

Modèles Symboliques de Systèmes Dynamiques pour la Conception de Systèmes Embarqués Sûrs

Antoine Girard

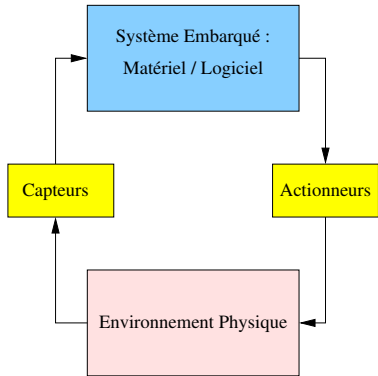
Laboratoire Jean Kuntzmann, Université Joseph Fourier
antoine.girard@imag.fr



*Colloque en hommage à Louis Bolliet
Grenoble, 16 mai 2008*

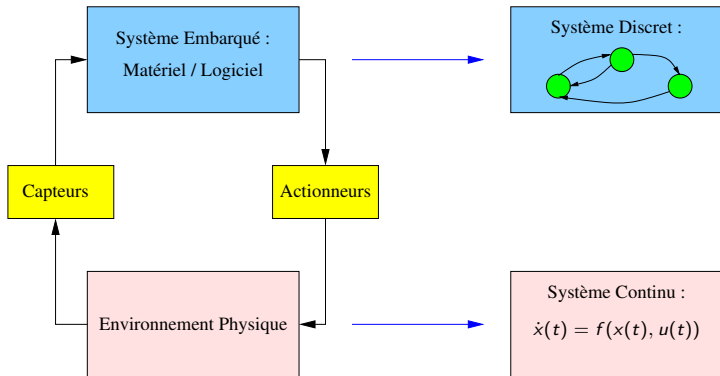


Informatique Embarquée

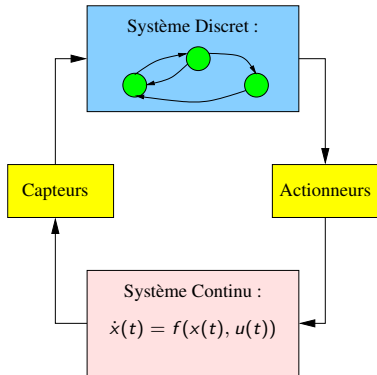


- Fonction du système embarqué : régulation d'un environnement physique.
- Prise en compte des propriétés dynamiques de l'environnement physique pour la conception.
- Domaines d'application : transport, robotique, médecine...
- Sûreté de fonctionnement est critique.

Modélisation Mathématique



Système Dynamique Hybride



- Analyse d'un système dynamique hybride nécessaire pour la conception du système embarqué.
- Difficulté majeure : comportement ni énumérable, ni continu.
- Solution proposée : utilisation de modèles symboliques pour la dynamique continue.

Modèle Symbolique d'un Système Continu

- Système discret dont la dynamique est équivalente à celle du système continu :

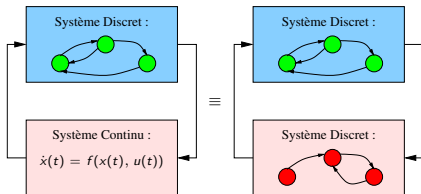


Modèle Symbolique d'un Système Continu

- Système discret dont la dynamique est équivalente à celle du système continu :



- L'analyse du système hybride se ramène à celle d'un système discret :



Modèle Symbolique d'un Système Continu

- Permet d'utiliser des outils algorithmiques pour la vérification ou la conception : model checking, contrôle par supervision...

Modèle Symbolique d'un Système Continu

- Permet d'utiliser des outils algorithmiques pour la vérification ou la conception : model checking, contrôle par supervision...
- Cependant, un système dynamique continu non-trivial n'admet généralement pas de système discret équivalent.

Modèle Symbolique d'un Système Continu

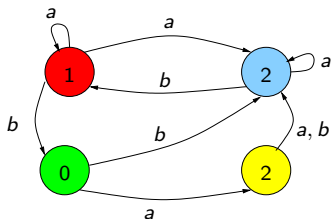
- Permet d'utiliser des outils algorithmiques pour la vérification ou la conception : model checking, contrôle par supervision...
- Cependant, un système dynamique continu non-trivial n'admet généralement pas de système discret équivalent.
- Demander une équivalence stricte est trop forte :
 - Ensemble d'états infini/fini,
 - Oubli fondamental : ensemble d'états du système continu est un espace métrique (notion quantitative d'approximation),
 - Recherche d'un système discret approximativement équivalent.

