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

Othman Nasri[1], Hervé Guéguen[2], Marie-Anne Lefebvre[2]

[1] LRI, Université de Paris Sud 11, CNRS & INRIA Saclay Île-de-France
bât 490, 91405 Orsay Cedex Francce
othman.nasri@lri.fr

[2] SUPELEC/IETR, Rennes
UMR 6164 – Université de Rennes 1, CNRS
CS 47601, 35576 Cesson-Sévigné cedex, France.
{*herve.gueguen ; marie-anne.lefebvre*}*@supelec.fr*

Résumé— **Nous présentons dans ce papier une approche permettant l'analyse d'atteignabilité des systèmes hybrides non linéaires. L'idée sur laquelle elle se base consiste à construire une approximation de systèmes non-linéaires, sous forme de systèmes affines par morceaux avec incertitudes, pour laquelle des approches efficaces de calcul d'atteignabilité ont été proposées. Pour ce faire, nous commençons par générer une partition de l'espace d'état du système non-linéaire. Ensuite, nous approchons localement, dans chaque élément de cette partition, le système non-linéaire par un système affine. Nous rajoutons à la fin l'erreur d'approximation au modèle affine. De cette manière, au lieu d'étudier un système non-linéaire complexe, nous étudions localement un système affine avec incertitudes.**

Mots-clés— **Systèmes hybrides non-linéaires, vérification formelle, sûreté, atteignabilité, hybridisation, abstractions.**

I. Introduction

La vérification formelle de la propriété de sûreté, qui consiste à prouver que le système répond bien aux exigences, en particulier de sécurité, et aux spécifications de performances qui lui ont été imposées, est l'un des principaux enjeux des systèmes dynamiques hybrides (discret/continu). Une des manières de réaliser cette vérification consiste globalement à déterminer l'évolution du système et à comparer cette évolution avec les configurations que l'on souhaite interdire. Autrement dit, il est possible par le biais de l'analyse d'atteignabilité de conclure quant au respect ou non de cette propriété. Cette analyse consiste à déterminer s'il est possible d'atteindre une certaine région de l'espace d'état hybride à partir d'une région initiale. La résolution peut reposer sur le calcul de l'espace atteignable discret et continu [1]. Le calcul de l'espace atteignable discret peut classiquement poser des problèmes d'explosion combinatoire, cependant dans l'état actuel des travaux c'est le calcul de l'espace atteignable continu qui est le plus limitant. En effet, ce calcul est souvent complexe et/ou pas décidable [2]. Ceci est en particulier vrai quand la dynamique continue est non triviale. On ne peut alors espérer obtenir que des sur-approximations de l'ensemble atteignable pour pouvoir tout de même vérifier la propriété du sûreté.

Ce papier se concentre sur ce sujet et vise à construire une approche, basée sur la méthode d'hybridisation, permettant l'analyse d'atteignabilité des systèmes hybrides régis par une dynamique continue non-linéaire : $\dot{x} = f(x),\ x \in Inv$: une région invariante, polyèdrale et convexe de l'espace d'état. Nous considérons des classes de systèmes hybrides pour lesquels la transition d'un état discret à un autre s'effectue sur des conditions liées à l'état continu, (par ex. franchissement d'hyper-plans).

Hormis certaines approches telles que celles basées sur l'arithmétique d'intervalles [3] ou celles utilisées dans l'outil CheckMate [4], l'analyse d'atteignabilité sur les systèmes non-linéaires passe souvent par une simplification de la dynamique. Cette simplification consiste généralement à approcher le champ de vecteurs f par un champ de vecteurs affine par morceaux plus simple à étudier [5],[6], [7]. Pour ce faire, on construit un maillage de la région $Inv = \bigcup_{i \in I} \Omega_i$. On approche ensuite, dans chaque élément Ω_i, le champ de vecteurs f par un champ de vecteurs affine f_i. Pour préserver les caractéristiques dynamiques du système initial, on intègre à ce modèle l'erreur d'approximation sous forme d'un terme d'incertitude (bornée). Nous remplaçons alors l'étude du système original non-linéaire par celle d'un système affine par morceaux avec incertitudes, $\dot{x} = f_i(x) + u,\ x \in \Omega_i$, pour lequel des approches efficaces de calcul d'atteignabilité ont été proposées.

La finesse de cette approximation est étroitement liée à la taille des cellules issues de la partition. Comme nous le verrons en détail, il est possible d'évaluer facilement les coefficients de linéarisation en utilisant la méthode des moindres carrés. De plus, en considérant f de classe C^1, l'erreur d'approximation peut être estimée avec une précision de bonne qualité.

