Département de formation doctorale en automatique

École doctorale IAEM Lorraine

Université de Lorraine

Observation et détection de modes pour la synchronisation des systèmes chaotiques : une approche unifiée

THÈSE

présentée et soutenue publiquement le 17 Décembre 2013

pour l'obtention du

Doctorat de l'Université de Lorraine

Spécialité Automatique, Traitement du Signal et des Images, Génie Informatique

par

Meriem HALIMI

Composition du jury

Président :	Olivier BACHELIER	Professeur, LIAS IUT Université de Poitiers, Poitiers
Rapporteurs :	Noureddine MANAMANNI	Professeur, CReSTIC Universitté de Reims Champagne Ardenne, Reims
	Krishna BUSAWON	Professeur, NCRLab Northumbria University, Royaume-Uni
Examinateur :	Laurent LARGER	Professeur, FEMTO-ST Université de Franche-Comté, Besançon
Directeur :	Gilles MILLERIOUX	Professeur, CRAN Université de Lorraine, Nancy
Co-directeur :	Jamal DAAFOUZ	Professeur, CRAN Université de Lorraine, Nancy

Centre de Recherche en Automatique de Nancy — UMR 7039

Mis en page avec la classe thloria.

Remerciements

Avant d'aborder le contenu de cette thèse, je tiens à remercier tout ceux qui, de près ou de loin, m'ont permis de réaliser ces travaux.

J'adresse mes remerciements à Gilles Millérioux et à Jamal Daafouz pour m'avoir encadré durant ces trois années.

Je désire remercier le jury qui a accepté d'évaluer cette thèse.

Je remercie l'ensemble des membres du CRAN que j'ai côtoyé durant ces années : C. Fengwei, C. Floriane, B. Gérard, G. Hugues, S. Julien, G. Marion, M. Tatiana et L. Vincent et qui ont contribué à la bonne ambiance des pauses café.

J'aimerais adresser un remerciement particulier à A. Faiza, pour son aide, sa gentillesse et son soutien tout au long de ces années.

Ces remerciements ne seraient pas complets sans une pensée pour des amis de longue date, Amina, Amine, Boulaid et Hanane. Merci de m'avoir aidé et encouragé, et pour m'avoir changé les idées quand j'en avais besoin.

Mes dernières pensées iront vers ma famille, mon frère Houssam Eddine, ma sœur Sara et surtout mes parents, pour m'avoir permis de poursuivre mes études jusqu'à aujourd'hui et soulagé de quelques contraintes de la vie quotidienne.

A mon père et à ma mère
Ils sauront pourquoi...

Table des matières

Table des figures

Liste des tableaux

Acronymes

LPV	Linear Parameter Varying
BMI	Bilinear Matrix Inegalities
LMI	Linear Matrix Inegalities
ISS	Input-to-State Stability
GAS	Globalement Asymptotiquement Stable
UIO	Unknown Input Observer
SISO	Single Input Single Output
MIMO	Multiple Input Multiple Output
BD	Backward Discernablity
FD	Forward Discernability
PWO	PathWise Observability
SARX	Switched Auto-Regressive eXogenous

N. B	Comme d'usage, de nombreuses terminologies anglo-saxonnes ne sont pas traduites et l'acronyme associé reste conservé dans ce manuscrit

Notations

Ω	Attracteur chaotique
Ω_ρ	Ensemble compact auquel appartient ρ_k
Ω_{σ_s}	Noyau de la matrice d'observabilité $\mathcal{O}_{\sigma_s}$, $\Omega_{\sigma_s} = ker(\mathcal{O}_{\sigma_s})$
$\mathcal{J}$	Ensemble contenant les valeurs de $\sigma(k)$, $\sigma(k) \in \mathcal{J}$
Φ	Ensemble convexe, $\Phi = \left\{ \mu_k \in \mathbb{R}^N, \mu_k = \left[\mu_k^{(1)}, \cdots, \mu_k^{(N)} \right], \mu_k^{(i)} \geq 0, \forall k \text{ et } \sum_{i=1}^{N} \mu_k^{(i)} = 1 \right\}$
λ_L	Exposant de Lyapunov
ν_e	Fonction de chiffrement
ν_d	Fonction de déchiffrement
$\mathbb{N}$	Ensemble des entiers
$\mathbb{R}$	Ensemble des nombres réels
$\mathbb{R}^n$	Ensemble des nombres réels de dimension n
$\mathbb{R}_+$	Ensemble des nombres réels non négatifs
$\mathcal{L}(\rho_k), \mathcal{L}(\hat{\rho}_k)$	Gains à temps variant d'un observateur polytopique
$\mathcal{M}$	Ensemble des entrées
$\mathcal{O}_{\sigma_s}$	Matrice d'observabilité
$\mathcal{P}(\rho_k)$	Matrice définie positive à temps variant, $\mathcal{P}(\rho_k) = \sum_{i=1}^{N} \xi_k^{(i)}(\rho_k) P_i$

$\mathcal{R}(X)$	Ensemble image engendré par les colonnes de X
$\mathcal{R}_{\sigma_s}$	Ensemble des séquences σ_i telles que σ_s n'est pas discernable de σ_i
$\mathcal{R}^*$	Ensemble des séquences ayant un résidu nul
$\mathcal{S}$	Ensemble des entiers $s \in \mathcal{S}$ qui permettent d'identifier d'une manière unique une séquence $\sigma_s \in \mathcal{J}^{h+1}$
$\mathcal{X}$	Ensemble des vecteurs d'état
$\mathcal{X}_0$	Ensemble des conditions initiales
$\mathcal{Y}$	Ensemble des sorties
$\mathbf{1}$	Matrice identité de dimension appropriée
$\mathbf{0}$	Matrice nulle de dimension appropriée
$(\bullet)$	Blocs d'une matrice induits par symétrie
$\|.\|$	Valeur absolue
$\|M\|$	Norme spectrale de la matrice M, $\|M\| = \sqrt{\lambda_{max}(M^T M)}$, où λ_{max} est la plus grande des valeurs propres de $M^T M$
$ker(M)$	Noyau de la matrice M
$\|x\|$	Norme euclidienne du vecteur x, $\|x\| = \sqrt{x^T x}$
$\|z\|_2$	Norme euclidienne de la séquence $\{z\}$, $\|z\|_2 = \sqrt{\sum_{k=0}^{\infty} z_k^T z_k}$
$\|z\|_\infty$	Norme supérieure de la séquence $\{z\}$, $\|z\|_\infty = \sup_{k \in \mathbb{N}} \|z_k\|$
$\|x\|_\infty$	Norme infinie du vecteur x, $\|x\|_\infty = \max_i \|x^{(i)}\|$
$\mathcal{D}_\rho$	Polytope auquel appartient ρ_k
$\mathcal{D}_\rho^*$	Polytope minimal auquel appartient ρ_k
$\mathcal{D}_A$	Polytope auquel appartient $A(\rho_k)$
θ, λ	Paramétrage des communications chaotiques
$ln(.)$	Logarithme népérien

$rang(M)$	Rang de la matrice M
$\hat{m}_k$	Signal information reconstruit
ρ_{o_i}	Sommets du polytope $\mathcal{D}_\rho$
$\{z\}$	Séquence d'échantillons $z_k,\ z_{k+1}, \ldots$ sans temps discret initial et final explicite, $k \in \mathbb{N}$
ρ_k	Vecteur des paramètres variant d'un système à description polytopique
$\rho_{[k_1,k_2]}$	Séquence ρ_k dans l'intervalle $[k_1, k_2]$, $\rho_{[k_1,k_2]} = \rho_{k_1}\rho_{k_1+1}\cdots\rho_{k_2}$
$\hat{y}_k$	Vecteur de sortie estimé d'un système dynamique en temps discret
α	Taux de décroissance
$\hat{x}_k$	Vecteur d'état estimé d'un système dynamique en temps discret
$\lambda,\ \lambda_i$	Valeur propre, $i^{\text{ème}}$ valeur propre
$\sigma(k)$	Loi de commutation, $\sigma(k) : \mathbb{N} \to \mathcal{J} = \{1, \cdots, J\}$
$\gamma(k)$	Loi de commutation, $\gamma(k) : \mathbb{N} \to \mathcal{J}' = \{1, \cdots, J'\}$
σ^*	Séquence active
$\sigma_{[k_1,k_2]}$	Séquence $\sigma(k)$ dans l'intervalle $[k_1, k_2]$, $\sigma_{[k_1,k_2]} = \sigma(k_1)\sigma(k_1+1)\cdots\sigma(k_2)$
$\tau(k)$	Retard inconnu associé au vecteur d'état, $\tau(k) \in \mathcal{T} = \{1, \cdots, \alpha\}$
$\tau'(k)$	Retard inconnu associé à l'entrée, $\tau'(k) \in \mathcal{T}' = \{1, \cdots, \alpha'\}$
$A,\ A_{\sigma(k)}$	Matrice dynamique
$A(\rho_k)$	Matrice dynamique à description polytopique
$A^{(i)}$	Sommets du polytope $\mathcal{D}_A$
$B,\ B_{\sigma(k)}$	Matrice de commande
$C,\ C_{\sigma(k)}$	Matrice d'observation
d	Degré de discernabilité
$D_{\sigma(k)}$	Matrice de transfert direct
e_k	Erreur de reconstruction d'état

$E_{\sigma(k)}$	Matrice d'état
f	Fonction d'état
f_w	Fonction d'état en présence de perturbation
F_i, G_i	Matrices inconnues d'une LMI
h_θ	Fonction de sortie
h	Taille de l'horizon de détection
k	Temps discret
K	Période de commutation
L_θ	Dimension de θ
L_ρ	Dimension de ρ_k
m_k	Signal information ou texte clair
n	Dimension du vecteur x_k
N	Nombre de sommets du polytope
P, P_i	Matrices définies positives
r	Retard inhérent
$r_{k,i}, r_{h,\sigma}$	Résidus
S	Nombre de séquences σ_s admissibles dans $\mathcal{J}^{h+1}$
t	Temps continu
T_{σ_s}	Matrice d'entrée
T'_{σ_s}	Matrice de transfert direct
u_k	Entrée de commande
V	Fonction de Lyapunov
$X^\dagger$	Inverse généralisée de X satisfaisant $X^\dagger X$ symétrique, $XX^\dagger$ symétrique, $XX^\dagger X = X$ et $X^\dagger XX^\dagger = X^\dagger$.Si X est inversible alors $X^\dagger = X^{-1}$
$X > 0$	Matrice définie positive X

$X < 0$	Matrice définie négative X
$X \geq 0$	Matrice définie semi-positive X
$X \leq 0$	Matrice définie semi-négative X
X^T	Transposée de la matrice X
x_k	Vecteur d'état d'un système dynamique en temps discret
$x(t)$	Vecteur d'état d'un système dynamique en temps continu
y_k	Vecteur de sortie d'un système dynamique en temps discret
y_{k_1,k_2}	Vecteur des sorties successives y_k dans l'intervalle $[k_1, k_2]$, $y_{k_1,k_2} = \begin{bmatrix} y_{k_1} \\ y_{k_1+1} \\ \vdots \\ y_{k_2} \end{bmatrix}$
$z^{(i)}$	$i^{\text{ème}}$ composante d'un vecteur réel z
z^T	Transposée du vecteur z
w_k	Entrée de perturbation

Introduction Générale

De par les progrès considérables dans les technologies de la communication au cours des dernières décennies, la sécurité des échanges d'informations est devenue une préoccupation majeure de nos jours. Dans ce contexte, la cryptographie joue un rôle prépondérant car l'information est principalement véhiculée par des réseaux publics. L'objectif principal de la cryptographie est, précisément, de dissimuler le contenu des informations transmises par le biais de canaux non sécurisés, en d'autres termes, à garantir la protection et la confidentialité des communications. Malgré la diversité des techniques cryptographiques, deux grandes classes sont généralement distinguées : le chiffrement à clé publique et le chiffrement à clé symétrique (aussi appelé chiffrement à clé privée) [Menezes et al., 1996]. Voyons à présent comment les systèmes dynamiques jouent un rôle dans ce contexte.
Le chaos est l'une des dynamiques les plus complexes que peuvent exhiber les systèmes non linéaires. Une des définitions formelles du chaos est due à RL Devaney [Devaney, 1989]. Un système dynamique est dit chaotique au sens de Devaney s'il remplit deux propriétés : la transitivité et la densité des points périodiques. Ces deux notions font appel à des concepts topologiques que l'on ne détaillera pas ici. On peut montrer que la sensibilité aux conditions initiales, qui est la propriété souvent associée à un comportement chaotique, est en fait une conséquence de ces deux autres propriétés. Les signaux générés par les systèmes chaotiques présentent des propriétés statistiques proches de l'aléatoire en dépit d'être déterministes. Cela peut constituer ainsi un des moyens pour mettre en œuvre les principes de confusion et de diffusion requis par Shannon pour les systèmes cryptographiques [Shannon, 1949]. Une toute première proposition en ce sens a été faite en 1989 [Matthews, 1989]. Depuis, de nombreuses techniques ont été proposées pour masquer l'information en utilisant les propriétés du chaos. Cette nouvelle approche de chiffrement est communément appelée cryptographie fondée sur le chaos (ou "chaotique"). Pour illustrer la forte activité dans ce domaine, nous mentionnons les travaux de synthèse [Amigó et al., 2007] [Alvarez and Li, 2006] [Hasler, 1998] [Millérioux et al., 2008] [Ogorzalek, 1993] [Yang, 2004].

Dans le cadre du chiffrement symétrique, le déchiffrement de l'information claire nécessite la synchronisation de l'émetteur et du récepteur. Pour le chiffrement chaotique, qui s'apparente à un principe de chiffrement symétrique [Millérioux et al., 2008], la synchronisation, communément appelée synchronisation du chaos depuis les travaux de Pecora et Caroll au début des années 90 [Pecora and Caroll, 1990] [Carroll and Pecora, 1991], est assurée par des observateurs [Grassi and Mascolo, 1997], [Itoh et al., 1997], [Millérioux, 1997], [Nijmeijer and Mareels, 1997]. Il s'avère que la plupart des systèmes chaotiques à temps discret sont décrits par des équations d'état admettant pour fonction de transition et fonction de sortie des non-linéarités polynomiales ou affines à commutation (incluant les systèmes linéaires à commutation). Sous certains conditions, ces systèmes peuvent être réécrits sous une forme unifiée Linéaire à Paramètres Variant (LPV) polytopique [Halimi et al., 2013]. Nous montrerons dans ce manuscrit que les observateurs polytopiques associés constituent un moyen efficace d'assurer la synchronisation du chaos pour de

nombreux principes de chiffrement chaotique. L'efficacité sera évaluée en termes de performances et de robustesse.

Pour la synchronisation du chaos impliquant des systèmes affines à commutation, la détection de mode va se révéler une question principale à plusieurs niveaux. Les systèmes affines à commutation sont des systèmes pour lesquels les matrices de l'espace d'état peuvent prendre des valeurs dans un ensemble fini de matrices. L'indice correspondant au système affine actif est appelé "mode" ou "état discret". La façon avec laquelle les indices évoluent dans le temps suit une règle dite "loi de commutation".

Considérons tout d'abord, la synchronisation du chaos pour des principes de chiffrement impliquant des systèmes chaotiques affines à commutation. La dynamique affine active n'est pas nécessairement connue côté récepteur si les frontières des régions associées à chaque dynamique affine de l'émetteur et qui partitionnent l'espace d'état dépendant de composantes de l'état non accessibles. La détermination de la dynamique active se pose en termes de détection de mode d'un système affine à commutation. Le problème est identique si le système chaotique de l'émetteur est un système à commutation dont la loi dépend de l'information à chiffrer qui, par définition dans le cadre du chiffrement, est inconnue.
Le problème de la détection de mode présente un intérêt qui va bien au-delà de la synchronisation du chaos. De nombreuses applications nécessitent la connaissance du mode, par exemple pour le contrôle par retour d'état de type gain scheduling [Apkarian et al., 1995], la commande tolérante aux défauts [Lunze and Richter, 2008] ou pour le diagnostic [Frank, 1990]. Notons que différentes terminologies ayant une signification semblable sont utilisées dans la littérature : la reconstruction de mode, la détection de mode ou l'estimation de mode. Une détection de mode à base de modèles, appelée espace de parité, associée à la notion de discernabilité fera l'objet d'une études approfondie dans ce manuscrit.

Enfin, il s'avère qu'au cours des deux dernières décennies, il y a eu un intérêt croissant pour les systèmes chaotiques à retard dans les communications sécurisées. En effet, les retards augmentent la dimension du système, ce qui est intéressant pour améliorer la complexité des dynamiques [Zheng et al., 2008]. Un travail pionnier qui traite des systèmes de communication opto-électroniques a été d'abord rapporté dans [Mirasso et al., 1996]. Depuis, les performances ont été améliorées et de nos jours, des systèmes de communication très haut débit peuvent être conçus comme dans [Lavrov et al., 2010]. Un aperçu général sur ce sujet peut être trouvé dans [Uchida et al., 2005] où l'intérêt des systèmes chaotiques laser avec rétroaction non linéaire retardée est souligné. On notera également les travaux [Zheng et al., 2008] [Zheng et al., 2009] [Datcu et al., 2012] où le recours à des schémas de chiffrement chaotique à retard est proposé. Nous proposerons dans ce manuscrit un principe de chiffrement chaotique par injection de retard dans le cas des systèmes à temps discret et étudierons le problème de l'estimation du retard pour le déchiffrement ou la cryptanalyse lorsqu'il jouera le rôle de clé secrète. En effet, le problème de l'estimation du retard pour les systèmes en temps discret est plutôt rare. Bien qu'un examen et une comparaison des approches d'estimation de retards variant dans le temps ont été proposées dans la littérature, voir [Bjorklund and Ljung, 2003] et plus récemment dans [Belkoura et al., 2009] par exemple, la plupart des méthodes disponibles sont consacrées aux systèmes continus. Là encore, l'intérêt dépasse le cadre strict du chiffrement chaotique. En effet, des retards sont inhérents à de nombreux systèmes physiques réels, tels que les systèmes mécaniques, des procédés chimiques, la biologie, les systèmes de transport ou de communication et de modèles économétriques. La considération des retards fait aussi sens pour les systèmes en temps

discret, en particulier dans le contexte des systèmes contrôlés en réseau. Lorsque le réseau est une ressource partagée par plusieurs utilisateurs, les retards inhérents à la transmission des mesures ou de contrôle apparaissent. Ils sont dans de nombreuses situations inconnus et/ou variant dans le temps.

Le plan général de ce manuscrit est le suivant

- Le Chapitre 1 est constitué de rappels sur les systèmes de chiffrement chaotiques connus dans la littérature. Ensuite, un système de chiffrement fondée sur l'injection de retard sera proposé pour les systèmes à temps discret.

- Le Chapitre 2 traite de la synthèse d'observateurs polytopiques dans un cadre général, puis dans le cadre du chiffrement chaotique. Nous rappellerons tout d'abord comment un système chaotique à non linéarité polynomiale peut être réécrit comme un système LPV polytopique. Les systèmes affines à commutation, autre classe importante de systèmes chaotiques, pouvant être considérés comme des cas particuliers de systèmes LPV polytopiques, une présentation unifiée pour la synthèse d'observateurs polytopiques sera faite. Cette présentation reposera sur des approches existantes de la littérature utilisant des Inégalités Matricielles Linéaires (LMI) qui permettent de garantir non seulement la stabilité mais également des performances. On illustrera alors l'utilisation des observateurs polytopiques pour assurer le déchiffrement relatif à différentes techniques de chiffrement chaotique.

- Le Chapitre 3 est consacré au problème de la détection de mode pour les systèmes affines à commutation. Nous effectuerons une présentation unifiée des principales méthodes de détection de mode fondées sur le modèle de type espace de parité, qui s'appliquent pour les systèmes linéaires et affines à commutation. Une comparaison de ces méthodes sera ensuite opérée. Le problème d'unicité de la détection de mode associé à la notion de discernabilité sera étudié en détails.

- Le Chapitre 4 illustre les applications de la détection de mode. Nous nous intéresserons à la synchronisation des systèmes chaotiques affines à commutation. Nous montrerons également comment l'estimation de retards variables peut être reformulée comme un problème de détection de mode dans un cadre général, puis comment elle peut être utilisé pour le déchiffrement et la cryptanalyse des chiffrements pas injection de retard.

Les travaux ont fait l'objet des publications suivantes.

Chapitre de livres

1. M. Halimi, G. Millérioux, J. Daafouz, Polytopic observers for LPV discrete-time systems, *Robust Control and Linear Parameter Varying Approaches, Lecture Notes in Control and Information Sciences Volume 437, pp 97-124*, 2013.

Congrès avec comité de lecture

2. M. Halimi, G. Millérioux, J. Daafouz, A hybrid approach for the estimation of time-varying delays of discrete-time systems, *IFAC Joint conference, 11th Workshop on Time-Delay Systems*, February 4-6, 2013 Grenoble, France.

3. M. Halimi, Estimation de retards variables pour les systèmes linéaires à commutation à temps discret, *5èmes Journées Doctorales / Journées Nationales MACS*, 11-12 Juillet, 2013 Strasbourg, France.

Papiers soumis

4. M. Halimi, G. Millérioux, An LPV framework for chaos synchronization in communication, *European Physical Journal Special Topic*.

5. M. Halimi, G. Millérioux, J. Daafouz, Mode detection and discernability as a framework for the estimation of time-varying delays, *13th ECC'14*, 2014 Strasbourg, France.

6. M. Halimi, G. Millérioux, J. Daafouz, A tutorial on model-based mode detection for discrete-time switched linear and affine systems, *Automatica*.

7. M. Halimi, G. Millérioux, J. Daafouz, A ciphering method based on time-varying delayed chaotic systems, *IEEE Transactions on Circuits and Systems II*.

Chapitre 1

Systèmes de chiffrement chaotique

Sommaire

1.1 Introduction

Ce chapitre a pour but principal de mettre en exergue les problèmes d'Automatique associés au chiffrement chaotique qui seront étudiés dans les chapitres qui suivent. Le plan de ce chapitre est le suivant. La section 1.2 introduit la notion de chaos et rappelle la caractéristique essentielle des systèmes chaotiques, à savoir la sensibilité aux conditions initiales. Dans la Section 1.3, quelques exemples de systèmes chaotiques à temps discret et continu sont donnés. La Section 1.4 est consacrée à un aperçu général des systèmes de chiffrement, les plus populaires, fondés sur la synchronisation du chaos.

1.2 Chaos et sensibilité aux conditions initiales

Considérons un système dynamique défini par

$$x_{k+1} = f(x_k) \tag{1.1}$$

où $x_k \in \mathbb{R}$ est le vecteur d'état et $f : \mathbb{R} \to \mathbb{R}$ une fonction non linéaire. La suite $x_0, x_1, \cdots$ est appelée orbite ou trajectoire de phase.

La sensibilité aux conditions initiales communément appelée effet papillon a été popularisée par le météorologue Edward Lorenz. Elle se caractérise par le fait que la distance entre deux trajectoires de phase initialement voisines, tend à augmenter de manière drastique (souvent exponentielle) au cours du temps. Ainsi, la moindre erreur ou simple imprécision sur la condition initiale interdit de décider quelle sera la trajectoire effectivement suivie à long terme et en conséquence, de faire une prédiction autre que statistique sur le devenir à long terme du système, bien que l'on traite de systèmes déterministes. En simulation, les erreurs d'arrondis peuvent être à l'origine de ce phénomène. Ceci est illustré dans la Figure 1.1.

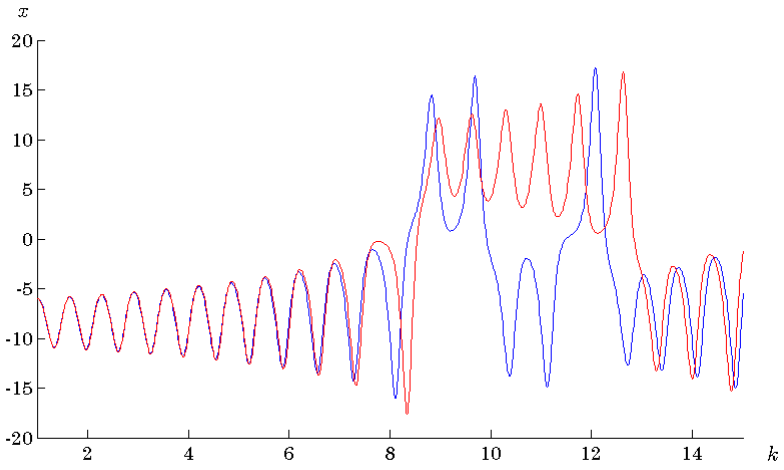


FIGURE 1.1 – Évolution dans le temps pour deux conditions initiales très proches d'un signal chaotique

Le mathématicien russe Alexander Lyapunov s'est penché sur le phénomène de sensibilité

aux conditions initiales et a proposé une grandeur permettant de la qualifier. Cette grandeur est appelée "exposant de Lyapunov". Ainsi, l'exposant de Lyapunov permet de caractériser quantitativement le caractère chaotique d'un système.
Supposons que la condition initiale x_0 de (1.1) soit affectée d'une erreur infinitésimale E_0. Après k itérations, l'erreur initiale E_0 sera donc amplifiée d'un facteur $\left|\frac{E_k}{E_0}\right|$. Notons que l'erreur diminue lorsque le facteur est inférieur à 1 et augmente s'il est supérieur à 1. On a la formule suivante :

$$\left|\frac{E_k}{E_0}\right| = \left|\frac{E_k}{E_{k-1}}\right| \left|\frac{E_{k-1}}{E_{k-2}}\right| \cdots \left|\frac{E_2}{E_1}\right| \left|\frac{E_1}{E_0}\right|$$

d'où

$$ln\left(\left|\frac{E_1}{E_0}\right|\right) = \sum_{i=1}^{k} ln\left(\left|\frac{E_i}{E_{i-1}}\right|\right)$$

Il suffit alors de calculer ce produit pour déterminer la façon dont s'amplifie l'erreur initiale. Lyapunov introduit la limite donnée par la formule suivante :

$$\lambda_L = \lim_{k\to\infty} \frac{1}{k} \sum_{i=1}^{k} ln\left(\left|\frac{df(x_{i-1})}{dx_{i-1}}\right|\right) \in \mathbb{R} \tag{1.2}$$

- Si $\lambda_L < 0$, l'orbite est attractive vers un point fixe ou une orbite périodique. Il caractérise les systèmes dissipatifs. Ce type de système exhibe une stabilité asymptotique.
- Si $\lambda_L = 0$, les orbites issues de conditions initiales différentes, gardent une séparation constante, ni ne convergent, ni divergent l'une par rapport à l'autre. Un système physique avec un tel exposant est dit conservatif.
- Si $\lambda_L > 0$, l'orbite est chaotique.

La notion d'exposant de Lyapunov se généralise aux systèmes de dimension $n > 1$ (voir [Eckmann and Ruelle, 1992]).

1.3 Exemples de systèmes chaotiques

1.3.1 Exemples de systèmes à temps continu

On rappelle les deux systèmes ci-dessous car ils ont une importance historique dans l'histoire du chaos même si par la suite, on ne s'intéressera plus qu'aux systèmes à temps discret.

1.3.1.1 Système de Lorenz

Le physicien Edward Lorenz travaillait sur un modèle mathématique simplifié de convection. Il utilisa un modèle à trois variables dynamiques x, y et z. Le système de Lorenz est un exemple célèbre de systèmes différentiels au comportement chaotique pour certaines valeurs de paramètres. Le modèle implique trois équations différentielles [Cuomo et al., 1993]

$$\begin{cases} \dot{x}^{(1)} = \sigma(x^{(2)} - x^{(1)}) \\ \dot{x}^{(2)} = rx^{(1)} - x^{(2)} - x^{(1)}x^{(3)} \\ \dot{x}^{(3)} = -bx^{(3)} + x^{(1)}x^{(2)} \end{cases} \tag{1.3}$$

σ, r, b représentent des paramètres.

L'attracteur chaotique de Lorenz est donné sur la Figure 1.2 pour les valeurs numériques $\sigma = 10$, $r = 28$, et $b = \frac{8}{3}$.

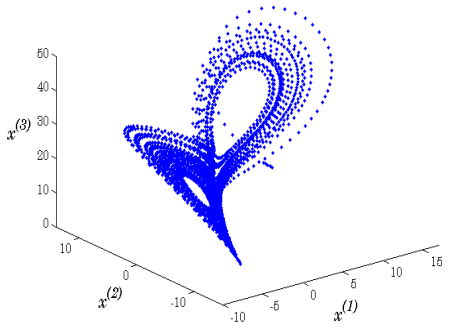


FIGURE 1.2 – Attracteur chaotique de Lorenz

1.3.1.2 Système de Rössler

Le système de Rössler, proposé par l'Allemand Otto Rössler, est lié à l'étude de l'écoulement des fluides. Il découle des équations de Navier-Stokes. Les équations de ce système ont été découvertes à la suite de travaux en cinétique chimique. Ce système est défini par les équations suivantes [Rössler, 1976]

$$\begin{cases} \dot{x}^{(1)} = -(x^{(2)} + x^{(3)}) \\ \dot{x}^{(2)} = x^{(1)} + ax^{(2)} \\ \dot{x}^{(3)} = b + x^{(3)}(x^{(1)} - c) \end{cases} \tag{1.4}$$

a, b, c représentent des paramètres.

L'attracteur chaotique de Rössler est donné sur la Figure 1.3 pour les valeurs numériques $a = 0.398$, $b = 2$ et $c = 4$.

1.3.2 Exemples de systèmes à temps discret

1.3.2.1 Récurrence de Hénon

La récurrence de Hénon est un modèle proposé en 1976 par le mathématicien Michel Hénon. Le modèle d'état associé est [Douglas, 1992]

$$\begin{cases} x_{k+1}^{(1)} = a - (x_k^{(1)})^2 + bx_k^{(2)} \\ x_{k+1}^{(2)} = x_k^{(1)} \end{cases} \tag{1.5}$$

a, b représentent des paramètres.

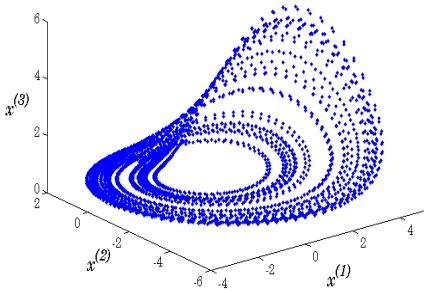


FIGURE 1.3 – Attracteur chaotique de Rössler

L'attracteur chaotique de Hénon est représenté sur la Figure 1.4 pour les valeurs numériques $a = 1.4$ et $b = 0.3$.

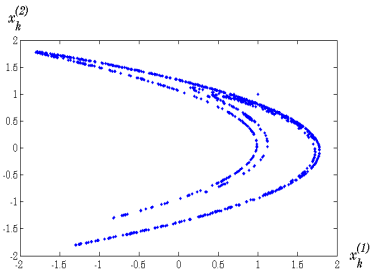


FIGURE 1.4 – Attracteur chaotique de Hénon

1.3.2.2 Récurrence de Lozi

La récurrence de Lozi est obtenue en remplaçant $(x_k^{(1)})^2$ dans la récurrence de Hénon (1.5) par $\left|x_k^{(1)}\right|$ et en modifiant la valeur des paramètres. Elle peut être trouvée dans [Peitgen et al., 1992] et est donnée par la représentation d'état suivante

$$\begin{cases} x_{k+1}^{(1)} = 1 - a\left|x_k^{(1)}\right| + x_k^{(2)} \\ x_{k+1}^{(2)} = bx_k^{(1)} \end{cases} \tag{1.6}$$

a, b représentent des paramètres.

L'attracteur chaotique de Lozi est représenté sur la Figure 1.5 pour les valeurs numériques $a = 1.7$ et $b = 0.5$.

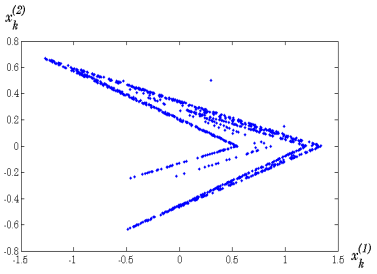


FIGURE 1.5 – Attracteur chaotique de Lozi

1.3.2.3 Récurrence de Duffing

La récurrence de Duffing est donnée par la représentation d'état suivante

$$\begin{cases} x_{k+1}^{(1)} = x_k^{(2)} \\ x_{k+1}^{(2)} = -bx_k^{(1)} + ax_k^{(2)} - (x_k^{(2)})^3 \end{cases} \tag{1.7}$$

a, b représentent des paramètres.

L'attracteur chaotique de Duffing est représenté sur la Figure 1.6 pour les valeurs numériques $a = 2.75$ et $b = 0.2$.

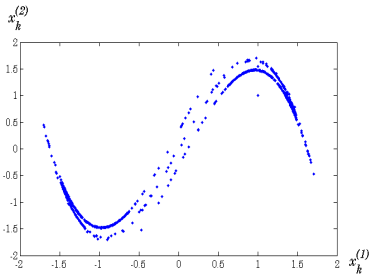


FIGURE 1.6 – Attracteur chaotique de Duffing

1.3.2.4 Récurrence d'Ikeda

Cette récurrence a été proposée d'abord par Ikeda pour modéliser la propagation de la lumière à travers un résonateur optique non linéaire. Elle est souvent utilisée dans une forme modifiée donnée par le modèle d'état suivant [K.Ikeda, 1979]

$$\begin{cases} x_{k+1}^{(1)} = 1 + a(x_k^{(1)} cos(\theta_k) - x_k^{(2)} sin(\theta_k)) \\ x_{k+1}^{(2)} = a(x_k^{(1)} sin(\theta_k) + x_k^{(2)} cos(\theta_k)) \end{cases} \tag{1.8}$$

avec

$$\theta_k = 0.4 - \frac{6}{1 + (x_k^{(1)})^2 + (x_k^{(2)})^2}$$

a représente un paramètre.

L'attracteur chaotique d'Ikeda est représenté sur la Figure 1.7 pour la valeur numérique $a = 0.9$.

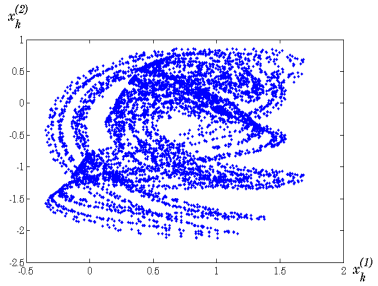


FIGURE 1.7 – Attracteur chaotique d'Ikeda

1.3.2.5 Suite logistique

La suite logistique est un modèle simplifié de l'évolution d'une population d'une espèce animale. Elle est définie par l'équation [May, 1976]

$$x_{k+1} = \theta x_k (1 - x_k) \tag{1.9}$$

θ représente un paramètre.
La grandeur x_k représente le pourcentage de cette espèce dans son environnement l'année k et θ un facteur de proportionnalité.

L'attracteur chaotique de la suite logistique est donné sur la Figure 1.8 pour la valeur numérique $\theta = 4$.

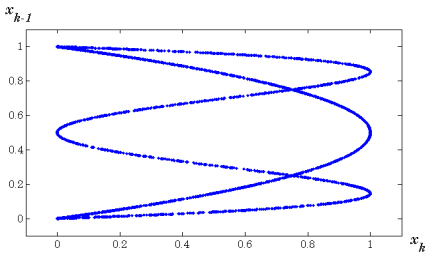


FIGURE 1.8 – Attracteur chaotique de la suite logistique

1.4 Systèmes de chiffrement chaotique

D'une manière générale, le chiffrement chaotique consiste à "mélanger" à chaque instant k, une information claire $m_k \in \mathcal{M}$ avec un échantillon $x_k \in \mathcal{X}$ d'une séquence chaotique. Le "mélange" peut être réalisé de plusieurs façons qui seront détaillées dans la suite. Le schéma général est donné sur la Figure 1.9. Le générateur de la séquence chaotique est construit à partir d'un système dynamique. Il est usuellement décrit à l'aide d'une fonction de transition d'état f avec le vecteur d'état correspondant $x_k \in \mathcal{X}$, la dimension du système étant n. La fonction f est paramétrée par un vecteur θ de dimension L_θ qui représente le secret. En effet, l'hypothèse de Kerkhoff [Kerkhoff, 1883] suppose que l'on connait parfaitement le système excepté la clé secrète. Seule une partie du vecteur d'état x_k obtenue par l'intermédiaire d'une fonction h, pouvant également être paramétrée par θ, appelée sortie et notée par $y_k \in \mathcal{Y}$, est transmise à travers le canal public vers le récepteur. La sortie y_k est généralement de faible dimension et devrait être unidimensionnelle dans le cas idéal. Dans ce qui suit, nous supposerons donc que y_k est un scalaire (dimension 1), l'émetteur étant ainsi limité à un système mono entrée mono sortie (Single Input Single Output (SISO)). Le récepteur est un système dynamique avec une dynamique $\tilde{f}$ et avec la fonction de sortie $\tilde{h}$, les deux étant paramétrées par $\hat{\theta}$. Son vecteur d'état est noté $\hat{x}_k$. Les deux fonctions $\tilde{f}$ et $\tilde{h}$ doivent être correctement choisies pour récupérer l'information claire $m_k \in \mathcal{M}$ au niveau du récepteur. Une première condition est que $\hat{\theta} = \theta$.

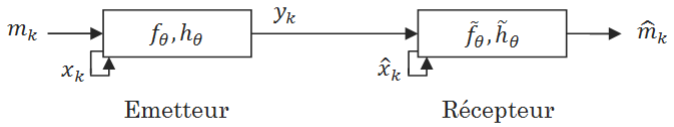


FIGURE 1.9 – Schéma bloc illustrant la synchronisation du chaos

Différentes architectures utilisant ces éléments de base ont été proposées. Elles reposent toutes sur le principe que l'information $m_k \in \mathcal{M}$ délivrée par le récepteur vérifie $\hat{m}_k = m_k$ si $\hat{x}_k = x_k$. En d'autres termes, les séquences chaotiques de l'émetteur et du récepteur, doivent être synchronisées pour que l'information claire m_k soit correctement récupérée. C'est le principe de la synchronisation du chaos.

Synchronisation du chaos

Dans le domaine de la communication, la synchronisation consiste à forcer un système esclave à se synchroniser avec un système maître. Du point de vue des systèmes dynamiques, l'opération de synchronisation consiste à rapprocher les trajectoires d'état des deux systèmes jusqu'à ce qu'elles finissent par être confondues. Soit M une matrice constante de dimension appropriée et $\mathcal{X}_0$ un ensemble non vide de conditions initiales. Il existe deux principaux concepts de la synchronisation :

Définition 1 *Synchronisation asymptotique*

$$\lim_{k\to\infty} \|Mx_k - \hat{x}_k\| = 0 \qquad \forall \hat{x}_0 \in \mathcal{X}_0 \tag{1.10}$$

Définition 2 *Synchronisation en temps fini*

$$\exists k_f < \infty,\ \|Mx_k - \hat{x}_k\| = 0 \quad \forall \hat{x}_0 \in \mathcal{X}_0 \ \ et \ \ \forall k \geq k_f \tag{1.11}$$

Dans la pratique, les mesures ont une précision finie, donc l'erreur d'une synchronisation asymptotique peut être considérée comme nulle après un temps transitoire fini. La synchronisation peut être considérée comme un problème de reconstruction d'état. En 1997, plusieurs papiers ([Grassi and Mascolo, 1997], [Itoh et al., 1997], [Millérioux, 1997], [Nijmeijer and Mareels, 1997]) ont mis en évidence cette analogie. En conséquence, les observateurs ont souvent été proposés comme structures du récepteur. Si seulement une partie des composantes est reconstruite, l'observateur est un observateur réduit et $rang(M) < n$. Si toutes les composantes du vecteur d'état sont reconstruites, l'observateur est un observateur plein et M est la matrice d'identité.