Plan de l'Exposé

1. Equivalence approchée de systèmes dynamiques
 - Systèmes de transitions
 - Bisimulation approchée
2. Modèles symboliques de systèmes continus
 - Construction du modèle symbolique
 - Résultat d'approximation
3. Applications
 - Contrôle d'un pendule
 - Contrôle d'un convertisseur de puissance DC/DC

Système de Transitions

- Modèle abstrait de système dynamique (discret ou continu).
- Un système de transitions T est défini par
 - un ensemble (fini ou infini) d'états Q ;
 - un ensemble (fini ou infini) d'étiquettes ou actions L ;
 - une relation de transition $\longrightarrow \subseteq Q \times L \times Q$;
 - un ensemble d'observation O ;
 - une fonction d'observation $H : Q \rightarrow O$.



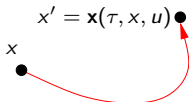
Système Dynamique Continu

- Un système dynamique continu Σ est défini par
 - un ensemble d'états \mathbb{R}^n ;
 - un ensemble (fini ou infini) d'entrées U ;
 - un champ de vecteurs $f : \mathbb{R}^n \times U \rightarrow \mathbb{R}^n$.
- Soit $\mathbf{u} : \mathbb{R}^+ \rightarrow U$ une fonction d'entrée continue par morceaux, on dénote par $\mathbf{x}(t, \mathbf{x}, \mathbf{u})$ la solution de l'équation différentielle :

$$\dot{\mathbf{x}}(t) = f(\mathbf{x}(t), \mathbf{u}(t)), \mathbf{x}(0) = \mathbf{x}.$$

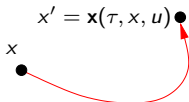
Système de Transitions de Σ

- Soit $\tau > 0$ un paramètre d'échantillonnage en temps, on associe le système de transitions $T_\tau(\Sigma)$ où :
 - l'ensemble d'états est $Q = \mathbb{R}^n$;
 - l'ensemble des actions est $L = U$;
 - la transition $x \xrightarrow{u} x'$ ssi $\mathbf{x}(\tau, x, u) = x'$;
 - l'ensemble d'observation est $O = \mathbb{R}^n$;
 - la fonction d'observation est l'application identique.



Système de Transitions de Σ

- Soit $\tau > 0$ un paramètre d'échantillonnage en temps, on associe le système de transitions $T_\tau(\Sigma)$ où :
 - l'ensemble d'états est $Q = \mathbb{R}^n$;
 - l'ensemble des actions est $L = U$;
 - la transition $x \xrightarrow{u} x'$ ssi $\mathbf{x}(\tau, x, u) = x'$;
 - l'ensemble d'observation est $O = \mathbb{R}^n$;
 - la fonction d'observation est l'application identique.

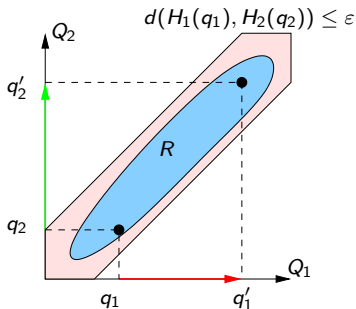


- On veut déterminer un **système de transitions avec des ensembles d'états et d'actions finis et approximativement équivalent à $T_\tau(\Sigma)$.**

Notion d'Equivalence Approchée¹

Soit T_1 et T_2 des systèmes de transitions observés sur un espace métrique commun (O, d) , et $\varepsilon \in \mathbb{R}^+$, une relation $R \subseteq Q_1 \times Q_2$ est une **relation de bisimulation ε -approchée** si pour tout $(q_1, q_2) \in R$:

- $d(H_1(q_1), H_2(q_2)) \leq \varepsilon$;
- $\forall q_1 \xrightarrow{1} q'_1, \exists q_2 \xrightarrow{2} q'_2$,
tel que $(q'_1, q'_2) \in R$;
- $\forall q_2 \xrightarrow{2} q'_2, \exists q_1 \xrightarrow{1} q'_1$,
tel que $(q'_1, q'_2) \in R$.