Nous commencerons par présenter brièvement, dans la section II, les principes de base d'une approche permettant l'analyse d'atteignabilité des systèmes hybrides à dynamique linéaire [8]. Nous rappellerons ensuite dans la section III une extension de cette approche afin de traiter des systèmes affines avec incertitude [9]. Nous présenterons enfin dans la section IV l'extension de la précédente approche afin d'analyser l'atteignabilité des systèmes non-linéaires.

II. Atteignabilité des systèmes affines sans incertitudes

Cette section retrace les différentes phases de la construction d'une approche permettant de manière simple le calcul de l'espace atteignable sur un système affine et sans incer-

titudes [8]. La dynamique continue du système considéré est complètement connue et spécifiée par l'équation (1). Uniquement pour simplifier l'explication, le système est considéré de dimension 2 et la matrice A est non singulière.

$$x'(t) = Ax(t) + b,\ x \in Inv \tag{1}$$

Inv est une région invariante, polyédrale et convexe de l'espace d'état auquel l'état continu doit appartenir. Le but est alors de calculer l'espace atteignable à partir d'une région polytopique $Init$, défini par (2).

$$\{x | \exists x_0 \in Init, \exists t \geq 0,\ s.a.\ x = \Phi(t)\ with\ x_0 = \Phi(0),\\ \forall \tau \in [0,t]\ \dot{\Phi}(\tau) = A\Phi(\tau) + b\ and\ \Phi(\tau) \in Inv\} \tag{2}$$

Après une abstraction de la dynamique continue, cet espace atteignable n'est autre que l'enveloppe convexe des espaces atteignables calculés à partir des sommets de la région initiale. La construction de cette abstraction est fondée sur une partition de l'espace d'état dont les éléments permettent la définition d'une dynamique simplifiée sous forme d'inclusions différentielles. Ce calcul basé sur une partition spatiale plutôt que sur un échantillonnage temporel permet, s'il converge, de s'affranchir des problèmes d'horizon temporels infinis.

Comme décrit dans [8], il est possible de générer une famille de droites passant par le point d'équilibre et orthogonales à des vecteurs q_i formés par combinaison convexe de deux vecteurs quelconques des sous-espaces propres de la matrice A. Chaque élément de la partition est alors défini par l'intersection de la région Inv avec la cellule définie par (3).

$$(q_i^T(x - x_e) \geq 0) \wedge (q_{i+1}^T(x - x_e) \leq 0) \tag{3}$$

où $x_e = -A^{-1}b$ définit le point d'équilibre. La dynamique continue dans cette cellule peut alors être abstraite par une inclusion différentielle définie par l'équation (4), où le vecteur $\gamma_i = (A^{-1})^T q_i$ est orthogonal au vecteur dérivée $\dot{x}$ sur la frontière associée à q_i d'une cellule.

$$(\gamma_i^T \dot{x} \geq 0) \wedge (\gamma_{i+1}^T \dot{x}) \leq 0) \tag{4}$$

L'espace atteignable à partir d'un point x_0 est alors le résultat donné par la conjonction de (3) et (5).

$$(\gamma_i^T(x - x_0) \geq 0) \wedge (\gamma_{i+1}^T(x - x_0) \leq 0) \tag{5}$$

La première étape du calcul d'atteignabilité est illustrée sur la figure 1.

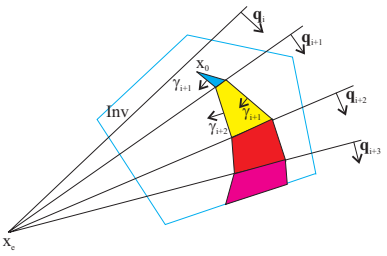

Fig. 1. Espace atteignable dans le polyèdre Inv à partir du point x_0

III. Atteignabilité des systèmes affines avec incertitudes

L'objectif de cette section est de rappeler comment les principes de la section précédente pourront être étendus à des systèmes caractérisés par (1) où b peut varier dans un polytope [9]. Cela peut correspondre à des systèmes affines avec incertitudes ou à des systèmes linéaires avec entrées bornées. Le problème est alors de calculer une sur-approximation de la région caractérisée par (2). Le fait de considérer b inconnu et variable rend ce problème plus complexe.