Différents systèmes de chiffrement, correspondant à des moyens distincts de brouiller une information, ont attiré l'attention des chercheurs au cours des années. Ils sont rappelés dans les paragraphes suivants.

1.4.1 Masquage additif

Ce schéma a d'abord été proposé dans [Cuomo et al., 1993] et [Wu and Chua, 1993]. L'information m_k devant être masquée est simplement ajoutée à la sortie y_k de l'émetteur (Figure 1.10) :

$$\begin{cases} x_{k+1} = f_\theta(x_k) \\ y_k = h_\theta(x_k) + m_k \end{cases} \tag{1.12}$$

Avec cette méthode, l'information confidentielle est additionnée à un signal chaotique (la sortie d'un système chaotique), et le signal résultant est envoyé au récepteur. Les équations génériques du récepteur sont :

$$\begin{cases} \hat{x}_{k+1} = \tilde{f}_\theta(\hat{x}_k, y_k) \\ \hat{y}_k = \tilde{h}_\theta(\hat{x}_k) = h_\theta(x_k) \end{cases} \tag{1.13}$$

La grandeur y_k qui apparaît dans (1.13) révèle le couplage unidirectionnel entre l'émetteur et le récepteur. À condition que la synchronisation (1.10) ou (1.11) puisse être assurée, la récupération de l'information claire est réalisée par

$$\hat{m}_k = y_k - \tilde{h}_\theta(\hat{x}_k) = y_k - h_\theta(x_k)$$

L'inconvénient est que l'information ne peut pas être exactement récupérée. En effet, m_k agit comme une perturbation sur le canal et empêche le récepteur d'être exactement synchronisé. Ni (1.10), ni (1.11) ne peuvent être exactement respectées. En conséquence, $\hat{x}_k \neq x_k$, $\hat{y}_k \neq y_k$, et, finalement $\hat{m}_k \neq m_k$ quel que soit k.
Il est à noter que dans ce schéma, la dynamique du système chaotique n'est pas modifiée par l'information claire à la différence des deux schémas qui suivent.

1.4.2 Modulation

1.4.2.1 Commutation chaotique

La commutation chaotique est aussi appelée modulation chaotique ou Chaos Shift Keying. Une telle technique a été principalement proposée dans le cadre des communications numériques.

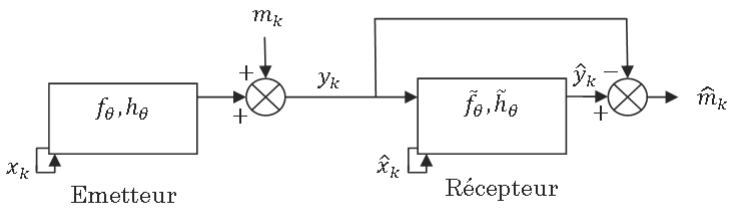


FIGURE 1.10 – Masquage additif

Une description détaillée peut être trouvée dans [Kolumban et al., 1998], même si la méthode a été proposée quelques années auparavant, par exemple, en 1993 [Dedieu et al., 1993]. En fait, du côté de l'émetteur, à chaque symbole $m_k = m^i$ appartenant à un ensemble fini $\{m^1 \cdots m^N\}$, est associé un signal chaotique émanant d'une dynamique f_θ^i et une fonction de sortie h_θ^i $(i = 1 \cdots N)$. Par conséquent, dans la description de l'émetteur, l'indice i dépend de m_k.

$$\begin{cases} x_{k+1} = f_\theta^{i(m_k)}(x_k) \\ y_k = h_\theta^{i(m_k)}(x_k) \end{cases} \tag{1.14}$$

Le cas le plus simple correspond à une information binaire et seulement deux dynamiques chaotiques différentes f^1, f^2 sont nécessaires. En fonction de la valeur courante du symbole m_k à l'instant $k = jK$ $(j \in N)$, un commutateur est déclenché périodiquement tous les K échantillons. Pendant l'intervalle de temps $[jK, (j+1)K - 1]$, l'information m_k est supposée être constante, et le signal chaotique y_k du système, qui a été activé par la commutation, est transmis à travers le canal (Figure 1.11).

L'objectif au niveau du récepteur est de décider quel est le système chaotique f_θ^i qui a produit la

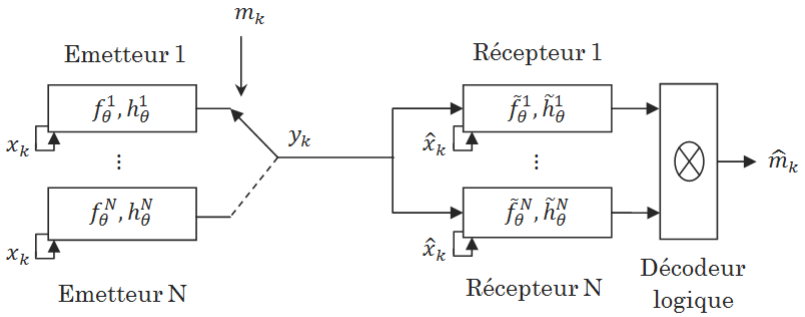


FIGURE 1.11 – Commutation chaotique

séquence $\{y_k\}_{jK,\cdots,(j+1)K-1}$. À cette fin, la partie réceptrice est composée d'autant de systèmes, c'est-à-dire N, que côté émetteur

$$\begin{cases} \hat{x}_{k+1} = \tilde{f}_\theta^i(\hat{x}_k, y_k) \\ \hat{y}_k = \tilde{h}_\theta^i(\hat{x}_k) \end{cases} \tag{1.15}$$

La synchronisation (1.10) ou bien (1.11) (où la grandeur x_0 doit être remplacée par x_{jK}) est obtenue par un couplage unidirectionnel à travers la variable y_k qui est impliquée dans $\tilde{f}_\theta^i$ de l'équation (1.15). La fonction $\tilde{f}_\theta^i$ correspond à la dynamique du récepteur qui peut être celle d'un observateur par exemple. Seul l'un des N récepteurs peut être synchronisé en fonction de la valeur de m_k qui est constante à l'intérieur de l'intervalle de temps $[jK, (j+1)K-1]$. Un décodeur logique simple, permet de récupérer l'information originale lors de l'analyse des résidus $r_{k,i}$, où

$$r_{k,i} = y_k - \tilde{h}_\theta^i(\hat{x}_k)$$

Lorsqu'une information à valeurs multiples est considérée [Palaniyandi and Lakshmanan, 2001], le nombre de récepteurs augmente et un mécanisme logique sophistiqué, situé après la banque de récepteurs, est nécessaire.

En ce qui concerne le contexte avec bruit, la technique de modulation est intéressante parce qu'elle bénéficie de certaines propriétés d'immunité. Dans un contexte sans bruit, elle est beaucoup moins intéressante, car elle souffre du fait que chaque commutation de m_k provoque un transitoire dans le processus de synchronisation. Ceci motive l'exigence que m_k doit être constante dans un intervalle de temps et empêche des transmissions à haut débit. Au manque d'efficacité s'ajoute le nombre rédhibitoire de récepteurs lorsque N devient très grand.

1.4.2.2 Modulation paramétrique

Fondamentalement, il existe deux types de modulations paramétriques : discrète et continue. La configuration correspondant à une modulation de paramètres discrets ([Dedieu et al., 1993] [Parlitz et al., 1993]) est représentée dans la Figure 1.12 a. Dans un tel cas, un paramètre λ (différent de la clé θ) d'un système chaotique unique, prend les valeurs $\lambda(m_k) = \lambda^i$ sur un ensemble fini $\{\lambda^1, \cdots, \lambda^N\}$ conformément à une règle prescrite. Pour les informations binaires, le paramètre de l'émetteur ne prend que deux valeurs distinctes λ^1, λ^2. Sur l'intervalle de temps $[jK, (j+1)K-1]$, l'information m_k est supposée être constante et le signal chaotique y_k est transmis à travers le canal. Ainsi, l'émetteur obéit aux équations d'état :

$$\begin{cases} x_{k+1} = f_\theta^{\lambda(m_k)}(x_k) \\ y_k = h_\theta^{\lambda(m_k)}(x_k) \end{cases} \tag{1.16}$$

La partie récepteur peut être constituée d'une banque de N systèmes dynamiques, généralement des observateurs, chacun d'eux étant couplé de manière unidirectionnelle avec l'émetteur par y_k

$$\begin{cases} \hat{x}_{k+1} = \tilde{f}_\theta^{\lambda^i}(\hat{x}_k, y_k) \\ \hat{y}_k = \tilde{h}_\theta^{\lambda^i}(\hat{x}_k) \end{cases} \tag{1.17}$$

Un seul observateur, celui ayant la même valeur λ^i de l'émetteur qui a réellement délivré la séquence $y_{[jK,(j+1)K-1]}$, peut être synchronisé sous la forme (1.10) ou (1.11) (où la grandeur x_0 doit être remplacée par x_{jK}) sur l'intervalle de temps $[jK, (j+1)K-1]$. Ainsi, encore une fois, un simple décodeur logique permet de récupérer l'information originale lors de l'analyse des résidus

$$r_{k,i} = y_k - \tilde{h}_\theta^{\lambda^i}(\hat{x}_k)$$

Pour la modulation continue représentée sur la Figure 1.12 b, l'information claire m_k prend des valeurs dans un continuum. Par conséquent, un nombre infini de systèmes dynamiques, côté

récepteur, serait nécessaire. De ce fait, pour la récupération de $\lambda_k(m_k)$ et donc de m_k, on a recours à des techniques adaptatives et des procédures d'identification ([Anstett et al., 2004] [Dedieu and Ogorzalek, 1997] [Fradkov and Markov, 1997] [Huijberts et al., 2000]).

Pour la modulation à la fois discrète et continue, la fonction délivrant $\lambda(m_k)$ doit être bijective de telle sorte que l'information m_k puisse être récupérée d'une manière unique en inversant λ.

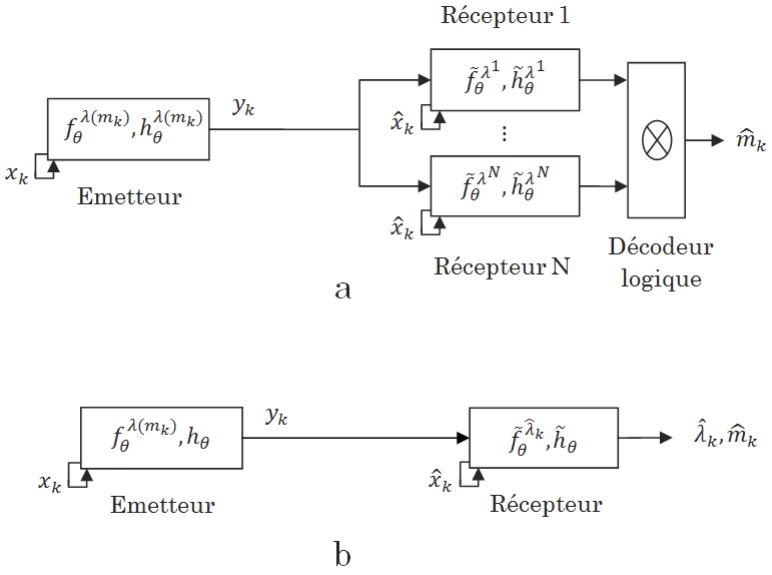


FIGURE 1.12 – Modulation paramétrique

En conclusion, pour la modulation paramétrique et pour la commutation chaotique, l'information m_k doit être constante pendant un intervalle de temps prescrit pour faire face aux transitoires induits par la reconstruction d'état ou le processus d'identification. Ainsi, ces techniques limitent considérablement les applications à haut débit et, par conséquent, elles ne sont pas très attrayantes pour le chiffrement.

1.4.3 Transmission à deux canaux

Le principe de la transmission à deux canaux est donné sur la Figure 1.13. Un premier canal est utilisé pour transmettre la sortie y_k d'un système chaotique autonome ayant la dynamique f_θ et la fonction de sortie h_θ. Par ailleurs, une fonction ν_e, dépendant d'une grandeur variant dans le temps, par exemple, le vecteur d'état x_k du système chaotique, chiffre l'information m_k et délivre $u_k = \nu_e(x_k, m_k)$. Ensuite, le signal u_k est transmis par l'intermédiaire d'un second canal. L'ensemble des équations régissant l'émetteur est

$$\begin{cases} x_{k+1} = f_\theta(x_k) \\ y_k = h_\theta(x_k) \\ u_k = \nu_e(x_k, m_k) \end{cases} \tag{1.18}$$

Au niveau du récepteur, une synchronisation parfaite remplissant (1.10) ou (1.11) peut être atteinte en faisant appel à un observateur. En conséquence, l'information claire m_k peut être

récupérée correctement par une structure d'observateur

$$\begin{cases} \hat{x}_{k+1} = \tilde{f}_\theta(\hat{x}_k, y_k) \\ \hat{y}_k = \tilde{h}_\theta(\hat{x}_k) \end{cases} \tag{1.19}$$

associée à

$$\hat{m}_k = \nu_d(\hat{x}_k, u_k) \tag{1.20}$$

La fonction de déchiffrement ν_d doit vérifier

$$\hat{m}_k = \nu_d(\hat{x}_k, u_k) = m_k \quad \text{lorsque} \quad \hat{x}_k = x_k \tag{1.21}$$

Cette technique a été proposée, par exemple, dans [Jiang, 2002] [Millérioux and Mira, 1998]. L'avantage réside dans le fait que, contrairement aux approches fondées sur la modulation, l'information m_k est autorisée à commuter à chaque instant discret k sans induire des transitoires de synchronisation pour chaque symbole. La récupération n'est erronée que pour un nombre limité de premières valeurs de l'information claire. Cependant, une transmission impliquant deux canaux peut être non satisfaisante pour des applications haut débit.

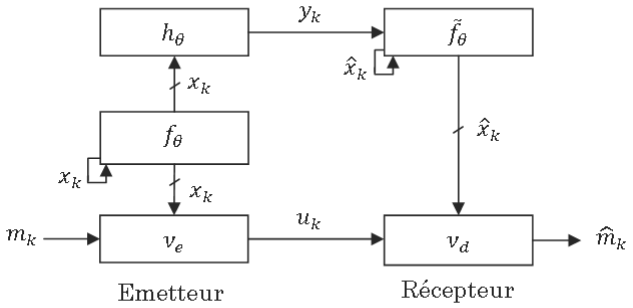


FIGURE 1.13 – Transmission à deux canaux

1.4.4 Méthode par inclusion

Des terminologies différentes, mais équivalentes peuvent être rencontrées dans la littérature se référant à la même technique : inclusion [Lian and Liu, 2000] [Millérioux and Daafouz, 2004], modulation non autonome [Yang, 2004] ou modulation chaotique directe [Hasler, 1998]. Les raisons de cette diversité sont les suivantes. Côté émetteur, l'information $m_k \in \mathcal{M}$ est directement injectée (ou, comme il est aussi généralement dit, plongée) dans une dynamique chaotique f_θ. Le système qui en résulte se transforme en un système non autonome, car l'information agit comme une entrée exogène. Injecter m_k dans la dynamique peut être considéré comme une "modulation" de l'espace des phases. Seule la sortie y_k du système est transmise. L'information m_k peut être incluse simplement dans la dynamique f_θ ou également au niveau de la fonction de sortie h_θ.

Le système de chiffrement par inclusion, représenté sur la Figure 1.14, est décrit par

$$\begin{cases} x_{k+1} = f_\theta(x_k, m_k) \\ y_k = h_\theta(x_k, m_k) \end{cases} \tag{1.22}$$

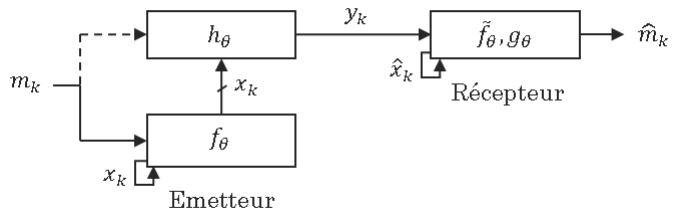


FIGURE 1.14 – Inclusion

Pour la récupération de l'information, côté récepteur, deux mécanismes ont été proposés dans la littérature : l'approche système inverse [Feldmann et al., 1996] et l'approche observateur à entrée inconnue (Unknown Input Observer (UIO)) [Inoue and Ushio, 2001] [Boutayeb et al., 2002] [Millérioux and Daafouz, 2003] [Boutat-Baddas et al., 2004] [Millérioux and Daafouz, 2004] [Millérioux and Daafouz, 2006]. Les équations génériques régissant un système inverse ou un observateur à entrée inconnue pour (1.22) sont

$$\begin{cases} \hat{x}_{k+1} = \tilde{f}_\theta(\hat{x}_k, y_k, \cdots, y_{k+r}) \\ \hat{m}_k = g_\theta(\hat{x}_k, y_{k+r}) \end{cases} \tag{1.23}$$

avec g de telle sorte que

$$\hat{m}_k = g_\theta(\hat{x}_k, y_{k+r}) = m_k \quad \text{lorsque} \quad \hat{x}_k = x_k \tag{1.24}$$

où $r \in \mathbb{N}$ représente le nombre de sorties retardées nécessaires. Cet entier est lié au degré relatif ou au degré inhérent du système.

1.4.5 Injection du retard

L'utilisation des systèmes chaotiques à retard dans les communications sécurisées a suscité récemment beaucoup d'attention afin d'améliorer la complexité des dynamiques [Zheng et al., 2008] notamment dans les communication opto-électroniques [Mirasso et al., 1996]. Cependant, la plupart des systèmes de chiffrement chaotique qui ont été proposés utilisent des systèmes chaotiques à retard à temps continu. Nous proposons ici un système de chiffrement fondé sur l'injection du retard pour les systèmes chaotiques à temps discret. Le schéma est représenté sur la Figure 1.15. Le retard $\tau(k)$ est le résultat d'un chiffrement au travers d'une fonction ν_e bijective $\tau(k) = \nu_e(m_k)$, m_k représentant l'information claire. Ainsi, le chiffrement obéit à

$$\begin{cases} x_{k+1} = f_\theta(x_k, x_{k-\tau(k)}) \\ y_k = h_\theta(x_k) \\ \tau(k) = \nu_e(m_k) \end{cases} \tag{1.25}$$

Le récepteur doit dans un premier temps délivrer un estimé $\hat{\tau}(k)$ de $\tau(k)$ pour retrouver ensuite m_k. La fonction de déchiffrement ν_d doit obéir à

$$\hat{m}_k = \nu_d(\hat{\tau}(k)) = m_k \quad \text{lorsque} \quad \hat{\tau}(k) = \tau(k) \tag{1.26}$$

L'estimation de $\tau(k)$ sera traitée dans le Chapitre 4.

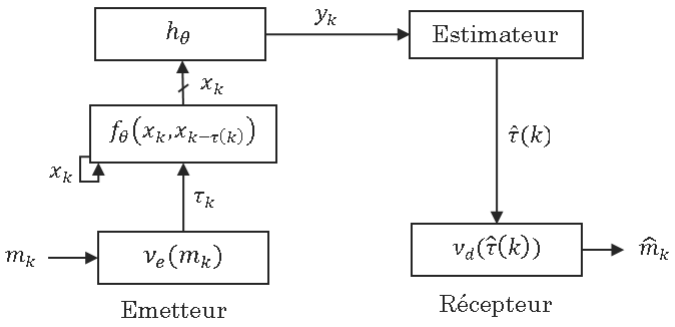


FIGURE 1.15 – Injection du retard

1.5 Conclusion

Nous avons rappelé les principales architectures de systèmes cryptographiques chaotiques proposés depuis les années 90 dans la littérature. Ces principes de chiffrement chaotique soulèvent des questions propres à l'Automatique. Nous en retiendrons deux principales : la synthèse d'observateurs et la détection de mode. Nous détaillons ci-dessous ces deux questions.

– Synthèse d'observateurs

Nous avons vu que les observateurs étaient nécessaires pour assurer la synchronisation, dans notre contexte synchronisation du chaos, des vecteurs d'état côté émetteur et récepteur. La synchronisation est en effet une condition requise pour pouvoir récupérer l'information claire pour la technique de modulation paramétrique, de commutation chaotique ou pour la transmission à deux canaux. Pour la technique de chiffrement par inclusion, la synchronisation est assurée par des observateurs à entrées inconnues. Il s'avère que la plupart des systèmes chaotiques à temps discret sont décrits par des équations d'état admettant pour fonction de transition et fonction de sortie des non-linéarités polynomiales ou affines à commutation. La synchronisation du chaos fondée sur les techniques de reconstruction d'état fait l'objet du Chapitre 2. Un traitement unifié pour ces différentes classes de systèmes chaotiques sera opéré.

– Problèmes de détection de mode

La détection de mode se pose à plusieurs niveaux.

- Tout d'abord, lorsqu'il s'agit d'assurer la synchronisation du chaos pour des schémas impliquant des systèmes chaotiques affines à commutation, on peut envisager la situation où la dynamique affine active n'est pas nécessairement connue côté récepteur si cette dernière dépend d'une variable non accessible. Les frontières des régions associées à chaque dynamique affine peuvent en effet dépendre de composantes du vecteur d'état non accessibles. La détermination de la dynamique active peut alors se poser en termes de détection de mode. La détection de mode pour les systèmes affines à commutation associée à la notion essentielle de discernabilité est étudiée dans un cadre général au Chapitre 3. La détection de mode pour le cas spécifique de la synchronisation du chaos à base l'observateur fait l'objet de la première partie du Chapitre 4.
- La détection de mode peut également être une solution pour le déchiffrement dans le cas de la méthode par injection de retard. En effet, on peut montrer, de manière originale, que le problème d'estimation d'un retard variable peut être formulé comme un problème de détection de mode

également. Ceci fait l'objet de la seconde partie du Chapitre 4.

Chapitre 2

Observateurs pour la synchronisation des systèmes chaotiques admettant une description LPV polytopique

Sommaire

2.1 Introduction

Dans les systèmes de chiffrement chaotique présentés au cours du chapitre précédent, nous avons constaté que la synchronisation des vecteurs d'état côté émetteur et récepteur est une étape nécessaire pour la reconstruction de l'information claire. Cette étape est fondée sur la conception d'observateurs pour la technique de modulation paramétrique, pour la commutation chaotique ou pour la transmission à deux canaux. Des observateurs à entrées inconnues sont requis pour la technique de chiffrement par inclusion.

Nous avons relevé au Chapitre 1 que de nombreux systèmes chaotiques à temps discret sont décrits par des équations d'état admettant pour fonction de transition et fonction de sortie des non-linéarités polynomiales ou affines à commutation. Nous rappellerons dans ce chapitre comment un système chaotique à non linéarité polynomiale, ou linéaire à commutation, peut être réécrit comme un système Linéaire à Paramètres Variant (LPV) c'est-à-dire un modèle linéaire (par extension affine) dont la représentation d'état dépend d'un vecteur de paramètres qui peut varier dans le temps. Depuis plusieurs années, ces systèmes ont fait l'objet d'une attention particulière, à la fois dans le contrôle [Apkarian et al., 1995] [Packard and Balas, 1997] [Leith and Leithead, 2000] [Scherer, 2001] [Lee and Park, 2007] [Farhood and Dullerud, 2010] et dans l'observation et le filtrage [Bara et al., 2001] [Sato, 2006] [Toth et al., 2007] [Heemels et al., 2010]. Ces techniques de modélisation LPV ont suscité beaucoup d'intérêt car elles fournissent une procédure systématique pour concevoir des observateurs. Une revue des principaux résultats sur la synthèse d'observateurs LPV polytopiques reposant sur l'utilisation des LMI [Ghaoui et al., 2000] est effectuée dans la seconde partie de ce chapitre avant une illustration de leur utilisation dans le contexte de la synchronisation du chaos.

Le plan détaillé de ce chapitre est le suivant. Dans la Section 2.2, quelques définitions de base sont rappelées, y compris les notions de stabilité asymptotique et de "Input-to-State Stability" (ISS). Dans la Section 2.3, la réécriture d'un modèle non linéaire d'un système chaotique sous la forme d'un modèle LPV est expliquée. Dans la Section 2.4, on rappelle le concept d'observateurs polytopiques et leur synthèse fondée sur la notion de stabilité poly-quadratique. La Section 2.5 traite le cas où le système LPV est soumis à des perturbations ou lorsque le paramètre est connu avec une incertitude bornée. Les conditions pour garantir des performances comme l'ISS, le taux de décroissance, le gain crête-à-crête et le gain $\mathcal{L}_2$ sont détaillées. Dans la Section 2.6, on propose une extension des résultats aux observateurs polytopiques à entrées inconnues, à la fois dans le cas déterministe, bruité ou incertain. L'ensemble de cette synthèse dans un cadre général est emprunté au Chapitre 5 de l'ouvrage [Halimi et al., 2013]. Enfin, la Section 2.7 illustre l'utilisation des observateurs polytopiques dans le cadre du chiffrement chaotique.

2.2 Prérequis

2.2.1 Définitions

Définition 3 *Une fonction $\varphi : \mathbb{R}_+ \to \mathbb{R}_+$ appartient à la classe $\mathcal{K}$ si elle est continue, strictement croissante et $\varphi(0) = 0$, et à la classe $\mathcal{K}_\infty$ si en plus $\varphi(s) \to \infty$ lorsque $s \to \infty$*

Définition 4 *Une fonction $\beta : \mathbb{R}_+ \times \mathbb{R}_+ \to \mathbb{R}_+$ appartient à la classe $\mathcal{KL}$ si pour chaque $k \in \mathbb{N}$ fixé, $\beta(.,k) \in \mathcal{K}$ et pour chaque $s \in \mathbb{R}_+$, $\beta(s,.)$ est décroissante et $\lim_{k\to\infty} \beta(s,k) = 0$.*

Considérons le système non linéaire à temps discret

$$x_{k+1} = f(x_k) \tag{2.1}$$

et le système non linéaire perturbé

$$x_{k+1} = f_w(x_k, w_k) \tag{2.2}$$

avec $x_k \in \mathbb{R}^n$ le vecteur d'état, $w_k \in \mathbb{R}^{d_w}$ une entrée de perturbation inconnue.

Définition 5 *Le système* (2.1) *est dit globalement asymptotiquement stable (GAS) s'il existe une $\mathcal{KL}$ fonction β de telle sorte que, pour chaque $x_0 \in \mathbb{R}^n$, la trajectoire d'état correspondante satisfait pour tout $k \in \mathbb{N}$*

$$\|x_k\| \leq \beta(\|x_0\|, k)$$

Définition 6 *Le système* (2.2) *est dit ISS par rapport à w_k s'il existe une $\mathcal{KL}$ fonction β et une $\mathcal{K}$ fonction γ de telle sorte que, pour toutes les séquences d'entrée $\{w\}$, pour chaque $x_0 \in \mathbb{R}^n$, la trajectoire d'état correspondante satisfait pour tout $k \in \mathbb{N}$*

$$\|x_k\| \leq \beta(\|x_0\|, k) + \gamma(\|w\|_\infty) \tag{2.3}$$

Si β peut être pris de la forme $\beta(s,k) = ds\zeta^k$ avec $d \geq 0$ et $0 < \zeta < 1$, ζ est le facteur de décroissance (en anglais 'decay factor') pour le système (2.1) et la fonction γ est le gain ISS pour (2.2).

Avant d'expliquer la réécriture d'un système chaotique sous la forme d'un modèle LPV, nous allons d'abord faire quelques rappels sur les modèles LPV.

2.2.2 Modèles LPV

Un système LPV peut être donné par la forme suivante :

$$\begin{cases} x_{k+1} = A(\rho_k)x_k + Bu_k \\ y_k = Cx_k + Du_k \end{cases} \tag{2.4}$$

où $x_k \in \mathbb{R}^n$ est le vecteur d'état, $u_k \in \mathbb{R}^m$ est l'entrée, $y_k \in \mathbb{R}^p$ est le vecteur de sortie, $A \in \mathbb{R}^{n\times n}$ est la matrice dynamique qui dépend du vecteur de paramètres variant dans le temps $\rho_k = \left[\ \rho_k^{(1)}, \rho_k^{(2)}, ..., \rho_k^{(L_\rho)}\ \right] \in \mathbb{R}^{L_\rho}$, $B \in \mathbb{R}^{n\times m}$ est la matrice d'entrée, $C \in \mathbb{R}^{p\times n}$ est la matrice de sortie et $D \in \mathbb{R}^{p\times m}$ est la matrice de transfert direct.

Remarque 1 *Notons qu'on peut étendre* (2.4) *aux systèmes affines à paramètre variant dans le temps donnés par*

$$\begin{cases} x_{k+1} = A(\rho_k)x_k + B(\rho_k)u_k + E(\rho_k) \\ y_k = C(\rho_k)x_k + D(\rho_k)u_k \end{cases} \tag{2.5}$$

Notons que dans le reste de ce chapitre, le système (2.4) sera considéré par souci de simplification mais que l'extension des résultats à (2.5) est directe.

Motivé par la plupart des cas rencontrés en pratique, nous supposons que chaque composante $\rho_k^{(i)}$ $(i = 1, \ldots, L_\rho)$ de ρ_k se situe dans une plage bornée $[\rho_{min}^{(i)}, \rho_{max}^{(i)}]$. Par conséquent, ρ_k se situe dans un ensemble borné $\Omega_\rho \subset \mathbb{R}^{L_\rho}$. La dépendance de $A(\rho_k)$ par rapport à ρ_k peut prendre plusieurs formes, en particulier, affine et polytopique.

Pour la décomposition affine, la matrice $A(\rho_k)$ est de classe C^1 par rapport à ρ_k et vérifie

$$A(\rho_k) = \bar{A}^{(0)} + \sum_{j=1}^{L_\rho} \rho_k^{(j)} \bar{A}^{(j)} \tag{2.6}$$

où $\bar{A}^{(0)}$ et $\bar{A}^{(j)}$ sont des matrices constantes obtenues en séparant les termes constants et les termes fonction de $\rho_k^{(j)}$.

Pour la décomposition polytopique, la matrice $A(\rho_k)$ est donnée par

$$A(\rho_k) = \sum_{i=1}^{N} \xi_k^{(i)}(\rho_k) A^{(i)} \tag{2.7}$$

où N est le nombre de sommets du polytope $\mathcal{D}_\rho$, et ξ_k appartient à l'ensemble compact Φ

$$\Phi \;=\; \left\{ \mu_k \in \mathbb{R}^N, \mu_k = \left[\mu_k^{(1)}, \ldots, \mu_k^{(N)}\right], \mu_k^{(i)} \geq\; 0 \;\forall\; i \text{ et } \sum_{i=1}^{N} \mu_k^{(i)} \;=\; 1 \right\}$$

En raison de la convexité de Φ, l'ensemble des matrices $\{A^{(1)}, \ldots, A^{(N)}\}$ définit un polytope noté $\mathcal{D}_A$ et les matrices $A^{(i)}$ correspondent aux sommets de $\mathcal{D}_A$. Ci-après, pour des raisons de simplicité et chaque fois que possible, la dépendance des paramètres $\xi_k^{(i)}$ de ρ_k sera omise, la notation $\xi_k^{(i)}$ sera utilisée à la place de $\xi_k^{(i)}(\rho_k)$. Dans le reste de ce chapitre, il sera supposé que la matrice $A(\rho_k)$ dans (2.4) est réécrite sous la forme polytopique (2.7).

Remarque 2 *Pour les systèmes affines* (2.5)*, la décomposition polytopique peut être effectuée en considérant un vecteur augmenté $\bar{\rho}_k$ qui implique tous les vecteurs de paramètres associés aux matrices respectives A, B, C, D et E pour obtenir une description polytopique qui obéit à*

$$\begin{bmatrix} A(\bar{\rho}_k) & B(\bar{\rho}_k) \\ C(\bar{\rho}_k) & D(\bar{\rho}_k) \end{bmatrix} = \sum_{i=1}^{N} \xi_k^{(i)} \begin{bmatrix} A^{(i)} & B^{(i)} \\ C^{(i)} & D^{(i)} \end{bmatrix}, \quad \xi_k \in \Phi$$

$$E(\bar{\rho}_k) = \sum_{i=1}^{N} \xi_k^{(i)} E^{(i)}, \quad \xi_k \in \Phi$$

Il est important de mentionner que la décomposition affine (2.6) peut être réécrite sous la forme polytopique (2.7). En effet, puisque ρ_k appartient à un ensemble borné Ω_ρ, il peut être intégré dans un polytope $\mathcal{D}_\rho$ dont les sommets sont $\rho_{o_i}, \ldots, \rho_{o_N} \in \mathbb{R}^{L_\rho}$, de telle sorte que

$$\rho_k = \sum_{i=1}^{N} \xi_k^{(i)} \rho_{o_i}, \; \xi_k \in \Phi \tag{2.8}$$

En substituant (2.8) dans (2.6) on trouve :

$$A(\rho_k) = \bar{A}^{(0)} + \sum_{j=1}^{L_\rho}(\sum_{i=1}^{N} \xi_k^{(i)} \rho_{o_i}^{(j)})\bar{A}^{(j)},\ \xi_k \in \Phi \tag{2.9}$$

Comme $\sum_{i=1}^{N} \xi_k^{(i)} = 1$ et $A^{(0)}$ est une matrice constante, il s'ensuit que $A^{(0)} = \sum_{i=1}^{N} \xi_k^{(i)} A^{(0)}$ et par conséquent (2.9) se transforme en :

$$A(\rho_k) = \sum_{i=1}^{N} \xi_k^{(i)}(\bar{A}^{(0)} + \sum_{j=1}^{L_\rho} \rho_{o_i}^{(j)} \bar{A}^{(j)}),\ \xi_k \in \Phi \tag{2.10}$$

L'identification de (2.7) et (2.10) donne

$$A^{(i)} = \bar{A}^{(0)} + \sum_{j=1}^{L_\rho} \rho_{o_i}^{(j)} \bar{A}^{(j)} \tag{2.11}$$

La contrainte "$\xi_k \in \Phi$" est équivalente à "$\rho_k \in \mathcal{D}_\rho$". Puisque $\Omega_\rho \subseteq \mathcal{D}_\rho$, il convient de souligner que la description polytopique (2.7) peut décrire une classe plus large de systèmes que celle d'origine, ce qui conduit à un certain conservatisme. Toutefois, lorsque les composantes $\rho_k^{(j)}$ $(j = 1, \ldots, L_\rho)$ de (2.6) sont indépendantes, Ω_ρ se transforme en un polytope spécifique $\mathcal{D}_\rho$ appelé hypercube avec $N = 2^{L_\rho}$ sommets et dans ce cas $\Omega_\rho = \mathcal{D}_\rho$.

2.2.3 Recherche du polytope minimal

Il peut arriver que l'obtention analytique du polytope $\mathcal{D}_\rho$ soit une tâche difficile voire impossible. En outre, il peut être intéressant, pour des raisons de conservatisme, d'obtenir un polytope minimal. Supposons que nous pouvons obtenir, par simulation ou expérimentalement, un nombre suffisant de vecteurs ρ_k, collectés dans un ensemble fini Γ_ρ de cardinalité N_ρ, pour décrire l'ensemble Ω_ρ avec une précision adéquate. Le polytope minimal $\mathcal{D}_\rho^*$ dans lequel Ω_ρ est intégré peut ainsi être considéré comme l'enveloppe convexe de l'ensemble des points Γ_ρ. Nous rappelons qu'un élément d'un ensemble fini de points est un point extrême, s'il n'est pas une combinaison convexe des autres points de cet ensemble. Par conséquent, trouver $\mathcal{D}_\rho^*$ revient à trouver les points extrêmes de Γ_ρ. Il s'avère que le calcul peut être effectué par des méthodes classiques. Elles sont brièvement rappelées ci-dessous alors qu'un examen détaillé est fourni dans [Millerioux et al., 2005].

Le calcul de l'enveloppe convexe pour la dimension $L_\rho = 2$ a été largement étudié et plusieurs algorithmes efficaces sont disponibles. Le plus populaire est celui de la "numérisation de Graham" (en anglais Graham scan) [Graham, 1973]. Il est fondé sur le fait que l'angle entre deux faces consécutives (formées par trois sommets consécutifs) de l'enveloppe convexe est inférieur à π. La complexité de l'algorithme est $O(N_\rho log N_\rho)$. Cet algorithme a un inconvénient majeur dû au fait qu'il ne peut pas être étendu à une dimension supérieure à 2. Un autre algorithme efficace appelé "Quick hull" est fondé sur l'approche "diviser pour régner". Différentes déclinaisons existent par exemple [Eddy, 1977] et [Preparata and Shamos, 1985]. Un tel algorithme utilise la propriété que, étant donné un triangle formé par trois points de l'ensemble d'origine, les points strictement à l'intérieur de ce triangle n'appartiennent pas à l'enveloppe convexe. Par conséquent, ils peuvent être ignorés. La complexité de cet algorithme est également $O(N_\rho log N_\rho)$. En

outre, il peut être facilement étendu à n'importe quelle dimension (voir [Allison and Noga, 1997] pour la dimension $L_\rho = 3$). Cependant, la complexité grandit rapidement et devient rédhibitoire pour de grandes dimensions. L'algorithme Quick hull est celui qui est incorporé dans la fonction *convhull* du logiciel Matlab. L'algorithme de "l'échantillonnage aléatoire" présenté dans [Chatterjee and Chatterjee, 1990] est fondé sur des projections itératives sur des hyperplans choisis au hasard. Enfin, une approche de type programmation linéaire est proposée dans [Pardalos et al., 1995] et fait appel à la résolution d'un problème d'optimisation.

2.2.4 Décomposition polytopique en ligne

Dans ce paragraphe, on rappelle [Anstett et al., 2004] une façon de calculer en ligne le vecteur $\xi_k = \left[\xi_k^{(1)} \cdots \xi_k^{(N)}\right]^T$ impliqué dans la décomposition polytopique (2.8) de ρ_k et (2.7) de $A(\rho_k)$. Le vecteur ξ_k est solution de

$$\begin{array}{c} W_k = Z \;\; \xi_k \\ t.q \;\; \xi_k^{(i)} \geq 0, \quad i = 1, \ldots, N \end{array} \tag{2.12}$$

où

$$W_k = [\rho_k^{(1)} \cdots \rho_k^{(L_\rho)} \; 1]^T \quad \text{et} \quad Z = \begin{bmatrix} \rho_{o_1}^{(1)} & \cdots & \rho_{o_N}^{(1)} \\ \vdots & \cdots & \vdots \\ \rho_{o_1}^{(L_\rho)} & & \rho_{o_N}^{(L_\rho)} \\ 1 & \ldots & 1 \end{bmatrix}$$

les éléments ρ_{o_i} (sommets du polytope $\mathcal{D}_\rho$) sont donnés, la matrice Z de dimension $(L_\rho + 1) \times N$ est de ce fait constante et connue. En effet, il est supposé que ρ_k est accessible en ligne, hypothèse usuelle dans le cadre des systèmes LPV et retenue ici comme souligné précédemment.

