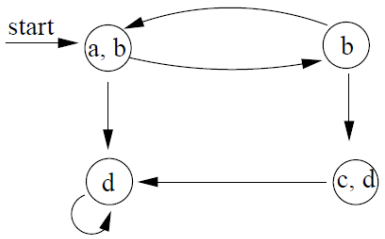
Validation des systèmes embarqués : Model Checking

TD3 : NuSMV

Nga Nguyen

Question 1 : Installez NuSMV (http://nusmv.fbk.eu/) et testez les exemples en cours (Compteur modulo 4 et Request)

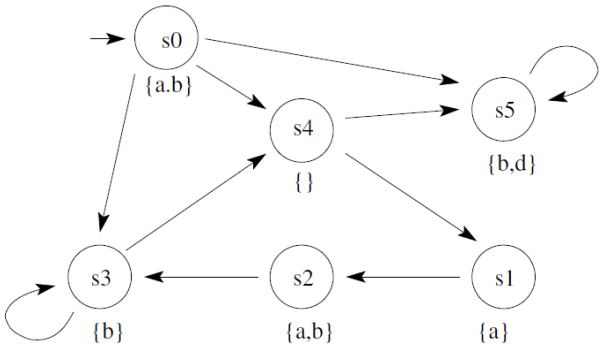
Question 2 : Vérifiez si les formules CTL suivantes sont vraies par rapport à la structure Kripke donnée en utilisant NuSMV.



1. $\mathbf{EG}\, d$
2. $\mathbf{EF}\, \mathbf{EG}\, d$
3. $\mathbf{EF}\, \mathbf{AG}\, d$
4. $\mathbf{AG}\, \mathbf{EF}\, d$
5. $\mathbf{A}\, [b\, \mathbf{U}\, c]$
6. $\mathbf{A}\, [b\, \mathbf{U}\, d]$

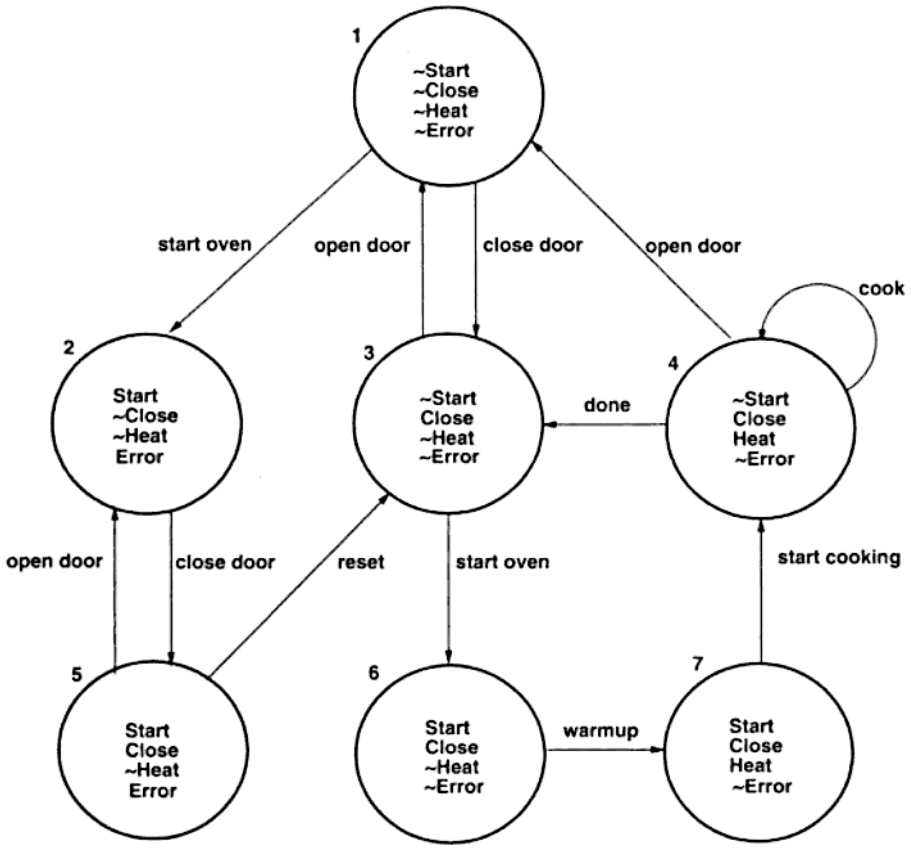
Question 3 : Vérifiez si les formules CTL suivantes sont vraies par rapport à la structure Kripke donnée en utilisant NuSMV.

a. $\mathbf{A}(a\, \mathbf{U}\, b)$
b. $\mathbf{AX}\, \mathbf{E}(a\, \mathbf{U}\, b)$
c. $\mathbf{AX}\, \mathbf{EX}\, \mathbf{A}(a\, \mathbf{U}\, b)$
d. $\mathbf{AG}\, \mathbf{AF}\, \mathbf{A}(a\, \mathbf{U}\, b)$
e. $\mathbf{AG}(d \Rightarrow \mathbf{AG}\, \neg a)$



Question 4 : Votre micro-onde est-t-il dangereux ? ☺

a. AG(Close -> AX(!Start -> !Error))
b. AG(Heat -> AX(!Close -> Error))
c. AG(Error -> A [Error U !Start])
d. AG EF Heat
e. A [!Heat U Close]



Question 5 : **Triple Modular Redundant System**

Considérons un système Triple Modular Redundant (TMR) avec 3 processeurs et un électeur. Dans un souci de fiabilité (possibilité qu'un processeur tombe en panne), un programme est lancé sur les 3 processeurs. L'électeur prend la majorité des votes des sorties des 3 processeurs. Si un processeur tombe en panne, le système peut toujours fournir un résultat fiable. Chaque composant est réparable. On suppose qu'à un moment donné, un seul composant peut tomber en panne et on répare un composant à la fois. Lorsque l'électeur tombe en panne, la totalité du système tombe en panne. Lorsque l'électeur est réparé, le système repart avec la totalité des composants qui fonctionnent. On considère que le système est opérationnel lorsque nous avons au moins deux processeurs en état de fonctionnement (en plus de l'électeur).

1. Construire le système de transitions représentant le TMR.
2. Traduire les énoncés suivants en formules CTL et pour chacune dire si le système la satisfait :
   a) Il se peut que le système ne tombe jamais en panne. (*Possibly the system never goes down*)
   b) Le système ne tombe jamais en panne. (*Invariantly the system never goes down*)
   c) Il est toujours possible de redémarrer le système. (*It's always possible to start as new*)
   d) Le système finit toujours par tomber en panne et est toujours opérationnel jusqu'au moment où il tombe en panne. (*The system always eventually goes down and is operational until going down*)