Afin de simplifier l'explication de la nouvelle approche, nous considérons que le domaine d'incertitude est un segment d'extrémités b_0 and b_1. Toute valeur du paramètre b (notée b_α) peut être alors caractérisée par (6).

$$b_\alpha = (1 - \alpha)b_0 + \alpha b_1\ avec\ \alpha \in [0,1] \tag{6}$$

L'abstraction proposée se base sur une partition en *cellules* de la région invariante Inv telles que dans chacune d'elles il est possible d'approcher le champ de vecteurs par une inclusion différentielle. Pour construire ces cellules, nous procédons de la manière suivante. A partir d'une famille de vecteurs $\{q_i\}$ [1], on construit une partition en cellules de l'espace d'état pour chaque vecteur extrême de l'incertitude. Dans notre cas, il n'y a que deux partitions à considérer : l'une associée à $b_\alpha = b_0$ et l'autre associée à $b_\alpha = b_1$. Notons $S_{i,0}$ (resp. $S_{i,1}$) la cellule caractérisée par (3) quand $b = b_0$ (resp. $b = b_1$). On définit alors les nouvelles cellules $C_{i,j} = S_{i,0} \cap S_{j,1}$ (voir figure 2) pour lesquelles il est possible de calculer une inclusion différentielle valable pour toutes les valeurs d'incertitude à partir des inclusions différentielles F_i et F_j associées aux cellules $S_{i,0}$ et $S_{j,1}$[9].

$$\begin{array}{l} x'_0 \in F_i = \{z \mid (\gamma_i^T z \geq 0)\ \wedge\ (\gamma_{i+1}^T z \leq 0)\} \\ x'_1 \in F_j = \{z \mid (\gamma_j^T z \geq 0)\ \wedge\ (\gamma_{j+1}^T z \leq 0)\} \end{array} \tag{7}$$

Cette inclusion différentielle, notée $F_{i,j}$, est définie comme

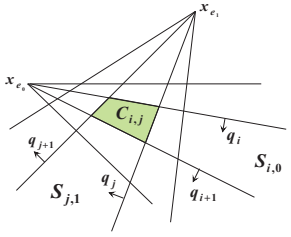

Fig. 2. Cellule

la plus petite enveloppe convexe des vecteurs dérivées pour toutes les valeurs de α : $\forall \alpha \in [0,1]$

$$\begin{array}{rcl} \dot{x}_\alpha \in F_{i,j} & = & convex\_hull(F_i, F_j) \\ & = & \{x' \mid (\gamma_m^T x' \prec_m 0) \wedge (\gamma_n^T x' \prec_n 0)\} \end{array} \tag{8}$$

où γ_m et γ_n sont deux des quatre vecteurs spécifiant les frontières de F_i et F_j, et $\prec_m$ et $\prec_n$ les inégalités associées. L'espace atteignable dans la cellule $C_{i,j}$ à partir

1. C'est la famille de vecteurs générée dans le cas d'un système autonome pour décrire les éléments de la partition de l'espace d'état.

d'un point $x_0 \in C_{i,j}$, noté $Att_{i,j}(x_0)$, est alors caractérisé par l'équation (9).

$$Att_{i,j}(x_0) = C_{i,j} \cap \{x|(\gamma_m^T(x-x_0) \prec_m 0) \wedge (\gamma_n^T(x-x0) \prec_n 0)\} \quad (9)$$

Chaque frontière de la cellule $C_{i,j}$ peut être traversée dans les deux sens sous certaines conditions [9]. La vérification de ces conditions de garde permet d'identifier les nouvelles cellules à considérer dans l'itération suivante de la procédure de l'analyse d'atteignabilité.

Exemple

Considérons une dynamique continue définie par les paramètres suivants :

$$A = \begin{pmatrix} 0 & 1 \\ -4 & -5 \end{pmatrix},\ b_0 = \begin{pmatrix} 0 \\ 4 \end{pmatrix},\ b_1 = \begin{pmatrix} -1 \\ 19 \end{pmatrix} \quad (10)$$

où b_0 et b_1 sont les sommets du domaine d'incertitude. Cette dynamique continue est associée à une région invariante caractérisée par (11).

$$Inv : \begin{pmatrix} 1 & 0 \\ -1 & 0 \\ 0 & 1 \\ 0 & -1 \\ 3 & -2 \end{pmatrix} x \leq \begin{pmatrix} 10 \\ 10 \\ 10 \\ 1 \\ 15 \end{pmatrix} \quad (11)$$

L'espace atteignable à partir du point $x_0 = \begin{pmatrix} 4 \\ 5 \end{pmatrix} \in Inv$ quand le paramètre b varie entre b_0 et b_1 est illustré sur la figure 3.

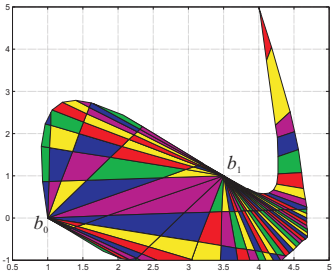

Fig. 3. Espace atteignable à partir du point x_0 pour la dynamique définie par (10)

