

Calcul d'atteignabilité pour des systèmes non-linéaires par approximations affines garanties

Othman NASRI

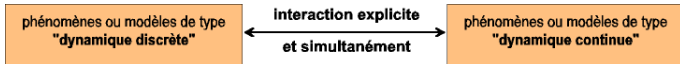
Supélec / IETR - Rennes

Réunion du Groupe de travail Méthodes Ensemblistes

Jeudi 19 juillet 2007

Système Dynamique Hybride

- **Système hybride :**



- **Modèle hybride :** cadre générale de modélisation pour les systèmes complexes.

- dynamiques continues (EDO, EDP, Equa.Diff.Stochastiques).
- dynamiques discrètes (automates, processus de Markov).

- **Communautés scientifiques impliquées :**

- *automatique, informatique,*
 - ✓ modélisation, contrôle optimal de processus, conception, analyse,...
- *toute communauté ayant une activité modélisation /simulation de systèmes,*
 - ✓ tous les domaines de l'industrie : transport, énergie, information, biologie,...

La sûreté de ces systèmes est généralement critique

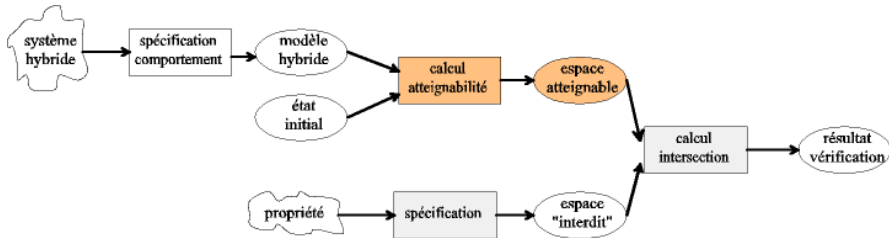
Vérification de propriétés et atteignabilité

● Définition

La vérification de propriétés sur un système hybride doit permettre de garantir que ce système répond bien aux:

- ✓ exigences de sécurité.
- ✓ spécifications de performances qui lui ont été imposées.

● Problématique



Contexte et objectif

Contexte

- Vérification de la propriété de sûreté pour les Systèmes Hybrides

- ▶ Calcul d'atteignabilité

⇒ Dynamique continue $x' = f(x)$ (Problème)

- ▶▶ Hybridisation :

⇒ Trouver des régions D_k et des vecteurs Γ_k tels que:

$$\forall x \in D_k \Rightarrow \Gamma_k^T \cdot x' \leq 0$$

objectif

Calculer l'espace atteignable d'un système hybride dont la dynamique continue est **non-linéaire**.

Plan

- 1 Atteignabilité des Systèmes linéaires
 - Systèmes linéaires sans perturbations
 - Systèmes linéaires soumis à des perturbations

- 2 Atteignabilité des systèmes non-linéaires
 - Contexte et problématique
 - Algorithme de calcul d'atteignabilité
 - Calcul de domaine d'incertitude
 - Espace atteignable dans P_i
 - Calcul de l'espace atteignable global

Structure de l'abstraction linéaire

$$x' = Ax + b$$

1 Hyperplans

- $q_k^T x = K_{k,b}$

$$q_k = (1 - \alpha)v_1 + \alpha v_2$$

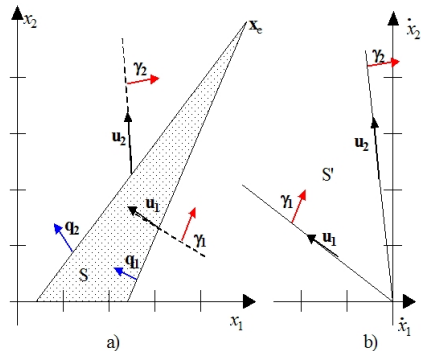
2 Secteurs

- $$\begin{cases} q_i^T x \geq K_{i,b} \\ q_{i+1}^T x \leq K_{i+1,b} \end{cases}$$

3 Inclusions différentielles

- $$\begin{cases} \gamma_i^T x' \geq 0 \\ \gamma_{i+1}^T x' \leq 0 \end{cases}$$

$$q_i^T = \gamma_i^T A$$



Sous-espace Atteignable

$$\begin{cases} \gamma_i^T (x - x_0) \geq 0 \\ \gamma_{i+1}^T (x - x_0) \leq 0 \end{cases}$$