¹[Girard & Pappas; 2007]

Notion d'Equivalence Approchée

- Les systèmes de transitions T_1 et T_2 sont **approximativement bisimilaires avec précision ε** (noté $T_1 \sim_\varepsilon T_2$) si :
 - Pour tout $q_1 \in Q_1$, il existe $q_2 \in Q_2$, tel que $(q_1, q_2) \in R$;
 - Pour tout $q_2 \in Q_2$, il existe $q_1 \in Q_1$, tel que $(q_1, q_2) \in R$.
- Remarque : si $\varepsilon = 0$, on retrouve la notion usuelle de bisimulation (“exacte”).

Plan de l'Exposé

1. Equivalence approchée de systèmes dynamiques
 - Systèmes de transitions
 - Bisimulation approchée
2. Modèles symboliques de systèmes continus
 - Construction du modèle symbolique
 - Résultat d'approximation
3. Applications
 - Contrôle d'un pendule
 - Contrôle d'un convertisseur de puissance DC/DC

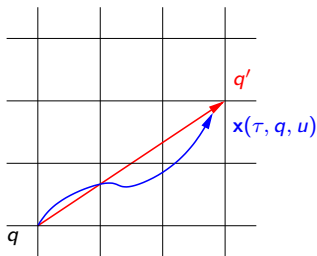
Construction du Modèle Symbolique

- Approximation discrète de l'ensemble d'états \mathbb{R}^n :

$$[\mathbb{R}^n]_\eta = \left\{ q \in \mathbb{R}^n \mid q_i = k_i \frac{2\eta}{\sqrt{n}}, k_i \in \mathbb{Z}, i = 1, \dots, n \right\},$$

où $\eta \in \mathbb{R}^+$ est un paramètre d'échantillonnage en espace.

- Approximation de la relation de transition (pour U fini) :



Construction du Modèle Symbolique

- On définit le système de transitions discret $T_{\tau,\eta}(\Sigma)$ où :
 - l'ensemble d'états est $Q = [\mathbb{R}^n]_{\eta}$;
 - l'ensemble des actions est $L = U$;
 - la transition $q \xrightarrow{u} q'$ ssi $\|\mathbf{x}(\tau, q, u) - q'\| \leq \eta$;
 - l'ensemble d'observation est $O = \mathbb{R}^n$;
 - la fonction d'observation est donnée par $H(q) = q \in \mathbb{R}^n$.

Construction du Modèle Symbolique

- On définit le système de transitions discret $T_{\tau,\eta}(\Sigma)$ où :
 - l'ensemble d'états est $Q = [\mathbb{R}^n]_{\eta}$;
 - l'ensemble des actions est $L = U$;
 - la transition $q \xrightarrow{u} q'$ ssi $\|\mathbf{x}(\tau, q, u) - q'\| \leq \eta$;
 - l'ensemble d'observation est $O = \mathbb{R}^n$;
 - la fonction d'observation est donnée par $H(q) = q \in \mathbb{R}^n$.
- Les systèmes $T_{\tau}(\Sigma)$ et $T_{\tau,\eta}(\Sigma)$ sont ils approximativement bisimilaires ?

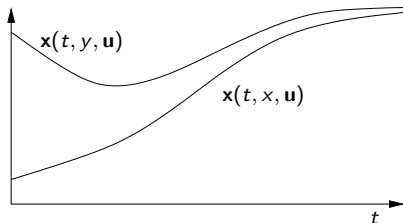
Construction du Modèle Symbolique

- On définit le système de transitions discret $T_{\tau,\eta}(\Sigma)$ où :
 - l'ensemble d'états est $Q = [\mathbb{R}^n]_{\eta}$;
 - l'ensemble des actions est $L = U$;
 - la transition $q \xrightarrow{u} q'$ ssi $\|\mathbf{x}(\tau, q, u) - q'\| \leq \eta$;
 - l'ensemble d'observation est $O = \mathbb{R}^n$;
 - la fonction d'observation est donnée par $H(q) = q \in \mathbb{R}^n$.
- Les systèmes $T_{\tau}(\Sigma)$ et $T_{\tau,\eta}(\Sigma)$ sont ils approximativement bisimilaires ?
- Oui, si Σ est **incrémentalement stable**.