IV. Atteignabilité des systèmes hybrides non-linéaires

Nous souhaitons élargir dans cette section l'approche de l'analyse d'atteignabilité présentée dans la section III aux systèmes hybrides dont la dynamique continue est régie par des équations différentielles non-linéaires :

$$\dot{x}(t) = f(x(t)),\ x \in Inv \subset R^n \quad (12)$$

Généralement, cette analyse s'effectue en deux phases. La première consiste à simplifier la dynamique non-linéaire par une dynamique affine par morceaux, plus simple à étudier. Pour ce faire, on se donne un maillage de la région $Inv = \bigcup_{i \in I} \Omega_i$, et dans chaque élément, Ω_i, de ce maillage, on approche localement le champ de vecteurs f par un champ de vecteurs affine f_i, $\forall i \in I$,

$$f(x(t)) \approx f_i(x(t)) = A_i x(t) + b_i,\ \ x(t) \in \Omega_i.$$

La deuxième phase consiste à estimer l'erreur d'approximation puis à l'intégrer, sous forme d'une entrée incertaine mais bornée, au modèle en ajoutant au champ de vecteurs linéaires f_i un terme d'incertitude $u(t)$. Dans chaque élément Ω_i du maillage, la dynamique non-linéaire du système hybride est alors approchée par une dynamique affine avec incertitudes de la forme (13) :

$$f_i(x(t)) = A_i x(t) + b_i + u(t), \quad (13)$$

avec $x(t) \in \Omega_i$ et $u(t) \in U_i \subset R^n$. En conséquence, dans chaque élément Ω_i, l'analyse d'atteignabilité du système initial peut être effectuée grâce à l'analyse d'atteignabilité d'un système hybride affine avec incertitudes exposée dans la section III.

La principale tâche consiste alors à estimer efficacement les paramètres A_i, b_i et U_i dans chaque élément Ω_i du maillage.

A. Estimation des paramètres A_i et b_i dans une maille Ω_i

Pour estimer les paramètres A_i et b_i définis dans l'équation (13) nous avons opté pour l'utilisation de la méthode de régression linéaire. Cette méthode n'exige aucune forme géométrique particulière sur les éléments du maillage et elle permet une approximation de bonne qualité. Les mailles Ω_i pourront être alors choisies comme des hyper-cubes d'un maillage uniforme.

La linéarisation en utilisant la méthode de régression linéaire s'effectue en deux étapes. La première consiste à créer un nuage de points. La deuxième consiste à construire un modèle affine, $f_i(x) = A_i x + b_i,\ \ x \in \Omega_i$, en utilisant par exemple la méthode des moindres carrés afin d'approcher au mieux le champ de vecteurs non-linéaire f.

B. Calcul du domaine d'incertitude U_i

Le calcul du polyèdre U_i, comme nous le verrons, découle de l'utilisation de l'inégalité des accroissement finis.

Pour bien ajuster le domaine d'incertitude U_i, on doit estimer efficacement la fonction erreur $x \to e(x) = f(x) - A_i x - b_i$ sur Ω_i. A cet effet, nous commençons, tout d'abord, par estimer l'erreur sur les sommets, notés $\{x^1, ..., x^p\}$ d'une grille G_h de pas h aussi petit que l'on veut, créée sur Ω_i. L'idée est de trouver un polyèdre, noté $Rect_i$, qui ajuste au mieux le nuage des points $\{y^1, ..., y^p\}$, image de $\{x^1, ..., x^p\}$ par la fonction e. Un choix efficace de représentation polyèdrale pour ajuster au mieux ce nuage des points consiste à utiliser les rectangles orientés [10].

Nous pouvons maintenant procéder au calcul du domaine d'incertitude U_i pour l'ensemble des points de Ω_i. Ce calcul est basé sur le théorème 1.

Théorème 1 : Si la fonction non-linéaire f est de classe C^1 sur Ω_i et s'il existe une matrice carrée $M_i \in M_{n,n}(R)$ telle que : $\forall j, k = 1, ..., n,\ \forall\ x \in \Omega_i$

$$\mid J_{j,k}(x) \mid\ = \mid \frac{\partial e_j(x)}{\partial x_k} \mid\ \leq\ M_{i_{j,k}}$$

Alors $\forall\, x \in\ \Omega_i,\ \exists\, \hat{x} \in\ \Omega_i$ tel que,

$$\| e(x) - e(\hat{x}) \|_\infty \leq \max_{j\in[1,...,n]} (\sum_{k=1}^{k=n} M_{i_{j,k}}).\frac{h}{2}$$