2.3 Modèles pour la description des systèmes chaotiques

Les systèmes chaotiques à temps discret à non-linéarité polynomiale peuvent être modélisés par des systèmes LPV sous certaines conditions. Le modèle LPV peut résulter d'une linéarisation instantanée le long de la trajectoire mais ce modèle n'est alors qu'une approximation du système non linéaire réel. Ainsi, la stabilité et les performances du système non linéaire sur la base de l'approximation LPV ne sont pas nécessairement garanties [Leith and Leithead, 2000]. Par conséquent, il est préférable de s'intéresser à une description exacte au sens défini dans la Proposition 1 ci-après. Un tel objectif a été étudié dans les travaux rapportés dans [Bruzelius, 2004] ou dans le papier [Millerioux et al., 2005].

Considérons le système chaotique à temps discret

$$x_{k+1} = g(x_k, u_k) \tag{2.13}$$

où $x_k \in \mathcal{X} \subseteq \mathbb{R}^n$ est le vecteur d'état et $u_k \in \mathbb{R}^m$ est l'entrée.

L'objectif est de réécrire le système (2.13) sous la forme d'un système LPV donné par (2.4). On a la proposition suivante.

Proposition 1 *[Halimi et al., 2013] Si les conditions suivantes sont respectées*
- *Il existe une fonction* $\rho : \mathbb{R}^n \to \mathbb{R}^{L_\rho}$ *de telle sorte que* $A(\rho(x_k))x_k + Bu_k = g(x_k, u_k)$
- $\rho(x_k)$ *ne dépend que de signaux mesurés*
- $\rho(x_k)$ *est borné lorsque* x_k *se situe dans l'ensemble admissible* $\mathcal{X} \subseteq \mathbb{R}^n$

alors le système non linéaire (2.13) *admet une description LPV exacte sous la forme de* (2.4) *avec* $\rho_k = \rho(x_k)$.

Il est intéressant de souligner que, le plus souvent, la description LPV n'est pas unique, et plusieurs fonctions ρ peuvent être candidates. En outre, le modèle LPV résultant décrit une classe plus large de systèmes que celle non-linéaire d'origine. En effet, une trajectoire du système non linéaire est également une trajectoire du modèle LPV, mais l'inverse n'est pas nécessairement vrai. Plus formellement, un système LPV est une inclusion différentielle linéaire paramétrée par le vecteur ρ_k. Cependant, il n'y a aucune inclusion différentielle linéaire unique d'un système non linéaire. Le choix peut être guidé par l'objectif de réduire le conservatisme des conditions de stabilité. Il peut également être intéressant de choisir une fonction appropriée ρ de telle sorte que les domaines d'attraction des deux modèles coïncident le plus possible [Bruzelius, 2004]. L'exemple 1 de la Section 2.7 permettra de clarifier ce point pour les système chaotiques.

Les systèmes linéaires ou affines à commutation admettent également une description du type (2.4) ou (2.5) polytopique (2.7). La seule différence est que l'ensemble Ω_ρ n'est plus un continuum mais un ensemble fini comme l'illustrera l'exemple 2 de la Section 2.7.

2.4 Observateurs polytopiques dans le contexte déterministe

2.4.1 Observabilité et détectabilité

2.4.1.1 Observabilité

On note $\mathcal{O}_{\rho_{[k,k+n-1]}}$ la matrice d'observabilité de (2.4) définie, pour $n > 1$, comme

$$\mathcal{O}_{\rho_{[k,k+n-1]}} = \begin{bmatrix} C \\ CA(\rho_k) \\ \vdots \\ CA^{\rho_k}_{\rho_{k+n-2}} \end{bmatrix} \tag{2.14}$$

où $\rho_{[k,k+n-1]} = \rho_k, \cdots, \rho_{k+n-1}$, et $A^{\rho_k}_{\rho_{k+n-2}} = A(\rho_{k+n-2})A(\rho_{k+n-3})\cdots A(\rho_k)$. Pour $n = 1$, $\mathcal{O}_{\rho_{[k,k+n-1]}}$ se réduit à $\mathcal{O}_{\rho_{[k,k]}} = C$.

L'observabilité des systèmes LPV peut être caractérisée par le théorème suivant emprunté à [Toth et al., 2007].

Théorème 1 *[Toth et al., 2007] Le système (2.4) est complètement observable si pour tout* $k \in \mathbb{N}$, $rang(\mathcal{O}_{\rho_{[k,k+n-1]}}) = n$.

En d'autres termes, la notion d'observabilité est définie comme dans le cas linéaire lorsqu'on considère toutes les trajectoires possibles du paramètre $\rho_k \in \Omega_\rho$. Le Théorème 1 est une extension directe de la condition d'observabilité indiquée dans [Park and Verriest, 1990] qui traite des systèmes linéaires variant dans le temps. Ainsi, dans le Théorème 1, la contrainte "pour tout

$k \in \mathbb{N}$" peut être réinterprétée dans le cas des systèmes LPV comme "pour tout $\rho_k \in \Omega_\rho$".

Le problème est que, dans le cas général, le nombre de trajectoires de $\rho_k \in \Omega_\rho$, et ainsi le nombre de vecteurs $\rho_{[k,k+n-1]}$ est infini. Notons que l'observabilité des paires $(C, A^{(i)})$ attribuée aux sommets du polytope $\mathcal{D}_A$ n'induit pas nécessairement l'observabilité de tous les couples $(C, A(\rho_k))$. Ceci est illustré sur l'exemple suivant.

Exemple 1 *Considérons le système obéissant à la forme (2.4) avec*

$$A(\rho_k) = \begin{bmatrix} 0.6+\rho_k & 1 \\ 1 & 0 \end{bmatrix} \quad et \quad C = \begin{bmatrix} 1 & 0.5 \end{bmatrix}$$

Le paramètre ρ_k appartient à l'intervalle [0 1].
La matrice d'observabilité est donnée par

$$\mathcal{O}_{\rho_{[k,k+1]}} = \begin{bmatrix} 1 & 0.5 \\ \rho_k + 1.1 & 1 \end{bmatrix}$$

Les matrices d'observabilité pour les paires respectives (C, A_1) et (C, A_2), avec $A_1 = A(0)$ et $A_2 = A(1)$ vérifient numériquement

$$\mathcal{O}_{[0,*]} = \begin{bmatrix} 1 & 0.5 \\ 1.1 & 1 \end{bmatrix} \quad et \quad \mathcal{O}_{[1,*]} = \begin{bmatrix} 1 & 0.5 \\ 2.1 & 1 \end{bmatrix}$$

*où * représente une valeur arbitraire de ρ_{k+1} puisque la matrice d'observabilité dépend exclusivement de ρ_k.*

Il est clair que $rang(\mathcal{O}_{[0,*]}) = rang(\mathcal{O}_{[1,*]}) = 2$. Cependant, pour $\rho_k = 0.9$, la matrice d'observabilité vérifie numériquement

$$\mathcal{O}_{[0.9,*]} = \begin{bmatrix} 1 & 0.5 \\ 2 & 1 \end{bmatrix}$$

et donc $rang(\mathcal{O}_{[0.9,*]}) = 1$. En conséquence, les deux paires (C, A_1) et (C, A_2) sont observables alors que l'observabilité n'est pas satisfaite à l'intérieur du polytope $\mathcal{D}_A$ lorsque $\rho_k = 0.9$.

2.4.1.2 Détectabilité

La détectabilité des systèmes LPV peut être définie de différentes manières. On retiendra celle proposée dans [Wu, 1995], où la détectabilité est définie en ayant recours à la stabilité quadratique.

Théorème 2 *[Wu, 1995] Le système LPV (2.4) est quadratiquement détectable, s'il existe une matrice $P = P^T > 0$ et une fonction $\rho_k \in \Omega_\rho \mapsto \mathcal{L}(\rho_k) \in I\!R^{n \times m}$ telles que*

$$(A(\rho_k) + \mathcal{L}(\rho_k)C)^T P + P(A(\rho_k) + \mathcal{L}(\rho_k)C) < 0 \quad \forall \rho_k \in \Omega_\rho$$

Concernant les Théorème 1 et 2, il s'avère que leur vérification nécessite la considération d'un nombre infini de vecteurs ρ_k en général. En conclusion, l'utilisation pratique de l'observabilité et de la détectabilité est souvent d'un intérêt limité. On peut préférer des conditions constructives telles que les approches LMI qui garantissent ces propriétés en même temps qu'on effectue la synthèse de l'observateur.

Ainsi, nous allons rappelé dans la suite d'une façon détaillée les techniques de synthèse d'observateurs fondées sur l'utilisation des LMI..

2.4.2 Synthèse d'observateurs

On suppose que la matrice $A(\rho_k)$ dans (2.4) admet la forme polytopique (2.7).

Un observateur polytopique pour (2.4) obéit à la description suivante

$$\begin{cases} \hat{x}_{k+1} = A(\rho_k)\hat{x}_k + Bu_k + \mathcal{L}(\rho_k)(y_k - \hat{y}_k) \\ \hat{y}_k = C\hat{x}_k + Du_k \end{cases} \tag{2.15}$$

où $\hat{x}_k \in \mathbb{R}^n$, $\hat{y}_k \in \mathbb{R}^p$ et $\mathcal{L}$ est une matrice de gain à temps variant fonction de ρ_k qui vérifie

$$\mathcal{L}(\rho_k) = \sum_{i=1}^{N} \xi_k^{(i)}(\rho_k) L^{(i)}, \quad \xi_k \in \Phi \tag{2.16}$$

Les grandeurs $\xi_k^{(i)}(\rho_k)$ dans (2.16) coïncident, pour chaque instant discret k, avec ceux qui sont impliqués dans la décomposition polytopique (2.7) de $A(\rho_k)$, ce qui n'est pas restrictif puisque ρ_k est mesuré.

A partir de (2.4) et (2.15), l'erreur de reconstruction $e_k = x_k - \hat{x}_k$ est gouvernée par la dynamique

$$e_{k+1} = (A(\rho_k) - \mathcal{L}(\rho_k)C)\, e_k \tag{2.17}$$

La dynamique de l'erreur de reconstruction d'état est non linéaire puisque A et $\mathcal{L}$ dépendent de ρ_k. Toutefois, (2.17) peut être considérée comme un système LPV polytopique autonome avec le vecteur d'état $e_k \in \mathbb{R}^n$. En effet, à partir de (2.7) et (2.16), et en tenant compte de la coïncidence entre les $\xi_k^{(i)}$ impliqués dans (2.16) et (2.7), nous obtenons

$$e_{k+1} = \sum_{i=1}^{N} \xi_k^{(i)} (A^{(i)} - L^{(i)}C) e_k, \quad \xi_k \in \Phi \tag{2.18}$$

La stabilité asymptotique globale autour du point d'équilibre $e^* = 0$ peut être assurée par un choix approprié des gains $L^{(i)}$ $(i = 1, \ldots, N)$ impliqués dans (2.16). À cette fin, le théorème suivant est central.

Théorème 3 *[Daafouz et al., 2002] S'il existe des matrices symétriques P_i, des matrices G_i et des matrices F_i vérifiant, $\forall (i,j) \in \{1...N\} \times \{1...N\}$, les LMI*

$$\begin{bmatrix} P_i & (\bullet)^T \\ G_i A^{(i)} - F_i C & G_i^T + G_i - P_j \end{bmatrix} > 0 \tag{2.19}$$

alors l'observateur polytopique (2.15) *avec le gain* $\mathcal{L}(\rho_k) = \sum_{i=1}^{N} \xi_k^{(i)}(\rho_k) L^{(i)}$ *et* $L^{(i)} = G_i^{-1} F_i$ *garantit que le système* (2.17) *est globalement asymptotiquement stable.*

Preuve 1 *La preuve détaillée est donnée dans [Daafouz et al., 2002]. Il est démontré que (2.19) assure l'existence d'une fonction de Lyapunov* $V : I\!R^n \times I\!R^{L_\rho} \to I\!R_+$ *définie par* $V(e_k, \rho_k) = e_k^T \mathcal{P}(\rho_k) e_k$ *avec* $\mathcal{P}(\rho_k) = \sum_{i=1}^{N} \xi_k^{(i)}(\rho_k) P_i$ *et* $\xi_k \in \Phi$*, appelée fonction de Lyapunov poly-quadratique, vérifiant pour tout* $e_k \in I\!R^n$*, pour tout* $\xi_k \in \Phi$

$$V(e_{k+1}, \rho_{k+1}) - V(e_k, \rho_k) < 0 \tag{2.20}$$

Cette fonction assure la stabilité poly-quadratique de (2.17) *qui est suffisante pour la stabilité asymptotique globale.*

Dans [Millerioux et al., 2005], il est démontré qu'une condition moins conservative (2.19) assurant la stabilité poly-quadratique de (2.18) et donc de (2.17) est obtenue lorsque les matrices $A^{(i)}$ sont obtenues à partir des sommets ρ_{o_i} du polytope minimal $\mathcal{D}_\rho^*$ dans lequel Ω_p est inclus.

2.4.3 Taux de décroissance (Decay rate)

La convergence asymptotique globale de (2.17) vers $e^* = 0$ avec un taux de décroissance $\alpha > 1$ est formalisée comme suit :

$$\forall e_0 \in \mathbb{R}^n, \quad \lim_{k \to \infty} \alpha^k \|e_k\| = 0 \tag{2.21}$$

et permet de spécifier un comportement transitoire.

En d'autres termes, (2.21) traduit le fait que $\|e_k\|$ décroît plus vite que α^{-k}. Une condition suffisante pour la convergence globale de (2.17) vers $e^* = 0$ avec un taux de décroissance α est donnée par le théorème suivant.

Théorème 4 *[Millérioux and Daafouz, 2001] S'il existe des matrices symétriques* P_i*, des matrices* F_i *et* G_i *vérifiant, pour un scalaire prescrit* κ*,* $\forall (i,j) \in \{1, \cdots, N\} \times \{1, \cdots, N\}$*, les LMI*

$$\begin{bmatrix} \kappa P_i & (\bullet)^T \\ G_i A^{(i)} - F_i C & G_i^T + G_i - P_j \end{bmatrix} > 0 \tag{2.22}$$

alors l'observateur polytopique (2.15) *avec un gain* $\mathcal{L}(\rho_k) = \sum_{i=1}^{N} \xi_k^{(i)}(\rho_k) L^{(i)}$ *et* $L^{(i)} = G_i^{-1} F_i$ *assure la convergence globale de* (2.17) *avec un taux de décroissance* α *supérieur ou égal à* $\kappa^{-\frac{1}{2}}$ $(0 < \kappa < 1)$.

Preuve 2 *La preuve est détaillée dans [Millérioux and Daafouz, 2001]. Il est démontré que (2.22) assure l'existence d'une fonction de Lyapunov* $V : I\!R^n \times I\!R^{L_\rho} \to I\!R_+$*, définie par* $V(e_k, \rho_k) = e_k^T \mathcal{P}(\rho_k) e_k$ *avec* $\mathcal{P}(\rho_k) = \sum_{i=1}^{N} \xi_k^{(i)}(\rho_k) P_i$ *et* $\xi_k \in \Phi$*, appelée fonction de Lyapunov poly-quadratique, assurant pour tout* $e_k \in I\!R^n$*, pour tout* $\xi_k \in \Phi$

$$V(e_{k+1}, \rho_{k+1}) - \kappa V(e_k, \rho_k) < 0 \tag{2.23}$$

ce qui est suffisant pour obtenir (2.21) *avec* $\alpha \geq \kappa^{-\frac{1}{2}}$.

2.5 Observateurs polytopiques dans un contexte stochastique ou incertain

Dans cette section, nous nous intéressons au cas où le système (2.4) est soumis à des perturbations et obéit à

$$\begin{cases} x_{k+1} = A(\rho_k)x_k + Bu_k + Ew_k^d \\ y_k = Cx_k + Du_k + Hw_k^o \end{cases} \tag{2.24}$$

où $w_k^d \in \mathbb{R}^{d_{w^d}}$ est la perturbation agissant sur la dynamique à travers E tandis que $w_k^o \in \mathbb{R}^{d_{w^o}}$ est la perturbation agissant sur la sortie à travers H.
Dans un tel cas, l'équation (2.17) de l'erreur de la reconstruction d'état $e_k = x_k - \hat{x}_k$ devient

$$e_{k+1} = (A(\rho_k) - \mathcal{L}(\rho_k)C)e_k + v_k \tag{2.25}$$

avec $v_k = Ew_k^d - \mathcal{L}(\rho_k)Hw_k^o$.

Nous pouvons également être intéressés par le cas où ρ_k n'est pas directement accessible, et où seulement un paramètre estimé $\hat{\rho}_k \in \Omega_{\hat{\rho}}$ est disponible. Le niveau d'incertitude Δ satisfait $\|\rho_k - \hat{\rho}_k\|_\infty < \Delta$. L'observateur polytopique (2.15) peut prendre alors la forme

$$\begin{cases} \hat{x}_{k+1} = A(\hat{\rho}_k)\hat{x}_k + Bu_k + \mathcal{L}(\hat{\rho}_k)(y_k - \hat{y}_k) \\ \hat{y}_k = C\hat{x}_k + Du_k \end{cases} \tag{2.26}$$

avec

$$\mathcal{L}(\hat{\rho}_k) = \sum_{i=1}^{N} \hat{\xi}_k^{(i)}(\hat{\rho}_k)L^{(i)} \tag{2.27}$$

Dans un tel cas, (2.25) reste vérifiée à condition que ρ_k soit remplacé par $\hat{\rho}_k$ et donc $v_k = \Delta A(\rho_k, \hat{\rho}_k)x_k$ avec $\Delta A(\rho_k, \hat{\rho}_k) = A(\rho_k) - A(\hat{\rho}_k)$.

2.5.1 Notion d'ISS

La notion d'ISS permet d'assurer la robustesse de l'observateur vis-à-vis des perturbations ou des incertitudes. De nombreuses approches permettant d'obtenir des conditions suffisantes pour garantir l'ISS sont fondées sur la notion de fonctions de Lyapunov ISS.

Définition 7 *[Heemels et al., 2010] Soit $d_1, d_2 \in \mathbb{R}_+$, soit $a, b, c, l \in \mathbb{R}_+$ et $a \leq b$ et soit $\alpha_1(s) = as^l, \alpha_2(s) = bs^l, \alpha_3(s) = cs^l$ et $\tau \in \mathcal{K}$. Une fonction $V : \mathbb{R}^n \times \mathbb{R}^{L_\rho} \to \mathbb{R}_+$ qui satisfait*

$$\alpha_1(\|e_k\|) \leq V(e_k, \rho_k) \leq \alpha_2(\|e_k\|) \tag{2.28}$$

$$V(e_{k+1}, \rho_{k+1}) - V(e_k, \rho_k) \leq -\alpha_3(\|e_k\|) + \tau(\|v_k\|) \tag{2.29}$$

pour tout $e_k \in \mathbb{R}^n$, tout $v_k \in \mathbb{R}^n$ et tout $\rho_k \in \Omega_\rho$ est appelée Fonction de Lyapunov ISS pour (2.25).

Théorème 5 *[Sontag, 1989, Jiang and Wang, 2001] Si le système* (2.25) *admet une fonction de Lyapunov ISS, alors* (2.25) *est ISS par rapport à v_k, s'il existe une $\mathcal{KL}$ fonction β et une $\mathcal{K}$ fonction γ de telle sorte que, pour toutes les séquences $\{v\}$, pour tout $e_0 \in \mathbb{R}^n$, pour tout $k \in \mathbb{N}$*

$$\|e_k\| \leq \beta(\|e_0\|, k) + \gamma(\|v\|_\infty) \tag{2.30}$$

2.5.1.1 Lien entre la stabilité poly-quadratique et l'ISS

Théorème 6 *[Millérioux et al., 2004] Si les LMI* (2.19) *sont faisables, le système* (2.25) *est ISS par rapport à v_k et*

$$\|e_k\| \leq \sqrt{\frac{c_2}{c_1}}\left(1-\frac{c_3-\delta}{c_2}\right)^{k/2}\|e_0\| + \sqrt{\frac{c_2+\delta^{-1}c_4^2}{c_1}\cdot\frac{c_2}{c_3-\delta}}\cdot\|v\|_\infty \tag{2.31}$$

c_1, c_2, c_3, c_4 et δ sont des scalaires fonction des valeurs propres des matrices provenant de la solution de (2.19). *La grandeur $(1-\frac{c_3-\delta}{c_2})^{1/2}$ est appelée le facteur de décroissance.*

En d'autres termes, l'observateur polytopique (2.15) avec un gain $\mathcal{L}(\rho_k)$ donné par (2.16) et obtenu à partir de la solution de (2.19), assure la stabilité poly-quadratique de (2.17), et garantit également l'ISS de (2.25) en présence de perturbations et/ou d'incertitudes bornées sur ρ_k.

Preuve 3 *La preuve est détaillée dans [Millérioux et al., 2004]. Il est démontré que* (2.19) *assure l'existence d'une fonction de Lyapunov ISS définie par $V : \mathbb{R}^n \times \mathbb{R}^{L_\rho} \to \mathbb{R}_+$ avec $\mathcal{P}(\rho_k) = \sum_{i=1}^{N}\xi_k^{(i)}(\rho_k)P_i$ et $\xi_k \in \Phi$, ce qui est suffisant pour déduire* (2.31).

2.5.1.2 Minimisation du gain ISS

Le problème est que le facteur de décroissance et le gain ISS en (2.31) ne peuvent être prescrits à l'avance. Le théorème suivant est une première solution au problème.

Théorème 7 *[Heemels et al., 2010] S'il existe des matrices symétriques P_i, des matrices G_i, des matrices F_i, vérifiant, pour un scalaire prescrit $\sigma_{ev} \geq 1$, $\forall (i,j) \in (1,\ldots,N)\times(1,\ldots,N)$, les LMI*

$$\begin{bmatrix} G_i^T+G_i-P_j & \mathbf{0} & G_iA^{(i)}-F_iC & G_i \\ (\bullet)^T & \mathbf{1} & \mathbf{1} & \mathbf{0} \\ (\bullet)^T & (\bullet)^T & P_i & \mathbf{0} \\ (\bullet)^T & (\bullet)^T & (\bullet)^T & \sigma_{ev}\mathbf{1} \end{bmatrix} > 0 \tag{2.32}$$

alors l'observateur polytopique (2.15) *avec le gain $\mathcal{L}(\rho_k) = \sum_{i=1}^{N}\xi_k^{(i)}(\rho_k)L^{(i)}$ et $L^{(i)} = G_i^{-1}F_i$, garantit que le système* (2.25) *est ISS par rapport à v_k et*

$$\|e_k\| \leq \sqrt{\sigma_{ev}}(1-\frac{1}{\sigma_{ev}})^{k/2}\|e_0\| + \sigma_{ev}\|v\|_\infty \tag{2.33}$$

Preuve 4 *La preuve détaillée est fournie dans [Heemels et al., 2010]. Il est démontré que* (2.32) *assure l'existence d'une fonction de Lyapunov ISS définie par $V : \mathbb{R}^n \times \mathbb{R}^{L_\rho} \to \mathbb{R}_+$ avec $\mathcal{P}(\rho_k) = \sum_{i=1}^{N}\xi_k^{(i)}(\rho_k)P_i$ et $\xi_k \in \Phi$ qui vérifie pour tout $e_k \in \mathbb{R}^n$, tout $v_k \in \mathbb{R}^n$ et tout $\xi_k \in \Phi$ de* (2.25), *les conditions suivantes*

$$\begin{aligned} \|e_k\|^2 \leq V(e_k,\rho_k) &\leq \sigma_{ev}\|e_k\|^2 \\ V(e_{k+1},\rho_{k+1}) - V(e_k,\rho_k) &\leq -\|e_k\|^2 + \sigma_{ev}\|v_k\|^2 \end{aligned} \tag{2.34}$$

L'existence de V est suffisante pour obtenir (2.33).

Si on désire optimiser le gain ISS en minimisant σ_{ev} dans (2.33), dans la mesure où σ_{ev} apparaît de façon linéaire dans les inégalités matricielles (2.32), le problème suivant doit être résolu

$$\begin{array}{l} \min \quad \sigma_{ev} \\ t.q\ (2.32) \end{array} \tag{2.35}$$

qui est un problème convexe.

2.5.1.3 Découplage du taux de décroissance et du gain ISS

Il est intéressant de souligner que, dans la formulation précédente, et en particulier lorsqu'on considère (2.33), la grandeur σ_{ev} est à la fois impliquée dans le facteur de décroissance et dans le gain ISS. Le réglage indépendant fait l'objet du théorème suivant.

Théorème 8 *[Millérioux and Bloch, 2013] S'il existe des matrices symétriques P_i, des matrices G_i, des matrices F_i et deux nombres réels $\mu > 0$ et ν vérifiant, pour un $\lambda \in]0\ 1[$ prescrit, $\forall (i,j) \in \{1 \cdots N\} \times \{1 \cdots N\}$, les LMI*

$$\begin{bmatrix} (1-\lambda)P_i & (\bullet)^T & (\bullet)^T \\ \boldsymbol{0} & \mu \boldsymbol{1} & (\bullet)^T \\ G_i A^{(i)} - F_i C & G_i & G_i^T + G_i - P_j \end{bmatrix} > 0 \tag{2.36}$$

et

$$\begin{bmatrix} \lambda P_i & (\bullet)^T & (\bullet)^T \\ \boldsymbol{0} & (\nu-\mu)\boldsymbol{1} & (\bullet)^T \\ \boldsymbol{1} & \boldsymbol{0} & \nu \boldsymbol{1} \end{bmatrix} > 0 \tag{2.37}$$

alors l'observateur polytopique (2.15) *avec le gain $\mathcal{L}(\rho_k) = \sum_{i=1}^{N} \xi_k^{(i)}(\rho_k) L^{(i)}$ avec $L^{(i)} = G_i^{-1} F_i$, garantit que le système* (2.25) *est ISS par rapport à v_k et*

$$\|e_k\| \leq \sqrt{\nu\lambda\mu}(1-\lambda)^{k/2} \|e_0\| + \nu \|v\|_\infty \tag{2.38}$$

Preuve 5 *La preuve détaillée est fournie dans [Millérioux and Bloch, 2013]. Il est démontré que* (2.36)-(2.37) *assure l'existence d'une fonction de Lyapunov ISS $V : \mathbb{R}^n \times \mathbb{R}^{L_\rho} \to \mathbb{R}_+$ avec $\mathcal{P}(\rho_k) = \sum_{i=1}^{N} \xi_k^{(i)}(\rho_k) P_i$ et $\xi_k \in \Phi$ qui vérifie pour tout $e_k \in \mathbb{R}^n$, tout $v_k \in \mathbb{R}^n$ et tout $\xi_k \in \Phi$, les conditions suivantes*

$$\frac{1}{\nu\lambda} \|e_k\|^2 \leq V(e_k, \rho_k) \leq \mu \|e_k\|^2 \tag{2.39}$$

$$V(e_{k+1}, \rho_{k+1}) - V(e_k, \rho_k) \leq -\frac{1}{\nu} \|e_k\|^2 + \mu \|v_k\|^2 \tag{2.40}$$

L'existence de V est suffisante pour obtenir (2.38).

Remarque 3 *Il peut être montré [Millérioux and Bloch, 2013] que les conditions (2.36)-(2.37) sont moins conservatives que* (2.32) *et que* (2.32) *est un cas particulier de (2.36)-(2.37) lorsque $\nu = \sigma_{ev}, \lambda = \frac{1}{\sigma_{ev}}$ et $\mu = \sigma_{ev}$.*

Remarque 4 *Les inégalités matricielles (2.36)-(2.37) ne sont pas linéaires en raison des produits λP_i dans (2.36). En fait, elles se réduisent à des LMI si λ est fixé. Par conséquent, elles peuvent être facilement résolues du fait que λ est un scalaire et que l'intervalle de λ est borné puisque $\lambda \in]0,1[$. En conséquence, une recherche de type dichotomie par exemple peut être réalisée et $\lambda = \frac{1}{\sigma_{ev}}$, qui est une solution de (2.32), peut être utilisée en tant que valeur initiale admissible.*

Si on désire optimiser le gain ISS en minimisant ν dans (2.38), dans la mesure où ν apparaît de façon linéaire dans les inégalités matricielles (2.37), pour un $\lambda \in]0\ 1[$ prescrit, le problème suivant doit être résolu

$$\begin{array}{c} \min \quad \nu \\ t.q\ (2.36) - (2.37) \end{array} \tag{2.41}$$

qui est un problème convexe.

2.5.2 Gain crête-à-crête

Le gain crête-à-crête (en anglais peak-to-peak gain) de l'équation d'erreur d'état (2.25) est défini comme étant le rapport

$$\sup_{0<\|v\|_\infty<\infty,\ \rho_k\in\Omega_\rho} \frac{\|e\|_\infty}{\|v\|_\infty} \tag{2.42}$$

Le gain crête-à-crête est défini de la même manière que dans le cas linéaire, mis à part que, toutes les trajectoires possibles $\rho_k \in \Omega_\rho$ doivent être considérées.

Le théorème suivant permet d'assurer un gain crête-à-crête.

Théorème 9 *Si les LMI (2.32) (resp. (2.36)-(2.37)) sont vérifiées, alors l'observateur polytopique (2.15) avec le gain $\mathcal{L}(\rho_k) = \sum_{i=1}^{N} \xi_k^{(i)}(\rho_k) L^{(i)}$ et $L^{(i)} = G_i^{-1} F_i$, garantit que l'erreur e_k de (2.25) admet un gain crête à crête inférieur à σ_{ev} (resp. plus petit que ν). On obtient respectivement*

$$\sup_{0<\|v\|_\infty<\infty,\ \rho_k\in\mathcal{D}_\rho} \frac{\|e\|_\infty}{\|v\|_\infty} < \sigma_{ev} \tag{2.43}$$

$$\sup_{0<\|v\|_\infty<\infty,\ \rho_k\in\mathcal{D}_\rho} \frac{\|e\|_\infty}{\|v\|_\infty} < \nu \tag{2.44}$$

Preuve 6 *Le résultat peut être directement déduit de l'inégalité (2.33) (resp. (2.38)) en prenant la limite de k à l'infini, et en supposant que $\|e_0\| = 0$.*

Notons que (2.32) ou (2.36)-(2.37) garantit que le gain crête-à-crête est borné pour toutes les trajectoires possibles de ρ_k dans $\mathcal{D}_\rho \supseteq \Omega_\rho$.

La minimisation du gain crête-à-crête peut être réalisée en minimisant sa borne supérieur donnée par (2.43) et (2.44). La minimisation est obtenue par (2.35) ou (2.41).

2.5.3 Gain $\mathcal{L}_2$

Soit $z_k = \tilde{H}e_k$ une combinaison linéaire de l'erreur de reconstruction d'état e_k obéissant à la dynamique (2.25).

Définition 8 *Le gain $\mathcal{L}_2$ de l'équation d'erreur (2.25) est défini comme*

$$\sup_{\|v\|_2 \neq 0,\ \rho_k \in \Omega_\rho} \frac{\|z\|_2}{\|v\|_2} \tag{2.45}$$

De même que pour le gain crête-à-crête, le gain $\mathcal{L}_2$ est défini de la même façon que dans le cas linéaire, mis à part que, toutes les trajectoires possibles $\rho_k \in \Omega_\rho$ doivent être considérées.

Théorème 10 *[Millérioux and Daafouz, 2004] S'il existe des matrices symétriques P_i, des matrices G_i et des matrices F_i, vérifiant, pour un nombre réel donné σ_2, $\forall (i,j) \in \{1 \cdots N\} \times \{1 \cdots N\}$, les LMI*

$$\begin{bmatrix} P_i & (\bullet)^T & (\bullet)^T & (\bullet)^T \\ \boldsymbol{0} & \sigma_2 \boldsymbol{1} & (\bullet)^T & (\bullet)^T \\ G_i A^{(i)} - F_i C & G_i E - F_i H & G_i^T + G_i - P_j & (\bullet)^T \\ \tilde{H} & \boldsymbol{0} & \boldsymbol{0} & \sigma_2 \boldsymbol{1} \end{bmatrix} > 0 \tag{2.46}$$

alors l'observateur polytopique (2.15) avec un gain $\mathcal{L}(\rho_k) = \sum_{i=1}^{N} \xi_k^{(i)}(\rho_k) L^{(i)}$ et $L^{(i)} = G_i^{-1} F_i$, assure que l'erreur e_k de (2.25) admet un gain $\mathcal{L}_2$ plus petit que σ_2.

Preuve 7 *La preuve suit les mêmes lignes de raisonnement que celles indiquées dans [Millérioux and Daafouz, 2004]. Il est démontré que (2.46) assure l'existence d'une fonction de Lyapunov $V : \mathbb{R}^n \times \mathbb{R}^{L_\rho} \to \mathbb{R}_+$ définie par $V(e_k, \rho_k) = e_k^T \mathcal{P}(\rho_k) e_k$ avec $\mathcal{P}(\rho_k) = \sum_{i=1}^{N} \xi_k^{(i)}(\rho_k) P_i$ et $\xi_k \in \Phi$, vérifiant pour tout $e_k \in \mathbb{R}^n$, tout $\xi_k \in \Phi$*

$$V(e_{k+1}, \rho_{k+1}) - V(e_k, \rho_k) + \sigma_2^{-1} (\tilde{C} e_k)^T (\tilde{C} e_k) - \sigma_2 v_k^T v_k < 0$$

ce qui est suffisant pour obtenir

$$\sup_{\|v\|_2 \neq 0,\ \rho_k \in \mathcal{D}_\rho} \frac{\|z\|_2}{\|v\|_2} < \sigma_2$$

Puisque σ_2 apparaît d'une manière linéaire en (2.46), le problème de minimisation

$$\begin{array}{l} \min \quad \sigma_2 \\ t.q\ (2.46) \end{array} \tag{2.47}$$

est un problème convexe.

Notons que (2.46) garantit que le gain $\mathcal{L}_2$ soit borné pour toutes les trajectoires possibles de ρ_k dans $\mathcal{D}_\rho \supseteq \Omega_\rho$.

2.6 Observateurs à entrées inconnues

On propose dans cette section une extension des observateurs polytopiques dans le cas à entrées inconnues pour les systèmes LPV. La dynamique de l'erreur de la reconstruction d'état et son analyse sont étudiées à la fois dans le cas déterministe (considération de l'Équation (2.4)) et dans le cas où le système (2.4) est soumis à des perturbations (considération de l'Equation (2.24)).

2.6.1 Notation et définitions

Dans le cas déterministe, lorsque le système (2.4) est commandé par une séquence d'entrée $u_{[0,\infty]}$, la sortie y_{k+i} de (2.4) $(i = 0, \cdots, \infty)$ vérifie

$$y_{k+i} = C(\rho_{k+i}) A^{\rho_k}_{\rho_{k+i-1}} x_k + \sum_{j=0}^{i} \mathcal{T}_{i,j}(\rho_k) u_{k+j} \tag{2.48}$$

avec

$$\mathcal{T}_{i,j}(\rho_k) = C(\rho_{k+i}) A^{\rho_{k+j+1}}_{\rho_{k+i-1}} B(\rho_{k+j}) \text{ si } j \leq i-1, \quad \mathcal{T}_{i,i}(\rho_k) = D(\rho_{k+i})$$

En empilant les sorties (2.48), on obtient

$$y_{k,k+i} = \mathcal{O}_{\rho_{[k,k+i]}} x_k + T_{\rho_{[k,k+i]}} u_{k,k+i} \tag{2.49}$$

où $\rho_{[k,k+i]}$ dénote le paramètre à temps variant ρ_k dans l'intervalle $[k, k+i]$
et

$$\mathcal{O}_{\rho_{[k,k+i]}} = \begin{bmatrix} C(\rho_k) \\ C(\rho_{k+1})A(\rho_k) \\ \vdots \\ C(\rho_{k+i}) A^{\rho_k}_{\rho_{k+i-1}} \end{bmatrix} \tag{2.50}$$

$$u_{k,k+i} = \begin{bmatrix} u_k \\ u_{k+1} \\ \vdots \\ u_{k+i} \end{bmatrix} \tag{2.51}$$

$$y_{k,k+i} = \begin{bmatrix} y_k \\ y_{k+1} \\ \vdots \\ y_{k+i} \end{bmatrix} \tag{2.52}$$

et la matrice $T_{\rho_{[k,k+i]}}$ définie comme suit.

$$\text{Pour } i < 0 \;\; T_{\rho_{[k,k+i]}} = \mathbf{0}, \text{ pour } i = 0 \;\; T_{\rho_{[k,k]}} = D(\rho_k) \;\; \text{et pour } i > 0,$$

$T_{\rho_{[k,k+i]}} =$

$$\begin{bmatrix} D(\rho_k) & \mathbf{0}_{p\times m} & \cdots & \cdots & \cdots \\ C(\rho_{k+1})B(\rho_k) & D(\rho_{k+1}) & \mathbf{0}_{p\times m} & \cdots & \cdots \\ \vdots & \vdots & \ddots & \ddots & \ddots \\ \vdots & \vdots & \ddots & \ddots & \ddots \\ C(\rho_{k+i}) A^{\rho_{k+1}}_{\rho_{k+i-1}} B(\rho_k) & C(\rho_{k+i}) A^{\rho_{k+2}}_{\rho_{k+i-1}} B(\rho_{k+1}) & \cdots & C(\rho_{k+i})B(\rho_{k+i-1}) & D(\rho_{k+i}) \end{bmatrix} \tag{2.53}$$

où

$$\begin{aligned} A_{\rho_{k_1}}^{\rho_{k_0}} &= A(\rho_{k_1})A(\rho_{k_1-1})\dots A(\rho_{k_0}) \text{ si } k_1 \geq k_0 \\ &= \mathbf{1}_n \text{ si } k_1 < k_0 \end{aligned}$$

est la matrice de transition.

Pour le système (2.24) commandé par une séquence d'entrée $u_{[0,\infty]}$, les sorties y_{k+i} de (2.24) $(i = 0, \cdots, \infty)$ s'écrivent

$$y_{k+i} = C(\rho_{k+i})A_{\rho_{k+i-1}}^{\rho_k} x_k + \sum_{j=0}^{i} \mathcal{T}_{i,j}(\rho_k)u_{k+j} + \sum_{j=0}^{i} \mathcal{S}_{i,j}(\rho_k)w_{k+j}^d + Hw_{k+i}^o \tag{2.54}$$

avec

$$\mathcal{T}_{i,j}(\rho_k) = C(\rho_{k+i})A_{\rho_{k+i-1}}^{\rho_{k+j+1}}B(\rho_{k+j}) \text{ si } j \leq i-1, \quad \mathcal{T}_{i,i}(\rho_k) = D(\rho_{k+i})$$
$$\mathcal{S}_{i,j}(\rho_k) = C(\rho_{k+i})A_{\rho_{k+i-1}}^{\rho_{k+j+1}}E \text{ si } j \leq i-1, \quad \mathcal{S}_{i,i}(\rho_k) = \mathbf{0}$$

En empilant les sorties (2.54), on obtient

$$y_{k,k+i} = \mathcal{O}_{\rho_{[k,k+i]}}x_k + T_{\rho_{[k,k+i]}}u_{k,k+i} + F_{\rho_{[k,k+i]}}w_{k,k+i}^d + N_{\rho_{[k,k+i]}}w_{k,k+i}^o \tag{2.55}$$

avec

$$w_{k,k+i}^d = \begin{bmatrix} w_k^d \\ w_{k+1}^d \\ \vdots \\ w_{k+i}^d \end{bmatrix} \tag{2.56}$$

$$w_{k,k+i}^o = \begin{bmatrix} w_k^o \\ w_{k+1}^o \\ \vdots \\ w_{k+i}^o \end{bmatrix} \tag{2.57}$$

La matrice $N_{\rho_{[k,k+i]}}$ est définie comme suit.

$$N_{\rho_{[k,k]}} = \mathbf{0}, \qquad N_{\rho_{[k,k+1]}} = \begin{bmatrix} H & \mathbf{0}_{p\times d_{w^o}} \\ \mathbf{0}_{p\times d_{w^o}} & H \end{bmatrix} \tag{2.58}$$

et pour $i > 1$, $N_{\rho_{[k,k+i]}}$ est définie récursivement

$$N_{\rho_{[k,k+i+1]}} = \begin{bmatrix} N_{\rho_{[k,k+i]}} & \mathbf{0}_{(i+1)\cdot p\times d_{w^o}} \\ \mathbf{0}_{p\times d_{w^o}\cdot(i+1)} & H \end{bmatrix} \tag{2.59}$$

La matrice $F_{\rho_{[k,k+i]}}$ est définie comme suit.