Stabilité Incrémentale

- Le système dynamique continu Σ est **incrémentalement globalement asymptotiquement stable** (δ -GAS) si il existe une fonction β de classe \mathcal{KL} telle que, pour toute fonction d'entrée $\mathbf{u} : \mathbb{R}^+ \rightarrow U$, pour tout $t \in \mathbb{R}^+$, $x, y \in \mathbb{R}^n$,

$$\|\mathbf{x}(t, x, \mathbf{u}) - \mathbf{x}(t, y, \mathbf{u})\| \leq \beta(\|x - y\|, t) \xrightarrow[t \rightarrow +\infty]{} 0.$$



- Intuitivement, système avec mémoire limitée.

Résultat d'Approximation²

- Soit $\tau > 0$, $\eta > 0$ des paramètres d'échantillonnage en temps et en espace ; si Σ est δ -GAS, alors $T_\tau(\Sigma)$ et $T_{\tau,\eta}(\Sigma)$ sont approximativement bisimilaires.

²[Girard, Pola & Tabuada ; 2008]

Résultat d'Approximation²

- Soit $\tau > 0$, $\eta > 0$ des paramètres d'échantillonnage en temps et en espace ; si Σ est δ -GAS, alors $T_\tau(\Sigma)$ et $T_{\tau,\eta}(\Sigma)$ sont approximativement bisimilaires.
- Une précision arbitraire ε peut être garantie en choisissant convenablement le paramètre η (relation explicite).

²[Girard, Pola & Tabuada ; 2008]

Résultat d'Approximation²

- Soit $\tau > 0$, $\eta > 0$ des paramètres d'échantillonnage en temps et en espace ; si Σ est δ -GAS, alors $T_\tau(\Sigma)$ et $T_{\tau,\eta}(\Sigma)$ sont approximativement bisimilaires.
- Une précision arbitraire ε peut être garantie en choisissant convenablement le paramètre η (relation explicite).
- Si on ne s'intéresse à la dynamique de Σ que sur un compact de \mathbb{R}^n , alors $T_{\tau,\eta}(\Sigma)$ a un nombre fini d'états.

²[Girard, Pola & Tabuada ; 2008]

Résultat d'Approximation²

- Soit $\tau > 0$, $\eta > 0$ des paramètres d'échantillonnage en temps et en espace ; si Σ est δ -GAS, alors $T_\tau(\Sigma)$ et $T_{\tau,\eta}(\Sigma)$ sont approximativement bisimilaires.
- Une précision arbitraire ε peut être garantie en choisissant convenablement le paramètre η (relation explicite).
- Si on ne s'intéresse à la dynamique de Σ que sur un compact de \mathbb{R}^n , alors $T_{\tau,\eta}(\Sigma)$ a un nombre fini d'états.
- Résultat généralisable si U est compact (nécessite un échantillonnage de U).

²[Girard, Pola & Tabuada ; 2008]

Plan de l'Exposé

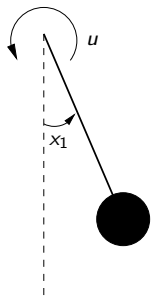
1. Equivalence approchée de systèmes dynamiques
 - Systèmes de transitions
 - Bisimulation approchée
2. Modèles symboliques de systèmes continus
 - Construction du modèle symbolique
 - Résultat d'approximation
3. Applications
 - Contrôle d'un pendule
 - Contrôle d'un convertisseur de puissance DC/DC

Contrôle d'un Pendule

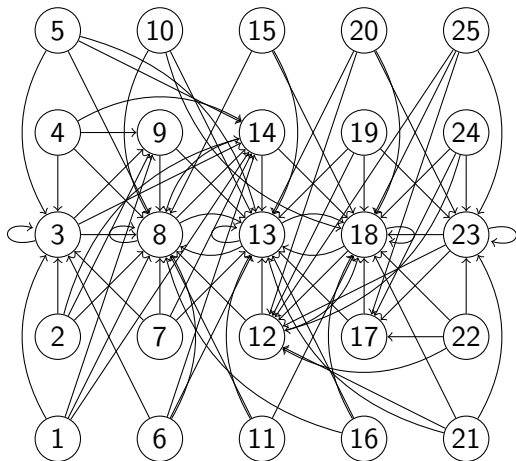
- Equation du mouvement d'un pendule contrôlé :

$$\begin{cases} \dot{x}_1 = x_2 \\ \dot{x}_2 = -\frac{g}{l} \sin(x_1) - \frac{k}{m} x_2 + u \\ -1.5 \leq u \leq 1.5 \end{cases}$$