Preuve 1 : Soient x un point de Ω_i et G_h une grille, créée sur Ω_i, de pas h aussi petit que l'on veut. Choisissons $\hat{x} \in \Omega_i$, le sommet de G_h le plus proche de x. Suite à ce choix, comme illustré sur la figure 4, il facile de montrer que : $\forall\, j = 1, ..., n$

$$|x_j - \hat{x}_j| \ \leq\ \frac{h}{2} \tag{14}$$

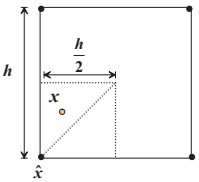

Fig. 4. Choix de $\hat{x}$; le sommet le plus proche de x

Vu que la fonction erreur e est supposée de classe C^1 sur Ω_i, il est possible d'appliquer le théorème des accroissements finis pour chacune de ses composantes, c'est-à-dire $\forall\, j = 1, ..., n,\ \exists\, c \in\,]x, \hat{x}[$ [2] tel que

$$e_j(x) - e_j(\hat{x}) \ =\ \sum_{k=1}^{k=n} J_{j,k}(c)(x_k - \hat{x}_k)$$

D'après les hypothèses du théorème 1 et l'équation (14), on déduit que : $\forall\, j = 1, ..., n$

$$|e_j(x) - e_j(\hat{x})| \ \leq\ \sum_{k=1}^{k=n} M_{i_{j,k}} |x_k - \hat{x}_k| \ \leq\ (\sum_{k=1}^{k=n} M_{i_{j,k}})\frac{h}{2}$$

Finalement, on conclut que :

$$\begin{aligned} \| e(x) - e(\hat{x}) \|_\infty \ &=\ \max_{j\in[1,...,n]} |e_j(x) - e_j(\hat{x})| \\ &\leq\ \max_{j\in[1,...,n]} (\sum_{k=1}^{k=n} M_{i_{j,k}}).\frac{h}{2} \end{aligned}$$

A partir du théorème 1, on peut déduire le résultat suivant :

Lemme 1 :

$$U_i = Rect_i \oplus \mathrm{B}(0, \varepsilon_\mathrm{i}(\mathrm{h}))$$

avec

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

où, $\mathrm{B}(0, \varepsilon_\mathrm{i}(\mathrm{h})) = \{\mathrm{x} \in \mathrm{R^n} \ /\ \ \| \mathrm{x} \|_\infty \leq \varepsilon_\mathrm{i}(\mathrm{h})\}$ est la boule de centre 0 et de rayon $\varepsilon_i(h)$, et le symbole $\oplus$ représente la somme de Minkowski.

Preuve 2 : On se donne une grille G_h de pas h et de sommets $\{x^1, ..., x^p\}$, créée sur Ω_i. D'après le théorème 1, $\forall\, x \in \Omega_i,\ \exists$ un sommet $\hat{x} \in \{x^1, ..., x^p\}$ tel que,

$$\| e(x) - e(\hat{x}) \|_\infty \leq \max_{j\in[1,...,n]} (\sum_{k=1}^{k=n} M_{i_{j,k}}).\frac{h}{2}$$

Comme $e(x) = e(\hat{x}) + (e(x) - e(\hat{x}))$ avec $e(\hat{x}) \in Rect_i$, on déduit que : $U_i = Rect_i \oplus \mathrm{B}(0, \varepsilon_\mathrm{i}(\mathrm{h}))$.

L'identification du système affine avec incertitude associé à une cellule Ω_i est décrite par l'algorithme 1 où $\mathcal{V}$ est un ensemble fini de points dans Ω_i.

2. $\forall\, k = 1, ..., n,\ \ c_k \in]x_k, \hat{x}_k[$

Algorithme 1 Calcul de f_i, le système affine avec incertitude qui approche le système non-linéaire f dans Ω_i

◇ Données : f, Ω_i, $\mathcal{V}$, *un pas* h
◇ Résultats : f_i
Début
- Calcul des paramètres A_i et b_i du modèle de la régression linéaire en utilisant le nuage de points $\mathcal{V}$
- Calcul de la fonction $x \to e(x) = f(x) - A_i x - b_i$
- Calcul de la matrice M_i:
  $\forall\ j, k \in [1, ..., n],\ \ M_{i_{j,k}} = \sup_{x\in\Omega_i} (\frac{\partial e_j(x)}{\partial x_k})$
- Création de la grille G_h de pas h
- Calcul de $\{y^1, ..., y^p\} = e(\{x^1, ..., x^p\})$
- Calcul de $\varepsilon_i(h) = \max_{j\in[1,...,n]} (\sum_{k=1}^{k=n} M_{i_{j,k}})\frac{h}{2}$
- Calcul de $Rect_i$ enveloppant $\{y^1, ..., y^p\}$
- Calcul de $U_i = Rect_i \oplus \mathrm{B}(0, \varepsilon_\mathrm{i}(\mathrm{h}))$
- Calcul de $f_i(x) = A_i x + b_i + u$ où $x \in \Omega_i$ et $u \in U_i$

Fin

C. Atteignabilité locale

Dans chaque cellule Ω_i du maillage, la dynamique continue non-linéaire est approximée par une dynamique continue affine avec incertitude. Il reste alors à appliquer l'approche développée dans la section précédente afin de calculer l'espace atteignable local.

