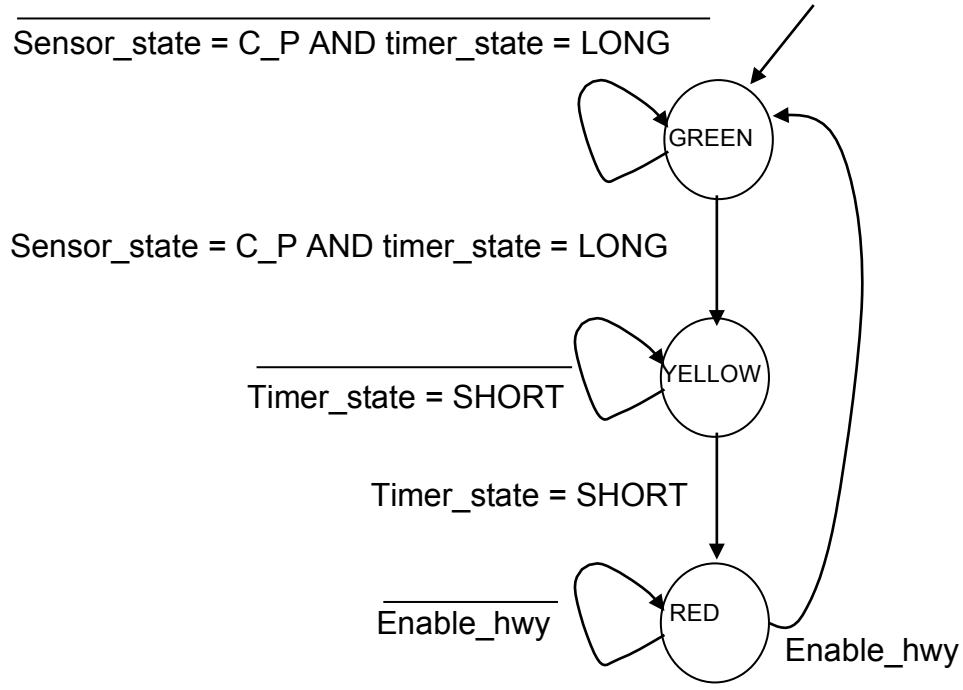

Figure 2.d. Le contrôle du feu de la route principale.
Ces transitions sont toutes déterministes.

Cet automate peut activer le signal `RESTART` du temporisateur et autoriser le passage au vert du feu de la route secondaire en positionnant le signal `Enable_small`.

Proposez une modélisation en NuSMV de ce système. Vous pourrez proposer une modélisation plus réaliste du capteur (mais il faudra introduire d'autres signaux).

Vous chercherez à vérifier des propriétés suivantes :

- si un des feux est à GREEN alors l'autre est forcément ORANGE ou RED
- chaque feux repassera dans l'état GREEN
- une voiture restant suffisamment longtemps en attente d'accès au carrefour finira par y avoir accès.

Vous serez amenés à introduire des contraintes d'équité pour assurer la progression du système.