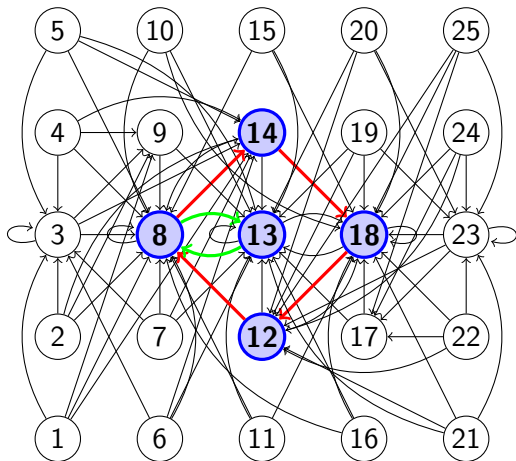
- Système dynamique incrémentalement stable.
- Calcul d'un modèle symbolique de précision $\varepsilon = 0.25$ avec $\tau = 2$, $\eta = 0.2$.



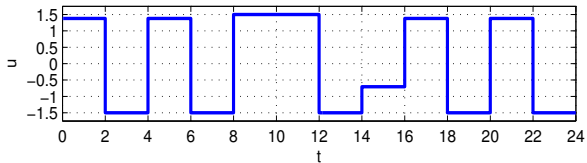
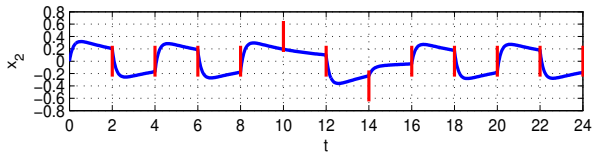
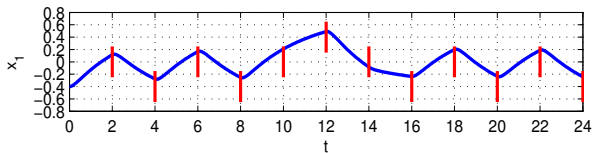
Modèle Symbolique d'un Pendule



Contrôle du Modèle Symbolique

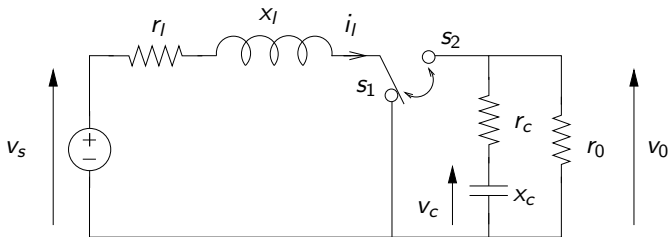


Trajectoire Correspondante du Pendule



Contrôle d'un Convertisseur de Puissance DC/DC

- Circuit électrique avec commutateur :



- Variable d'états $x(t) = [i_l(t), v_c(t)]^T$.
- Objectif : réguler la tension de sortie (propriété d'invariance).

Convertisseur de Puissance DC/DC

- Dynamique continue du système :