D. Exemple

On se donne un système hybride de dimension 2 dont la dynamique continue est régie par l'équation différentielle non-linéaire suivante :

$$x' = f(x_1, x_2) = \left\{ \begin{array}{l} x_2 - x_1 + (x_1 - 1,85)^2 \\ x_2 - x_1^3 + 3x_1 \end{array} \right. \tag{15}$$

Nous voulons calculer l'espace atteignable à partir d'un point initial $x_0 = \begin{pmatrix} -3 \\ 0 \end{pmatrix}$ dans l'hyper-cube Ω_i centré en x_0 et de taille $l = 1$. La procédure de calcul est décrite ci-dessous :

i. Nous avons calculé tout d'abord les paramètres A_i et b_i dans Ω_i en utilisant la régression linéaire sur un nuage de points $\mathcal{V}$ formé par les 25 sommets d'une grille de taille $\frac{l}{5}$ créée sur Ω_i :

$$A_i = \begin{pmatrix} -5.2650 & 1.0000 \\ 2.7101 & 1.0000 \end{pmatrix},\ b_i = \begin{pmatrix} 3.3719 \\ -0.0346 \end{pmatrix}$$

ii. Ensuite, nous avons calculé M_i, la matrice qui borne la matrice Jacobienne de la fonction d'erreur e dans Ω_i :

$$M_i = \begin{pmatrix} 0.7825 & 0.0000 \\ 0.5607 & 0.0000 \end{pmatrix}$$

iii. Puis, nous avons créé une seconde grille G_h de taille $h = \frac{l}{100}$. Nous avons utilisé le nuage de points, défini par les 10201 sommets de G_h, pour calculer le rectangle orienté $Rect_i$ dont les sommets sont définis par les colonnes de la matrice suivante :

$$\begin{pmatrix} -0.0271 & -0.0314 & 0.0325 & 0.0368 \\ -0.0274 & -0.0224 & 0.0322 & 0.0272 \end{pmatrix}$$

iv. Finalement, les sommets de l'hyper-rectangle U_i sont calculés ($\varepsilon_i(h) = 0.0028$).

$$\begin{pmatrix} -0.0273 & -0.0342 & 0.0327 & 0.0396 \\ -0.0302 & -0.0222 & 0.0350 & 0.0269 \end{pmatrix}$$

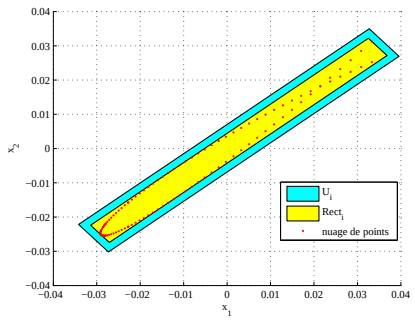

Fig. 5. Calcul de $Rect_i$ et U_i

v. Après identification des paramètres A_i, b_i et U_i, on peut procéder au calcul de l'espace atteignable à partir du point x_0 (cf. figure 6).

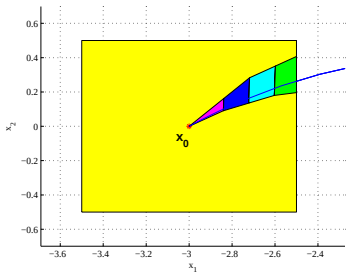

Fig. 6. Espace atteignable local à partir du point x_0 pour la dynamique définie par l'équation (15)

E. Calcul de l'espace atteignable global

Les sections précédentes ont permis de présenter la démarche du calcul d'atteignabilité locale c'est-à-dire sur un domaine $\Omega_i \in Inv$ sur lequel est linéarisée la fonction non-linéaire. Le calcul de l'espace atteignable global repose sur l'itération de tels calculs pour les différents éléments du maillage. Les points restant à préciser pour définir complètement l'algorithme global concernent le choix des éléments du maillage et la détermination des éléments successeurs suite au calcul local dans une maille.

Comme la méthode de régression linéaire retenue n'impose aucune contrainte sur la géométrie de Ω_i, nous allons choisir désormais un maillage en pavés de Inv pour approcher le champ de vecteurs f. On cherche à calculer l'espace atteignable, $Att(Init)$, à partir de la région initiale $Init$. Les éléments du maillage initialement pris en compte sont donc ceux qui ont une intersection non nulle avec $Init$. Comme il n'existe pas de contrainte sur le choix du maillage, on s'efforcera de le choisir tel que la région $Init$ soit incluse, si possible, dans une seule maille. A partir de la région d'entrée, $Init_i$, dans chacune des mailles actives [3]