<u>Hyperplan</u> :	$q_i^T x = K_{i,b}$	$q_i \Rightarrow$	face d'entrée
<u>Test</u> :	$q_i^T x' \geq 0$	$q_{i+1} \Rightarrow$	face de sortie



Prise en compte de l'incertitude

Modélisation de l'incertitude

$$x' = Ax + b(t)$$

avec $b(t) \in \text{Dom}$: Polyèdre

$$b_{\alpha(t)} = (1 - \alpha(t))b_0 + \alpha(t)b_1, \text{ avec } \alpha(t) \in [0, 1]$$

Abstraction

1 Cellules

$$\bullet (q_i^T x \geq K_{i,b0}) \wedge (q_{i+1}^T x \leq K_{i+1,b0})$$

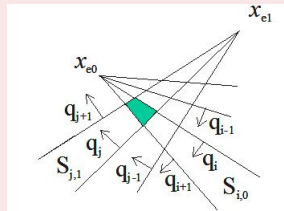
$$F_i = (\gamma_i^T x' \geq 0) \wedge (\gamma_{i+1}^T x' \leq 0)$$

$$\bullet (q_j^T x \geq K_{j,b1}) \wedge (q_{j+1}^T x \leq K_{j+1,b1})$$

$$F_j = (\gamma_j^T x' \geq 0) \wedge (\gamma_{j+1}^T x' \leq 0)$$

2 Inclusions Différentielles

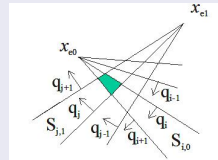
$$\bullet \dot{x} \in F_{i,j} = \text{ConvexHull}(F_i, F_j)$$



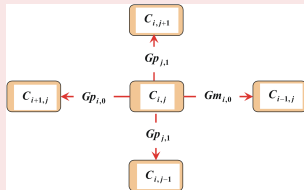
Procédure de calcul d'atteignabilité

Étapes

- 1 Recherche des cellules actives
- 2 Calcul de l'inclusion différentielle dans chaque cellule
- 3 Calcul de l'espace atteignable dans chaque cellule
- 4 Vérification des conditions de transition dans chaque cellule



Gardes



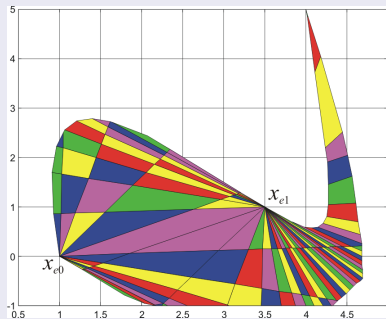
- $Gp_{i,0} = \begin{cases} \text{faux} & \text{si } q_i^T(b_1 - b_0) \leq 0 \text{ et } q_i \text{ vect.p.g} \\ \text{vrai} & \text{sinon} \end{cases}$
- $Gm_{i,0} = \begin{cases} \text{faux} & \text{si } q_i^T(b_1 - b_0) \geq 0 \\ q_i^T(Ax + b_1) \leq 0 & \text{sinon} \end{cases}$

Exemple

Données

$$A = \begin{bmatrix} 0 & 1 \\ -4 & -5 \end{bmatrix}, b_0 = \begin{bmatrix} 0 \\ 4 \end{bmatrix}, b_1 = \begin{bmatrix} -1 \\ 19 \end{bmatrix}, Inv : \begin{bmatrix} 1 & 0 \\ -1 & 0 \\ 0 & 1 \\ 0 & -1 \\ 3 & -2 \end{bmatrix} x \leq \begin{bmatrix} 10 \\ -10 \\ 10 \\ -1 \\ 15 \end{bmatrix}$$

Résultat



Linéarisation par morceaux de dynamique non-linéaire

Principe

Dynamique non-linéaire:

$$x' = f(x)$$

, avec

$$x \in Inv$$

Approximation affine garantie:

$$x' \simeq f_{app}(x) = A_i x(t) + b_i + u(t)$$

, avec

$$x \in P_i \subset Inv$$

et

$$u(t) \in U_i: \text{Polyèdre}$$

$$\forall x \in P_i \subset Inv \Rightarrow f(x) \in A_i x + b_i + U_i$$

Problèmes

■ détermination des paramètres A_i et b_i

- 1 Interpolation aux sommets d'un simplexe.
- 2 Linéarisation autour d'un point de l'invariant.
- 3 **Régression linéaire** sur un nuage de points. ◀

■ détermination de domaine d'incertitude U_i

Objectif

Approximation de l'espace atteignable de dynamique non-linéaire.

