Projet Systèmes Hybrides : Propriétés (2)

Frédéric Gouaisbaut, Pauline Ribot

LAAS-CNRS

11 janvier 2023

Sommaire

Propriétés dans les SED

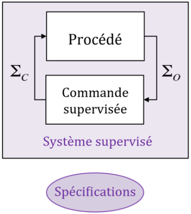
- Accessibilité : $Ac(A) = \{x \in X \mid \exists m \in \Sigma^* \text{ avec } \delta^*(x_0, m) = x\}$.
  Un état x est accessible s'il existe un chemin entre x_0 et x.
  Un automate A est accessible si tous ces états sont accessibles : $Ac(A) = X$.
- Coaccessibilité : $Co(A) = \{x \in X \mid \exists m \in \Sigma^*, \text{ avec } \delta^*(x, m) \in X_f\}$.
  Un état x est co-accessible s'il existe un chemin reliant x à un état marqué.
  Un automate A est coaccessible si tous ces états sont coaccessibles : $Co(A) = X$.
- Automate non bloquant : $Ac(A) \subseteq Co(A)$.
  Un automate est bloquant s'il existe un état x accessible ne permettant pas d'atteindre un état marqué de X_f. Un automate est non bloquant s'il existe un chemin depuis n'importe quel état accessible de la commande vers un état marqué.

Analyse des SED

- Propriétés de safety and de blocage dans les automates déterministes : problème d'atteignabilité d'états non désirés.
- Propriété d'observabilité dans un SED partiellement observable : estimation/reconstruction de trajectoires pour analyser le fonctionnement et détecter l'occurrence d'un événement non désiré et non observable [LW88][Ram86].
- Propriété de contrôlabilité (issue de la commande supervisée [RW87])
- Propriété de stabilité dans les SED [GM91][ÖWA91]

Remarque : le model-checking est une technique de vérification formelle qui vérifie que la commande valide une spécification donnée en explorant toutes les trajectoires possibles pour identifier les erreurs.

Contrôlabilité de la commande supervisée - 1



- Procédé : système physique en fonctionnement qui envoie tous les événements observables E_o (contrôlables ou non) à la commande supervisée et reçoit les événements contrôlables autorisés à se produire. Son évolution dépend également des événements non contrôlables.
- Spécifications : ensemble de contraintes et d'objectifs que le système supervisé doit respecter
- Commande supervisée : système recevant les événements observables générés par le procédé et lui renvoyant la liste des événements contrôlables E_c autorisés à se produire

Contrôlabilité de la commande supervisée - 2

Vérification de l'obtention des deux propriétés suivantes :

- Contrôlabilité : la commande supervisée ne contient aucun événement non contrôlable causant des transitions vers des états spécifiquement interdits
- Non blocage : il existe un chemin depuis n'importe quel état accessible de la commande supervisée vers un état marqué

Observabilité dans un SED

Observabilité : définie comme la capacité à reconstruire la connaissance de l'état quand seulement l'occurrence de certains événements est disponible comme quantités directement observables.

K et M deux langages sur E : K est dit observable pour M, E_o et E_c si pour tout $s \in \overline{K}$ ($\overline{K} = L(S/G)$) et pour tout $\sigma \in E_c$,

$$(s\sigma \notin \overline{K}) \text{ and } (s\sigma \in M) \Rightarrow P_o^{-1}[P_o(s)]\sigma \cap \overline{K} = \emptyset. \tag{1}$$

(il n'y a pas dans $\overline{K}$ des séquences qui ont la même trajectoire observable que s continuée par σ).

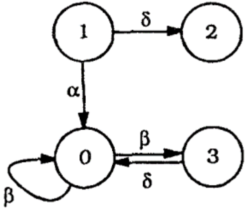
Si on ne peut pas différencier 2 trajectoires, alors ces trajectoires nécessite la même action de contrôle.

Stabilité d'un SED - 1

Extension de la théorie de la commande supervisée de Ramadge & Wonham : on cherche une méthode de commande supervisée pour rétablir un comportement autorisé après l'occurrence d'un ou plusieurs événements anormaux.