3. Initialisées à l'intersection de $Init$ avec Ω_i.

Algorithme 2 Procédure d'atteignabilité globale

```
1  ◇ Données : Inv, f, Init, un pas h
2  ◇ Résultats : Att(Init) l'espace atteignable global
3  Début
4      Calcul de PA et ZE
5      SuccPA←∅, SuccZE←∅
6      TantQue PA ≠ ∅ Faire
7          Pour i variantDe 1 à Cardinal(PA) Faire
8              - Calcul de Att_i(ZE_i)
9              - Calcul de (Ω_j, ZE_j)_{j∈I} = Succ(Ω_i, ZE_i)
10             - Mise à jour:
11                . insertion de (Ω_j)_{j∈I} dans SuccPA
12                . insertion (Init_j)_{j∈I} dans SuccZE
13                . Att(Init)←Att(Init) ∪ Att_i(ZE_i)
14         FinPour
15         PA←SuccPA, ZE←SuccZE
16         SuccPA←∅, SuccZE←∅
17     FinTantQue
18 Fin
```

Ω_i, on calcule l'espace atteignable localement $Att_i(Init_i)$ dans la maille correspondante. On itère alors le calcul sur les mailles successeurs c'est-à-dire celles qui ont une intersection non vide avec l'espace atteignable $Att_i(Init_i)$. De plus, il est possible de se restreindre aux mailles Ω_j qui ont une intersection non réduite à un point avec Ω_i (voir figure 7). On répète cette procédure jusqu'à la validation d'un test d'arrêt (par exemple, jusqu'à l'obtention d'un espace atteignable global invariant). Les étapes du calcul de

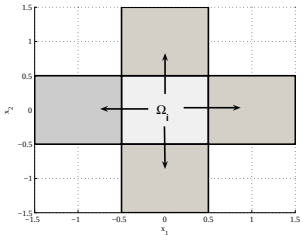

Fig. 7. Successeurs possibles de Ω_i en dimension 2

$Att(Init)$ sont exprimées par l'algorithme 2. La variable PA (resp. ZE) représente l'ensemble des pavés actifs, c'est-à-dire, les pavés Ω_i sur lesquels on procède au calcul de l'espace atteignable local (resp. l'ensemble des zones d'entrée $ZE_i = Init_i$ dans chaque pavé $\Omega_i \in$ PA).

F. Exemple

Reprenons l'exemple (15). L'objectif est de calculer l'espace atteignable à partir d'un domaine $Init = x_0$, noté $Att(Init)$. En plus des données définies précédemment, nous avons supposé que le domaine invariant, Inv, est défini par les contraintes suivantes :

$$Inv : \begin{pmatrix} 0 & -5 \\ 4 & -5 \end{pmatrix} x \leq \begin{pmatrix} 2 \\ -16 \end{pmatrix}$$

Pour réduire la quantité de calculs, les éléments du maillage seront construits à la volée. Nous considérons alors la premiere cellule active, notée Ω_1, celle contenant x_0 (Ω_1

sera par exemple centré en x_0). En appliquant l'approche présentée dans la section III, l'espace atteignable à partir du point x_0, $Att_1(x_0)$, est alors calculé. Pour réitérer le calcul, nous devons identifier les mailles successeurs ainsi que les domaines initiaux qui leur sont associés. Comme illustré sur la figure 8, il y a qu'une seule maille successeur, notée Ω_2. La zone d'entrée (ou le domaine initial) dans Ω_2, noté ZE_2 est alors le segment défini par l'intersection de $Att_1(x_0)$ avec Ω_2. On réitère l'analyse d'atteignabilité sur la nouvelle maille Ω_2 à partir de ZE_2. A ce stade, l'espace atteignable globale n'est autre que l'union de Att_1 et Att_2 (voir figure 8). Il reste donc à poursuivre l'analyse d'atteignabilité jusqu'à la validation du test d'arrêt (voir figure 9).

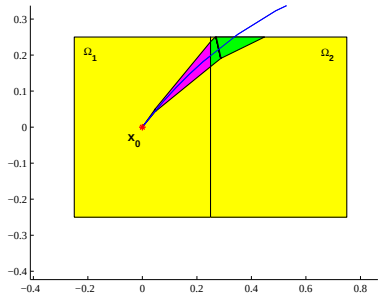

Fig. 8. Les deux premieres étapes de la procédure d'atteignabilité globale

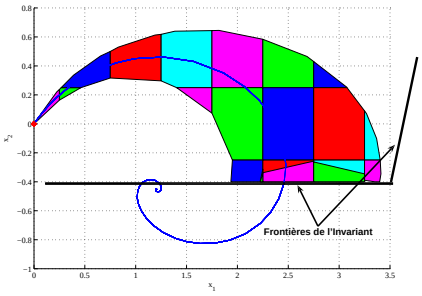

Fig. 9. Espace atteignable global à partir du point x_0 pour la dynamique définie par l'équation (15)