Algorithme 1

Étape 1 : P_i est donné à priori.

Étape 2 : Calcul de la régression linéaire dans le domaine P_i :

- 1 Création d'un nuage de points dans le domaine P_i .
- 2 Utilisation de la méthode des moindres carrés pour calculer A_i et b_i .

Étape 3 : Calcul du domaine d'incertitude U_i :

- 1 Création d'une **Grille** de pas h dans le domaine P_i .
- 2 Recherche d'un domaine **Rect_i** enveloppant l'image des sommets de **Grille** par la fonction erreur,

$$e(s) = f(s) - A_i s - b_i, \text{ avec } s \in \text{Grille.}$$

- un rectangle.
- un **hyper-rectangle orienté**. ◀

- 3 Utiliser le théorème des accroissements finis pour calculer le domaine U_i ;

Si g est une fonction de $[a, b] \rightarrow \mathbb{R}$, continue sur $[a, b]$, et dérivable sur $]a, b[$, alors il existe $c \in]a, b[$ tel que :

$$g(b) - g(a) = g'(c)(b - a)$$

Étape 4 : Calcul d'atteignabilité dans $P_i \leftarrow (A_i, b_i, U_i, x_0)$.

Estimation de l'erreur:

$$e(x) = f(x) - A_i x - b_i$$

Hypothèses

- e une fonction C^1 sur P_i et $\forall j, k = 1, \dots, n$,
- la valeur de l'erreur en chaque sommet de **Grille**.

$$|J_{j,k}(x)| = \left| \frac{\partial e_j(x)}{\partial x_k} \right| \leq M_{j,k}$$

Résultats

- 1 $\forall x \in P_i$, le sommet s de **Grille**, le plus proche de x , est tel que:

$$\forall j = 1, \dots, n$$

$$|e_j(x) - e_j(s)| \leq \sup_{x \in P_i} \left| \sum_{k=1}^n J_{j,k}(x)(x_k - s_k) \right| \leq \left(\sum_{k=1}^n M_{j,k} \right) \cdot \frac{h}{2}$$

$$\Downarrow$$

$$e(s) - \varepsilon_i(h) \leq e(x) \leq e(s) + \varepsilon_i(h)$$

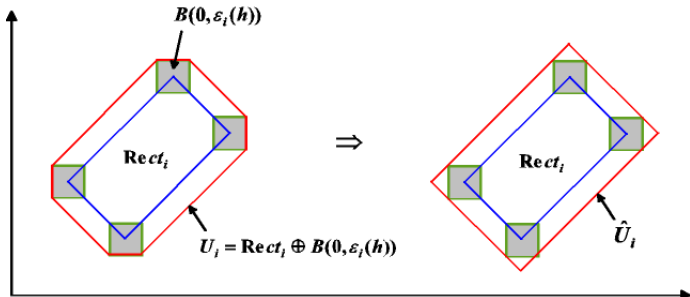
avec

$$\varepsilon_i(h) = \max_{j \in [1, \dots, n]} \left(\sum_{k=1}^n M_{j,k} \right) \frac{h}{2}$$

- 2 U_i est une sur-approximation de $Rect_i$, obtenue par élargissement des faces de $Rect_i$ d'une quantité $\varepsilon_i(h)$:

$$U_i = Rect_i \oplus B(0, \varepsilon_i(h))$$

Sur-approximation du domaine d'incertitude U_i



Exemple: Espace atteignable dans le domaine P_i

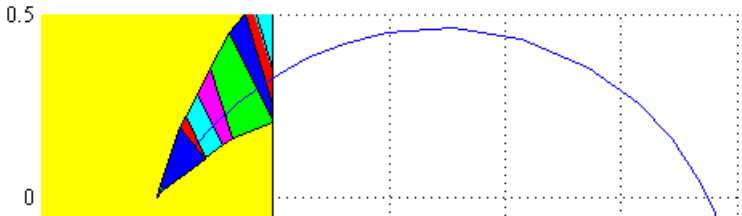
① Dynamique non-linéaire: $x' = f(x_1, x_2) = \begin{cases} x_2 + x_1 \cdot x_2 + 1 \\ x_2^2 - x_1 + 1 \end{cases}$, avec $x_0 = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$.