Pour $i \leq 0$ $F_{\rho_{[k,k+i]}} = \mathbf{0}$ et pour $i > 0$,

$$F_{\rho_{[k,k+i]}} = \begin{bmatrix} \mathbf{0}_{p\times d_{w^d}} & \mathbf{0}_{p\times d_{w^d}} & \cdots & \cdots & \cdots \\ C(\rho_{k+1})E & \mathbf{0}_{p\times d_{w^d}} & \mathbf{0}_{p\times d_{w^d}} & \cdots & \cdots \\ \vdots & \vdots & \ddots & \ddots & \ddots \\ \vdots & \vdots & \ddots & \ddots & \ddots \\ C(\rho_{k+i})A_{\rho_{k+i-1}}^{\rho_{k+1}}E & C(\rho_{k+i})A_{\rho_{k+i-1}}^{\rho_{k+2}}E & \cdots & C(\rho_{k+i})E & \mathbf{0}_{p\times d_{w^d}} \end{bmatrix} \tag{2.60}$$

Des notions centrales pour la conception de l'observateur à entrées inconnues sont l'inversibilité à gauche et le retard inhérent.

Définition 9 *[Millérioux and Daafouz, 2009] Le système LPV* (2.4) *est* inversible à gauche *s'il est possible de reconstruire l'entrée u_0 à partir d'un nombre fini de $r+1$ mesures de y_i ($i = 0, \ldots, r$), connaissant le vecteur d'état x_0 et la séquence $\rho_{[0,r]}$ du paramètre ρ_k. Le plus petit entier r pour lequel* (2.4) *est inversible à gauche est appelé le* retard inhérent à gauche.

La Définition 9 est une extension de la notion introduite dans [Silverman, 1969] pour les systèmes MIMO linéaires. Rappelons ici que le retard inhérent généralise la notion du degré relatif qui ne vaut que pour les systèmes SISO ou pour les systèmes MIMO avec considération séparée de chacune des sorties.

Théorème 11 *[Millérioux and Daafouz, 2009] Le système LPV* (2.4) *est* inversible à gauche *s'il existe un entier non négatif $r < \infty$ de telle sorte que pour tout $\rho_k \in \Omega_\rho$,*

$$rang(T_{\rho_{[k,k+r]}}) - rang(T_{\rho_{[k+1,k+r]}}) = m \tag{2.61}$$

où m est la dimension de l'entrée.

2.6.2 Cas déterministe

L'observateur polytopique à entrées inconnues proposé pour le système (2.4) obéit aux équations suivantes

$$\left\{ \begin{array}{lcl} \hat{x}_{k+r+1} & = & \bar{P}_{\rho_{[k,k+r]}} \hat{x}_{k+r} + \bar{Q}_{\rho_{[k,k+r]}} y_{k,k+r} + \mathcal{L}(\rho_k)(y_k - \hat{y}_{k+r}) \\ \hat{y}_{k+r} & = & C(\rho_k)\hat{x}_{k+r} \end{array} \right. \tag{2.62}$$

avec $\bar{Q}_{\rho_{[k,k+r]}}$ qui s'écrit

$$\bar{Q}_{\rho_{[k,k+r]}} = B(\rho_k)\bar{I}_m T^{\dagger}_{\rho_{[k,k+r]}} + Y(\rho_k)(\mathbf{1}_{p(r+1)} - T_{\rho_{[k,k+r]}} T^{\dagger}_{\rho_{[k,k+r]}}) \tag{2.63}$$

avec

$$\bar{I}_m = (\mathbf{1}_m \ \mathbf{0}_{m\times(m\cdot r)}) \tag{2.64}$$

et

$$\bar{P}_{\rho_{[k,k+r]}} = A(\rho_k) - \bar{Q}_{\rho_{[k,k+r]}} \mathcal{O}_{\rho_{[k,k+r]}} \tag{2.65}$$

Soit $e_k = x_k - \hat{x}_{k+r}$ l'erreur de la reconstruction d'état. En supposant que le Théorème 11 soit vérifié, on obtient, à partir de (2.4) et (2.62)-(2.65)

$$\begin{array}{rcl} e_{k+1} & = & (A(\rho_k) - B(\rho_k)\bar{I}_m T^{\dagger}_{\rho_{[k,k+r]}} \mathcal{O}_{\rho_{[k,k+r]}} \\ & & -Y(\rho_k)(\mathbf{1}_{p(r+1)} - T_{\rho_{[k,k+r]}} T^{\dagger}_{\rho_{[k,k+r]}}) \mathcal{O}_{\rho_{[k,k+r]}} \\ & & -\mathcal{L}(\rho_k)C(\rho_k))e_k \end{array} \tag{2.66}$$

La matrice $Y(\rho_k)$ est une matrice arbitraire qui joue le rôle d'un paramétrage. Toutefois, il convient de souligner que, dans certains cas particuliers, un choix arbitraire de $Y(\rho_k)$ peut ne pas convenir à la reconstruction d'état (voir [Darouach et al., 1994] dans le cas linéaire).

Pour résoudre ce problème, le calcul de $Y(\rho_k)$ devrait être inclus dans la synthèse. Dans cette perspective, nous procédons au changement de variable $\tilde{A}(\rho_k) = A(\rho_k) - B(\rho_k)\bar{I}_m T^{\dagger}_{\rho_{[k,k+r]}}\mathcal{O}_{\rho_{[k,k+r]}}$, $\tilde{\mathcal{L}}(\rho_k) = [Y(\rho_k) \;\; \mathcal{L}(\rho_k)]$ et $\tilde{C}(\rho_k) = \begin{bmatrix} (\mathbf{1}_{p(r+1)} - T_{\rho_{[k,k+r]}} T^{\dagger}_{\rho_{[k,k+r]}})\mathcal{O}_{\rho_{[k,k+r]}} \\ C(\rho_k) \end{bmatrix}$.
En conséquence, (2.66) se transforme en :

$$e_{k+1} = (\tilde{A}(\rho_k) - \tilde{\mathcal{L}}(\rho_k)\tilde{C}(\rho_k))e_k \tag{2.67}$$

Le problème de garantir la stabilité asymptotique globale de (2.67) autour de $e^* = 0$ peut être traité de la même manière que dans les sections précédentes consacrées aux observateurs polytopiques. Ainsi, le recours à la stabilité poly-quadratique est encore possible.

2.6.3 Cas stochastique

On s'intéresse au cas où le système (2.4) est soumis à des perturbations et obéit à (2.24).

Supposant que le Théorème 11 soit vérifié, on obtient à partir de (2.4) et de l'observateur polytopique à entrées inconnues (2.62), après quelques manipulations lourdes mais élémentaires, l'erreur de reconstruction $e_k = x_k - \hat{x}_{k+r}$

$$\begin{array}{rcl} e_{k+1} & = & (\bar{P}_{\rho_{[k,k+r]}} - \mathcal{L}(\rho_k)C(\rho_k))e_k + (Ew^d_k - \mathcal{L}(\rho_k)Hw^o_k) \\ & & -\bar{Q}_{\rho_{[k,k+r]}}(F_{\rho_{[k,k+r]}}w^d_{k,k+r} + N_{\rho_{[k,k+r]}}w^o_{k,k+r}) \end{array} \tag{2.68}$$

En remplaçant l'expression (2.63) de $\bar{Q}_{\rho_{[k,k+r]}}$ dans $\bar{P}_{\rho_{[k,k+r]}}$, on obtient

$$\begin{array}{rcl} e_{k+1} & = & (A(\rho_k) - B(\rho_k)\bar{I}_m T^{\dagger}_{\rho_{[k,k+r]}}\mathcal{O}_{\rho_{[k,k+r]}} \\ & & -Y(\rho_k)(\mathbf{1}_{p(r+1)} - T_{\rho_{[k,k+r]}}T^{\dagger}_{\rho_{[k,k+r]}})\mathcal{O}_{\rho_{[k,k+r]}} \\ & & -\mathcal{L}(\rho_k)C(\rho_k))e_k + Ew^d_k - \mathcal{L}(\rho_k)Hw^o_k \\ & & -(B(\rho_k)\bar{I}_m T^{\dagger}_{\rho_{[k,k+r]}} + Y(\rho_k)(\mathbf{1}_{p(r+1)} - T_{\rho_{[k,k+r]}}T^{\dagger}_{\rho_{[k,k+r]}})) \\ & & (F_{\rho_{[k,k+r]}}w^d_{k,k+r} + N_{\rho_{[k,k+r]}}w^o_{k,k+r}) \end{array} \tag{2.69}$$

Comme dans le cas précédent, $Y(\rho_k)$ est une matrice arbitraire qui joue le rôle d'un paramétrage et nous devrions procéder au changement de variable $\tilde{A}(\rho_k) = A(\rho_k) - B(\rho_k)\bar{I}_m T^{\dagger}_{\rho_{[k,k+r]}}\mathcal{O}_{\rho_{[k,k+r]}}$, $\tilde{\mathcal{L}}(\rho_k) = [Y(\rho_k) \;\; \mathcal{L}(\rho_k)]$,
$\tilde{C}(\rho_k) = \begin{bmatrix} (\mathbf{1}_{p(r+1)} - T_{\rho_{[k,k+r]}} T^{\dagger}_{\rho_{[k,k+r]}})\mathcal{O}_{\rho_{[k,k+r]}} \\ C(\rho_k) \end{bmatrix}$.
En conséquence, (2.69) se transforme en :

$$e_{k+1} = (\tilde{A}(\rho_k) - \tilde{\mathcal{L}}(\rho_k)\tilde{C}(\rho_k))e_k + v_k \tag{2.70}$$

avec :

$$\begin{array}{rcl} v_k & = & Ew^d_k - \mathcal{L}(\rho_k)Hw^o_k \\ & & -(B(\rho_k)\bar{I}_m T^{\dagger}_{\rho_{[k,k+r]}} + Y(\rho_k)(\mathbf{1}_{p(r+1)} - T_{\rho_{[k,k+r]}}T^{\dagger}_{\rho_{[k,k+r]}})) \\ & & (F_{\rho_{[k,k+r]}}w^d_{k,k+r} + N_{\rho_{[k,k+r]}}w^o_{k,k+r}) \end{array}$$

Encore une fois, le problème de la conception d'observateur polytopique à entrées inconnues pour garantir les performances de convergence autour de $e^* = 0$ de (2.70) peut être traité de la même manière que dans les sections précédentes consacrées aux observateurs polytopiques.

2.7 Exemples illustratifs

Dans cette section, plusieurs exemples sont considérés. L'exemple 1 illustre la méthode qui permet d'obtenir une description polytopique LPV d'un système chaotique à non linéarité polynomiale, ainsi que le choix d'une fonction appropriée ρ_k. La réécriture d'un système chaotique linéaire à commutation sous forme polytopique est illustrée dans l'exemple 2. Le but de l'exemple 3 est d'illustrer une méthode de recherche du polytope $\mathcal{D}_\rho$ associé à un attracteur chaotique. L'exemple 4 illustre la synthèse d'observateurs polytopiques pour la synchronisation du chaos dans le contexte déterministe et stochastique. Finalement, l'exemple 5 illustre la synchronisation du chaos dans un système de chiffrement chaotique.

2.7.1 Exemple 1

Considérons la récurrence chaotique à non linéarité polynomiale donnée par

$$\begin{cases} x_{k+1}^{(1)} = x_k^{(2)} \\ x_{k+1}^{(2)} = -2\left(x_k^{(1)}\right)^3 + 2\,x_k^{(1)} + 0.3\,x_k^{(1)}x_k^{(2)} \\ y_k = x_k^{(1)} \end{cases} \tag{2.71}$$

Son attracteur Ω est illustré sur la Figure 2.1 (a). La récurrence (2.71) peut être réécrite sous la forme d'un système LPV donné par (2.4). À cette fin, nous choisissons ρ_k comme le vecteur de paramètre obéissant à

$$\rho_k^{(1)} = -2\left(x_k^{(1)}\right)^2 + 2$$
$$\rho_k^{(2)} = 0.3\,x_k^{(1)}$$

Alors, (2.71) peut être réécrite comme un système LPV de la forme (2.4) avec

$$A(\rho_k) = \begin{bmatrix} 0 & 1 \\ \rho_k^{(1)} & \rho_k^{(2)} \end{bmatrix},\ B = \mathbf{0},\ C = [1\ \ 0] \text{ et } D = \mathbf{0}$$

Un tel choix pour ρ_k répond aux conditions de la Proposition 1. En particulier, ρ_k est accessible à partir de la sortie y_k. En effet, $\rho_k^{(1)} = -2\,(y_k)^2 + 2$ et $\rho_k^{(2)} = 0.3\,y_k$. La variation de ρ_k est illustrée sur la Figure 2.1 (b).

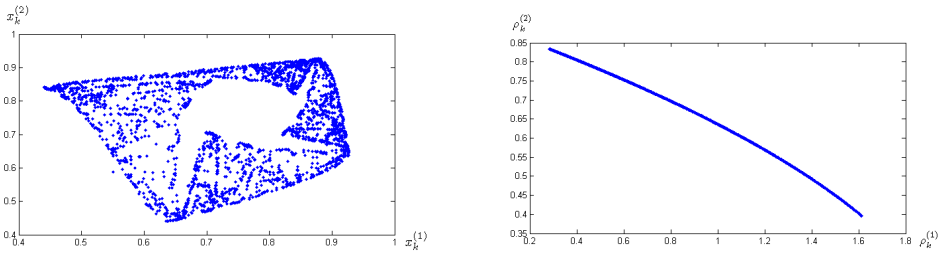
Une autre possibilité est de choisir ρ_k tel que $\rho_k^{(1)} = -2\left(x_k^{(1)}\right)^2 + 2$ et $\rho_k^{(2)} = 0.3\,x_k^{(2)}$, ce qui implique

$$A(\rho_k) = \begin{bmatrix} 0 & 1 \\ \rho_k^{(1)} + \rho_k^{(2)} & 0 \end{bmatrix},\ B = \mathbf{0},\ C = [1\ \ 0] \text{ et } D = \mathbf{0}$$

Cependant, un tel choix ne répond pas aux conditions de la Proposition 1, vu que $x_k^{(2)}$ n'est pas accessible.

2.7.2 Exemple 2

Les systèmes linéaires à commutation admettent également une description (2.4). La seule différence est que l'ensemble Ω_ρ n'est plus un continuum mais un ensemble fini. Considérons la



(a) (b)

FIGURE 2.1 – (a) Attracteur Ω (b) Ensemble Γ_ρ

récurrence chaotique linéaire à commutation donnée par

$$\begin{cases} x_{k+1}^{(1)} = -1.7 \left| x_k^{(1)} \right| + x_k^{(2)} + x_k^{(3)} \\ x_{k+1}^{(2)} = 0.5\ x_k^{(1)} \\ x_{k+1}^{(3)} = x_k^{(3)} \\ y_k = 2\ x_k^{(1)} \end{cases} \tag{2.72}$$

Choisissons ρ_k comme le vecteur de paramètres obéissant à

$$\rho_k = \begin{cases} -1.7 & \text{si} \quad x_k^{(1)} \geq 0 \\ 1.7 & \text{si} \quad x_k^{(1)} < 0 \end{cases}$$

Alors, (2.72) peut être réécrite comme un système de la forme (2.4) avec

$$A(\rho_k) = \begin{bmatrix} \rho_k & 1 & 1 \\ 0.5 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix},\ B = \mathbf{0},\ C = [2 \ \ 0] \text{ et } D = \mathbf{0}$$

Le vecteur ρ_k ne prend ici que les valeurs extrêmes $\rho_{min} = -\ 1.7$ et $\rho_{max} = 1.7$. Le polytope $\mathcal{D}_\rho$ a deux sommets $\rho_{o_1} = \rho_{min} = -\ 1.7$ et $\rho_{o_2} = \rho_{max} = 1.7$, en réalité les deux seuls points de $\mathcal{D}_\rho$ qui sont visités. Un tel choix pour ρ_k répond aux conditions de la Proposition 1. En particulier, ρ_k est accessible à partir de la sortie y_k. En effet,

$$\rho_k = \begin{cases} -1.7 & \text{si} \quad y_k \geq 0 \\ 1.7 & \text{si} \quad y_k < 0 \end{cases}$$

2.7.3 Exemple 3

Considérons le système, avec le vecteur d'état $x_k = [x_k^{(1)} \quad x_k^{(2)} \quad x_k^{(3)} \quad x_k^{(4)}]^T$, donné par

$$\begin{cases} x_{k+1}^{(1)} &= \left(x_k^{(1)}\right)^2 - \left(x_k^{(2)}\right)^2 + ax_k^{(1)} + bx_k^{(2)} \\ x_{k+1}^{(2)} &= 2x_k^{(1)}x_k^{(2)} + cx_k^{(1)} + dx_k^{(2)} \\ x_{k+1}^{(3)} &= 0.1bx_k^{(2)} - 0.1\left(x_k^{(2)}\right)^2 + 0.1x_k^{(3)} \\ x_{k+1}^{(4)} &= 0.5x_k^{(1)} + 0.1x_k^{(2)} + 0.3x_k^{(4)} \\ y_k^{(1)} &= x_k^{(1)} \\ y_k^{(2)} &= x_k^{(2)} \end{cases} \tag{2.73}$$

avec $a = 0.9$, $b = -0.6013$, $c = 2$, et $d = 0.5$. Pour ces valeurs typiques de paramètres, le système présente un comportement chaotique. Une projection de l'attracteur chaotique correspondant dans l'espace de dimension 3 $(x_k^{(1)}, x_k^{(2)}, x_k^{(3)})$ est représentée sur la Figure 2.2.

Notre objectif est de réécrire (2.73) sous la forme LPV (2.4) polytopique (2.7) et de construire

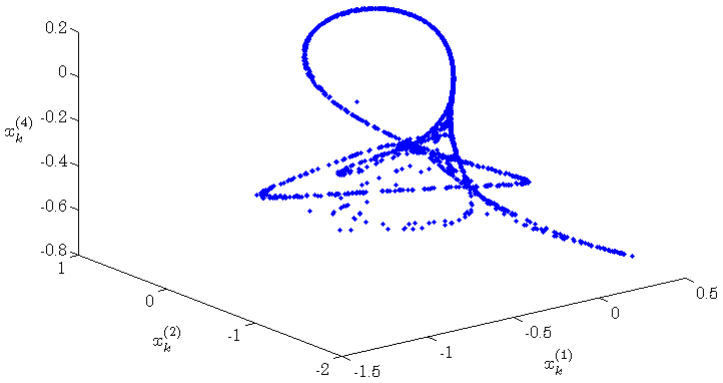


FIGURE 2.2 – Attracteur chaotique Ω dans l'espace de dimension 3 $(x_k^{(1)}, x_k^{(2)}, x_k^{(4)})$

le polytope $\mathcal{D}_\rho$. À cette fin, nous choisissons ρ_k comme le vecteur de paramètres obéissant à

$$\begin{aligned} \rho_k^{(1)} &= a + x_k^{(1)} \\ \rho_k^{(2)} &= b - x_k^{(2)} \end{aligned} \tag{2.74}$$

Alors, (2.73) peut être réécrit comme un système LPV de la forme (2.4) polytopique (2.7) avec

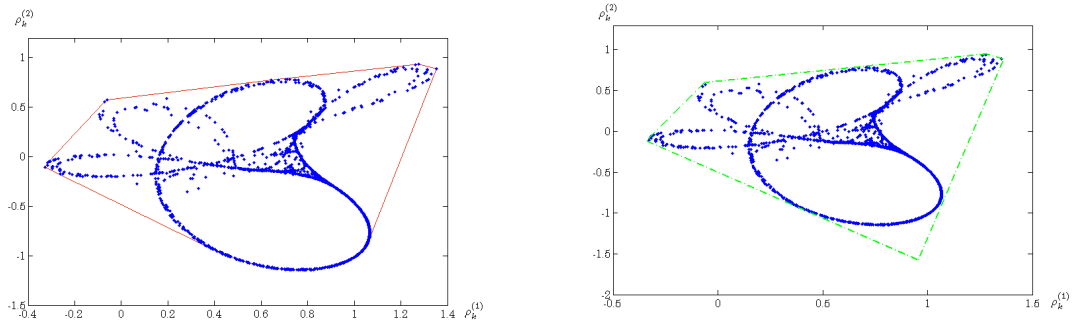
$$A(\rho_k) = \begin{bmatrix} \rho_k^{(1)} & \rho_k^{(2)} & 0 & 0 \\ c & d + 2(\rho_k^{(1)} - a) & 0 & 0 \\ 0 & 0.1\rho_k^{(2)} & 0.1 & 0 \\ 0.5 & 0.1 & 0 & 0.3 \end{bmatrix}$$

et

$$C = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

Les matrices B et D sont nulles puisque le système (2.73) est autonome.
Un tel choix pour ρ_k répond aux conditions de la Proposition 1 fournies dans la Section 2.3. En particulier, ρ_k est accessible à partir de la sortie y_k. En effet, $\rho_k^{(1)} = a + y_k^{(1)}$ et $\rho_k^{(2)} = b - y_k^{(2)}$.

Après simulation de (2.73) à partir de la condition initiale $x_0 = [-0.72 \quad -0.64 \quad 0.1 \quad 0]^T$ qui appartient à l'attracteur chaotique, nous recueillons 2000 vecteurs ρ_k qui constituent l'ensemble des données Γ_ρ. Ensuite, l'approche "Quick hull", correspondant à la fonction *convhull* du logiciel Matlab, est utilisée pour trouver le polytope minimal $\mathcal{D}_\rho^*$ qui englobe les données de Γ_ρ. Il s'avère que 108 sommets ρ_{o_i} ont été trouvés ($N = 108$). Les deux ensembles Ω_ρ et le polytope minimal $\mathcal{D}_\rho^*$ sont représentés sur la Figure 2.3(a). Un autre polytope $\mathcal{D}_\rho$ non minimal peut être choisi comme le montre la Figure 2.3(b). Le nombre des sommets a été réduit à 5 sommets mais le modèle est plus "conservatif".



(a) (b)

FIGURE 2.3 – Ensemble Ω_ρ et polytopes $\mathcal{D}_\rho^*$ (a) et $\mathcal{D}_\rho$ (b)

2.7.4 Exemple 4

Le but de cet exemple est d'illustrer la synthèse et les performances d'un observateur polytopique pour la synchronisation du chaos. La récurrence linéaire à commutation (2.72) introduite dans l'Exemple 2 est considérée. Le vecteur ρ_k prend deux valeurs extrêmes $\rho_{min} = -1.7$ et $\rho_{max} = 1.7$. Les matrices correspondantes $A^{(1)}$ et $A^{(2)}$ sont calculées à partir de (2.11) avec $L = 2$:

$$A^{(1)} = \begin{bmatrix} \rho_{min} & 1 & 1 \\ 0.5 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \text{ et } A^{(2)} = \begin{bmatrix} \rho_{max} & 1 & 1 \\ 0.5 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Les matrices B et D sont nulles puisque le système (2.72) est autonome.

Pour la reconstruction de x_k et donc la synchronisation du chaos, nous avons recours à un observateur polytopique de la forme (2.15). La toolbox *Yalmip* de Matlab est utilisée pour résoudre les LMI (2.19) qui permettent de calculer les gains $L^{(i)}$ de l'observateur.

– **Résultats**

– *Stabilité Poly-Quadratique*

Il s'avère que les LMI (2.19) sont faisables. Les gains qui en résultent sont respectivement $L^{(1)} = [-0.6997 \quad 0.2500 \quad 0.1836]^T$ et $L^{(2)} = [1.0003 \quad 0.2500 \quad 0.1836]^T$. Ensuite, les $\xi_k^{(i)}$ sont calculés à l'aide de l'équation (2.12). Une fois ceux-ci calculés, on procède au calcul du gain variant dans le temps $\mathcal{L}(\rho_k)$ en utilisant (2.16). Ces gains assurent la convergence asymptotique globale de l'observateur. L'état reconstruit $\hat{x}_k$ est calculé grâce à l'observateur polytopique (2.15). Le résultat est illustré sur la Figure 2.4.

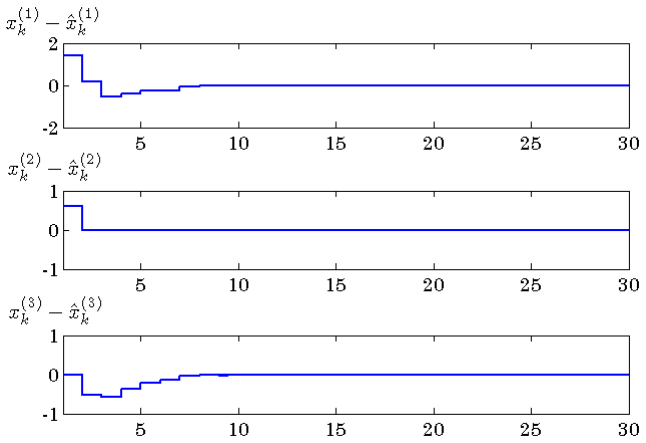


FIGURE 2.4 – Erreur de reconstruction de l'état $x_k - \hat{x}_k$

On considère maintenant le système donné par (2.24) avec

$$E = \begin{bmatrix} 0.5 \\ 0 \\ 0 \end{bmatrix}, \quad H = 0$$

– *Performances dans un contexte stochastique : ISS*

Nous nous intéressons à la résolution du problème (2.35) impliquant les LMI (2.32) afin de minimiser σ_{ev} dans le gain ISS de (2.33). La solution optimale est donnée par $\sigma_{ev}^* = 8.0087$ avec les gains correspondants $L^{(1)} = [-0.4316 \quad 0.2500 \quad 0.4184]^T$ et $L^{(2)} = [1.2684 \quad 0.2500 \quad 0.4184]^T$. Ensuite, afin de minimiser ν dans le gain ISS de (2.38), le problème (2.41) impliquant les LMI (2.36)-(2.37) est résolu pour différentes valeurs de λ appartenant à l'intervalle admissible $]0, 1[$. La variation de la solution optimale ν^* par rapport à λ est illustrée sur la Figure 2.5. Comme nous pouvons le voir, cette variation est convexe. Le meilleur gain ISS correspond à $\nu^* = 5.1973$, $\lambda^* = 0.4123$ et $\mu^* = 5.1940$. Les gains correspondants sont $L^{(1)} = [-0.5351 \quad 0.2500 \quad 0.3149]^T$ et $L^{(2)} = [1.1649 \quad 0.2500 \quad 0.3149]^T$. Comme prévu, on a $\sigma_{ev}^* > \nu^*$ puisque les LMI (2.32) sont plus conservatives que (2.36)-(2.37).

Il peut également être intéressant de comparer les facteurs de décroissance obtenus respectivement à partir de (2.32) et (2.36)-(2.37) pour le même gain ISS. Vérifions d'abord les conditions pour $\nu = \sigma_{ev}^* = 8.0087$, qui est, la valeur optimale de σ_{ev} lorsque (2.32) est considérée. D'une part, le facteur de décroissance est donné par : $\sqrt{1 - \frac{1}{\sigma_{ev}^*}} = 0.9355$. D'autre part, la solution de (2.36)-(2.37) pour $\nu = \sigma_{ev}^* = 8.0087$ donne $\mu^* = 3.3686$ et $\lambda^* = 0.4123$ et donc un facteur de

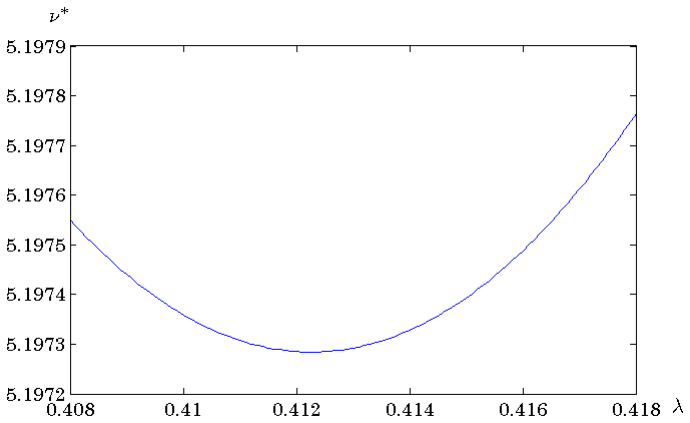


FIGURE 2.5 – Variation de ν^* par rapport à λ

décroissance $\sqrt{1-\lambda^*} = 0.7666$. Les gains correspondants sont $L^{(1)} = [-0.5351 \quad 0.2500 \quad 0.3149]^T$ et $L^{(2)} = [1.1649 \quad 0.2500 \quad 0.3149]^T$. Comme prévu, à cause du conservatisme, pour un même gain ISS, nous pouvons également obtenir un meilleur taux de décroissance lorsqu'on considère les LMI (2.36)-(2.37) au lieu de (2.32).

2.7.5 Exemple 5

Le but de cet exemple d'illustrer la synthèse d'un observateur polytopique pour assurer le déchiffrement pour la technique de chiffrement chaotique par commutation. On rappelle sur la Figure 2.6 le schéma de commutation chaotique. L'émetteur 1 et l'émetteur 2 sont gouvernés par

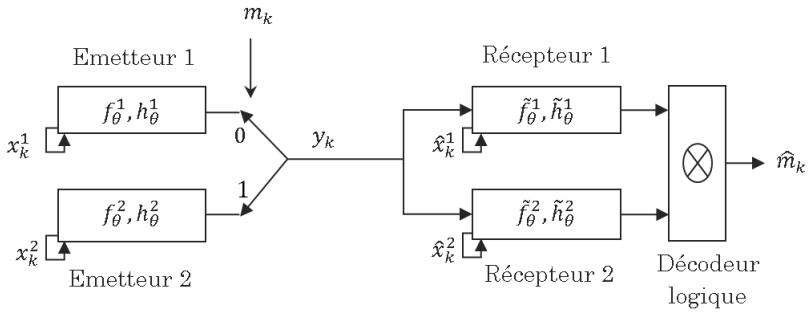


FIGURE 2.6 – Schéma de communication

les systèmes Υ_1 et Υ_2 respectifs

$$\Upsilon_1 \begin{cases} x_{k+1}^{(1,1)} = -1.4\left(x_k^{(1,1)}\right)^2 + x_k^{(2,1)} + x_k^{(3,1)} \\ x_{k+1}^{(2,1)} = 0.3\ x_k^{(1,1)} \\ x_{k+1}^{(3,1)} = x_k^{(3,1)} \\ y_k^1 = 0.4\ x_k^{(1,1)} \end{cases} \tag{2.75}$$

et

$$\Upsilon_2 \begin{cases} x_{k+1}^{(1,2)} = -0.825 x_k^{(1,2)} - 0.296 \left(x_k^{(1,2)}\right)^2 - x_k^{(2,2)} + 1.04 \left(x_k^{(1,2)}\right)^2 x_k^{(2,2)} - 1.04 \left(x_k^{(1,2)}\right)^4 x_k^{(2,2)} \\ x_{k+1}^{(2,2)} = 1.127\ x_k^{(1,2)} \\ y_k^2 = 0.5\ x_k^{(1,2)} \end{cases} \tag{2.76}$$

où x_k représente le vecteur d'état. L'information m_k est une information binaire, et par conséquent, peut prendre uniquement deux valeurs $m_1 = 0$ et $m_2 = 1$. Selon sa valeur courante, la sortie y_k^1 du système Υ_1 ou celle y_k^2 du système Υ_2 est commutée :

$$y_k = \begin{cases} y_k^1 & \text{si} \quad m_k = m_1 \\ y_k^2 & \text{si} \quad m_k = m_2 \end{cases} \tag{2.77}$$

Afin d'utiliser des observateurs polytopiques en tant que récepteur 1 et récepteur 2 pour retrouver m_k, nous devons réécrire (2.75) et (2.76) sous la forme LPV (2.4) polytopique (2.7).

– **Système Υ_1 (2.75) :**
Le paramètre ρ_k^1 est choisi comme suit

$$\rho_k^1 \quad = \quad -1.4\ x_k^{(1,1)} \tag{2.78}$$

Alors, le système (2.75) peut être réécrit comme un système LPV de la forme (2.4) polytopique (2.7) avec

$$A^1(\rho_k^1) = \begin{bmatrix} \rho_k^1 & 1 & 1 \\ 0.3 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad C^1 = \begin{bmatrix} 0.4 & 0 & 0 \end{bmatrix}$$

Les matrices B^1 et D^1 sont nulles puisque le système (2.75) est autonome. Notons qu'un tel choix pour ρ_k^1 répond aux conditions de la Proposition 1 fournies dans la Section 2.3. En particulier, ρ_k^1 est accessible à partir de la sortie y_k^1. En effet, $\rho_k^1 = -3.5 y_k^1$.

Le vecteur ρ_k^1 appartient à l'intervalle $\left[\min(\rho_k^1)\ \max(\rho_k^1)\right]$. Par conséquent, le polytope minimal $\mathcal{D}_{\rho^1}^*$ a 2 sommets $\rho_{o_1}^1$ et $\rho_{o_2}^1$ ($N = 2$) qui correspondent respectivement à $\min(-1.4\ x_k^{(1,1)})$ et $\max(-1.4\ x_k^{(1,1)})$. L'attracteur chaotique Ω^1 est illustré sur la Figure 2.7.

– **Système Υ_2 (2.76) :**
Nous choisissons ρ_k^2 comme le vecteur de paramètres obéissant à

$$\begin{array}{rcl} \rho_k^{(1,2)} & = & -0.825 - 0.296\ x_k^{(1,2)} \\ \rho_k^{(2,2)} & = & -1 + 1.04 \left(x_k^{(1,2)}\right)^2 - 1.04 \left(x_k^{(1,2)}\right)^4 \end{array} \tag{2.79}$$

Alors, le système (2.76) peut être réécrit comme un système LPV de la forme (2.4) polytopique (2.7) avec

$$A^2(\rho_k^2) = \begin{bmatrix} \rho_k^{(1,2)} & \rho_k^{(2,2)} \\ 1.127 & 0 \end{bmatrix}, \quad C^2 = \begin{bmatrix} 0.5 & 0 \end{bmatrix}$$

Les matrices B^2 et D^2 sont nulles puisque le système (2.76) est autonome. Le choix de ρ_k^2 répond aux conditions de la Proposition 1 fournies dans la Section 2.3. En particulier, ρ_k^2 est accessible à

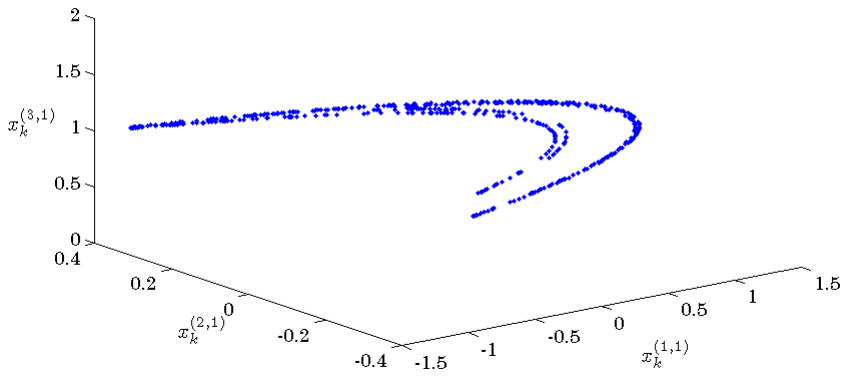
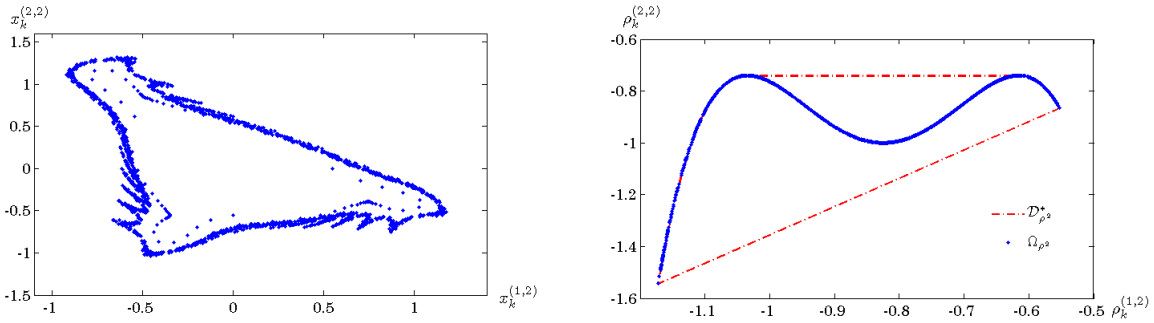


FIGURE 2.7 – Attracteur chaotique Ω^1 de Υ_1

partir de la sortie y_k^2. En effet, $\rho_k^{(1,2)} = -0.825 - 0.592\ y_k^2$ et $\rho_k^{(2,2)} = -1 + 4.16\left(y_k^2\right)^2 - 16.64\left(y_k^2\right)^4$.

Après simulation de (2.76), nous recueillons 500 vecteurs ρ_k^2 qui constituent l'ensemble des données Γ_{ρ^2}. Ensuite, l'approche "Quick hull", correspondant à la fonction *convhull* du logiciel Matlab, est utilisée pour trouver le polytope minimal $\mathcal{D}^*_{\rho^2}$ qui englobe les données de Γ_{ρ^2}. Il s'avère que 121 sommets $\rho^2_{o_i}$ ont été trouvés ($N = 121$). L'attracteur chaotique Ω^2 est illustré sur la Figure 2.8 (a). L'ensemble Ω_{ρ^2} et le polytope minimal $\mathcal{D}^*_{\rho^2}$ sont représentés sur la Figure 2.8 (b).



(a) (b)

FIGURE 2.8 – (a) Attracteur chaotique Ω^2 de Υ_2 (b) Ensemble Ω_{ρ^2} et polytope $\mathcal{D}^*_{\rho^2}$ de Υ_2

Pour la reconstruction de l'information claire m_k, nous avons recours pour le récepteur 1 et récepteur 2 à deux observateurs polytopiques de la forme (2.15) correspondant aux systèmes (2.75) et (2.76), comme il est indiqué sur la Figure 2.6. La toolbox *Yalmip* de Matlab est utilisée pour résoudre les LMI (2.19), nécessaires pour calculer les gains $L_1^{(i)}$ et $L_2^{(i)}$ des deux observateurs respectifs.