V. Conclusion

Ce papier détaille la construction d'une approche permettant de mener l'analyse d'atteignabilité sur un système hybride non-linéaire. Nous avons proposé en premier lieu une approximation du champ de vecteurs non-linéaire f par le biais d'une discrétisation de l'espace d'état réalisée sous forme d'un maillage sur lequel on calcule localement des approximations affines du champ de vecteurs f. La détermination de ces approximations doit être suffisamment élaborée afin d'obtenir un modèle réaliste qui préserve les caractéristiques dynamiques du système initial mais aussi suffisamment simple pour permettre sa mise en oeuvre algorithmique pour l'analyse d'atteignabilité. Nous avons utilisé le modèle de régression linéaire pour approximer localement le champ de vecteurs f. Ensuite, nous avons calculé localement, par le biais d'une idée qui découle du théorème des accroissement finis, le domaine d'incertitude. Le champ de vecteurs f est alors approximé localement (sur chaque élément du maillage) par un champ de vecteurs affine avec incertitudes.

Cette approche permet d'obtenir une sur-approximation de l'espace atteignable par une dynamique non-linéaire sous la forme d'une union de polyèdres. Basée sur des abstractions, elle peut conduire à des sur-approximations importantes mais sous une forme simple puisque l'espace atteignable est caractérisé par un nombre restreint de polyèdres, et donc de contraintes, ce qui se révèle intéressant lorsqu'on utilise le résultat du calcul d'atteignabilité. La précision et l'évaluation de la complexité du calcul de ces résultats reste un point à développer. L'efficacité du calcul peut encore être améliorée en ne considérant que les frontières de l'espace atteignable ce qui permettrait de ne pas prendre en compte les cellules intérieures. Cette amélioration demande une modification des algorithmes pour intégrer la notion de frontières et de leur évolution. Dans le cas des systèmes non-linéaires, elle permettrait de plus d'améliorer la précision des résultats en restreignant le raffinement au voisinage de ces frontières.

Les algorithmes présentés n'ont été implémentés qu'en dimension deux. Leur extension aux systèmes d'ordre plus élevé ne pose pas de problème de principe, par contre elle est principalement contrainte par la complexité du calcul liée aux dimensions des polyèdres manipulés et aux pseudo-compositions associées aux sommets du domaine d'incertitudes. Ici encore l'efficacité de l'implémentation constitue un défi intéressant pour la généralisation de ces approches.

Références

[1] O. Nasri, M.-A. Lefebvre, H. Guéguen et J. Zaytoon, "Sur la Vérification des Systèmes Hybrides". In JESA'07 : Journal Européen des Systèmes Automatisés, 41(n 7-8) : 855-883, 2007.

[2] G. Lafferriere, G. J. Pappas and S. Yovine, "A New Class of Decidable Hybrid Systems". In Hybrid Systems : Computation and Control : Second International Workshop, HSCC'99, LNCS 1569 (F. Vaandrager et J. van Schuppen (eds.)), pages 137-151, Springer, 1999.

[3] N.Ramdani, N.Meslem and Y.Candau, A hybrid bounding method for computing an over-approximation for the reachable space of uncertain nonlinear systems, IEEE Transactions on Automatic Control, to appear in October 2009.

[4] B. H. Krogh A. Chutinan B. I. Silva, K. Richeson, "Modeling and verification of hybrid dynamical system using CheckMate". In Proc. Int. Conf. on Automation of Mixed Processus ADMP, 2000.

[5] G. Frehse, "PhaVer : algorithmic verification of hybrid systems past HyTech". In Hybrid Systems : Computation and Control : 8th International Workshop, HSCC2005, Zurich, Switzerland, LNCS 3414 (M. Morari et L. Thiele (eds.)), pages 258-273, Springer, march 2005.

[6] J. Della Dora, A. Maignan et M. Mirica-Ruse, "Hybrid computation". In ISSAC'01, pages 101-108, 2001.

[7] E. Asarin, T. Dang et A. Girard, "Hybrization Methods for the Analysis of Nonlinear Systems". In Acta Informatica, 2007.

[8] M.A. Lefebvre et H. Guéguen, "Hybrid abstractions of affine systems". NonLinear Analysis, vol. 65, pages 1150-1167, September 2006.

[9] O. Nasri, M.A. Lefebvre, and H. Guéguen. "Abstraction based reachability computation for affine systems with bounded input". In CDC'06 : 45th IEEE Conference on Decision and Control, 13-15 December 2006. San Diego, California (USA).

[10] O. Stursberg et B. Krogh "Efficient representation and computation of reachable sets for hybrid systems" In Hybrid Systems : Computation and Control : 6th International Workshop, HSCC 2003, Prague, Czech Republic, LNCS 2623 (O. Maler et A. Pnueli (eds.)), pages 482-497, Springer, april 2003.