$$\dot{x} = A_u x + b, \quad u \in \{1, 2\}.$$

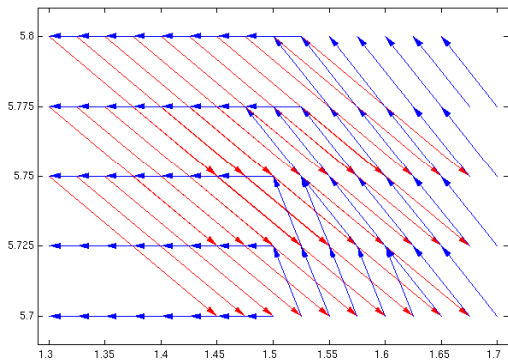
où

$$A_1 = \begin{bmatrix} -\frac{r_l}{x_l} & 0 \\ 0 & -\frac{1}{x_c} \frac{1}{r_0+r_c} \end{bmatrix}, \quad A_2 = \begin{bmatrix} -\frac{1}{x_l} \left(r_l + \frac{r_0 r_c}{r_0+r_c} \right) & -\frac{1}{x_l} \left(\frac{r_0}{r_0+r_c} \right) \\ \frac{1}{x_c} \frac{r_0}{r_0+r_c} & -\frac{1}{x_c} \frac{1}{r_0+r_c} \end{bmatrix}, \quad b = \begin{bmatrix} \frac{v_s}{x_l} \\ 0 \end{bmatrix}.$$

- Système dynamique incrémentalement stable.

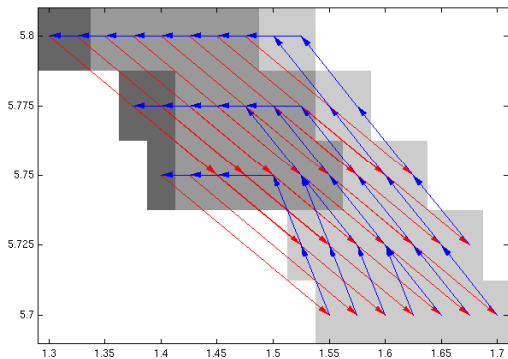
Modèle Symbolique du Convertisseur DC/DC

Premier modèle (inutile) : $\tau = 0.5$, $\eta = \frac{1}{40\sqrt{2}}$, $\varepsilon = 2.6$.



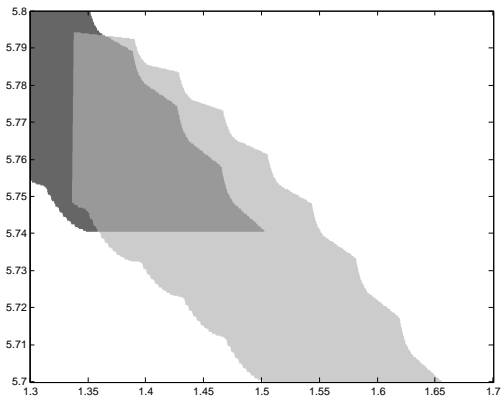
Contrôle du Modèle Symbolique

Superviseur du modèle symbolique pour la propriété d'invariance.



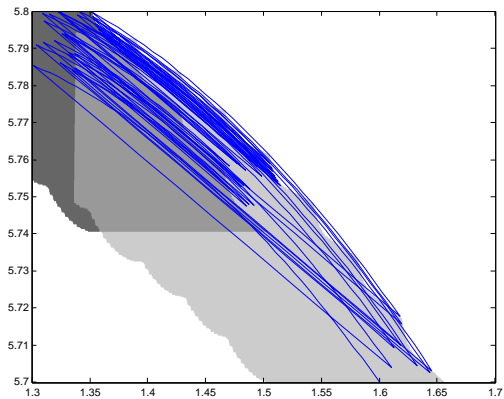
Contrôle du Modèle Symbolique (II)

Second Modèle : $\tau = 0.5$, $\eta = \frac{1}{4000\sqrt{2}}$, $\varepsilon = 0.026$ (642001 états !)



Contrôle du Convertisseur DC/DC

Trajectoire correspondante du convertisseur DC/DC :



Conclusions

- Contributions :
 - Extension quantitative de la notion de bisimulation
 - Modèles symboliques de systèmes dynamiques continus
 1. Modèles effectivement calculables
 2. Modèles arbitrairement précis
 - Application à des systèmes réalistes
- Perspectives :
 - Modèles symboliques multi-échelles
 - Calcul du modèle symbolique à la volée (i.e. pendant la synthèse de contrôleur)

Remerciements

Travail en collaboration avec :

- George J. Pappas, University of Pennsylvania
- Giordano Pola, University of L'Aquila
- Paulo Tabuada, University of California at Los Angeles

Avec la participation de :

- Georgios E. Fainekos, A. Agung Julius, University of Pennsylvania
- Jean Della Dora, Laboratoire Jean Kuntzmann
- Thao Dang, Goran Frehse, Oded Maler, Verimag