– **Résultats**

– *Stabilité Poly-Quadratique*

Il s'avère que les LMI (2.19) sont faisables pour les deux observateurs. Ensuite, les ξ_k^1 et ξ_k^2 sont calculés à l'aide de l'équation (2.12). Une fois ceux-ci calculés, on procède au calcul des deux gains variant dans le temps $\mathcal{L}_1(\rho_k)$ et $\mathcal{L}_2(\rho_k)$ en utilisant (2.16). Ces gains assurent la convergence asymptotique globale des deux observateurs. Les états reconstruits $\hat{x}_k^1$ et $\hat{x}_k^2$ sont calculés grâce à (2.15). Le résultat est illustré sur les Figures 2.9 et 2.10. La Figure 2.9 représente la convergence des erreurs de reconstruction d'état $x_k^{(1,1)} - \hat{x}_k^{(1,1)}$, $x_k^{(2,1)} - \hat{x}_k^{(2,1)}$ et $x_k^{(3,1)} - \hat{x}_k^{(3,1)}$ pour le système Υ_1, et la Figure 2.10 représente la convergence des erreurs de reconstruction d'état $x_k^{(1,2)} - \hat{x}_k^{(1,2)}$ et $x_k^{(2,2)} - \hat{x}_k^{(2,2)}$ pour le système Υ_2.

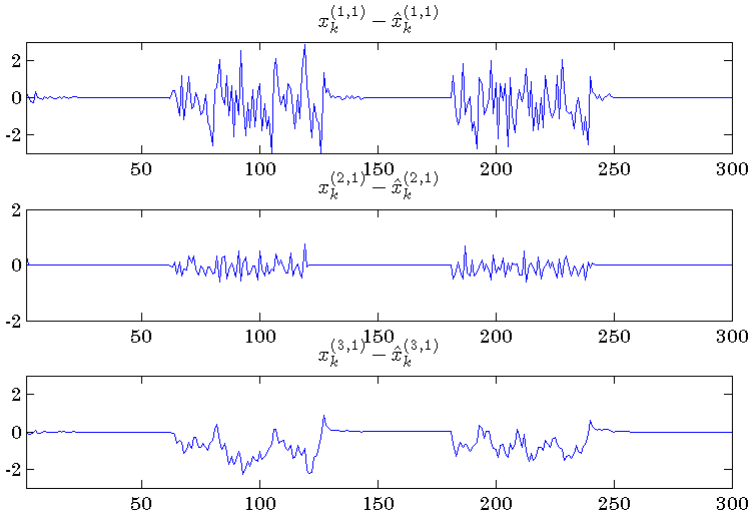


FIGURE 2.9 – Erreur de reconstruction de l'état $x_k^1 - \hat{x}_k^1$ de Υ_1

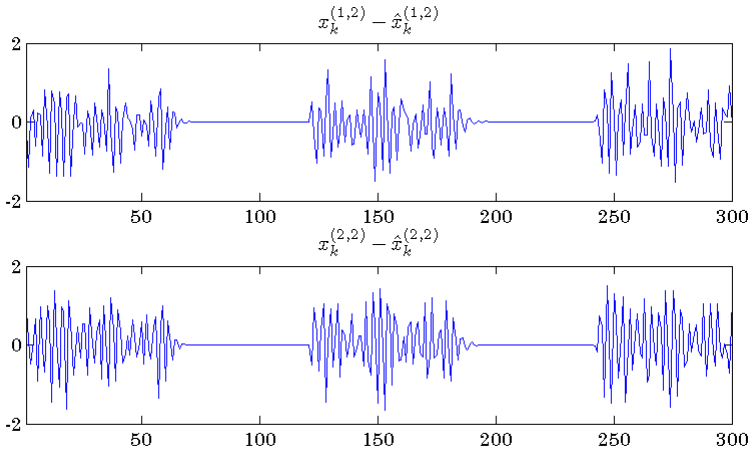


FIGURE 2.10 – Erreur de reconstruction de l'état $x_k^2 - \hat{x}_k^2$ de Υ_2

– *Reconstruction de l'information m_k*

La reconstruction de l'information m_k se fait à travers un décodeur logique. En effet, les erreurs de reconstruction associées à chaque récepteur sont analysées.

$$\hat{m}_k = \begin{cases} 0 \text{ si } x_k^{(1,1)} - \hat{x}_k^{(1,1)} = \mathbf{0} \text{ et } x_k^{(2,1)} - \hat{x}_k^{(2,1)} = \mathbf{0} \text{ et } x_k^{(3,1)} - \hat{x}_k^{(3,1)} = \mathbf{0} \\ 1 \text{ si } x_k^{(1,2)} - \hat{x}_k^{(1,2)} = \mathbf{0} \text{ et } x_k^{(2,2)} - \hat{x}_k^{(2,2)} = \mathbf{0} \end{cases} \tag{2.80}$$

En pratique, on remplace 0 par une tolérance ϵ. La reconstruction de l'information avec une tolérance $\epsilon = 10^{-3}$ est illustrée sur la Figure 2.11.

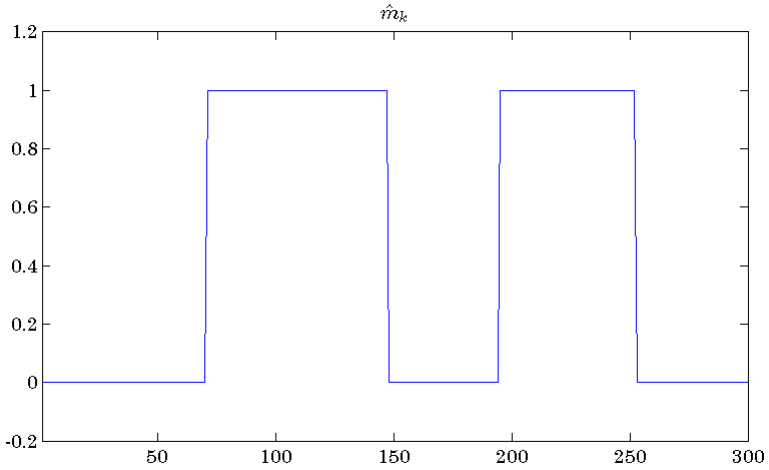


FIGURE 2.11 – Information reconstruite $\hat{m}_k$ pour $\epsilon = 10^{-3}$

2.8 Conclusion

Dans ce chapitre, nous avons rappelé comment un système chaotique à non linéarité polynomiale ou linéaire à commutation pouvait être réécrit sous forme unifiée LPV polytopique. Puis une revue des principaux résultats sur la synthèse d'observateurs LPV polytopiques reposant sur l'utilisation des LMI a été effectuée. On a rappelé le principe de la synthèse garantissant la stabilité, en particulier polyquadratique, dans le contexte non bruité, puis les performances en termes d'ISS, de gain crête-à-crête et de gain $\mathcal{L}_2$ dans le contexte avec perturbation ou incertitude. Une extension des résultats aux observateurs polytopiques à entrées inconnues, à la fois dans le cas déterministe, bruité ou incertain a été proposée. Nous avons finalement illustré l'utilisation des observateurs polytopiques pour de la synchronisation du chaos dans un cas général puis dans le cas du chiffrement de type commutation chaotique. D'autres exemples auraient permis d'illustrer de la même façon la synchronisation du chaos pour le masquage additif, la modulation paramétrique, la transmission à deux canaux et la méthode par inclusion.

Dans certains cas, pour les systèmes de chiffrement chaotiques impliquant des systèmes chaotiques affines à, la dynamique affine active n'est pas connue au niveau du récepteur car dépendant de composantes de l'état qui ne sont pas accessibles ou de l'information non accessible non plus par définition. Dans un tel cas, la synchronisation du chaos nécessite d'abord l'estimation de la dynamique active, qui peut se poser en termes de détection de mode d'un système hybride.

Comme souligné en conclusion du Chapitre 1, le problème de la détection de mode peut également se poser pour la méthode par injection de retard. Pour l'ensemble de ces raisons, il est important de s'intéresser au problème de détection de mode. C'est l'objet du Chapitre 3 qui traitera le problème dans un cadre général (au-delà du contexte du chaos) en se focalisant néanmoins sur la classe des systèmes affines à commutation. Le Chapitre 4 illustrera la détection de mode dans le contexte de chiffrement chaotique.

Chapitre 3

Détection de mode et discernabilité pour les systèmes affines à commutation

Sommaire

3.1 Introduction

On a vu dans les Chapitre 1 et 2 que la détection de modes joue un rôle important dans le contexte des communications chaotiques. Elle permet en effet de synchroniser des systèmes de chiffrement chaotiques impliquant des systèmes chaotiques affines à commutation, où la dynamique affine active n'est pas connue au niveau du récepteur car dépendant de composantes de l'état non accessibles ou de l'information (cas de la modulation paramétrique et commutation chaotique).

Depuis plusieurs décennies, le problème d'estimation de mode pour les systèmes à commutation a reçu beaucoup d'attention, à la fois pour les systèmes à temps discret et continu. Différentes approches et contextes ont été étudiés dans le cas discret. Nous pouvons diviser les méthodes de détection de modes en deux classes différentes : les approches fondées sur les données et les approches fondées sur le modèle. Les approches fondées sur les données sont le plus souvent fondées sur des lots de données et la détection de modes est réalisée conjointement avec l'identification des paramètres de chaque modèle local. Les principales méthodes fondées sur les données sont les approches algébriques [Vidal, 2004], les approches de classification [Ferrari-Trecate et al., 2003], les approches de l'erreur bornée [Bemporad et al., 2005], les approches fondées sur la parcimonie [Bako, 2011] et les approches fondées sur l'ordre du temps [Ohlsson and Ljung, 2013]. Toutes ces méthodes ne sont pas vraiment adaptées pour des applications en ligne telles que le contrôle par rétroaction de sortie ou de type gain scheduling, bien que certaines d'entre elles pourraient être adaptées. D'autre part, les approches fondées sur le modèle supposent que chaque modèle local est connu. Une classe des méthodes fondées sur le modèle considère également des lots de données d'entrée/sortie et la détection de modes ne peut être effectuée en ligne. Nous pouvons citer l'approche proposée dans [Borges et al., 2005] dont le principe repose sur la prise en compte de la dimension de sous-espaces prévus. Elle est un raffinement des travaux similaires fondées sur les sous-espaces proposés dans [Pekpe et al., 2004, Huang et al., 2004]. D'autres méthodes de détection de modes fondées sur les modèles font appel à des techniques à base de filtres. Les filtres visent à la fois la reconstruction de l'état continu et des modes. Ces méthodes sont fondées sur une banque ou un seul observateur asymptotique dont la convergence est conditionnée par un temps de séjour minimum de mode qui entraîne un retard dans la détection [Balluchi et al., 2002] [Jaluski et al., 2002]. Elles sont aussi appelées détection des défauts quand elles sont utilisées dans le diagnostic [Frank, 1990] [Venkatasubramanian et al., 2003b]. Pour détendre le comportement asymptotique de ces détecteurs, les approches fondées sur le modèle avec des horizons glissants, des stratégies ont été proposées. Les techniques à horizon glissant utilisent une quantité limitée d'informations pour l'estimation. Une estimation conjointe de l'état continu et des modes a été proposée dans [Alessandri et al., 2005]. Elle consiste à minimiser un critère impliquant à la fois les quantités estimées, à savoir l'état continu et l'état discret, et les données de sortie en déplaçant un intervalle de temps fini de temps. Enfin, les travaux [Borges et al., 2005] [Babaali and Egerstedt, 2005] [Domlan et al., 2007] sont exclusivement dédiés pour l'estimation des modes, indépendamment de l'estimation de l'état continu. Elles sont appelées dans la littérature consacrée au diagnostic, les approches fondées sur les espaces de parité. La détection de modes est fondée sur des techniques à horizon glissant et convient aux applications en ligne.

Un concept important dans la détection de modes est ce qu'on appelle la "discernabilité". D'une façon générale, la discernabilité reflète la capacité pour un détecteur de mode à discriminer une séquence de toutes les autres séquences. En d'autres termes, elle traite la question d'unicité de la solution délivrée par le détecteur. Une condition suffisante pour assurer la discernabilité

est l'observabilité [Vidal et al., 2002]. Cependant, des conditions moins restrictives peuvent être trouvées dans la littérature comme la discernabilité arrière (Backward Discernibility (BD)), la discernabilité avant (Forward Discernibility (FD)) [Babaali and Egerstedt, 2005] et la (η, ω)–discernabilité [Alessandri et al., 2005]. Pour les systèmes avec entrée, la discernabilité mérite un traitement spécial parce qu'elle dépend de la séquence d'entrée. À cet égard, l'"observation de mode actif" a été discutée dans [Babaali and Egerstedt, 2004], [Baglietto et al., 2007] et [Baglietto et al., 2009] où une distinction entre les séquences de contrôle discernables sur un horizon de temps fini ou infini est faite.

Malgré l'effervescence importante en ce qui concerne le problème de détection de modes fondée sur le modèle pour les systèmes à commutation, une vue unifiée des différentes méthodologies existantes et des concepts associés, en particulier la discernabilité, est manquante. L'objectif de ce chapitre est précisément d'y pallier. Des extensions de résultats seront également proposées. L'étude est faite dans un cadre général. Le Chapitre 4 sera consacré à l'application de la détection de modes pour le chiffrement chaotique.

Le plan de ce chapitre est le suivant. Dans la Section 3.2, une présentation unifiée des principales méthodes de détection de modes fondées sur des espaces de parité, qui s'appliquent pour les systèmes linéaires et affines à commutation, avec les structures de détecteurs de mode correspondantes, est effectuée. Dans la section 3.3, une étude comparative est réalisée. Le problème d'unicité de détection de modes est discuté dans la Section 3.4 à travers la notion de discernabilité. Une telle notion est centrale puisqu'elle garantit l'unicité de la solution délivrée par les détecteurs de mode. La section 3.5 est consacrée à des notions avancées de discernabilité et leur considération est motivée. La section 3.6 traite de la discernabilité arrière, une notion qui permet de réduire le coût de calcul de la détection de mode. Une procédure étape par étape complète est proposée dans la Section 3.7 et prend en considération l'initialisation et l'estimation permanente. Quelques exemples illustratifs sont introduits dans la Section 3.8.

3.2 Méthodes de détection de modes fondées sur le modèle

3.2.1 Préliminaires et positionnement du problème

Nous considérons le système affine à commutation à temps discret donné par

$$\begin{cases} x_{k+1} = A_{\sigma(k)}x_k + B_{\sigma(k)}u_k + E_{\sigma(k)} \\ y_k = C_{\sigma(k)}x_k + D_{\sigma(k)}u_k \end{cases} \tag{3.1}$$

où $k \in \mathbb{N}$ représente le temps discret, $x_k \in \mathbb{R}^n$ est le vecteur d'état, $y_k \in \mathbb{R}^m$ est la sortie, $u_k \in \mathbb{R}^p$ est l'entrée. La fonction σ est la loi de commutation définie par $\sigma : \mathbb{N} \to \mathcal{J} = \{1, \ldots, J\}$ qui attribue, à tout temps discret $k \in \mathbb{N}$, l'entier $\sigma(k) \in \mathcal{J}$. Les matrices $A_{\sigma(k)} \in \mathbb{R}^{n\times n}$, $B_{\sigma(k)} \in \mathbb{R}^{n\times p}$, $C_{\sigma(k)} \in \mathbb{R}^{m\times n}$, $D_{\sigma(k)} \in \mathbb{R}^{m\times p}$ et $E_{\sigma(k)} \in \mathbb{R}^{n\times 1}$ sont les matrices de l'espace d'état du système qui appartiennent aux ensembles respectifs $\{A_1, \ldots, A_J\}$, $\{B_1, \ldots, B_J\}$, $\{C_1, \ldots, C_J\}$, $\{D_1, \ldots, D_J\}$ et $\{E_1, \ldots, E_J\}$. Ci-après, $\sigma_{[k_1,k_2]}$ traduira la séquence finie de modes (également appelée "chemin" ou "path") $\sigma(k_1), \cdots, \sigma(k_2)$ dans l'intervalle de temps $[k_1, k_2]$. Une séquence active sera notée σ^*.

L'équation suivante obtenue en empilant les sorties successives y_k dans l'intervalle de temps

$[k-h,k]$ est centrale pour la suite.

$$y_{k-h,k} = \mathcal{O}_{\sigma_{[k-h,k]}} x_{k-h} + T_{\sigma_{[k-h,k]}} u_{k-h,k} + T'_{\sigma_{[k-h,k]}} \tag{3.2}$$

où

$$\mathcal{O}_{\sigma_{[k-h,k]}} = \begin{bmatrix} C_{\sigma(k-h)} \\ C_{\sigma(k-h+1)}A_{\sigma(k-h)} \\ \vdots \\ C_{\sigma(k-1)}A^{\sigma(k-h)}_{\sigma(k-2)} \\ C_{\sigma(k)}A^{\sigma(k-h)}_{\sigma(k-1)} \end{bmatrix} \tag{3.3}$$

$$T_{\sigma_{[k-h,k]}} = \begin{bmatrix} D_{\sigma(k-h)} & \mathbf{0} & \mathbf{0} \\ C_{\sigma(k-h+1)}B_{\sigma(k-h)} & D_{\sigma(k-h+1)} & \mathbf{0} \\ \vdots & \ddots & \vdots \\ C_{\sigma(k-1)}B^{\sigma(k-h)}_{\sigma(k-2)} & D_{\sigma(k-1)} & \mathbf{0} \\ C_{\sigma(k)}B^{\sigma(k-h)}_{\sigma(k-1)} & & D_{\sigma(k)} \end{bmatrix}$$

$$T'_{\sigma_{[k-h,k]}} = \begin{bmatrix} \mathbf{0} \\ C_{\sigma(k-h+1)}E_{\sigma(k-h)} \\ \vdots \\ C_{\sigma(k-1)}E^{\sigma(k-h)}_{\sigma(k-2)} \\ C_{\sigma(k)}E^{\sigma(k-h)}_{\sigma(k-1)} \end{bmatrix}$$

et

$$A^{k_2}_{k_1} = A_{k_1}A_{k_1+1}\cdots A_{k_2}$$

$$B^{k_2}_{k_1} = \begin{bmatrix} A^{k_2-1}_{k_1}B_{k_2} & \cdots & A^{k_1+1}_{k_1}B_{k_1+2} & A_{k_1}B_{k_1+1} & B_{k_1} \end{bmatrix}$$

$$E^{k_2}_{k_1} = A^{k_2-1}_{k_1}E_{k_2} + \cdots + A^{k_1+1}_{k_1}E_{k_1+2} + A_{k_1}E_{k_1+1} + E_{k_1}$$

$$y_{k_1,k_2} = \begin{bmatrix} y_{k_1} \\ y_{k_1+1} \\ \vdots \\ y_{k_2} \end{bmatrix}, \quad u_{k_1,k_2} = \begin{bmatrix} u_{k_1} \\ u_{k_1+1} \\ \vdots \\ u_{k_2} \end{bmatrix}$$

$\mathcal{O}_{\sigma_{[k-h,k]}}$ est la matrice d'observabilité dans la fenêtre d'observation finie $[k-h,k]$. Nous notons $\mathcal{S}$ l'ensemble des entiers $s \in \mathcal{S}$ qui permettent d'identifier, d'une manière unique, une séquence $\sigma_s \in \mathcal{J}^{h+1}$ dans l'intervalle de temps $[k-h,k]$ et $S \leq J^{h+1}$ le nombre de séquences admissibles dans $\mathcal{J}^{h+1}$. Par séquence admissible, on entend une séquence pour laquelle $\sigma(k+1)$ est compatible avec $\sigma(k)$ et la règle de transition définie par la fonction de commutation σ.

Étant donné les séquences d'Entrée/Sortie u_k et y_k sur un horizon glissant de longueur finie, nous nous intéresserons à la reconstruction de mode, c'est à dire de $\sigma(k)$. La question d'unicité de la solution délivrée par les détecteurs ainsi que la détermination d'une valeur appropriée pour h seront discutées dans la Section 3.3.

3.2.2 Détections de mode

Dans cette section, nous examinons, d'une manière unifiée, les principales méthodes de détection de modes fondées sur le modèle qui s'appliquent pour les systèmes affines à commutation et qui sont exclusivement dédiées à la détection de modes, contrairement à celles fondées sur l'estimation simultanée de l'état et du mode. Notons tout d'abord que les méthodes sont généralement présentées dans la littérature pour les systèmes linéaires à commutation mais, puisqu'elles peuvent être étendues aux systèmes linéaires affines à commutation d'une manière simple, c'est l'option que nous avons choisie pour ce chapitre. Soulignons que, en raison de leur structure, il s'avère que les détecteurs ne fournissent pas exclusivement le mode actif $\sigma^*(k)$ à l'instant k mais fournissent la totalité ou une partie de la séquence active σ^* dans l'intervalle du temps $[k-h, k]$. La façon avec laquelle le mode $\sigma(k)$ peut être délivré de la séquence active sera discutée plus tard dans ce chapitre.

3.2.2.1 Détection 1

On s'intéresse à la détection de modes qui a été proposée dans [Babaali and Egerstedt, 2005]. Le détecteur correspondant est fondé sur le fait qu'une séquence active σ^* vérifie

$$\sigma^* = \left\{ \sigma_s \in \mathcal{J}^{h+1} \;\; | \, y_{k-h,k} - T_{\sigma_s} u_{k-h,k} - T'_{\sigma_s} \in \mathcal{R}(\mathcal{O}_{\sigma_s}) \right\} \tag{3.4}$$

où $\mathcal{R}(\mathcal{O}_{\sigma_s})$ est l'ensemble image engendré par les colonnes de $\mathcal{O}_{\sigma_s}$.
Le lemme suivant sera utile pour la suite.

Lemme 1 *[Babaali and Egerstedt, 2005] Étant donné un vecteur Y' et une matrice $\mathcal{O}$, X étant inconnu, il s'avère que*

$$Y' \in \mathcal{R}(\mathcal{O}) \Leftrightarrow \exists X \, | \, Y' = \mathcal{O}X \Leftrightarrow (\mathcal{O}\mathcal{O}^\dagger - \boldsymbol{1})Y' = \boldsymbol{0} \tag{3.5}$$

Nous définissons une grandeur, appelée résidu,

$$r^1_{h,\sigma_s} = (\mathcal{O}_{\sigma_s}\mathcal{O}^\dagger_{\sigma_s} - \mathbf{1})(y_{k-h,k} - T_{\sigma_s} u_{k-h,k} - T'_{\sigma_s}) \tag{3.6}$$

On a alors la proposition suivante.

Proposition 2 *La séquence active σ^* dans l'intervalle de temps $[k-h, k]$ est une séquence $\sigma_s \in \mathcal{J}^{h+1}$ $(s \in \mathcal{S})$ telle que le résidu correspondant vérifie*

$$r^1_{h,\sigma_s} = \boldsymbol{0} \tag{3.7}$$

Preuve 8 *La preuve est une conséquence directe du Lemme 1, en remplaçant Y' par $y_{k-h,k} - T_{\sigma_s} u_{k-h,k} - T'_{\sigma_s}$ et $\mathcal{O}$ par $\mathcal{O}_{\sigma_s}$ dans* (3.5) *et en considérant* (3.4).

3.2.2.2 Détection 2

On s'intéresse maintenant à la détection de modes qui a été proposée dans [Domlan et al., 2007]. Pour une telle détection de modes, on suppose que le système est "PWO" (PathWise Observable), une notion introduite d'abord dans [Babaali and Egerstedt, 2003].

Définition 10 *([Babaali and Egerstedt, 2003]) Le système (3.1) est PathWise Observable s'il existe un entier h tel que chaque séquence $\sigma_s \in \mathcal{J}^{h+1}$ $(s \in \mathcal{S})$ de longueur $h+1$ est observable, i.e. satisfait $rang(\mathcal{O}_{\sigma_s}) = n$. Le plus petit entier h est appelé "indice de la PWO".*

En supposant que le système (3.1) est PWO, il existe une matrice non nulle, dite de projection, vérifiant

$$\Omega_{\sigma_s}\mathcal{O}_{\sigma_s} = \mathbf{0} \tag{3.8}$$

La matrice Ω_{σ_s} correspond au noyau à gauche de $\mathcal{O}_{\sigma_s}$. Soit le résidu défini par

$$r^2_{h,\sigma_s} = \Omega_{\sigma_s}(y_{k-h,k} - T_{\sigma_s}u_{k-h,k} - T'_{\sigma_s}) \tag{3.9}$$

La multiplication à gauche de l'équation (3.2) par Ω_{σ_s} et la considération de (3.8) conduisent à la proposition suivante énoncée dans [Domlan et al., 2007].

Proposition 3 *[Domlan et al., 2007] La séquence active σ^* dans l'intervalle de temps $[k-h, k]$ est une séquence $\sigma_s \in \mathcal{J}^{h+1}$ $(s \in \mathcal{S})$ telle que le résidu correspondant vérifie*

$$r^2_{h,\sigma_s} = \boldsymbol{0} \tag{3.10}$$

Remarque 5 *Si l'entrée u_k est inconnue, l'estimation du mode pour un système SO (Single Output) ne peut pas être effectuée ainsi car la détection nécessite la connaissance du modèle et des données entrées sorties u_k et y_k. Cependant, pour les systèmes MO (Multiple output), l'estimation peut être effectuée si on parvient à obtenir une équation ayant la forme*

$$Y_{\sigma_s} = \mathcal{Q}_{\sigma_s}x_{k-h} + \mathcal{F}_{\sigma_s} \tag{3.11}$$

où Y_{σ_s} contient des combinaisons linéaires de composantes de vecteur de sortie y_k. Ensuite, la détection 1 ou 2 peut être utilisée en remplaçant $y_{k-h,k} - T_{\sigma_s}u_{k-h,k} - T'_{\sigma_s}$ par $Y_{\sigma_s} - \mathcal{F}_{\sigma_s}$ et $\mathcal{O}_{\sigma_s}$ par $\mathcal{Q}_{\sigma_s}$. Ceci est illustré dans l'exemple numérique suivant.
Considérons le système SIMO donné par

$$\begin{cases} x_{k+1} = A_{\sigma(k)}x_k + B_{\sigma(k)}u_k \\ y_k = Cx_k \end{cases} \tag{3.12}$$

où $\sigma(k) \in \{1, 2\}$ et $A_1 = \boldsymbol{1}_3$, $A_2 = 2\ \boldsymbol{1}_3$, $B_1 = B_2 = \begin{bmatrix} 1 \\ 2 \\ 0 \end{bmatrix}$, $C = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{bmatrix}$.

Pour la séquence $\sigma_s = 111$, les égalités suivantes sont vérifiées.

$$\begin{aligned} y_{k-2} &= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{bmatrix} x_{k-2} \\ y_{k-1} &= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{bmatrix} x_{k-1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{bmatrix} x_{k-2} + \begin{bmatrix} 1 \\ 4 \end{bmatrix} u_{k-2} \\ 4\ y^{(1)}_{k-1} - y^{(2)}_{k-1} &= \begin{bmatrix} 4 & -2 & 0 \end{bmatrix} x_{k-2} \\ y_k &= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{bmatrix} x_k = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{bmatrix} x_{k-2} + \begin{bmatrix} 1 \\ 4 \end{bmatrix} u_{k-2} + \begin{bmatrix} 1 \\ 4 \end{bmatrix} u_{k-1} \\ 4\ y^{(1)}_k - y^{(2)}_k &= \begin{bmatrix} 4 & -2 & 0 \end{bmatrix} x_{k-2} \end{aligned}$$

Pour obtenir l'équation (3.11), nous considérons le vecteur Y_{σ_s} donné par

$$Y_{\sigma_s} = \begin{bmatrix} y_{k-2} \\ 4\ y^{(1)}_{k-1} - y^{(2)}_{k-1} \\ 4\ y^{(1)}_k - y^{(2)}_k \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 4 & -2 & 0 \\ 4 & -2 & 0 \end{bmatrix} x_{k-2}$$

qui est bien de la forme (3.11) pour $\sigma_s = 111$. Cette démarche doit être effectuée pour chaque séquence de modes $\sigma_s \in \mathcal{J}^{h+1}$ $(s \in \mathcal{S})$ afin d'obtenir des équations indépendantes de l'entrée inconnue.

3.2.2.3 Détection 3

Indépendamment du problème de détection de modes, une condition nécessaire et suffisante pour obtenir une écriture Entrée/Sortie équivalente, appelée représentation SARX, pour les modèles d'espace d'état affines à commutation a été proposée dans [Paoletti et al., 2008]. Il se trouve qu'une nouvelle détection de modes peut être dérivée de ce travail. C'est le but de ce qui suit. Avant d'aller plus loin, rappelons d'abord le résultat central établi dans [Paoletti et al., 2008]. Notons qu'il est repris ici avec les notations de ce chapitre.

Théorème 12 *[Paoletti et al., 2008] Le système (3.1) admet une représentation SARX équivalente, si et seulement si, pour chaque séquence de modes $\sigma_s \in \mathcal{J}^{h+1}$ $(s \in \mathcal{S})$, il existe un entier $h \in I\!N$ et une matrice $\Xi_s^{(1)}$ vérifiant*

$$\Xi_s^{(1)} \mathcal{O}_{\sigma_{[k-h,k-1]}} = C_{\sigma(k)} A_{\sigma(k-1)}^{\sigma(k-h)} \tag{3.13}$$

Corollaire 1 *[Paoletti et al., 2008] Lorsque le Théorème 12 est vérifié, le modèle SARX s'écrit*

$$y_k = \Xi_s \; v_k \tag{3.14}$$

avec

$$v_k = \begin{bmatrix} y_{k-h,k-1}^T & u_{k-h,k}^T & \mathbf{1} \end{bmatrix}^T$$

et

$$\Xi_s = \begin{bmatrix} \Xi_s^{(1)} & \Xi_s^{(2)} & \Xi_s^{(3)} \end{bmatrix}$$

où

- $\Xi_s^{(1)}$ *est la solution de (3.13),*
- $\Xi_s^{(2)} = \begin{bmatrix} C_{\sigma(k)} B_{\sigma(k-1)}^{\sigma(k-h)} & D_{\sigma(k)} \end{bmatrix} - \Xi_s^{(1)} T_{\sigma_{[k-h,k-1]}}$,
- $\Xi_s^{(3)} = \begin{bmatrix} C_{\sigma(k)} E_{\sigma(k-1)}^{\sigma(k-h)} \end{bmatrix} - \Xi_s^{(1)} T'_{\sigma_{[k-h,k-1]}}$.

À partir de ces résultats, la détection de modes obéit à la proposition suivante.

Proposition 4 *Lorsque le Théorème 12 est vérifié, la séquence active σ^* dans l'intervalle de temps $[k-h,k]$ est une séquence $\sigma_s \in \mathcal{J}^{h+1}$ $(s \in \mathcal{S})$ telle que le résidu correspondant vérifie*

$$r_{h,\sigma_s}^3 = \mathbf{0} \tag{3.15}$$

avec

$$r_{h,\sigma_s}^3 = \begin{bmatrix} H_s & \mathbf{1} \end{bmatrix} (y_{k-h,k} - T_{\sigma_{[k-h,k]}} u_{k-h,k} - T'_{\sigma_{[k-h,k]}}) \tag{3.16}$$

où

$$H_s = -(C_{\sigma(k)} A_{\sigma(k-1)}^{\sigma(k-h)} \mathcal{O}_{\sigma_{[k-h,k]}}^{\dagger} + Q_\sigma^T (\mathbf{1} - \mathcal{O}_{\sigma_{[k-h,k]}} \mathcal{O}_{\sigma_{[k-h,k]}}^{\dagger})) \tag{3.17}$$

et Q_σ une matrice arbitraire.

Preuve 9 *Lorsque le Théorème 12 est vérifié, l'équation (3.13) admet une solution explicite qui vérifie*

$$\Xi_s^{(1)} = C_{\sigma(k)} A_{\sigma(k-1)}^{\sigma(k-h)} \mathcal{O}_{\sigma_{[k-h,k]}}^{\dagger} + Q_\sigma^T (\mathbf{1} - \mathcal{O}_{\sigma_{[k-h,k]}} \mathcal{O}_{\sigma_{[k-h,k]}}^{\dagger}) \tag{3.18}$$

avec Q_σ une matrice arbitraire.
Par ailleurs, selon le Corollaire 1, la différence $y_k - \Xi_{\sigma_s} v_k = \mathbf{0}$ et satisfait les égalités successives suivantes.

$$
\begin{aligned}
y_k - \Xi_s v_k = \; & \mathbf{0} \\
= \; & y_k - \begin{bmatrix} \Xi_s^{(1)} & \Xi_s^{(2)} & \Xi_s^{(3)} \end{bmatrix} \begin{bmatrix} y_{k-h,k-1} \\ u_{k-h,k} \\ \mathbf{1} \end{bmatrix} \\
= \; & y_k - \Xi_s^{(1)} y_{k-h,k-1} - \Xi_s^{(2)} u_{k-h,k} - \Xi_s^{(3)} \\
= \; & \begin{bmatrix} -\Xi_s^{(1)} & \mathbf{1} \end{bmatrix} \begin{bmatrix} y_{k-h,k-1} \\ y_k \end{bmatrix} - (\begin{bmatrix} C_{\sigma(k)} B_{\sigma(k-1)}^{\sigma(k-h)} & D_{\sigma(k)} \end{bmatrix} - \Xi_s^{(1)} T_{\sigma_{[k-h,k-1]}}) u_{k-h,k} \\
& - (\begin{bmatrix} C_{\sigma(k)} E_{\sigma(k-1)}^{\sigma(k-h)} \end{bmatrix} - \Xi_s^{(1)} T'_{\sigma_{[k-h,k-1]}}) \\
= \; & \begin{bmatrix} -\Xi_s^{(1)} & \mathbf{1} \end{bmatrix} y_{k-h,k} - \begin{bmatrix} -\Xi_s^{(1)} & \mathbf{1} \end{bmatrix} \begin{bmatrix} T_{\sigma_{[k-h,k-1]}} \\ C_{\sigma(k)} B_{\sigma(k-1)}^{\sigma(k-h)} \quad D_{\sigma(k)} \end{bmatrix} u_{k-h,k} \\
& - \begin{bmatrix} -\Xi_s^{(1)} & \mathbf{1} \end{bmatrix} \begin{bmatrix} T'_{\sigma_{[k-h,k-1]}} \\ C_{\sigma(k)} E_{\sigma(k-1)}^{\sigma(k-h)} \end{bmatrix} \\
= \; & \begin{bmatrix} H_s & \mathbf{1} \end{bmatrix} (y_{k-h,k} - T_{\sigma_{[k-h,k]}} u_{k-h,k} - T'_{\sigma_{[k-h,k]}})
\end{aligned}
$$

Par conséquent, $H_s = -\Xi_s^{(1)}$. Pour $\sigma_s = \sigma^*$, on trouve que

$$r_{h,\sigma^*}^3 = \mathbf{0}$$

ce qui achève la démonstration.

3.3 Étude comparative

Cette section a pour objectif de comparer les différentes détections de mode susmentionnées.

3.3.1 Comparaison de la structure des détecteurs de mode

Les détecteurs présentés en Section 3.2.2 peuvent être écrits d'une manière unifiée, et nous avons la proposition suivante.

Proposition 5 *La séquence active σ^* dans l'intervalle de temps $[k-h, k]$ est une séquence $\sigma_s \in \mathcal{J}^{h+1}$ $(s \in \mathcal{S})$ telle que le résidu correspondant vérifie*

$$r_{h,\sigma_s} = \mathbf{0} \tag{3.19}$$

avec

$$r_{h,\sigma_s} = \Lambda_{\sigma_s}(y_{k-h,k} - T_{\sigma_s} u_{k-h,k} - T'_{\sigma_s}) \tag{3.20}$$

où

- $\Lambda_{\sigma_s} = (\mathcal{O}_{\sigma_s} \mathcal{O}_{\sigma_s}^\dagger - \mathbf{1})$ *pour le détecteur 1*
- $\Lambda_{\sigma_s} = \Omega_{\sigma_s}$ *pour le détecteur 2*
- $\Lambda_{\sigma_s} = \begin{bmatrix} H_s & \mathbf{1} \end{bmatrix}$ *pour le détecteur 3*

avec $\mathcal{O}_{\sigma_s}$ définie par (3.3), *Ω_{σ_s} la solution de* (3.8) *et H_s définie par* (3.17).

Preuve 10 *Voir respectivement* (3.6) (3.9) *et* (3.16).

Malgré cette similitude de structure, des distinctions importantes doivent être soulignées. C'est l'objet du paragraphe suivant.

3.3.2 Comparaison de la taille de l'horizon de détection

Il se trouve que la résolution de l'équation (3.19) peut conduire à plusieurs solutions $\sigma_s \in \mathcal{J}^{h+1}$ ($s \in \mathcal{S}$) et σ^* correspond à une solution spécifique. L'unicité de la solution dépend de la matrice Λ_{σ_s}, qui à son tour, dépend de h. Par exemple, supposons que $\Lambda_{\sigma_s} = \mathbf{0}$. Dans un tel cas, la condition (3.19) est toujours satisfaite et donc, n'importe quelle séquence σ_s annule le résidu r_{h,σ_s}. Par conséquent, il est clair que $\Lambda_{\sigma_s} = \mathbf{0}$ n'est pas satisfaisante et correspond au pire de cas. Ceci étant, par la suite, on va chercher une exigence minimale de la taille de l'horizon de détection afin de garantir l'existence d'une matrice non nulle Λ_{σ_s}. Notons que pour le détecteur 3, la non nullité est garantie par construction. Les conditions garantissant l'unicité de la solution délivrée par les détecteurs fera l'objet de la Section 3.4.

3.3.2.1 Détecteur 1

Le théorème énoncé dans [Barata and Hussein, 2012] sera utile dans la suite et il est rappelé ci-dessous.

Théorème 13 *[Barata and Hussein, 2012] Pour toute matrice X, il s'avère que*

$$ker(X) = \mathcal{R}(\mathbf{1} - X^{\dagger}X) \tag{3.21}$$

Proposition 6 *Pour le détecteur 1, la limite inférieure de l'horizon de détection est le plus petit entier h qui vérifie*

$$h > rang(\mathcal{O}_{\sigma_s}) - 1 \tag{3.22}$$

Preuve 11 *Pour le détecteur 1, $\Lambda_{\sigma_s} = (\mathcal{O}_{\sigma_s}\mathcal{O}^{\dagger}_{\sigma_s} - \mathbf{1})$. La limite inférieure de h doit garantir que $(\mathcal{O}_{\sigma_s}\mathcal{O}^{\dagger}_{\sigma_s} - \mathbf{1})$ ne se réduit pas à la matrice nulle pour tout $s \in \mathcal{S}$, ce qui est équivalent à vérifier que $ker(\mathcal{O}_{\sigma_s})$ n'est pas nulle d'après le Théorème 13. C'est précisément ce que l'inégalité* (3.22) *assure.*

3.3.2.2 Détecteur 2

Proposition 7 *Pour le détecteur 2, la limite inférieure de l'horizon de détection h est la dimension du système, qui est le plus petit entier tel que*

$$h > n - 1 \tag{3.23}$$

Preuve 12 *Pour le détecteur 2, puisque $\Lambda_{\sigma_s} = ker(\mathcal{O}_{\sigma_s})$, la limite inférieure de h doit garantir que $ker(\mathcal{O}_{\sigma_s})$ ne se réduit pas à la matrice nulle pour tout $s \in \mathcal{S}$. C'est précisément ce que l'inégalité* (3.23) *assure, en substituant $rang(\mathcal{O}_{\sigma_s})$ par n dans* (3.22), *puisqu'il est supposé que la PWO est vérifiée, ce qui est équivalent à $rang(\mathcal{O}_{\sigma_s}) = n$.*

3.3.2.3 Détecteur 3

Contrairement aux détecteurs 1 et 2, l'existence de Λ_{σ_s} n'est pas toujours garantie puisque (3.13) doit être vérifiée. D'autre part, si (3.13) est vérifiée, Λ_{σ_s} n'est pas nulle par construction. Le but de cette section est de réécrire (3.13) en termes d'exigence minimale que h doit vérifier pour s'assurer de l'existence de Λ_{σ_s}.
Tout d'abord, le lemme standard suivant est rappelé.