$$P_i = \text{Rect} \left\{ \begin{array}{cccc} -0.5 & 0.5 & 0.5 & -0.5 \\ -0.5 & -0.5 & 0.5 & 0.5 \end{array} \right\}$$

② Approximation affine garantie: $x' \simeq f_{app} = A_i x + b_i + u(t)$.

$$A_i = \begin{bmatrix} 0 & 1 \\ -4 & -5 \end{bmatrix}, \quad b_i = \begin{bmatrix} 1 \\ 1.03 \end{bmatrix}, \quad b_i + u(t) \in \text{Rect} \left\{ \begin{array}{cccc} 0.94 & 0.94 & 1.06 & 1.07 \\ 0.99 & 1.06 & 1.07 & 1.00 \end{array} \right\}.$$

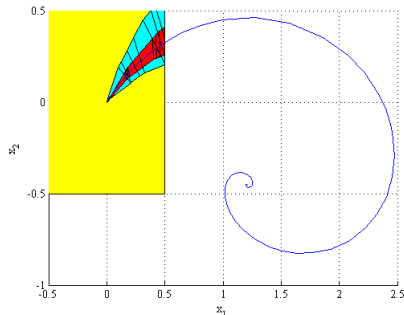
③ Espace atteignable dans P_i :



Algorithme 2: amélioration de l'espace atteignable

Données de l'algorithme:

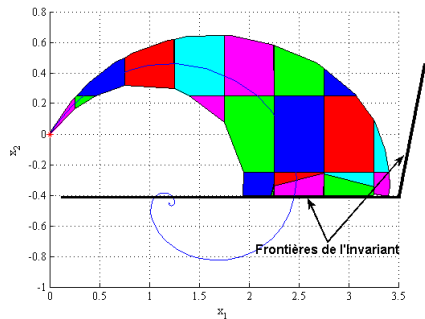
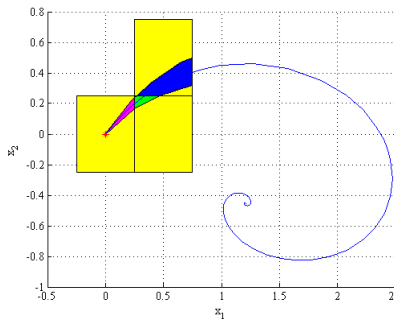
- P_i .
- Grille.
- Reach, l'espace atteignable dans P_i .
- le nombre de raffinements.



Étapes de l'algorithme:

- 1 utiliser le nuage de points, donnés par les sommets de *Reach*, pour recalculer la régression linéaire, A_i et b_i .
- 2 recalculer le domaine d'incertitude U_i :
- 3 calculer le nouvel espace atteignable $\Leftarrow (A_i, b_i, U_i)$

Espace atteignable global



Futur travaux

- 1 Optimisation de la réalisation.
- 2 Application de la réalisation à d'autre exemples.
- 3 Extension de la réalisation au dimension supérieure.

Bibliographie



T-A. Henzinger, P-H. Ho and H. Wong-Toi

Algorithmic analysis of non-linear hybrid systems.

Special issue on hybrid system, P-J.Antsaklis, A.Nrde (Eds), IEEE Transaction on Automatic Control, 43(4):540–554, 1998.



H. Guéguen and J. Zaytoon.

On the formal verification of hybrid systems.

Control Engineering Practice, Elsevier, 2004.



O. Stursberg and B. Krogh

Efficient representation and computation of reachable sets for hybrid systems

Hybrid Systems: Computation and Control, LNCS-2623, 96–109, 2003.



M-A. Lefebvre.

Abstractions pour la vérification de sûreté des systèmes hybrides.

IETR-Supélec, PhD thesis Univ Rennes 1, (in French) 2004.



O. Nasri, M-A. Lefebvre and H. Guéguen

Abstraction based reachability computation for affine systems with bounded input.

CDC'06 : 45th IEEE Conference on Decision and Control, San Diego, California USA.

Merci pour votre attention!!