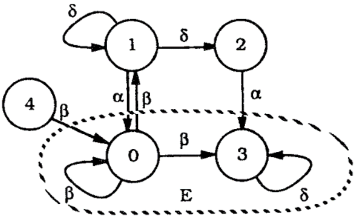
- Définition des états autorisés E (*legal*) et des états interdits (*illegal*)
- On teste si toutes les trajectoires possibles à partir des états permettent de revenir dans ces états autorisés, de telle sorte que le système se répare en un nombre fini de transitions.
  Un état x est stable si toutes les trajectoires à partir de x permettent de rejoint E en un nombre fini de transitions.

Stabilité d'un SED - 2



- Etat bloquant (*dead state*) : état à partir duquel aucun événements ne peut se produire
- Etat vivant : état n'amenant pas à un état bloquant

Stabilité d'un SED - 3



- Ensemble d'états autorisés (légaux) $E \subseteq X : E = \{0, 3\}$.
- Etat x stable si tous les chemins à partir de x permettent de rejoint E en un nombre fini de transitions, donc ici états 2 et 3 stables.
- Etat 1 non stable à cause du cycle avec δ , états 0 et 4 sont non stables même si $O \in E$ car la transition avec β mène à l'état 1.

Remarque : Un système stabilisable est un système pour lequel il existe un superviseur qui rende le système stable (utilisation d'algorithmes pour construire un superviseur stabilisant minimal basé sur le concept de régions d'attraction).

Définitions

- La notion de stabilité est une notion plus délicate à définir pour les systèmes hybrides.
- En général, l'utilisation d'états fictifs (timer, état discret) oblige à considérer la notion de stabilité d'un ensemble (et non pas la stabilité d'un point d'équilibre).
  Par exemple, l'état d'un système asservi par une loi de commande à temps discret et un bloqueur est $\begin{bmatrix} x \\ u \\ \tau \end{bmatrix}$. Si nous voulons prouver que l'état du système à TC converge vers 0, nous allons nous intéresser à la stabilité de l'ensemble

$$\mathcal{A} = \{0\} \times \mathbb{R}^m \times [0, T_e]$$

Définitions

Avant toute chose, définissons une notion de distance :

$$|x|_{\mathcal{A}} = \inf_{y \in \mathcal{A}} |x - y|,$$

où $|.|$ est une distance pour $\mathbb{R}^n$. Une définition de la stabilité exponentielle (on aurait pu imaginer un autre type de stabilité) :

Definition

On considère un ensemble $\mathcal{A}$ fermé. Cet ensemble est dit GES (globalement exponentiellement stable) ssi, il existe a, b deux scalaires positifs tels que les solutions ϕ du système hybride $\mathcal{H}$ s'écrivent :

$$|\phi(t,j)|_{\mathcal{A}} \leq ae^{(-b(t+j))}|\phi(0,0)|_{\mathcal{A}}, \forall (t,j) \in dom(\phi)$$

Prouver qu'un ensemble est stable n'est pas forcément facile directement, on utilise alors des conditions suffisantes déterminées à l'aide de fonction de Lyapunov.

Utilisation des fonctions de Lyapunov

Idées générales :

- On choisit une fonction de Lyapunov [1].
- L'idée générale est que cette fonction de Lyapunov doit décroitre le long des trajectoires :
  - La fonction de Lyapunov décroit durant le flot et les sauts.
  - La fonction de Lyapunov n'augmente pas durant le flot, mais décroit durant les sauts (il faut suffisamment de sauts).
  - La fonction de Lyapunov n'augmente pas durant les sauts, mais décroit durant le flot (Les états du système restent dans le flot suffisamment longtemps).
  - On peut imaginer également qu'une augmentation limitée est compensée par une plus forte décroissance.

1. Qui se trouve ressembler à la distance $|.|_{\mathcal{A}}$.

RKV Garg and SI Marcus.
Stability of discrete event system behavior.
IFAC Proceedings Volumes, 24(5) :17–22, 1991.

Feng Lin and Walter Murray Wonham.
On observability of discrete-event systems.
Information sciences, 44(3) :173–198, 1988.

Cüneyt M Özveren, Alan S Willsky, and Panos J Antsaklis.
Stability and stabilizability of discrete event dynamic systems.
Journal of the ACM (JACM), 38(3) :729–751, 1991.

Peter J Ramadge.
Observability of discrete event systems.
In *1986 25th IEEE conference on decision and control*, pages 1108–1112. IEEE, 1986.

Peter J Ramadge and W Murray Wonham.
Supervisory control of a class of discrete event processes.

SIAM journal on control and optimization, 25(1) :206–230, 1987.