Lemme 2 *Pour deux matrices W et Z, l'équation $WX = Z$, avec X inconnue, admet une solution si et seulement si $rang\,([W \;\; Z]) = rang(W)$ ($[W \;\; Z]$ représente la concaténation horizontale des matrices W et Z).*

On a la proposition suivante.

Proposition 8 *Pour le détecteur 3, la limite inférieure de l'horizon de détection est le plus petit entier h qui vérifie*

$$rang(\mathcal{O}_{\sigma_{[k-h,k]}}) = rang(\mathcal{O}_{\sigma_{[k-h,k-1]}}) \tag{3.24}$$

Preuve 13 *En se basant sur le Lemme 2, avec $X = {\Xi_s^{(1)}}^T$, $W = {\mathcal{O}_{\sigma_{[k-h,k-1]}}}^T$ et $Z = (C_{\sigma(k)} A_{\sigma(k-1)}^{\sigma(k-h)})^T$, tester si (3.13) a une solution est équivalent à vérifier la condition de rang suivante*

$$rang(\begin{bmatrix} {\mathcal{O}_{\sigma_{[k-h,k-1]}}}^T & (C_{\sigma(k)} A_{\sigma(k-1)}^{\sigma(k-h)})^T \end{bmatrix}) = rang({\mathcal{O}_{\sigma_{[k-h,k-1]}}}^T)$$

ce qui est équivalent à

$$rang(\begin{bmatrix} \mathcal{O}_{\sigma_{[k-h,k-1]}} \\ C_{\sigma(k)} A_{\sigma(k-1)}^{\sigma(k-h)} \end{bmatrix}) = rang(\mathcal{O}_{\sigma_{[k-h,k-1]}})$$

qui est finalement équivalent à (3.24). *La limite inférieure de h vérifiant* (3.24) *garantit l'existence de Λ_{σ_s}, et par construction, si tel est le cas, $\begin{bmatrix} H_s & \mathbf{1} \end{bmatrix}$ ne se réduit pas à la matrice nulle pour tout $s \in \mathcal{S}$.*

En d'autres termes, la limite inférieure de l'horizon de détection doit être choisie de telle sorte que le rang des matrices d'observabilité reste fixe considérant deux horizons de longueur successive h et $h+1$.

Remarque 6 *La limite inférieure h donnée dans [Domlan et al., 2007] pour le détecteur 2 et correspondant à la PWO, à savoir $rang(\mathcal{O}_{\sigma_{[k-h,k]}}) = n$, est restrictive et est un cas particulier de* (3.24) *puisque* (3.24) *admet $h < n$ comme solution.*

3.3.3 Comparaison des détecteur 2 et détecteur 1

Proposition 9 *Pour une même taille de l'horizon h compatible avec* (3.22) *et* (3.23), *le détecteur 2 est équivalent au détecteur 1.*

Preuve 14 *Tenant compte du fait que $\Lambda_{\sigma_s} = (\mathcal{O}_{\sigma_s} \mathcal{O}_{\sigma_s}^{\dagger} - \mathbf{1})$ pour le détecteur 1 et $\Lambda_{\sigma_s} = \Omega_{\sigma_s}$ pour le détecteur 2, il s'agit d'une conséquence directe du Théorème 13.*

3.3.4 Comparaison des détecteur 3 et détecteur 2

Proposition 10 *Pour une même taille de l'horizon h compatible avec* (3.23) *et* (3.24)*, le détecteur 3 est un cas particulier du détecteur 2.*

Preuve 15 *Selon la Proposition 5,* $\Lambda_{\sigma_s} = \Omega_{\sigma_s}$ *pour le détecteur 2 et* $\Lambda_{\sigma_s} = \begin{bmatrix} H_s & \mathbf{1} \end{bmatrix}$ *pour le détecteur 3. Nous devons montrer que toute solution* $\Lambda_{\sigma_s} = \Omega_{\sigma_s}$ *de* (3.10) *est également une solution de* (3.15) *mais l'inverse n'est pas vrai. À cette fin, nous devons démontrer que*

$$\begin{bmatrix} H_s & \mathbf{1} \end{bmatrix}^T \subseteq ker(\mathcal{O}_{\sigma_s}^T) \tag{3.25}$$

Les égalités suivantes sont vérifiées.

$$\begin{aligned}
\mathcal{O}_{\sigma_{[k-h,k]}}^T \begin{bmatrix} H_s & \mathbf{1} \end{bmatrix}^T &= \begin{bmatrix} \mathcal{O}_{\sigma_{[k-h,k-1]}} \\ C_{\sigma(k)} A_{\sigma(k-1)}^{\sigma(k-h)} \end{bmatrix}^T \begin{bmatrix} -\Xi_s^{(1)} & \mathbf{1} \end{bmatrix}^T \\
&= \begin{bmatrix} \mathcal{O}_{\sigma_{[k-h,k-1]}}^T & (C_{\sigma(k)} A_{\sigma(k-1)}^{\sigma(k-h)})^T \end{bmatrix} \begin{bmatrix} -\Xi_s^{(1)^T} \\ \mathbf{1} \end{bmatrix} \\
&= -\mathcal{O}_{\sigma_{[k-h,k-1]}}^T \Xi_s^{(1)^T} + (C_{\sigma(k)} A_{\sigma(k-1)}^{\sigma(k-h)})^T \\
&= -(\Xi_s^{(1)} \mathcal{O}_{\sigma_{[k-h,k-1]}})^T + (C_{\sigma(k)} A_{\sigma(k-1)}^{\sigma(k-h)})^T \\
&= -(C_{\sigma(k)} A_{\sigma(k-1)}^{\sigma(k-h)})^T + (C_{\sigma(k)} A_{\sigma(k-1)}^{\sigma(k-h)})^T \\
&= \mathbf{0}
\end{aligned}$$

ce qui signifie que $\begin{bmatrix} H_s & \mathbf{1} \end{bmatrix}^T \subseteq ker(\mathcal{O}_{\sigma_{[k-h,k]}}^T)$.
D'autre part, par définition Ω_{σ_s} *est le noyau de* $\mathcal{O}_{\sigma_s}$*, on a*

$$N_l(\Omega_{\sigma_s}) = (m(h+1) - rank(\mathcal{O}_{\sigma_s}))$$

et

$$N_l(\begin{bmatrix} H_s & \mathbf{1} \end{bmatrix}) = m$$

où $N_l(X)$ *désigne le nombre de lignes de la matrice* X.
Par conséquent, dans le cas particulier où $rang(\mathcal{O}_{\sigma_s}) < mh$*, on a*

$$N_l(\Omega_{\sigma_s}) > N_l(\begin{bmatrix} H_s & \mathbf{1} \end{bmatrix})$$

Étant donné que Ω_{σ_s} *est de rang plein par définition du noyau, dans ce cas, une solution du détecteur 2 ne peut pas être une solution du détecteur 3. Cela achève la preuve.*

Remarque 7 *Dans le cas particulier où* $rang(\mathcal{O}_{\sigma_s}) = mh$*, le détecteur 3 est équivalent au détecteur 2. En effet, dans un tel cas,* $N_l(\Omega_{\sigma_s}) = N_l(\begin{bmatrix} H_s & \mathbf{1} \end{bmatrix})$.
Comme Ω_{σ_s} *ne contient que des vecteurs lignes indépendants par définition du noyau à gauche, c'est également le cas pour* $\begin{bmatrix} H_s & \mathbf{1} \end{bmatrix}$*, puisque*

$$rang(\begin{bmatrix} H_s & \mathbf{1} \end{bmatrix}) = rang(\mathbf{1}) = N_l(\begin{bmatrix} H_s & \mathbf{1} \end{bmatrix})$$

Par conséquent, en vue de (3.25)*, le détecteur 3 est équivalent au détecteur 2.*

Notons que la condition $rang(\mathcal{O}_{\sigma_s}) > mh$ *ne peut pas être vérifiée étant donné que h obéit à la condition* (3.24)*,* $rang(\mathcal{O}_{\sigma_s}) \leq n$ *et* $m > 0$.

3.3.5 Conclusion sur les détecteurs

À partir de l'étude comparative précédente, nous pouvons définir un détecteur général qui englobe l'ensemble des détecteurs présentés précédemment et on a la proposition suivante.

Proposition 11 *Soit h le plus petit entier vérifiant*

$$rang(\mathcal{O}_{\sigma_{[k-h,k]}}) = rang(\mathcal{O}_{\sigma_{[k-h,k-1]}}) \tag{3.26}$$

La séquence active σ^* dans l'intervalle de temps $[k-h,k]$ est une séquence $\sigma_s \in \mathcal{J}^{h+1}$ $(s \in \mathcal{S})$ telle que le résidu correspondant vérifie

$$r_{h,\sigma_s} = \boldsymbol{0} \tag{3.27}$$

avec

$$r_{h,\sigma_s} = \Omega_{\sigma_s}(y_{k-h,k} - T_{\sigma_s} u_{k-h,k} - T'_{\sigma_s})$$

où Ω_{σ_s} est la solution de

$$\Omega_{\sigma_s}\mathcal{O}_{\sigma_s} = \boldsymbol{0}$$

Preuve 16 *Le noyau Ω_{σ_s} de $\mathcal{O}_{\sigma_s}$ englobe les solutions Λ_{σ_s} résumées dans la Proposition 5 de la sous section 3.3.1 comme il a été démontré dans la Preuve 14 et la Preuve 15. La taille de l'horizon h satisfaisant* (3.26) *englobe toutes les autres conditions* (3.22) *et* (3.23) *comme le souligne la Remarque 6.*

Comme une conséquence directe, le corollaire suivant s'applique.

Corollaire 1 *Le mode actif $\sigma^*(k)$ est le dernier élément de l'une des séquences σ_s qui sont solutions de* (3.27).

Dans la suite, nous nous intéressons à la question importante qui se pose en ce qui concerne un détecteur : la capacité de fournir une solution unique $\sigma^*(k)$. Puisque les solutions des détecteurs de modes, en raison de leur structure, sont des séquences de modes, il faut vérifier si un détecteur de mode est capable de discriminer la séquence active σ^* de toute autre séquence $\sigma_s \in \mathcal{J}^{h+1}$ $(s \in \mathcal{S})$. Cette notion est liée à la discernabilité.

3.4 Unicité

Plusieurs notions étroitement liées de discernabilité ont été proposées dans la littérature. Cette section a pour objectif d'en faire une synthèse.

3.4.1 Conditions pour la discernabilité

La notion de discernabilité a été largement discutée dans [Babaali and Egerstedt, 2005] et [Domlan et al., 2007]. Formellement, la discernabilité des séquences de modes obéit à la définition suivante qui est rappelée ici avec les notations de ce chapitre.
Les deux définitions suivantes sont générales. Elles sont fondées uniquement sur les résidus sans la considération de la structure spécifique des détecteurs de modes.

Définition 11 *[Babaali and Egerstedt, 2005, Domlan et al., 2007] Considérons deux séquences de modes σ_{s_i} et σ_{s_j} délivrées par (3.1) avec $(s_i, s_j) \in \mathcal{S}^2$. Supposons que σ_{s_i} est la séquence active. La séquence σ_{s_i} est discernable de σ_{s_j} dans une fenêtre d'observation de longueur $h+1$, si les résidus correspondants $r_{h,\sigma_{s_i}}$ et $r_{h,\sigma_{s_j}}$ ne sont pas simultanément nuls.*

Nous pouvons introduire la notion de discernabilité pour le système (3.1).

Définition 12 *Le système (3.1) est discernable si pour chaque paire de séquences $\sigma_{s_i} \in \mathcal{J}^{h+1}$, $\sigma_{s_j} \in \mathcal{J}^{h+1}$ avec $(s_i, s_j) \in \mathcal{S}^2$, σ_{s_i} est discernable de σ_{s_j}.*

Dans ce qui suit, les conditions sont particularisées au détecteur général défini dans la Proposition 11.
Une condition nécessaire et suffisante pour la discernabilité de deux séquences est prouvée dans [Domlan et al., 2007] et rappelée ci-dessous.

Théorème 14 *[Domlan et al., 2007] Considérons deux séquences de modes σ_{s_i} et σ_{s_j} délivrées par (3.1) avec $(s_i, s_j) \in \mathcal{S}^2$. Supposons que σ_{s_i} est la séquence active. Pour une séquence d'entrée donnée $u_{k-h,k}$, la séquence σ_{s_i} est discernable de σ_{s_j} dans une fenêtre d'observation de longueur $h+1$, pour presque toutes les conditions initiales x_{k-h}, si et seulement si, au moins l'une des conditions suivantes est satisfaite*

$$\Omega_{\sigma_{s_i}} \mathcal{O}_{\sigma_{s_j}} \neq \boldsymbol{0} \tag{3.28}$$

$$\Omega_{\sigma_{s_i}}((T_{\sigma_{s_j}} - T_{\sigma_{s_i}})u_{k-h,k} + (T'_{\sigma_{s_j}} - T'_{\sigma_{s_i}})) \neq \boldsymbol{0} \tag{3.29}$$

Les remarques suivantes peuvent être faites.

Remarque 8 *Le Théorème 14 est valable pour une séquence d'entrée donnée $u_{k-h,k}$. La question d'existence de la séquence d'entrée $u_{k-h,k}$ qui satisfait (3.29) n'est pas triviale. Elle a été abordée dans [Baglietto et al., 2007, Baglietto et al., 2009] où les notions de "séquences d'entrée discernables" et d'"observabilité active" ont été introduites.*

Remarque 9 *La condition (3.28) est une condition nécessaire et suffisante pour la discernabilité des systèmes linéaires à commutation sans entrée, ou bien les systèmes affines à commutation sans entrée avec une partie affine et une matrice de sortie constante. En effet, dans tous ces cas, les matrices d'entrée et de transfert direct sont nulles, induisant $T_{\sigma_s} = \boldsymbol{0}$. On a également $T'_{\sigma_s} = \boldsymbol{0}$ nulle pour les systèmes linéaires à commutation et la différence $T'_{\sigma_{s_j}} - T'_{\sigma_{s_i}}$ est nulle pour les systèmes affines à commutation avec une partie affine et une matrice de sortie constantes. Pour les systèmes avec entrée, (3.28) est une condition suffisante étant donné que (3.29) doit être prise en compte.*

Comme une conséquence directe, le corollaire suivant s'applique.

Corollaire 2 *Le mode actif $\sigma^*(k)$ est le dernier élément de la séquence σ_s qui est la solution de (3.27).*

Les conditions (3.28) et (3.29) dépendent de la structure du détecteur puisqu'elles impliquent les matrices Ω_{σ_i}. Une condition équivalente à (3.28) qui reste valable quelle que soit la structure du détecteur et ne nécessite pas le calcul des matrices Ω_{σ_i} est proposée ci-dessous.

Proposition 12 *La condition* (3.28) *est équivalente à*

$$rang(\begin{bmatrix}\mathcal{O}_{\sigma_{s_i}} & \mathcal{O}_{\sigma_{s_j}}\end{bmatrix}) > rang(\mathcal{O}_{\sigma_{s_j}}) \tag{3.30}$$

où $\begin{bmatrix}\mathcal{O}_{\sigma_{s_i}} & \mathcal{O}_{\sigma_{s_j}}\end{bmatrix}$ dénote la concaténation horizontale de $\mathcal{O}_{\sigma_{s_i}}$ et $\mathcal{O}_{\sigma_{s_j}}$.

Preuve 17 *Si (3.30) n'est pas vérifiée, cela est équivalent à*

$$rang(\begin{bmatrix}\mathcal{O}_{\sigma_{s_i}} & \mathcal{O}_{\sigma_{s_j}}\end{bmatrix}) = rang(\mathcal{O}_{\sigma_{s_j}})$$

Il est clair que $rang(\begin{bmatrix}\mathcal{O}_{\sigma_{s_i}} & \mathcal{O}_{\sigma_{s_j}}\end{bmatrix}) < rang(\mathcal{O}_{\sigma_{s_j}})$ *ne peut jamais être vérifiée. Cela signifie que* $\mathcal{O}_{\sigma_{s_i}} \in \mathcal{R}(\mathcal{O}_{\sigma_{s_j}})$. *À partir de (3.5) du Lemme 1, on trouve que*

$$\mathcal{O}_{\sigma_{s_i}} \in \mathcal{R}(\mathcal{O}_{\sigma_{s_j}}) \quad \Leftrightarrow \quad (\mathcal{O}_{\sigma_{s_j}}\mathcal{O}^{\dagger}_{\sigma_{s_j}} - \boldsymbol{1})\mathcal{O}_{\sigma_{s_i}} = 0 \tag{3.31}$$

Par ailleurs, selon le Théorème 13, $\mathcal{R}(\mathcal{O}_{\sigma_{s_j}}\mathcal{O}^{\dagger}_{\sigma_{s_j}} - \boldsymbol{1}) = ker(\mathcal{O}_{\sigma_{s_j}})$. *Par conséquent, puisque* $ker(\mathcal{O}_{\sigma_{s_j}}) = \Omega_{\sigma_{s_j}}$, *(3.31) est équivalent à*

$$\Omega_{\sigma_{s_j}}\mathcal{O}_{\sigma_{s_i}} = \boldsymbol{0}$$

Cela achève la preuve.

Notons que la condition (3.30) suit la définition de discernabilité proposée dans [Babaali and Egerstedt, 2004].
La considération du Théorème 14 et de la Proposition 12 donne le corollaire ci-dessous.

Corollaire 2 *Les équivalences suivantes sont vérifiées*

$$\begin{gathered} rang(\begin{bmatrix}\mathcal{O}_{\sigma_{s_i}} & \mathcal{O}_{\sigma_{s_j}}\end{bmatrix}) > rang(\mathcal{O}_{\sigma_{s_j}}) \\ \Leftrightarrow \\ \Omega_{\sigma_{s_j}}\mathcal{O}_{\sigma_{s_i}} \neq \mathbf{0} \\ \Rightarrow \\ \sigma_{s_i} \in \mathcal{J}^{h+1}\ (s_i \in \mathcal{S}) \text{ est discernable de } \sigma_{s_j} \in \mathcal{J}^{h+1}\ (s_j \in \mathcal{S}) \end{gathered}$$

La dernière implication devient une équivalence pour les systèmes vérifiant les conditions mentionnées dans la Remarque 9.

Proposition 13 *La discernabilité n'est pas réversible.*
Autrement dit, même si σ_{s_j} *est discernable de* σ_{s_i}, σ_{s_i} *peut ne pas être discernable de* σ_{s_j}.

Preuve 1 *Supposons que* σ_{s_i} *n'est pas discernable de* σ_{s_j} *alors*

$$\Omega_{\sigma_{s_j}}\mathcal{O}_{\sigma_{s_i}} = \boldsymbol{0}$$

Toutefois, par définition de $\Omega_{\sigma_{s_i}}$,

$$\Omega_{\sigma_{s_i}}\mathcal{O}_{\sigma_{s_i}} = \boldsymbol{0}$$

Par conséquent, $\Omega_{\sigma_{s_j}} \subseteq ker(\mathcal{O}_{\sigma_{s_i}})$ *ce qui implique que*

$$rang(ker(\mathcal{O}_{\sigma_{s_i}})) := rang(\Omega_{\sigma_{s_i}}) \geq rang(\Omega_{\sigma_{s_j}}) \tag{3.32}$$

A présent, supposons que $rang(\Omega_{\sigma_{s_i}}) \neq rang(\Omega_{\sigma_{s_j}})$*. Dans un tel cas,*

$$rang(\Omega_{\sigma_{s_i}}) > rang(\Omega_{\sigma_{s_j}}) \tag{3.33}$$

et puisque $\Omega_{\sigma_{s_j}}\mathcal{O}_{\sigma_{s_j}} = \boldsymbol{0}$ *par définition, cela implique que* $\Omega_{\sigma_{s_j}}$ *engendre* $ker(\mathcal{O}_{\sigma_{s_i}})$*. Cependant,* (3.33) *implique que* $\Omega_{\sigma_{s_i}}$ *n'engendre pas* $ker(\mathcal{O}_{\sigma_{s_j}})$*. Par conséquent, il est clair que*

$$\Omega_{\sigma_{s_i}}\mathcal{O}_{\sigma_{s_j}} \neq \boldsymbol{0}$$

Finalement, on se basant sur (3.28)*,* σ_{s_j} *est discernable de* σ_{s_i}*.*

3.4.2 Mesure de la discernabilité

Plusieurs grandeurs ont été proposées pour évaluer si la discernabilité est "forte" ou bien "faible". En d'autres termes, elles permettent de donner une mesure de la "distance" entre deux séquences que nous avons l'intention de discriminer. En fait, trois principales grandeurs ont été proposées dans la littérature : l'"observabilité des modes", le "degré de discernabilité" et le "conflit" entre deux séquences. Toutes ces grandeurs sont liées à (3.30) et par conséquent, donnent des conditions suffisantes pour les systèmes contrôlés. D'autre part, elles ne dépendent pas de la structure du détecteur. Elles sont rappelées ci-dessous et comparées les unes par rapport aux autres.

1) "Degré de discernabilité"
Dans [Babaali and Egerstedt, 2004], le "degré de discernabilité" est défini comme étant l'entier positif $d > 0$ satisfaisant

$$d = rang(\begin{bmatrix}\mathcal{O}_{\sigma_{s_i}} & \mathcal{O}_{\sigma_{s_j}}\end{bmatrix}) - rang(\mathcal{O}_{\sigma_{s_j}})$$

Lorsque (3.30) est vérifiée, on dit que σ_{s_i} est $d-$discernable de σ_{s_j}. Lorsque $d = 0$, cela veut dire que σ_{s_i} n'est pas discernable de σ_{s_j}.

2) "Conflit" entre deux séquences
Dans [Babaali and Egerstedt, 2004], le "conflit" de la séquence σ_{s_i} avec σ_{s_j} est donné par la grandeur $C(\sigma_{s_i}, \sigma_{s_j})$ définie par

$$C(\sigma_{s_i}, \sigma_{s_j}) = \mathcal{R}(\mathcal{O}_{\sigma_{s_i}}) \cap \mathcal{R}(\mathcal{O}_{\sigma_{s_j}})$$

La dimension du conflit est donnée par la grandeur $dim(C(\sigma_{s_i}, \sigma_{s_j}))$ et définie comme

$$dim(C(\sigma_{s_i}, \sigma_{s_j})) = rang(\mathcal{O}_{\sigma_{s_i}}) + rang(\mathcal{O}_{\sigma_{s_j}}) - rang(\begin{bmatrix}\mathcal{O}_{\sigma_{s_i}} & \mathcal{O}_{\sigma_{s_j}}\end{bmatrix})$$

Il s'ensuit que

$$dim(C(\sigma_{s_i}, \sigma_{s_j})) = 0 \Leftrightarrow rang(\begin{bmatrix}\mathcal{O}_{\sigma_{s_i}} & \mathcal{O}_{\sigma_{s_j}}\end{bmatrix}) = rang(\mathcal{O}_{\sigma_{s_i}}) + rang(\mathcal{O}_{\sigma_{s_j}}) \tag{3.34}$$

Lorsque $dim(C(\sigma_{s_i}, \sigma_{s_j})) = 0$, il n'y a aucun conflit et, à condition que $rang(\mathcal{O}_{\sigma_{s_i}}) \neq 0$ et $rang(\mathcal{O}_{\sigma_{s_j}}) \neq 0$. Par conséquent, σ_{s_i} est discernable de σ_{s_j} et σ_{s_j} est discernable de σ_{s_i}. Néanmoins, (3.34) est une condition suffisante pour que (3.30) soit vérifiée mais pas nécessaire. En

effet, une séquence σ_{s_i} peut être discernée d'une autre séquence σ_{s_j} même si $dim(C(\sigma_{s_i}, \sigma_{s_j})) \neq 0$. Rappelons que σ_{s_i} est discernable de σ_{s_j} implique que le degré de discernabilité d est tel que $d > 0$, et remarquant que $d = rang(\mathcal{O}_{\sigma_{s_i}}) - dim(C(\sigma_{s_i}, \sigma_{s_j}))$, σ_{s_i} est discernable de σ_{s_j} lorsque $dim(C(\sigma_{s_i}, \sigma_{s_j})) \leq rang(\mathcal{O}_{\sigma_{s_i}}) - 1$. En fait, $dim(C(\sigma_{s_i}, \sigma_{s_j})) = 0$ correspond au cas particulier $d = rang(\mathcal{O}_{\sigma_{s_i}})$. Par conséquent, le conflit entre deux séquences donne une condition plus restrictive que celle du degré de discernabilité.

3) Observabilité des modes

L'observabilité des modes a été considérée sous différentes terminologies selon les auteurs [Vidal et al., 2002],[Alessandri et al., 2005].

Proposition 14 *[Vidal et al., 2002],[Alessandri et al., 2005] Deux séquences σ_{s_i} et σ_{s_j} sont discernables si*

$$rang(\begin{bmatrix}\mathcal{O}_{\sigma_{s_i}} & \mathcal{O}_{\sigma_{s_j}}\end{bmatrix}) = 2n \tag{3.35}$$

La condition (3.35) exige que $rang(\mathcal{O}_{\sigma_i}) = n$ pour tout $i \in \{s_i, s_j\}$ avec $(s_i, s_j) \in \mathcal{S}^2$, c'est-à-dire que le système soit PWO. Soulignons que la PWO n'est pas équivalente à l'observabilité des modes. Elle n'est qu'une condition nécessaire. Par conséquent, l'observabilité des modes donne une condition plus restrictive que le conflit entre deux séquences.

Conformément à la Définition 11, si la discernabilité n'est pas vérifiée, cela signifie que plusieurs résidus peuvent s'annuler simultanément. L'estimation des séquences σ_s qui obéit à la Proposition 11 n'est pas possible. La section suivante est consacrée aux alternatives qui permettent de résoudre un tel problème.

3.5 Alternatives pour les systèmes non discernables

Nous introduirons $\mathcal{R}_{\sigma_{s_i}}$ $(s_i \in \mathcal{S})$ comme l'ensemble des séquences σ_{s_j} $(s_j \in \mathcal{S})$ tel que σ_{s_i} n'est pas discernable de σ_{s_j}. Nous précisons que dans la situation particulière soulignée dans la Remarque 9, $\mathcal{R}_{\sigma_{s_i}}$ peut être défini, selon (3.30), comme

$$\mathcal{R}_{\sigma_{s_i}} = \left\{\sigma_{s_j} : s_j \in \mathcal{S} \mid rang(\begin{bmatrix}\mathcal{O}_{\sigma_{s_i}} & \mathcal{O}_{\sigma_{s_j}}\end{bmatrix}) = rang(\mathcal{O}_{\sigma_{s_j}})\right\} \tag{3.36}$$

Soit $\mathcal{R}_{\sigma^*}$ l'ensemble de toutes les séquences ayant un résidu nul lorsque la séquence active est σ^*

$$\mathcal{R}_{\sigma^*} = \left\{\sigma_{s_j} : s_j \in \mathcal{S} \mid r_{h,\sigma_{s_j}} = \mathbf{0}\right\} \tag{3.37}$$

3.5.1 $\mathcal{R}$–discernabilité

La $\mathcal{R}$–discernabilité est proposée dans ce chapitre comme une extension de la discernabilité. Lorsqu'elle est vérifiée, elle permet de discriminer deux séquences même si leur résidu s'annule simultanément.

A présent, nous pouvons introduire la notion de $\mathcal{R}$–discernabilité

Définition 13 *Considérons deux séquences de modes σ_{s_i} et σ_{s_j} délivrées par (3.1) avec $(s_i, s_j) \in \mathcal{S}^2$. Supposons que σ_{s_i} est la séquence active. La séquence σ_{s_i} est $\mathcal{R}$–discernable de σ_{s_j} dans une fenêtre d'observation de longueur $h+1$, pour presque toutes les conditions initiales x_{k-h} si*

$$\mathcal{R}_{\sigma_{s_i}} \neq \mathcal{R}_{\sigma_{s_j}} \tag{3.38}$$

Notons que σ_{s_i} est toujours un élément de l'ensemble $\mathcal{R}_{\sigma_{s_i}}$, et lorsque la discernabilité est vérifiée, $\mathcal{R}_{\sigma_{s_i}}$ se réduit à un singleton. En effet, dans un tel cas, il se trouve que $\mathcal{R}_{\sigma_s} = \{\sigma_s\}$ pour toute $\sigma_s \in \mathcal{J}^{h+1}$ $(s \in \mathcal{S})$. Par conséquent, pour les systèmes discernables, (3.38) est toujours vérifiée ce qui veut dire que la discernabilité implique la $\mathcal{R}$–discernabilité.

Définition 14 *Le système (3.1) est $\mathcal{R}$–discernable si, pour toute paire de séquences $\sigma_{s_i} \in \mathcal{J}^{h+1}$, $\sigma_{s_j} \in \mathcal{J}^{h+1}$ avec $(s_i, s_j) \in \mathcal{S}^2$ et $s_i \neq s_j$, la condition (3.38) est satisfaite.*

Proposition 15 *Supposons que* (3.1) *est $\mathcal{R}$– discernable. La séquence active σ^* dans l'intervalle de temps $[k-h, k]$ est l'unique séquence $\sigma_s \in \mathcal{J}^{h+1}$ $(s \in \mathcal{S})$ telle que*

$$\mathcal{R}_{\sigma^*} = \mathcal{R}_{\sigma_s} \tag{3.39}$$

Preuve 18 *Il s'agit d'une conséquence directe de la définition de la $\mathcal{R}$–discernabilité.*

En d'autres termes, la discrimination est réalisée si l'ensemble $\mathcal{R}_{\sigma^*}$ correspondant à la séquence active diffère de tous les autres ensembles $\mathcal{R}_{\sigma_j}$ correspondant aux autres séquences $\sigma_j \in \mathcal{J}^{h+1}$ $(j \in \mathcal{S})$.

Comme une conséquence directe, le corollaire suivant s'applique.

Corollaire 3 *Le mode actif $\sigma^*(k)$ est le dernier élément de la séquence σ_s qui est la solution de* (3.39).

Un exemple illustrant la $\mathcal{R}$–discernabilité est donné en Section 3.8.2.

Dans le cas où la discernabilité et la $\mathcal{R}$–discernabilité ne sont pas satisfaites, la séquence active σ^* de longueur $h+1$ ne peut pas être discriminée de toutes les autres et donc, ne peut pas être estimée directement. Dans ce cas, une alternative a été proposée dans la littérature à travers la notion de (η, ω)–discernabilité [Alessandri et al., 2005]. Elle reflète la capacité de discriminer et donc d'estimer une partie de la séquence active. C'est l'objet de la sous-section suivante.

3.5.2 (η, ω)–Discernabilité

La notion de (η, ω)–discernabilité a été introduite dans [Alessandri et al., 2005]. Elle reflète la capacité de discriminer la sous-séquence active $\sigma^*_{[k-h+\eta, k-\omega]}$ de toutes les autres. Les grandeurs η et ω sont des entiers vérifiant $\eta \in \{0, \cdots, h\}$, $\omega \in \{0, \cdots, h\}$ et $\eta + \omega \leq h$. Clairement, la (η, ω)–discernabilité coïncide avec la discernabilité si $\eta = 0$ et $\omega = 0$. Dans la suite, nous considérons $\eta > 0$ ou $\omega > 0$. Les entiers η et ω doivent être choisis les plus petits possible pour obtenir une séquence estimée de longueur maximale. Soit $\sigma_{s[k-h+\eta, k-\omega]}$ $(s \in \mathcal{S})$ une séquence de modes $\sigma(k-h+\eta) \cdots \sigma(k-w)$. La (η, ω)–discernabilité obéit alors à la définition formelle suivante.

Définition 15 *[Alessandri et al., 2005] σ_{s_i} est (η, ω)–discernable de σ_{s_j} avec $(s_i, s_j) \in \mathcal{S}^2$, si $\sigma_{s_i[k-h+\eta, k-\omega]} \neq \sigma_{s_j[k-h+\eta, k-\omega]}$ et σ_{s_i} est discernable de σ_{s_j}.*

On introduit la notion de la (η, ω)–discernabilité pour le système (3.1).

Définition 16 *[Alessandri et al., 2005] Le système* (3.1) *est* (η,ω)*–discernable, si, pour chaque paire de séquences* $\sigma_{s_i} \in \mathcal{J}^{h+1}, \sigma_{s_j} \in \mathcal{J}^{h+1}$ *avec* $(s_i, s_j) \in \mathcal{S}^2$*,* σ_{s_i} *est* (η,ω)*–discernable de* σ_{s_j}*.*

À partir du Théorème 3, nous pouvons déduire des conditions permettant de vérifier la (η,ω)–discernabilité comme indiqué dans la proposition suivante.

Proposition 16 *Considérons deux séquences de modes* σ_{s_i} *et* σ_{s_j} *délivrées par* (3.1) *avec* $(s_i, s_j) \in \mathcal{S}^2$*. Supposons que* σ_{s_i} *est la séquence active. Pour une séquence d'entrée donnée* $u_{k-h,k}$*,* σ_{s_i} *est* (η,ω)*–discernable de* σ_{s_j} *dans une fenêtre d'observation de longueur* $h+1$*, pour presque toutes les conditions initiales* x_{k-h}*, si et seulement si, au moins l'une des conditions suivantes est vérifiée*

$$\Omega_{\sigma_{s_i}} \mathcal{O}_{\sigma_{s_j}} \neq \boldsymbol{0} \tag{3.40}$$

$$\Omega_{\sigma_{s_i}}((T_{\sigma_{s_j}} - T_{\sigma_{s_i}})u_{k-h,k} + (T'_{\sigma_{s_j}} - T'_{\sigma_{s_i}})) \neq \boldsymbol{0} \tag{3.41}$$

$$avec \quad \sigma_{s_i[k-h+\eta,k-\omega]} \neq \sigma_{s_j[k-h+\eta,k-\omega]}$$

Preuve 19 *La preuve est une conséquence directe de la considération à la fois de la Définition 15 de la* (η,ω)*–discernabilité et de* (3.28)-(3.29) *du Théorème 3.*

De même que pour la discernabilité, une condition équivalente à (3.40) qui reste vérifiée quelle que soit la structure du détecteur, et qui ne nécessite pas le calcul de $\Omega_{\sigma_{s_j}}$, peut être proposée.

Proposition 17 *La condition* (3.40) *est équivalente à*

$$\begin{aligned} &rang(\begin{bmatrix}\mathcal{O}_{\sigma_{s_i}} & \mathcal{O}_{\sigma_{s_j}}\end{bmatrix}) > rang(\mathcal{O}_{\sigma_{s_j}}) \\ &avec \quad \sigma_{s_i[k-h+\eta,k-\omega]} \neq \sigma_{s_j[k-h+\eta,k-\omega]} \end{aligned} \tag{3.42}$$

Preuve 20 *La preuve est une conséquence directe de la considération à la fois de la Définition 15 de la* (η,ω)*–discernabilité et de la Proposition 12.*

L'estimation de la sous-séquence active $\sigma^*_{[k-h+\eta,k-\omega]}$ peut être effectuée selon la proposition suivante.

Proposition 18 *Supposons que le système* (3.1) *est* (η,ω)*–discernable. La sous-séquence active* $\sigma^*_{[k-h+\eta,k-\omega]}$ *dans l'intervalle de temps* $[k-h,k]$ *est l'unique sous-séquence* $\sigma_{s[k-h+\eta,k-\omega]}$ *des séquences* $\sigma_s \in \mathcal{J}^{h+1}$ $(s \in \bar{\mathcal{S}})$ *telle que*

$$\sigma_s \in \mathcal{R}_{\sigma^*} \tag{3.43}$$

Preuve 21 *L'ensemble* $\mathcal{R}_{\sigma^*}$ *contient toutes les séquences* σ_{s_j} *ayant un résidu nul, et par conséquent, toutes les séquences* σ_{s_j} *telles que* σ^* *n'est pas discernable de* σ_{s^j}*. Puisque la* (η,ω)*–discernabilité est vérifiée, toutes ces séquence ont une partie* $\sigma_{s[k-h+\eta,k-\omega]}$ *commune. Par conséquent,* $\sigma_{s[k-h+\eta,k-\omega]}$ *est une sous-séquence unique.*

Comme une conséquence directe, le corollaire suivant s'applique.

Corollaire 4 *Le mode actif* $\sigma^*(k)$ *est le* $h+1-\omega$ *élément de la séquence* σ_s *qui est solution de* (3.43) *à l'instant* $k+\omega$*.*

Il est intéressant de souligner qu'une telle notion est une extension de la "discernabilité avant" (Forward Discernability (FD)) introduite dans [Babaali and Egerstedt, 2004]. En effet, la discernabilité avant reflète la capacité à déterminer un nombre prescrit λ' de modes $\sigma(k-h)\ldots\sigma(k-\lambda')$ dans une séquence de longueur $h+1$. Par conséquent, la discernabilité avant est équivalente à l'existence d'un entier λ' tel que la $(\eta=0,\omega=\lambda')$–discernabilité est vérifiée.

3.5.3 $\mathcal{R}(\eta,\omega)$–discernabilité

De même que pour la $\mathcal{R}$–discernabilité, on propose d'étendre la (η,ω)–discernabilité en introduisant la $\mathcal{R}(\eta,\omega)$–discernabilité. Elle permet d'estimer la sous-séquence active ${\sigma^*}_{[k-h+\eta,k-\omega]}$ lorsque la (η,ω)–discernabilité n'est pas vérifiée.

Rappelons que $\mathcal{R}_{\sigma_{s_i}}$ $(s_i \in \mathcal{S})$ est l'ensemble des séquences σ_{s_j} $(s_j \in \mathcal{S})$ tel que la séquence σ_{s_i} n'est pas discernable de la séquence σ_{s_j}.

Définition 17 *Considérons deux séquences de modes σ_{s_i} et σ_{s_j} délivrées par (3.1) avec $(s_i,s_j) \in \mathcal{S}^2$. Supposons que σ_{s_i} est la séquence active. Ensuite, une séquence σ_{s_i} est $\mathcal{R}(\eta,\omega)$–discernable de σ_{s_j} dans une fenêtre d'observation de longueur $h+1$, pour presque toutes les conditions initiales x_{k-h} si*

$$\mathcal{R}_{\sigma_{s_i}} \neq \mathcal{R}_{\sigma_{s_j}} \text{ avec } \sigma_{s_i[k-h+\eta,k-\omega]} \neq \sigma_{s_j[k-h+\eta,k-\omega]} \tag{3.44}$$

La proposition suivante permet d'effectuer l'estimation de $\sigma^*_{[k-h+\eta,k-\omega]}$.

Proposition 19 *Supposons que le système (3.1) est $\mathcal{R}(\eta,\omega)$–discernable. Soit $\mathcal{R}^{\eta,\omega}_{\sigma^*}$ l'ensemble défini comme*

$$\mathcal{R}^{\eta,\omega}_{\sigma^*} = \left\{ \sigma_{s_j} : s_j \in \mathcal{S} \mid \mathcal{R}_{\sigma^*} = \mathcal{R}_{\sigma_{s_j}} \right\} \tag{3.45}$$

La sous-séquence active ${\sigma^*}_{[k-h+\eta,k-\omega]}$ dans l'intervalle de temps $[k-h,k]$ est l'unique sous-séquence $\sigma_{s[k-h+\eta,k-\omega]}$ avec $s \in \mathcal{S}$ telle que

$$\sigma_s \in \mathcal{R}^{\eta,\omega}_{\sigma^*} \tag{3.46}$$

Preuve 22 *L'ensemble $\mathcal{R}^{\eta,\omega}_{\sigma^*}$ contient toutes les séquences σ_{s_j} telles que $\mathcal{R}_{\sigma^*} = \mathcal{R}_{\sigma_{s_j}}$, et par conséquent, toutes les séquences σ_{s_j} telles que σ^* n'est pas $\mathcal{R}$–discernable de σ_{s^j}. Puisque la $\mathcal{R}(\eta,\omega)$–discernabilité est vérifiée, toutes ces séquence ont une partie $\sigma_{s[k-h+\eta,k-\omega]}$ commune. Par conséquent, $\sigma_{s[k-h+\eta,k-\omega]}$ est une sous-séquence unique.*

Comme une conséquence directe, le corollaire suivant s'applique.

Corollaire 5 *Le mode actif $\sigma^*(k)$ est le $h+1-\omega$ élément de la séquence σ_s qui est solution de (3.46) à l'instant $k+\omega$.*

– **Discussion**

Si le système (3.1) est discernable ou $\mathcal{R}$–discernable, l'ensemble de la séquence active σ^* dans l'intervalle de temps $[k-h,k]$ peut être estimé à l'instant k avec la Proposition 10 et la Proposition 13 respectivement. Par conséquent, la discernabilité et la $\mathcal{R}$–discernabilité permettent d'estimer à l'instant $k=h$, la première séquence active σ^* dans l'intervalle de temps $[0,h]$ et donc, tous les modes $\sigma(k)$ pour $k=0,\ldots,h$. Par une approche à horizon glissant et donc en ligne, elles permettent également d'estimer aux instants $k>h$ la séquence active dans n'importe quel intervalle $[k-h,k]$ et donc tous les modes $\sigma(k)$ pour $k>h$. On parlera d'estimation permanente. En conséquence, la Proposition 10 et la Proposition 13 permettent d'atteindre l'estimation de tous les modes $\sigma(k)$ pour $k \geq 0$.

Si le système (3.1) est (η,ω)–discernable ou $\mathcal{R}(\eta,\omega)$–discernable, la sous-séquence $\sigma^*_{[k-h+\eta,k-\omega]}$ de la séquence active σ^* peut être estimée à l'instant k avec la Proposition 16 et la Proposition 17 respectivement. Par conséquent, la (η,ω)–discernabilité et la $\mathcal{R}(\eta,\omega)$–discernabilité permettent d'estimer à l'instant $k=h$, la première sous-séquence active $\sigma^*_{[\eta,h-\omega]}$ et donc, tous les modes $\sigma(k)$

pour $k = \eta, \ldots, h - \omega$. Toutefois, la première partie $\sigma^*_{[0,\eta-1]}$ de la séquence active ne peut pas être estimée. Par une approche à horizon glissant et donc en ligne, elles permettent également d'estimer aux instants $k > h$ la sous-séquence active $\sigma^*_{[k-h+\eta,k-\omega]}$. On parlera là aussi d'estimation permanente. En conséquence, la Proposition 16 et la Proposition 17 permettent l'estimation de tous les modes $\sigma(k)$ pour $k \geq \eta$.

La complexité de l'estimation de mode $\sigma(k)$ à l'instant k, en termes de quantité de données requise et de nombre de résidus à calculer et à analyser, peut être réduite. En effet, l'estimation de mode $\sigma(k)$ à l'instant k peut être effectuée en tenant compte du fait que tous les modes à l'instant $k' < k$ ont déjà été estimés et donc sont supposés être connus. À cet égard, la notion de discernabilité arrière (Backward Discernability (BD)), introduite dans [Babaali and Egerstedt, 2005], joue un rôle central. Elle fait l'objet de la section suivante.

3.6 Discernabilité arrière et estimation permanente

La discernabilité arrière reflète la capacité à discriminer deux séquences de même longueur dans l'intervalle de temps $[k-h, k]$ qui ne diffèrent que par leur dernier élément $\sigma(k)$. En conséquence, elle permet d'estimer ce dernier élément de la séquence.
Notons $\sigma^h i$ (*resp.* $\sigma^h j$) deux séquences de modes obtenues de la concaténation de la séquence σ^h de longueur h et d'un mode $i \in \mathcal{J}$ (*resp.* un mode $j \in \mathcal{J}$). Plus formellement, la discernabilité arrière obéit à la définition suivante.

Définition 18 *[Babaali and Egerstedt, 2005] Un mode actif i est discernable en arrière d'un autre mode j s'il existe un entier h tel que pour chaque séquence σ^h de longueur h, $\sigma^h i$ est discernable de $\sigma^h j$. Le plus petit entier h est appelé l'indice de discernabilité arrière de i par rapport à j.*

Á présent, on peut introduire la notion de discernabilité arrière du système (3.1).

Définition 19 *Le système (3.1) est discernable en arrière si, pour toutes les séquences $\sigma^h i \in \mathcal{J}^{h+1}$, $\sigma^h j \in \mathcal{J}^{h+1}$ avec $i \in \mathcal{J}$, $j \in \mathcal{J}$ et $\sigma^h \in \mathcal{J}^h$, le mode i est discernable en arrière du mode j.*

3.6.1 Conditions pour la discernabilité arrière

De même que pour la discernabilité, des conditions permettant de garantir la discernabilité arrière peuvent être données.

Proposition 20 *Pour une séquence d'entrée donnée $u_{k-h,k}$, un mode actif i est discernable en arrière d'un mode j dans une fenêtre d'observation de longueur $h+1$, pour presque toutes les conditions initiales x_{k-h}, si et seulement si, pour chaque séquence σ^h de longueur h, délivrée par* (3.1)*, au moins l'une des conditions suivantes est satisfaite*

$$\Omega_{\sigma^h j} \mathcal{O}_{\sigma^h i} \neq \boldsymbol{0} \tag{3.47}$$

$$\Omega_{\sigma^h j}((T_{\sigma^h i} - T_{\sigma^h j})u_{k-h,k} + (T'_{\sigma^h i} - T'_{\sigma^h j})) \neq \boldsymbol{0} \tag{3.48}$$

Preuve 23 *La preuve est une conséquence directe de la considération à la fois de la Définition 18 de la discernabilité arrière et de* (3.28)-(3.29) *du Théorème 14.*

Une condition équivalente à (3.47) qui reste vérifiée quelle que soit la structure du détecteur et ne nécessite pas le calcul de $\Omega_{\sigma^h j}$ peut être proposée.

Proposition 21 *La condition* (3.47) *est équivalente à*

$$rang(\begin{bmatrix}\mathcal{O}_{\sigma^h i} & \mathcal{O}_{\sigma^h j}\end{bmatrix}) > rang(\mathcal{O}_{\sigma^h j}) \tag{3.49}$$

Preuve 24 *La preuve est une conséquence directe de la considération à la fois de la Définition 18 de la discernabilité arrière et du Corollaire 2 en remplaçant σ_{s_i} par $\sigma^h i$ et σ_{s_j} par $\sigma^h j$.*

Une condition équivalente à (3.49) est proposée ici, et sera utile pour décider de la discernabilité arrière du (3.1) en examinant la propriété des matrices $A_{\sigma(k)}$.

Proposition 22 *Supposons qu'il existe un entier $h \in \mathbb{N}$ tel que* (3.26) *soit vérifiée. Un mode i est discernable en arrière d'un autre mode j si*

$$(C_i - C_j)A^{\sigma(k-h)}_{\sigma(k-1)} \neq \boldsymbol{0} \tag{3.50}$$

Preuve 25 *Supposons qu'il existe un entier $h \in \mathbb{N}$ tel que* (3.26) *soit vérifiée. Prenons $\sigma_{[k-h,k]} = \sigma^h j$,* (3.26) *est équivalente à*

$$rang(\mathcal{O}_{\sigma^h j}) = rang(\mathcal{O}_{\sigma^h}) \qquad \forall\ j \in \mathcal{J}$$

Par conséquent, (3.49) devient

$$rang(\begin{bmatrix}\mathcal{O}_{\sigma^h i} & \mathcal{O}_{\sigma^h j}\end{bmatrix}) > rang(\mathcal{O}_{\sigma^h}) \tag{3.51}$$

Notons V^i_{h+1}, V^j_{h+1} les dernières lignes de $\mathcal{O}_{\sigma^h i}$ et $\mathcal{O}_{\sigma^h j}$ respectivement.
Étant donné que les lignes de $\mathcal{O}_{\sigma^h i}$ coïncident avec les lignes de $\mathcal{O}_{\sigma^h j}$ excepté la dernière ligne, (3.51) est vérifiée si la ligne $\begin{bmatrix}V^i_{h+1} & V^j_{h+1}\end{bmatrix}$ n'est pas une combinaison linéaire des autres lignes de $[\mathcal{O}_{\sigma^h} \quad \mathcal{O}_{\sigma^h}]$, ce qui signifie qu'il existe un h–uplet $(\alpha_1, \cdots, \alpha_h) \in \mathbb{R}^h$ tel que

$$\begin{bmatrix}V^i_{h+1} & V^j_{h+1}\end{bmatrix} \neq \alpha_1 [V_1 \quad V_1] + \alpha_2 [V_2 \quad V_2] + \cdots + \alpha_h [V_h \quad V_h]$$

où V_l $(l = 1, \ldots, h)$ désigne la $l^{ème}$ ligne de $\mathcal{O}_{\sigma^h}$. Ceci est équivalent à

$$\begin{bmatrix}V^i_{h+1} & V^j_{h+1}\end{bmatrix} \neq [\alpha_1 V_1 + \cdots + \alpha_h V_h \quad \alpha_1 V_1 + \cdots + \alpha_h V_h]$$

et donc à

$$V^i_{h+1} \neq V^j_{h+1} \tag{3.52}$$

Puisque

$$V^i_{h+1} = C_i A^{\sigma(k-h)}_{\sigma(k-1)}$$

et

$$V_{h+1}^{j} = C_j A_{\sigma(k-1)}^{\sigma(k-h)}$$

nous obtenons

$$V_{h+1}^{i} \neq V_{h+1}^{j} \quad \Leftrightarrow \quad (C_i - C_j) A_{\sigma(k-1)}^{\sigma(k-h)} \neq \mathbf{0}$$

qui n'est rien d'autre que (3.50). Cela achève la preuve.

Remarque 10 *Si $C_{\sigma(k)} = C$, c'est-à-dire si la matrice de sortie ne dépend pas du mode,* (3.50) *devient*

$$C(A_i - A_j) A_{\sigma(k-2)}^{\sigma(k-h)} \neq \mathbf{0} \tag{3.53}$$

Remarque 11 *L'équation* (3.50) *signifie que si le produit $A_{\sigma(k-1)}^{\sigma(k-h)}$ n'est pas inversible, la discernabilité arrière du* (3.1) *est assurée si $(C_i - C_j)^T$ n'appartient pas au noyau de $A_{\sigma(k-1)}^{\sigma(k-h)^T}$. Par ailleurs, si toutes les matrices $A_{\sigma(k-1)} \cdots A_{\sigma(k-h)}$ sont de rang plein, alors $A_{\sigma(k-1)}^{\sigma(k-h)}$ est aussi de rang plein. Ainsi, le noyau du produit $A_{\sigma(k-1)}^{\sigma(k-h)^T}$ se réduit à zéro. En conséquence, $(C_i - C_j) A_{\sigma(k-1)}^{\sigma(k-h)} = \mathbf{0}$ est vérifiée lorsque $C_i = C_j$. Par conséquent, si $C_{\sigma(k)} = C$, le système (3.1) n'est pas discernable en arrière.*

En se basant sur la Proposition 22, nous avons la propriété suivante qui, contrairement à la discernabilité, s'applique à la discernabilité arrière.

Corollaire 3 *Supposons qu'il existe un entier $h \in I\!N$ tel que (3.26) est satisfaite. La discernabilité arrière est réversible.*

Preuve 26 *D'après la Proposition 22, un mode i est discernable en arrière d'un autre mode j si*

$$(C_i - C_j) A_{\sigma(k-1)}^{\sigma(k-h)} \neq \mathbf{0} \tag{3.54}$$

D'autre part, un mode j est discernable en arrière d'un autre mode i si

$$(C_j - C_i) A_{\sigma(k-1)}^{\sigma(k-h)} \neq \mathbf{0} \tag{3.55}$$

Clairement, (3.54) est équivalente à (3.55). Cela signifie que la discernabilité arrière est réversible.

Une nouvelle extension moins restrictive que la discernabilité arrière peut également être proposée. Nous la dénominerons ici la "(λ)–discernabilité arrière".

3.6.2 (λ)–Discernabilité arrière

La propriété de (λ)–discernabilité arrière permet de délivrer à l'instant k, le mode $\sigma(k-\lambda)$, sachant que les modes $\sigma(k-i)$ $(1+\lambda \leq i \leq h)$ ont déjà été estimés. La grandeur λ est un entier tel que $\lambda \in \{0, \cdots, h\}$. Le cas où $\lambda = 0$ permet de considérer la discernabilité arrière alors que $\lambda = h$ correspond à la $(\eta = 0, \omega = h)$–discernabilité. Plus formellement, la (λ)–discernabilité arrière obéit à la définition suivante.

Définition 20 *Un mode actif i est (λ)–discernable en arrière d'un autre mode j, s'il existe un entier λ tel que, pour chaque séquence $\sigma^{h-\lambda} \in \mathcal{J}^{h-\lambda}$ de longueur $h-\lambda$, et pour chaque paire de séquences ${\sigma_1}'$ et ${\sigma_2}'$ de longueur λ, $\sigma^{h-\lambda} i {\sigma_1}'$ est discernable de $\sigma^{h-\lambda} j {\sigma_2}'$.*

À présent, on introduit la notion de (λ)–discernabilité arrière pour le système (3.1).

Définition 21 *Le système (3.1) est (λ)–discernable en arrière si pour chaque paire de modes $(i,j) \in \mathcal{J}^2$, le mode i est (λ)–discernable en arrière du mode j.*

Des conditions garantissant la (λ)–discernabilité arrière sont données d'une manière similaire à celles de la discernabilité arrière.

Proposition 23 *Pour une séquence d'entrée donnée $u_{k-h,k}$, un mode actif i est (λ)–discernables en arrière d'un mode j dans une fenêtre d'observation de longueur $h+1$ pour presque toutes les conditions initiales x_{k-h}, si et seulement si, pour chaque séquence de modes $\sigma^{h-\lambda} \in \mathcal{J}^{h-\lambda}$ de longueur $h-\lambda$, et pour chaque paire de séquences ${\sigma_1}'$ et ${\sigma_2}'$ de longueur λ délivrées par* (3.1)*, au moins l'une des deux conditions suivantes est vérifiée*

$$\Omega_{\sigma^{h-\lambda} j {\sigma_1}'} \mathcal{O}_{\sigma^{h-\lambda} i {\sigma_2}'} \neq \boldsymbol{0} \tag{3.56}$$

$$\Omega_{\sigma^{h-\lambda} j {\sigma_1}'} ((T_{\sigma^{h-\lambda} i {\sigma_2}'} - T_{\sigma^{h-\lambda} j {\sigma_1}'}) u_{k-h,k} + (T'_{\sigma^{h-\lambda} i {\sigma_2}'} - T'_{\sigma^{h-\lambda} j {\sigma_1}'})) \neq \boldsymbol{0} \tag{3.57}$$

Preuve 27 *La preuve est une conséquence directe de la considération à la fois de la définition 20 de la (λ)–discernabilité arrière et de* (3.28)-(3.29) *du Théorème 14.*

Une condition équivalente à (3.56) qui reste vérifiée quelle que soit la structure du détecteur et qui ne nécessite pas le calcul des matrices $\Omega_{\sigma^{h-\lambda} i {\sigma_1}'}$ peut être proposée.

Proposition 24 *La condition* (3.56) *est équivalente à*

$$rang(\begin{bmatrix} \mathcal{O}_{\sigma^{h-\lambda} i {\sigma_1}'} & \mathcal{O}_{\sigma^{h-\lambda} j {\sigma_2}'} \end{bmatrix}) > rang(\mathcal{O}_{\sigma^{h-\lambda} j {\sigma_2}'}) \tag{3.58}$$

Preuve 28 *La preuve est une conséquence directe de la considération à la fois de la Définition 20 de la (λ)–discernabilité arrière et de la Proposition 12 en remplaçant σ_{s_i} par $\sigma^{h-\lambda} i {\sigma_1}'$ et σ_{s_j} par $\sigma^{h-\lambda} j {\sigma_2}'$.*

3.6.3 Estimation récursive

La discernabilité et la $\mathcal{R}$–discernabilité ou la (η,ω)–discernabilité et la $\mathcal{R}(\eta,\omega)$–discernabilité permettent d'estimer toute ou une partie de la séquence active initiale. Avec une approche à horizon glissant, elles permettent d'estimer le reste de la séquence. On parle de l'estimation permanente.

La discernabilité arrière et la (λ)–discernabilité arrière permettent d'estimer un mode spécifique dans une séquence, étant donné que les $h-1$ modes précédents d'une séquence pour la

discernabilité arrière ou les $h-\lambda-1$ modes précédents pour la (λ)–discernabilité arrière ont été déjà estimés. Par conséquent, comme une alternative, une procédure qui nécessite moins de calculs, permettant d'assurer l'estimation permanente après l'estimation de la séquence de modes initiale, peut être dérivée de la discernabilité arrière et la (λ)–discernabilité arrière. Elle est appelée l'estimation récursive et détaillée ci-dessous.

Proposition 25 *Supposons que le système* (3.1) *soit* (λ)*–discernable en arrière. Soit* σ^h *une séquence de longueur* h*. Soit* $\bar{\mathcal{S}}^{\sigma^h} \subset \mathcal{S}$ *l'ensemble des entiers* $s \in \mathcal{S}$ *tel que les séquences* $\sigma^h i$ *diffèrent entre elles pour tout* $i \in \mathcal{J}$*. Le mode actif* $\sigma^*(k)$ *dans l'intervalle de temps* $[k-h,k]$ *est l'unique mode* $\sigma(k)$ *de la séquence* $\sigma_s \in \mathcal{J}^{h+1}$ $(s \in \bar{\mathcal{S}}^{\sigma^h})$ *tel que le résidu correspondant vérifie*

$$r_{h,\sigma_s} = \boldsymbol{0} \tag{3.59}$$

avec

$$r_{h,\sigma_s} = \Omega_{\sigma_s}(y_{k-h,k} - T_{\sigma_s} u_{k-h,k} - T'_{\sigma_s})$$

où Ω_{σ_s} *est la solution de*

$$\Omega_{\sigma_s}\mathcal{O}_{\sigma_s} = \boldsymbol{0}$$

Preuve 29 *La preuve suit le même raisonnement que celui de la preuve de la Proposition 11 excepté que* $s \in \mathcal{S}$ *est remplacé par* $s \in \bar{\mathcal{S}}^{\sigma^h} \subset \mathcal{S}$*, ceci signifie que, pour une sous-séquence donnée* σ^h *de longueur* h*, seules les séquences* $\sigma^h i$ *qui diffèrent entre elles sont considérées.*

La pertinence de la Proposition 25 réside dans le fait que seuls les résidus des séquences $\sigma^h i$ $(i \in \mathcal{J})$ avec $\sigma^h \in \mathcal{J}^h$ résultant de l'estimation à l'instant $k-1$ doivent être testés par le détecteur. Cela permet de réduire considérablement le nombre de tests : J séquences à tester au lieu de J^{h+1} séquences.

Comme une conséquence directe, le corollaire suivant s'applique.

Corollaire 6 *Le mode actif* $\sigma^*(k)$ *est le dernier élément de la séquence* σ_s *qui est solution de* (3.59)*.*

Lorsque la (λ)–discernabilité arrière est satisfaite, l'estimation du mode $\sigma(k-\lambda)$ à l'instant k peut être effectuée selon la proposition suivante.

Proposition 26 *Supposons que le système* (3.1) *soit* (λ)*–discernable en arrière. Soit* $\sigma^{h-\lambda}$ *une séquence de longueur* $h-\lambda$*. Soit* $\bar{\mathcal{S}}^{\sigma^{h-\lambda}} \subset \mathcal{S}$ *l'ensemble des entiers* $s \in \mathcal{S}$ *tels que les séquences* $\sigma^{h-\lambda} i \sigma'_1$ *diffèrent entre elles pour tout* $i \in \mathcal{J}$ *et pour toute séquence* σ'_1 *et* σ'_2 *de longueur* λ*. Le mode actif* $\sigma^*(k-\lambda)$ *dans l'intervalle de temps* $[k-h,k]$ *est l'unique mode* $\sigma(k-\lambda)$ *de la séquence* $\sigma_s \in \mathcal{J}^{h+1}$ $(s \in \bar{\mathcal{S}}^{\sigma^{h-\lambda}})$ *tel que le résidu correspondant vérifie*

$$r_{h,\sigma_s} = \boldsymbol{0} \tag{3.60}$$

avec

$$r_{h,\sigma_s} = \Omega_{\sigma_s}(y_{k-h,k} - T_{\sigma_s} u_{k-h,k} - T'_{\sigma_s})$$

où Ω_{σ_s} *est la solution de*

$$\Omega_{\sigma_s}\mathcal{O}_{\sigma_s} = \boldsymbol{0}$$

Preuve 30 *La preuve suit le même raisonnement que celui de la preuve de la Proposition 11 mis à part que $s \in \mathcal{S}$ est remplacé par $s \in \bar{\mathcal{S}}^{\sigma_{h-\lambda}}$, ceci signifie que, pour une sous-séquence donnée $\sigma^{h-\lambda}$ de longueur $h-\lambda$, seuls les résidus pour lesquels le mode $\sigma(k-\lambda)$ diffère entre elles sont considérés, le reste de la séquence de longueur $\lambda+1$ est ignoré.*

La pertinence de la Proposition 26 réside dans le fait que seuls les résidus correspondant aux séquences $\sigma^{h-\lambda}\sigma'$ ($\sigma' \in \mathcal{J}^{\lambda+1}$) avec $\sigma^{h-\lambda} \in \mathcal{J}^{h-\lambda}$ résultant de l'estimation à l'instant $k-1$ doivent être testés par le détecteur. Cela permet de réduire le nombre de tests : $J^{\lambda+1}$ séquences à tester au lieu de J^{h+1} séquences (rappelons que $\lambda \leq h$).

Comme une conséquence directe, le corollaire suivant s'applique.

Corollaire 7 *Le mode actif $\sigma^*(k)$ est le $h+1-\lambda$ élément de la séquence σ_s qui est solution de* (3.60) *à l'instant $k+\lambda$.*

Remarque 12 *Lorsque la discernabilité arrière ou la (λ)–discernabilité arrière est considérée, une séquence de longueur égale à h ou à $h-\lambda$ respectivement doit être connue pour procéder à l'estimation permanente fondée sur une approche à horizon glissant. Si la discernabilité ou la $\mathcal{R}$–discernabilité est satisfaite, il a été souligné précédemment que la séquence active $\sigma^*_{[0,h]}$ peut être obtenue. D'autre part, si seulement la (η,ω)–discernabilité ou la $\mathcal{R}(\eta,\omega)$–discernabilité est satisfaite, à l'instant $k=h$, seule la sous-séquence active $\sigma^*_{[\eta,h-\omega]}$ dans l'intervalle de temps $[0,h]$ peut être estimée. Par conséquent, l'estimation initiale fondée sur la Proposition 18 ou la Proposition 19 doit être effectuée jusqu'à ce qu'une séquence de longueur égale à h soit estimée si la discernabilité arrière est vérifiée ou de longueur $h-\lambda$ si la (λ)–discernabilité arrière est vérifiée. Finalement, l'estimation permanente peut être effectuée pour $k > h+\omega+\eta-1$.*

3.7 Procédure globale de la détection de mode

Cette section a pour objectif de donner, en récapitulant les résultats précédents, une description détaillée de la procédure globale nécessaire pour l'estimation de mode pour le système (3.1). La procédure est divisée en deux parties : l'estimation de la première séquence appelée estimation initiale. Elle est suivie par l'estimation des séquences restantes, appelée estimation permanente. La détection de modes est réalisée à partir de la connaissance des données Entrée/Sortie dans une fenêtre d'observation de longueur $h+1$. Une telle fenêtre d'observation est décalée dans le temps pour l'estimation permanente. Il s'agit d'une approche à horizon glissant. L'estimation se fait donc en ligne.

Avant de poursuivre, nous rappelons les relations entre les différentes notions de discernabilité qui ont été discutées dans les sections précédentes. Les relations seront utiles pour une meilleure compréhension de la procédure globale. Elles sont présentées dans la Table 3.1.

Remarque 13 *Il est intéressant de souligner que si le système* (3.1) *est (η,ω)–discernable, il peut exister des entiers $\eta' < \eta$ et/ou $\omega' < \omega$ tels que* (3.1) *est $\mathcal{R}(\eta',\omega')$–discernable, et dans un tel cas, une séquence plus longue peut être estimée. Pour cette raison, il n'est pas obligatoire de tester la (η,ω)–discernabilité bien qu'on l'ait impliquée dans la procédure suivante.*

Étapes hors ligne
Étape 1 : horizon de détection h
Trouvez le plus petit entier h tel que (3.26) soit vérifiée.

Discernabilité $\Rightarrow$ $\mathcal{R}$–Discernabilité

Discernabilité $\Rightarrow$ Discernabilité arrière

$(\eta = 0, \omega = 0)$–Discernabilité $\Leftrightarrow$ Discernabilité

(η, ω)–Discernabilité $\Rightarrow$ $\mathcal{R}(\eta, \omega)$–Discernabilité

(0)–Discernabilité arrière $\Leftrightarrow$ Discernabilité arrière

(h)–Discernabilité arrière $\Leftrightarrow$ $(\eta = 0, \omega = h)$–Discernabilité

Discernabilité avant $\Leftrightarrow$ $(\eta = 0, \omega)$–Discernabilité

TABLE 3.1 – Relations entre les notions distinctes de discernabilité

Étape 2 : discernabilité
Vérifier si les conditions (3.28) et (3.29) du Théorème 14 sont satisfaites. Si la discernabilité est vérifiée, aller à l'étape 6. Sinon, aller à la prochaine étape.
Étape 3 : $\mathcal{R}$–discernabilité
Vérifiez si (3.38) est satisfaite. Si le système (3.1) est $\mathcal{R}$–discernable, aller à l'étape 6. Sinon, aller à la prochaine étape.
Step 4 : (η, ω)–discernabilité
Trouvez η et ω tels que (3.40) ou (3.41) de la Proposition 16 soit vérifiée. Les entiers sont initialisés à $\eta = 0$ et $\omega = 1$, ensuite augmentés jusqu'à ce que (3.40) ou (3.41) soit vérifiée. Aller à l'étape suivante.
Étape 5 : $\mathcal{R}(\eta, \omega)$–discernabilité
Trouvez η et ω tels que (3.44) soit satisfaite, les entiers sont initialisés à $\eta = 0$ et $\omega = 1$, ensuite augmentés jusqu'à ce que (3.44) soit vérifié. Ensuite, aller à l'étape suivante.
Étape 6 : discernabilité arrière
- Si la discernabilité (à partir de l'Étape 2) est satisfaite, la discernabilité arrière est automatiquement satisfaite selon la deuxième relation rapportée à la Table 3.1.
- Si la $\mathcal{R}$–discernabilité (à partir de l'Étape 3) ou si la $\mathcal{R}(\eta, \omega)$–discernabilité (à partir de l'Étape 5) est satisfaite, la discernabilité arrière doit être testée. La discernabilité arrière est testée avec (3.47) (ou alternativement avec (3.50)) et (3.48) de la Proposition 20. Si la discernabilité arrière est satisfaite, aller à l'étape 8. Sinon, aller à l'étape suivante.
Étape 7 : (λ)–discernabilité arrière
Vérifiez si (3.56) ou (3.57) de la Proposition 23 est satisfaite. L'entier λ est initialisé à $\lambda = 1$, ensuite augmenté jusqu'à ce que (3.56) ou (3.57) soit satisfaite. Aller à l'étape suivante.
Étapes en ligne
Étape 8 : estimation initiale
- Si le système (3.1) est discernable ou $\mathcal{R}$–discernable, à l'instant $k = h$, la séquence active σ^* dans l'intervalle de temps $[0, h]$ est estimée avec (3.27) de la Proposition 10 ou par (3.39) respectivement. Ensuite, aller à l'étape suivante.
- Si le système (3.1) est (η, ω)–discernable ou $\mathcal{R}(\eta, \omega)$–discernable, à l'instant $k = h$, la sous-séquence $\sigma^*_{[\eta, h-\omega]}$ de la séquence active σ^* est estimée par (3.43) de la Proposition 18 ou par (3.46) de la Proposition 19 respectivement. Ensuite, utiliser (3.43) ou (3.46) jusqu'à ce qu'une

séquence de longueur h ou $h-\lambda$ soit connue selon la Remarque 12. Si aucun η et ω n'est solution, la détection de modes ne peut pas être effectuée.

Étape 9 : estimation permanente

- Si la discernabilité arrière ou la (λ)–discernabilité arrière est satisfaite, l'estimation récursive est effectuée en faisant appel à la Proposition 25 ou à la Proposition 26 respectivement.
- Si ni la discernabilité arrière ni la (λ)–discernabilité arrière n'est satisfaite, utiliser (3.43) ou (3.46) respectivement.

Ces étapes peuvent être résumées dans le diagramme donné sur la Figure 3.1.

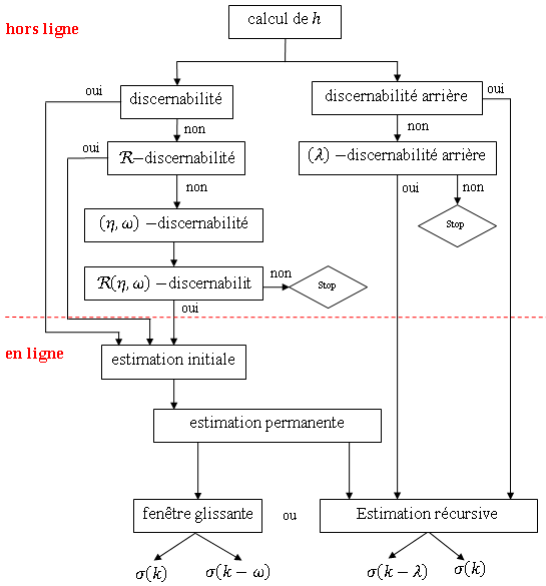


FIGURE 3.1 – Procédure d'estimation de modes

3.8 Exemples

3.8.1 Exemple 1 : estimation de mode pour un système discernable

Cet exemple vise à illustrer l'application de la détection de modes pour un système discernable. Considérons le système affine à commutation à temps discret ayant la forme (3.1), où

$$A_1 = \begin{bmatrix} -0.2 & 0 \\ 0 & 0.5 \end{bmatrix},\ A_2 = \begin{bmatrix} 0.7 & 0 \\ 0 & -0.3 \end{bmatrix},\ A_3 = \begin{bmatrix} 0.2 & 0 \\ 0 & 0.3 \end{bmatrix}$$

$$B_1 = \begin{bmatrix} 1.3 \\ 1 \end{bmatrix}, B_2 = \begin{bmatrix} 0 \\ 2 \end{bmatrix}, B_3 = B_1,\ E_i = \begin{bmatrix} 0.5 \\ 1 \end{bmatrix}$$

$$C_1 = \begin{bmatrix} 1 & 2 \end{bmatrix}, C_2 = \begin{bmatrix} 1 & 3 \end{bmatrix}, C_3 = \begin{bmatrix} 2 & 5 \end{bmatrix}$$

$$D_i = 0 \text{ avec } i \ = \ \sigma(k) \in \{1,\ 2,\ 3\}$$

L'estimation de $\sigma(k)$ est fondée sur le détecteur défini dans la Proposition 11.

Étapes hors ligne

Étape 1 : horizon de détection h
Le plus petit horizon de détection h qui vérifie (3.26) est $h = 2$.
Étape 2 : discernabilité
La discernabilité est testée à l'aide des conditions (3.28) et (3.29). Il s'avère que la discernabilité est vérifiée.
Étape 5 : discernabilité arrière
Étant donné que la discernabilité (à partir de l'Étape 2) est satisfaite, la discernabilité arrière est automatiquement satisfaite selon la deuxième relation indiquée à la Table 3.1.
Étapes en ligne
Étape 8 : estimation initiale
Puisque la discernabilité est vérifiée, à l'instant $k = 2$, la séquence active initiale σ^* dans l'intervalle de temps $[0, 2]$ peut être estimée.
Étape 9 : estimation permanente
Puisque la discernabilité arrière est vérifiée, une approche fondée sur une fenêtre glissante peut être utilisée pour l'estimation permanente. Seuls les résidus des séquences $\sigma^*_{[k-2,k-1]}j$ ($j \in \{1, 2, 3\}$) avec $\sigma^* \in \mathcal{J}^2$ résultant de l'estimation précédente doivent être vérifiés par le détecteur. Cela permet de réduire le nombre de tests : 3 séquences à tester au lieu de $3^3 = 27$ séquences. L'estimation permanente peut être réalisée pour $k > 2$. Le détecteur récupère avec succès le mode inconnu comme représenté sur la Figure 3.2.

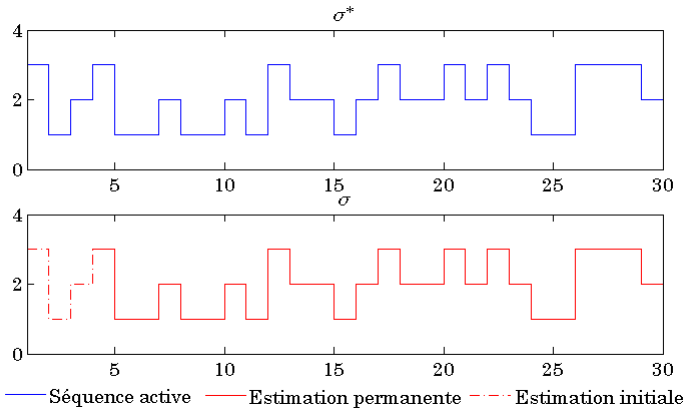


FIGURE 3.2 – Séquence active σ^* et séquence estimée σ

3.8.2 Exemple 2 : illustration de la notion de $\mathcal{R}$–discernabilité

Cet exemple est proposé pour illustrer la notion de $\mathcal{R}$–discernabilité. Considérons le système linéaire à commutation à temps discret ayant la forme (3.1) où

$$A_1 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \; A_2 = \begin{bmatrix} 1 & -0.5 \\ 1 & 0 \end{bmatrix}, \; C_1 = \begin{bmatrix} 2 & 0 \end{bmatrix}$$

$$C_2 = \begin{bmatrix} 1 & 2 \end{bmatrix}, \; E_1 = E_2 = \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \; B_1 = B_2 = \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \; D_1 = D_2 = 0$$

L'estimation de $\sigma(k)$ est fondée sur le détecteur défini dans la Proposition 11.
Étapes hors ligne

Étape 1 : horizon de détection
Le plus petit horizon de détection h qui vérifie (3.26) est $h = 2$.
Étape 2 : discernabilité
Puisque $B_1 = B_2 = \mathbf{0}$ et $E_1 = E_2 = \mathbf{0}$, (3.29) n'est jamais vérifiée selon la Remarque 3. Par conséquent, seul le test (3.28) ou alternativement (3.30) doit être effectué. Le résultat est indiqué dans la Table 3.2. Pour chaque séquence $\sigma_s \in \mathcal{J}^{h+1}$ avec $s \in \mathcal{S}$, les séquences non discernables correspondantes de même longueur, si elles existent, sont présentées sur la même ligne. À partir

Séquence σ_i	Séquences non discernable de σ_i
111	211
112	212
121	aucun
122	aucun
211	aucun
212	aucun
221	aucun
222	aucun

TABLE 3.2 – Séquences discernables

de la Table 3.2, il s'avère que la séquence 111 n'est pas discernable de la séquence 211 et la séquence 112 n'est pas discernable de 212. Par conséquent, le système n'est pas discernable pour $h = 2$ selon la Définition 3.
Étape 3 : $\mathcal{R}$–discernabilité
Puisque $B_1 = B_2 = \mathbf{0}$, et $E_1 = E_2 = 0$ les ensembles $\mathcal{R}_{\sigma_i}$ $(i = 1, \cdots, 8)$ sont construits à l'aide de (3.36). Ils sont $\mathcal{R}_{\sigma_1} = \{111, 211\}, \mathcal{R}_{\sigma_2} = \{112, 212\}, \mathcal{R}_{\sigma_3} = \{121\}, \mathcal{R}_{\sigma_4} = \{122\}, \mathcal{R}_{\sigma_5} = \{211\}, \mathcal{R}_{\sigma_6} = \{212\}, \mathcal{R}_{\sigma_7} = \{221\}, \mathcal{R}_{\sigma_8} = \{222\}$. Il s'avère que (3.38) est satisfaite pour tous $(s_i, s_j) \in \{1, \cdots, 8\} \times \{1, \cdots, 8\}$. Ils sont tous différents. Par conséquent, selon la Définition 13, la $\mathcal{R}$–discernabilité est vérifiée.
Étape 5 : discernabilité arrière
Puisque $B_1 = B_2 = \mathbf{0}$ et $E_1 = E_2 = \mathbf{0}$, la discernabilité arrière doit être testée seulement par (3.47) de la Proposition 20 ou alternativement par (3.50). Il s'avère que la discernabilité arrière est satisfaite.
Étapes en ligne
Étape 8 : estimation initiale
Puisque la $\mathcal{R}$–discernabilité est vérifiée, à l'instant $k = 2$, l'expérience montre que les résidus $r_{h,111}$ et $r_{h,211}$ sont nuls. Ainsi, selon (3.37), $\mathcal{R}_{\sigma^*} = \{111, 211\}$. Après avoir examiné les ensembles $\mathcal{R}_{\sigma_i}$, il s'avère que $\mathcal{R}_{\sigma^*} = \mathcal{R}_{\sigma_1}$, ce qui signifie que la séquence active initiale est $\sigma^*_{[0,2]} = \sigma_1 = 111$.
Étape 9 : estimation permanente
Puisque la discernabilité arrière est vérifiée, une approche fondée sur une fenêtre glissante peut être utilisée pour l'estimation permanente. Seuls les résidus des séquences $\sigma^*_{[k-2,k-1]}j$ $(j \in \{1, 2\})$ résultant de l'estimation à l'instant $k - 1$ doivent être vérifiés par le détecteur. Cela permet de réduire le nombre de tests : 2 séquences à tester au lieu de $2^3 = 8$ séquences. L'estimation permanente peut être réalisée pour $k > 2$ puisque la $\mathcal{R}$–discernabilité est satisfaite. Le détecteur récupère avec succès le mode inconnu comme représenté sur la Figure 3.3.

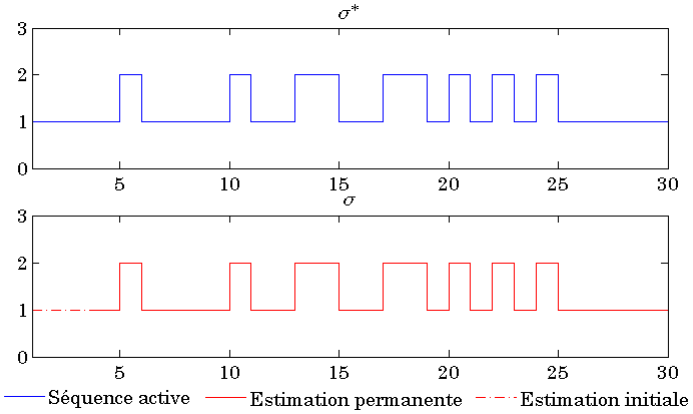


FIGURE 3.3 – Séquence active σ^* et séquence estimée σ

3.8.3 Exemple 3 : illustration des notions de (η, ω)–discernabilité et de $\mathcal{R}(\eta, \omega)$–discernabilité

Le même exemple que le précédent est considéré mis à part que $C_1 = C_2 = [2 \quad 0]$ et $E_1 = E_2 = [1 \quad 0]^T$. L'estimation de $\sigma(k)$ est fondée sur le détecteur défini dans la Proposition 11.

Étapes hors ligne

Étape 1 : horizon de détection

Le plus petit horizon de détection h qui vérifie (3.26) est $h = 2$.

Étape 2 : discernabilité

Puisque $B_1 = B_2 = \mathbf{0}$, $E_1 = E_2$ et $C_1 = C_2$, (3.29) n'est jamais vérifiée selon la Remarque 3. Par conséquent, seulement le test (3.28), ou alternativement (3.30) doit être effectué. Le résultat est indiqué dans la Table 3.3. Pour chaque séquence $\sigma_s \in \mathcal{J}^{h+1}$ avec $s \in \mathcal{S}$, les séquences non discernables correspondantes de même longueur, si elles existent, sont présentées sur la même ligne. À partir de la Table 3.3, il est clair qu'il n'existe aucune séquence qui soit discernable. Par

Séquence σ_i	Séquences non discernables de σ_i
111	112 211 212
112	111 211 212
121	122 221 222
122	121 221 222
211	212
212	211
221	222
222	221

TABLE 3.3 – Séquences discernables

conséquent la système (3.1) n'est pas discernable pour $h = 2$.

Étape 3 : $\mathcal{R}$–discernabilité

Puisque $B_1 = B_2 = \mathbf{0}$, $E_1 = E_2$ et $C_1 = C_2$, les ensembles $\mathcal{R}_{\sigma_i}$ $(i = 1, \ldots, 8)$ sont construits à partir de (3.36). Ils sont $\mathcal{R}_{\sigma_1} = \{111, 112, 211, 212\}$, $\mathcal{R}_{\sigma_2} = \{111, 112, 211, 212\}$, $\mathcal{R}_{\sigma_3} = \{121, 122, 221, 222\}$, $\mathcal{R}_{\sigma_4} = \{121, 122, 221, 222\}$, $\mathcal{R}_{\sigma_5} = \{211, 212\}$, $\mathcal{R}_{\sigma_6} = \{211, 212\}$, $\mathcal{R}_{\sigma_7} =$

$\{221, 222\}, \mathcal{R}_{\sigma_8} = \{221, 222\}$. Il s'avère que (3.38) n'est pas vérifiée pour tous $(s_i, s_j) \in \{1, \cdots, 8\} \times \{1, \cdots, 8\}$ puisque $\mathcal{R}_{\sigma_1} = \mathcal{R}_{\sigma_2}, \mathcal{R}_{\sigma_3} = \mathcal{R}_{\sigma_4}, \mathcal{R}_{\sigma_5} = \mathcal{R}_{\sigma_6}$ et $\mathcal{R}_{\sigma_7} = \mathcal{R}_{\sigma_8}$. Par conséquent, à partir de la Définition 13, on conclut que le système (3.1) n'est pas $\mathcal{R}$–discernable.

Étape 4 : (η, ω)–discernabilité

La propriété de (η, ω)–discernabilité est testée en utilisant (3.40) car (3.41) n'est jamais vérifiée puisque $B_1 = B_2 = \mathbf{0}$, $E_1 = E_2$ et $C_1 = C_2$. À partir de la Table 3.3, il s'avère que (3.40) est satisfaite pour $\eta = 1$ et $\omega = 1$ ce qui implique que la $(1, 1)$–discernabilité est vérifiée. Par conséquent, à l'instant $k = 2$, le détecteur peut délivrer le mode actif $\sigma^*(1)$ de la séquence active initiale. Cependant, le mode $\sigma(0)$ ne peut pas être estimé.

Étape 5 : $\mathcal{R}(\eta, \omega)$–discernabilité

La propriété de la $\mathcal{R}(\eta, \omega)$–discernabilité est testée en utilisant (3.44). Il s'avère que $\mathcal{R}_{\sigma_{s_i}} \neq \mathcal{R}_{\sigma_{s_j}}$ avec $(s_i, s_j) \in \{1, \cdots, 8\} \times \{1, \cdots, 8\}$ tel que $\sigma_{s_i[k-2,k-1]} \neq \sigma_{s_j[k-2,k-1]}$. Par exemple si σ_1 est la séquence active, alors $\mathcal{R}_{\sigma_{s_i}} \neq \mathcal{R}_{\sigma_i}$ avec $i \in \{3, 4, \cdots, 8\}$. Par conséquent, (3.44) est satisfaite pour $\eta = 0$ et $\omega = 1$ ce qui veut dire que le système (3.1) est $\mathcal{R}(0, 1)$–discernable. Ainsi, à l'instant $k = 2$, le détecteur est capable de délivrer la sous-séquence active $\sigma^*_{[0,1]}$ de la séquence active initiale. C'est une illustration de ce qui a été mentionné dans la procédure globale, si la (η, ω)–discernabilité est vérifiée, on peut trouver des entiers $\eta' \leq \eta$ et/ou $\omega' \leq \omega$ tels que la $\mathcal{R}(\eta', \omega')$–discernabilité est vérifiée. Dans cette exemple, $\eta' = 0 < \eta = 1$ et $\omega' = \omega = 1$.

3.9 Conclusion

Une présentation unifiée des méthodes fondées sur le modèle proposées dans la littérature pour les systèmes linéaires et affines à commutation à temps discret a été réalisée. On a procédé à une étude comparative. Les conditions relatives à l'existence de détecteurs ont été assouplies, et de nouvelles conditions relatives à la propriété de discernabilité ont été introduites. Une approche étape-par-étape a été détaillée pour l'estimation de mode.

Le chapitre suivant est consacré à l'application de la détection de modes dans le contexte des communications chaotiques.

Chapitre 4

Applications de la détection de mode

Sommaire

4.1 Introduction

Deux applications de la détection de mode seront examinées dans ce chapitre. Tout d'abord, nous nous intéresserons à l'application de la détection de mode pour la synchronisation des systèmes chaotiques affines à commutation. On a vu au Chapitre 1 et au Chapitre 2 que les observateurs polytopiques constituent une solution pour le déchiffrement de l'information dans le cadre de la modulation paramétrique, la commutation chaotique ou encore la transmission à deux canaux. Pour la méthode par inclusion ce sont des observateurs à entrées inconnues. On supposera ici, pour la synthèse de l'observateur que l'état discret de la loi de commutation n'est pas accessible car dépendant de composantes de l'état continu non mesurées et/ou de l'information à déchiffrer, qui est par définition, non accessible. Notre objectif sera dans un premier temps, d'estimer cette loi de commutation en utilisant une détection de mode qui s'inspire du Chapitre 3, ensuite d'estimer le vecteur d'état continu en faisant appel à des observateurs polytopiques pour assurer la synchronisation du chaos et donc le déchiffrement.

Dans ce chapitre, on proposera également une solution originale fondée sur la détection de mode pour l'estimation du retard dans la méthode de chiffrement par injection du retard.

Le plan de ce chapitre est le suivant. La Section 4.2 est dédiée à l'application de la détection de mode pour la synchronisation des systèmes chaotiques affines à commutation. Ensuite, dans les Sections 4.3 et 4.4, il sera montré comment le problème d'estimation de retards variant dans le temps pour les systèmes affines et les systèmes affines à commutations peut être formulé comme une détection de mode. Les conditions de discernabilité seront alors particularisées. Des exemples illustratifs sont proposés pour chaque application.

4.2 Synchronisation des systèmes chaotiques affines à commutation

4.2.1 Position du problème

Considérons le système chaotique affine à commutation autonome donné par

$$\left\{ \begin{array}{l} x_{k+1} = A_{\sigma(k)} x_k + E_{\sigma(k)} \\ y_k = C_{\sigma(k)} x_k \end{array} \right. \tag{4.1}$$

où $x_k \in \mathbb{R}^n$ est le vecteur d'état, $y_k \in \mathbb{R}^m$ est la sortie. La fonction σ est la loi de commutation définie par $\sigma : \mathbb{N} \to \mathcal{J} = \{1, \ldots, J\}$ qui détermine à chaque instant $k \in \mathbb{N}$, la dynamique affine active parmi les J dynamiques possibles. Les matrices $A_{\sigma(k)} \in \mathbb{R}^{n \times n}$, $C_{\sigma(k)} \in \mathbb{R}^{m \times n}$ et $E_{\sigma(k)} \in \mathbb{R}^{n \times 1}$ sont les matrices de l'espace d'état du système qui appartiennent aux ensembles respectifs $\{A_1, \ldots, A_J\}$, $\{C_1, \ldots, C_J\}$ et $\{E_1, \ldots, E_J\}$.

L'état discret, ou mode, $\sigma(k)$ dépend de l'état continu x_k et/ou de l'information m_k selon la loi

$$\sigma(k) = \left\{ \begin{array}{ll} 1 & \text{si } x_k \in \mathcal{R}_1 \text{ et/ou } m_k \in \mathcal{M}_1 \\ \vdots & \\ J & \text{si } x_k \in \mathcal{R}_J \text{ et/ou } m_k \in \mathcal{M}_J \end{array} \right. \tag{4.2}$$

où $\mathcal{R}_i$ $(i \in \mathcal{J})$ et $\mathcal{M}_i$ $(i \in \mathcal{J})$ sont des régions de $\mathbb{R}^n$ et de $\mathbb{R}^p$ qui forment une partition de l'espace d'état et des messages.

Nous avions supposé jusqu'à présent que le mode actif était connu. On lève ici cette restriction. Cette situation se rencontre lorsqu'on ne peut pas effectuer l'affectation (4.2) du vecteur d'état continu à une région $\mathcal{R}_i$ ou $\mathcal{M}_i$, x_k ou m_k n'étant pas accessible. Afin de reconstruire x_k par un observateur polytopique, nous devons donc d'abord ainsi estimer le mode $\sigma(k)$. À cette fin, nous proposons de faire appel à la détection de mode discutée au Chapitre 3 conformément au schéma illustré sur la Figure 4.1.

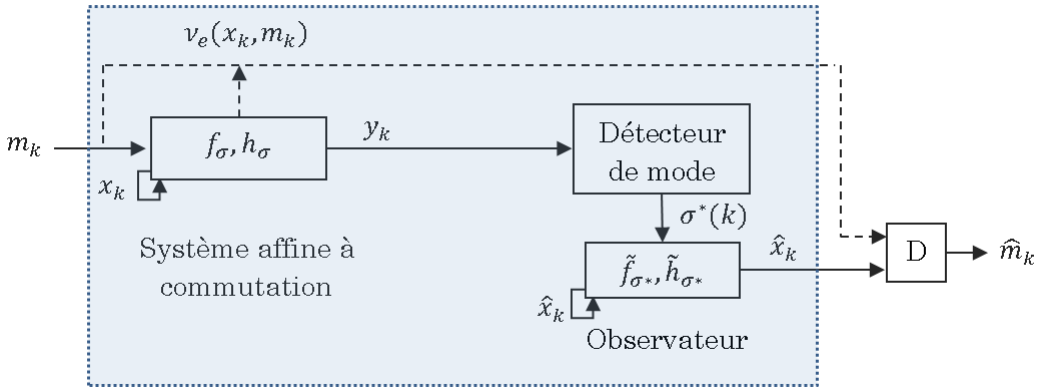


FIGURE 4.1 – Principe général d'un schéma de chiffrement

où D est le module qui délivre $\hat{m}_k$ en fonction de $\hat{x}_k$. Les flèches en pointillées doivent être considérées pour la transmission à deux canaux.
Selon la manière dont est "mélanger" m_k à x_k, le principe général de la Figure 4.1 peut représenter une modulation paramétrique, une commutation chaotique, une transmission à deux canaux ou une méthode par injection.

Dans ce qui suit, on n'intéresse seulement à la synchronisation de x_k et $\hat{x}_k$ (encadré) et non au processus D de récupération de l'information m_k.

Le détecteur utilisé sera celui donné dans la Proposition 11 du Chapitre 3 et la procédure suivra les étapes détaillées dans la Section 3.7.

4.2.2 Exemple

Considérons la récurrence chaotique affine à commutation donnée par

$$\begin{cases} x_{k+1}^{(1)} = -1.7 \left| x_k^{(1)} \right| + x_k^{(2)} + 1 \\ x_{k+1}^{(2)} = \ 0.5 \ x_k^{(1)} \\ \quad y_k = -1.5 \left| x_k^{(1)} \right| + 0.3 \ x_k^{(1)} + \ x_k^{(2)} \end{cases} \tag{4.3}$$

1. **Estimation du mode $\sigma(k)$**
   Le système (4.3) peut être réécrit sous la forme (3.1) où

$$A_1 = \begin{bmatrix} -1.7 & 1 \\ 0.5 & 0 \end{bmatrix},\ A_2 = \begin{bmatrix} 1.7 & 1 \\ 0.5 & 0 \end{bmatrix},\ C_1 = \begin{bmatrix} -1.2 & 1 \end{bmatrix},\ C_2 = \begin{bmatrix} 1.8 & 1 \end{bmatrix}$$

$$E_1 = E_2 = \begin{bmatrix} 1 \\ 0 \end{bmatrix},\ B_1 = B_2 = \begin{bmatrix} 0 \\ 0 \end{bmatrix},\ D_1 = D_2 = 0$$

   avec la loi de commutation $\sigma(k)$ définie comme

$$\sigma(k) = \begin{cases} 1 & \text{si } x_k^{(1)} \geq 0 \\ 2 & \text{si } x_k^{(1)} < 0 \end{cases}$$

   L'estimation de $\sigma(k)$ est fondée sur le détecteur défini dans la Proposition 11 du Chapitre 3 et suit la procédure globale de la Section 3.7.
   Étape 1 : horizon de détection
   Le plus petit horizon de détection h qui vérifie (3.26) est $h = 2$.

   – Estimation initiale
   Étape 2 : discernabilité
   La discernabilité est testée par (3.28) ou alternativement (3.30) et (3.29). Il se trouve que ces conditions sont vérifiées pour chaque séquence $\sigma_s \in \mathcal{J}^3$ avec $s \in \mathcal{S} = \{1, \cdots, 8\}$. Par conséquent, le système est discernable pour $h = 2$ selon la Définition 11 du Chapitre 3 et la première séquence active $\sigma^*_{[0,3]}$ peut être estimée.

   – Estimation permanente avec une approche à horizon glissant
   Étape 6 : discernabilité arrière
   Puisque la discernabilité est vérifiée, la discernabilité arrière est aussi vérifiée. Par conséquent, une approche fondée sur une fenêtre glissante peut être utilisée pour l'estimation permanente. Seuls les résidus des séquences $\sigma^*_{[k-2,k-1]}j$ $(j \in \{1, 2\})$ résultant de l'estimation à l'instant $k-1$ doivent être vérifiés par le détecteur. Cela permet de réduire le nombre de tests : 2 séquences à tester au lieu de $2^3 = 8$ séquences. L'estimation permanente peut être réalisée pour tout $k > 2$.

2. **Estimation de l'état continu x_k**

   Étape 1 : Réécriture du système (4.1) **sous la forme polytopique**.
   Choisissons ρ_k comme le vecteur de paramètre obéissant à

$$\rho_k = \begin{cases} -1 & \text{si } x_k^{(1)} \geq 0 \\ 1 & \text{si } x_k^{(1)} < 0 \end{cases}$$

   Alors, (4.3) peut être réécrite comme un système polytopique de la forme (2.5) conformément aux Remarques 1 et 2 du Chapitre 2.

$$A(\rho_k) = \begin{bmatrix} 1.7\ \rho_k & 1 \\ 0.5 & 0 \end{bmatrix},\ B(\rho_k) = \mathbf{0},\ C(\rho_k) = [1.5\ \rho_k + 0.3 \quad 1]$$

et

$$D(\rho_k) = \mathbf{0}, \quad E(\rho_k) = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

Un tel choix pour ρ_k répond aux conditions de la Proposition 1 du Chapitre 2. En particulier, ρ_k est accessible à partir de la loi de commutation $\sigma(k)$. En effet,

$$\rho_k = \begin{cases} -1 & \text{si } \sigma(k) = 1 \\ 1 & \text{si } \sigma(k) = 2 \end{cases}$$

Étape 2 : Recherche du polytope minimal $\mathcal{D}_\rho$ et de ses sommets
Pour un système défini à commutation, cette étape se réduit à rechercher les sommets. Ils correspondent ici aux deux valeurs prises par ρ_k. Ainsi, on a $\rho_{o_1} = \rho_{min} = -1$ et $\rho_{o_2} = \rho_{max} = 1$.
Étape 3 : Détermination des matrices sommets $A^{(i)}$ et $C^{(i)}$

$$A^{(1)} = \begin{bmatrix} 1.7 & \rho_{min} & 1 \\ 0.5 & & 0 \end{bmatrix} = \begin{bmatrix} -1.7 & 1 \\ 0.5 & 0 \end{bmatrix}$$

$$A^{(2)} = \begin{bmatrix} 1.7 & \rho_{max} & 1 \\ 0.5 & & 0 \end{bmatrix} = \begin{bmatrix} 1.7 & 1 \\ 0.5 & 0 \end{bmatrix}$$

et

$$C^{(1)} = \begin{bmatrix} -1.5 & \rho_{min} + 0.3 & 1 \end{bmatrix} = \begin{bmatrix} -1.2 & 1 \end{bmatrix}$$
$$C^{(2)} = \begin{bmatrix} -1.5 & \rho_{max} + 0.3 & 1 \end{bmatrix} = \begin{bmatrix} 1.8 & 1 \end{bmatrix}$$

$$E^{(1)} = E^{(2)} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

Étape 4 : Calcul des gains $L^{(i)}$
La matrice C dépendant également du paramètre ρ_k, les inégalités matricielles linéaires (2.19) doivent être adaptées conformément à la Remarque 2 du Chapitre 2 et deviennent

$$\begin{bmatrix} P_i & (\bullet)^T \\ G_i A^{(i)} - F_i C_i & G_i^T + G_i - P_j \end{bmatrix} > 0 \tag{4.4}$$

La résolution de ces LMI donnent les gains

$$L^{(1)} = \begin{bmatrix} 1.2419 & -0.2419 \end{bmatrix}^T, \quad L^{(2)} = \begin{bmatrix} 0.9568 & 0.2167 \end{bmatrix}^T$$

Étape 5 : Calcul du vecteur ξ_k
Le vecteur ξ_k pour le système (4.1) est calculé à chaque instant en résolvant l'équation (2.12).

Étape 6 : Calcul du gain $\mathcal{L}(\rho_k)$
Le gain polytopique $\mathcal{L}(\rho_k)$ est donné par (2.16) avec les vecteurs ξ_k et $L^{(i)}$ calculés précédemment.

Étape 7 : Calcul du vecteur $\hat{x}_k$
La reconstruction du vecteur d'état $\hat{x}_k$ est donnée à partir de l'observateur polytopique (2.15), par

$$\begin{cases} \hat{x}_{k+1} = A(\rho_k)\hat{x}_k + E(\rho_k) + \mathcal{L}(\rho_k)(y_k - \hat{y}_k) \\ \hat{y}_k = C(\rho_k)\hat{x}_k \end{cases} \tag{4.5}$$

Puisque la discernabilité est vérifiée, à l'instant $k = 2$, le détecteur délivre la séquence active $\sigma^*_{[0,2]}$ de la séquence active initiale qui permet à l'observateur polytopique de reconstruire l'état continu x_k dans l'intervalle de temps $[0, 2]$. Ensuite, pour l'estimation permanente ($k > 2$), puisque la discernabilité arrière est vérifiée, à chaque instant k, le détecteur délivre le mode actif $\sigma^*(k)$, ce qui permet à l'observateur polytopique de reconstruire le vecteur d'état x_k. La reconstruction du mode inconnu est illustrée sur la Figure 4.2 et l'erreur de reconstruction du vecteur d'état x_k est illustrée sur la Figure 4.3.

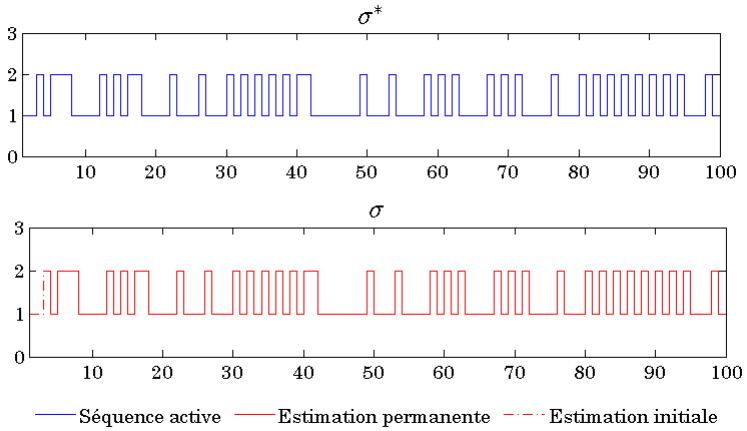


FIGURE 4.2 – Séquence active σ^* et séquence estimée σ

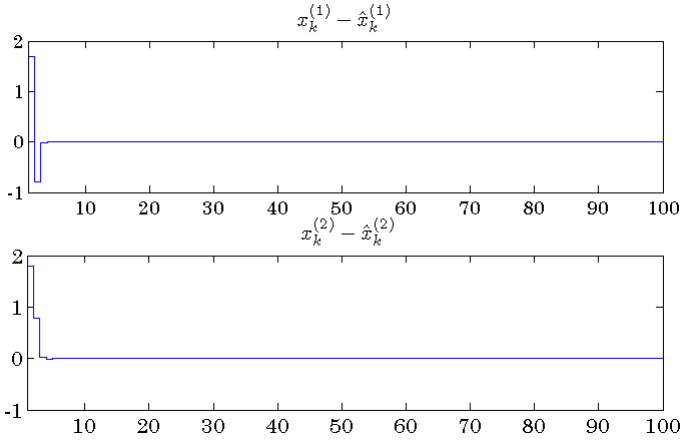


FIGURE 4.3 – Erreur de reconstruction de l'état continu

4.3 Estimation de retards variables pour les systèmes affines

On montre dans cette section que l'estimation de retards variables pour les systèmes affines peut être reformulée comme un problème de détection spécifique de mode. On étudie ensuite le problème de la discernabilité liée à cette spécificité. Les résultats établis dans cette section présentent un intérêt général du point de vue de l'automatique. Ils présentent un intérêt dans le

contexte du chiffrement chaotique lorsqu'ils seront étendus aux systèmes affines à commutation dans la Section 4.4.

4.3.1 Formulation hybride de l'estimation

Considérons le système affine à commutation à retard à temps discret donné par

$$\begin{cases} X_{k+1} = \mathcal{A}X_k + \mathcal{G}X_{k-\tau(k)} + \mathcal{B}U_{k-\tau'(k)} + \mathcal{E} \\ Y_k = \mathcal{C}X_k + \mathcal{D}U_k \end{cases} \tag{4.6}$$

où $k \in \mathbb{N}$ est le nombre naturel représentant le temps discret, $X_k \in \mathbb{R}^N$ est le vecteur d'état, $Y_k \in \mathbb{R}^M$ est la sortie, $U_k \in \mathbb{R}^P$ est l'entrée. Les matrices $\mathcal{A} \in \mathbb{R}^{N\times N}$, $\mathcal{G} \in \mathbb{R}^{N\times N}$, $\mathcal{B} \in \mathbb{R}^{N\times P}$, $\mathcal{C} \in \mathbb{R}^{M\times N}$, $\mathcal{D} \in \mathbb{R}^{M\times P}$ et $\mathcal{E} \in \mathbb{R}^{N\times 1}$ sont les matrices états. Les quantités $\tau(k)$ et $\tau'(k)$ sont les retards variant dans le temps associées respectivement au vecteur d'état et à l'entrée. Elles prennent des valeurs dans les ensembles finis respectifs $\mathcal{T} = \{0, 1, \cdots, \alpha\}$ et $\mathcal{T}' = \{0, 1, \cdots, \alpha'\}$. La variation de $\tau(k)$ et $\tau'(k)$ est supposée arbitraire. Le cas où $\tau(k)$ et $\tau'(k)$ ne sont pas directement accessibles est considéré. Par conséquent, l'objectif est d'estimer $\tau(k)$ et $\tau'(k)$ tandis que le modèle, les séquences U_k et Y_k sont supposées être connues et accessibles en ligne.

L'idée centrale de l'approche proposée pour l'estimation est de reformuler le problème comme un problème de détection de mode pour les systèmes affines à commutation. En effet, le même raisonnement que celui suggéré dans [Nikolakopoulos et al., 2005] [Tzes et al., 2005] [Hetel et al., 2008], pour des buts totalement différents, peut être suivi. L'approche consiste à réécrire le système (4.6) de la façon suivante.

Soit σ une fonction définie par $\sigma : \mathbb{N} \to \mathcal{J}$ qui, à chaque instant k, identifie de manière unique $(\tau(k), \tau'(k)) \in \mathcal{T} \times \mathcal{T}'$ avec la correspondance suivante $(\tau(k), \tau'(k)) = (0, 0) \leftrightarrow \sigma(k) = 1$, $(\tau(k), \tau'(k)) = (0, 1) \leftrightarrow \sigma(k) = 2$, ..., $(\tau(k), \tau'(k)) = (0, \alpha') \leftrightarrow \sigma(k) = \alpha' + 1$, $(\tau(k), \tau'(k)) = (1, 0) \leftrightarrow \sigma(k) = \alpha' + 2$, $(\tau(k), \tau'(k)) = (\alpha, 1) \leftrightarrow \sigma(k) = \alpha \cdot \alpha' + 1$, ..., $(\tau(k), \tau'(k)) = (\alpha, \alpha') \leftrightarrow \sigma(k) = (\alpha + 1) \cdot (\alpha' + 1)$. On pourra être amené dans la suite à écrire, sans aucune confusion, une séquence de mode $\sigma_s = \sigma(k)\sigma(k + 1) \ldots \sigma(k + h)$ ou $\sigma_s = (\tau(k), \tau'(k))(\tau(k + 1), \tau'(k + 1)) \ldots (\tau(k + h), \tau'(k + h))$. Finalement, on définit

$$x_k = \begin{bmatrix} X_k \\ X_{k-1} \\ X_{k-2} \\ \vdots \\ X_{k-\alpha} \end{bmatrix}, \quad u_k = \begin{bmatrix} U_k \\ U_{k-1} \\ U_{k-2} \\ \vdots \\ U_{k-\alpha'} \end{bmatrix}, \quad y_k = Y_k \tag{4.7}$$

Le système (4.6) peut être réécrit, d'une manière équivalente, sous la forme du système affine à commutation donné par (3.1)

$$\begin{cases} x_{k+1} = A_{\sigma(k)}x_k + B_{\sigma(k)}u_k + E_{\sigma(k)} \\ y_k = C_{\sigma(k)}x_k + D_{\sigma(k)}u_k \end{cases}$$

avec $n = (\alpha + 1)N$, $p = (\alpha' + 1)P$, $m = M$, une loi de commutation σ avec $J = (\alpha + 1)(\alpha' + 1)$

modes et les matrices d'état obéissant à la construction suivante

$$A_{\sigma(k)} = \begin{bmatrix} \mathcal{A}+\kappa(\tau(k))\mathcal{G} & \psi_1(\tau(k)) & \cdots & \psi_\alpha(\tau(k)) \\ \mathbf{1} & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \cdots & \mathbf{0} \\ \vdots & & \cdots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots\ \mathbf{1} & \mathbf{0} \end{bmatrix}$$

$$B_{\sigma(k)} = \begin{bmatrix} \psi'_0(\tau'(k)) & \psi'_1(\tau'(k)) & \cdots & \psi'_\alpha(\tau'(k)) \\ \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} \end{bmatrix}$$

$$E_{\sigma(k)} = \begin{bmatrix} \mathcal{E} \\ \mathbf{0} \end{bmatrix}, C_{\sigma(k)} = \begin{bmatrix} \mathcal{C} & \mathbf{0} \end{bmatrix}, D_{\sigma(k)} = \begin{bmatrix} \mathcal{D} & \mathbf{0} \end{bmatrix}$$

où κ est défini comme

$$\kappa(\tau(k)) = \begin{cases} 1 \text{ si } \tau(k) = 0 \\ 0 \text{ si } \tau(k) \neq 0 \end{cases}$$

ψ_i est défini pour $i = 1, \ldots, \alpha$ comme

$$\psi_i(\tau(k)) = \begin{cases} \mathcal{G} \text{ si } \tau(k) = i \\ \mathbf{0} \text{ si } \tau(k) \neq i \end{cases}$$

Finalement, ψ'_i est défini pour $i = 0, \ldots, \alpha$ comme

$$\psi'_i(\tau'(k)) = \begin{cases} \mathcal{B} & \text{si } \tau'(k) = i \\ \mathbf{0} & \text{si } \tau'(k) \neq i \end{cases}$$

Pour clarifier cette construction, considérons par exemple le système (4.6) avec $\tau(k) \in \{0, 1, 2\}$ et $\tau'(k) = 0$. Il peut être réécrit sous la forme (3.1) avec

$$x_k = \begin{bmatrix} X_k \\ X_{k-1} \\ X_{k-2} \end{bmatrix}, \quad u_k = U_k, \quad y_k = Y_k$$

et la loi de commutation σ a 3 modes.

$$A_0 = \begin{bmatrix} \mathcal{A}+\mathcal{G} & \mathbf{0} & \mathbf{0} \\ \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} \end{bmatrix}, \; A_1 = \begin{bmatrix} \mathcal{A} & \mathcal{G} & \mathbf{0} \\ \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} \end{bmatrix}, \; A_2 = \begin{bmatrix} \mathcal{A} & \mathbf{0} & \mathcal{G} \\ \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} \end{bmatrix}$$

$$B_i = \begin{bmatrix} \mathcal{B} \\ \mathbf{0} \\ \mathbf{0} \end{bmatrix}, E_i = \begin{bmatrix} \mathcal{E} \\ \mathbf{0} \\ \mathbf{0} \end{bmatrix},$$

$$C_i = \begin{bmatrix} \mathcal{C} & \mathbf{0} & \mathbf{0} \end{bmatrix}, \; D_i = 0 \quad i \in \{0, 1, 2\}$$

où $\sigma(k) = 1$ identifie $(\tau(k), \tau'(k)) = (0, 0)$, $\sigma(k) = 2$ identifie $(\tau(k), \tau'(k)) = (1, 0)$ et $\sigma(k) = 3$ identifie $(\tau(k), \tau'(k)) = (2, 0)$.

Ainsi, il est à présent clair que l'estimation de $\tau(k)$ et $\tau'(k)$ de (4.6) revient à estimer le mode $\sigma(k)$ de (3.1). Par conséquent, nous pouvons recourir au travail présenté dans le Chapitre 3. Cependant, la spécificité du problème doit être prise en compte car les matrices d'état ne sont pas arbitraires mais ont une structure spéciale. Plus précisément, le détecteur défini dans la Proposition 11 du Chapitre 3 étant considéré, nous étudierons dans la sous-section suivante la notion de discernabilité dans ce contexte. On rappelle que la discernabilité est en rapport avec la question d'unicité de la solution délivrée par le détecteur.

4.3.2 Unicité : spécificité des systèmes à retards

À cause de la restriction due à la structure spécifique des matrice d'état de (4.6), on peut s'attendre à ce que certaines propriétés de discernabilité ne soient plus vérifiées. C'est précisément ce qui est montré dans ce qui suit. Toutes les preuves sont fondées sur la recherche de séquences particulières pour lesquelles les propriétés ne sont pas satisfaites.

4.3.2.1 Discernabilité

Proposition 27 *Pour le système* (4.6)*, la discernabilité, la $\mathcal{R}$–discernabilité et la discernabilité arrière ne sont pas vérifiées.*

Preuve 31 *Considérons les deux séquences particulières $\sigma_{s_1} = \sigma_{s[k-h,k-1]}i$ et $\sigma_{s_2} = \sigma_{s[k-h,k-1]}j$ avec $i \neq j \in \mathcal{J}$. Pour* (4.6)*, les matrices $C_{\sigma(k)}$ et $D_{\sigma(k)}$ ne dépendent pas de $\sigma(k)$. Par conséquent, les matrices $\mathcal{O}$, T, et T' telles que définies dans (3.2) dépendent uniquement de $\sigma_{[k-h,k-1]}$. En outre*

$$T_{\sigma_{s_1}} = T_{\sigma_{s_2}}, \quad T'_{\sigma_{s_1}} = T'_{\sigma_{s_2}}$$

ce qui implique que (3.29) n'est pas vérifiée.
D'autre part

$$\mathcal{O}_{\sigma_{s_1}} = \mathcal{O}_{\sigma_{s_2}}$$

ce qui implique que (3.28) n'est pas vérifiée. Cela implique aussi que

$$\mathcal{R}_{\sigma_{s_1}} = \mathcal{R}_{\sigma_{s_2}}$$

pour tous $(s_1, s_2) \in \mathcal{S}^2$ et donc, la $\mathcal{R}$–discernabilité n'est pas vérifiée d'après la Définition 13 du Chapitre 3. Finalement, puisque la discernabilité arrière est un cas particulier de la discernabilité, et puisque la discernabilité arrière n'est pas vérifiée, la discernabilité n'est pas vérifiée non plus. Ceci achève la preuve.

Puisque ni la discernabilité ni la discernabilité arrière ne sont vérifiées, la totalité de la séquence active $\sigma_{s[k-h,k]}$ ne peut pas être estimée. Nous nous intéresserons donc à la propriété moins restrictive, à savoir la (η, ω)–discernabilité. Nous rappelons que cette propriété reflète la capacité de discrimination, et donc d'estimation, des sous-séquences $\sigma_{s[k-h+\eta,k-\omega]}$ pour $\eta > 0$ et/ou $\omega > 0$.

4.3.2.2 (η, ω)–Discernabilité

Proposition 28 *Le système* (4.6) *n'est pas* $(0, 1)$*–discernable.*

Preuve 32 *La $(\eta = 0, \omega = 1)$–discernabilité n'est pas satisfaite, si et seulement si, ni (3.40) ni (3.41) dans la Proposition 16 du Chapitre 3 n'est vérifiée.*
Considérons les deux séquences particulières $\sigma_{s_1} = (0,0)(0,0)\cdots(0,0)$ et $\sigma_{s_2} = (1,0)\ (0,0)\cdots(0,0)$

de longueur $h+1$. Notons que la condition $\sigma_{s_1[k-h,k-1]} \neq \sigma_{s_2[k-h,k-1]}$ requise dans la Proposition 16 est satisfaite. Les matrices d'observabilité respectives notées $\mathcal{O}_{\sigma_{s_1}}$ et $\mathcal{O}_{\sigma_{s_2}}$ sont

$$\mathcal{O}_{\sigma_{s_1}} = \begin{bmatrix} C_{(0,0)} \\ C_{(0,0)}A_{(0,0)} \\ \vdots \\ C_{(0,0)}{A_{(0,0)}}^h \end{bmatrix} = \begin{bmatrix} \mathcal{C} & \boldsymbol{0} & \cdots & \boldsymbol{0} \\ \mathcal{C}(\mathcal{A}+\mathcal{G}) & \boldsymbol{0} & \cdots & \boldsymbol{0} \\ \mathcal{C}(\mathcal{A}+\mathcal{G})^2 & \boldsymbol{0} & \cdots & \boldsymbol{0} \\ \vdots & \vdots & & \vdots \\ \mathcal{C}(\mathcal{A}+\mathcal{G})^h & \boldsymbol{0} & \cdots & \boldsymbol{0} \end{bmatrix}$$

$$\mathcal{O}_{\sigma_{s_2}} = \begin{bmatrix} C_{(1,0)} \\ C_{(0,0)}A_{(1,0)} \\ \vdots \\ C_{(0,0)}{A_{(0,0)}}^{h-1}A_{(1,0)} \end{bmatrix} = \begin{bmatrix} \mathcal{C} & \boldsymbol{0} & \boldsymbol{0} & \cdots & \boldsymbol{0} \\ \mathcal{C}\mathcal{A} & \mathcal{C}\mathcal{G} & \boldsymbol{0} & \cdots & \boldsymbol{0} \\ \mathcal{C}(\mathcal{A}+\mathcal{G})\mathcal{A} & \mathcal{C}(\mathcal{A}+\mathcal{G})\mathcal{G} & \boldsymbol{0} & \cdots & \boldsymbol{0} \\ \vdots & \vdots & \vdots & & \vdots \\ \mathcal{C}(\mathcal{A}+\mathcal{G})^{h-1}\mathcal{A} & \mathcal{C}(\mathcal{A}+\mathcal{G})^{h-1}\mathcal{G} & \boldsymbol{0} & \cdots & \boldsymbol{0} \end{bmatrix}$$

Notons V_1 la première colonne de $\mathcal{O}_{\sigma_{s_1}}$, et V_2, V_2' la première et la deuxième colonne de $\mathcal{O}_{\sigma_{s_2}}$ respectivement. Il apparaît clairement que $V_1 = V_2 + V_2'$. En conséquence,

$$rank([\mathcal{O}_{\sigma_{s_1}} \quad \mathcal{O}_{\sigma_{s_2}}]) = rank(\mathcal{O}_{\sigma_{s_2}}) \tag{4.8}$$

Conformément au Corollaire 2 du Chapitre 3, (4.8) est équivalente à

$$\Omega_{\sigma_{s_2}}\mathcal{O}_{\sigma_{s_1}} = \boldsymbol{0}$$

D'autre part, puisque $D_{\sigma(k)}$, $B_{\sigma(k)}$ et $E_{\sigma(k)}$ ne dépendent pas de $\tau(k)$, on a $D_{(0,0)} = D_{(1,0)}$, $B_{(0,0)} = B_{(1,0)}$ et $E_{(0,0)} = E_{(1,0)}$. En conséquence, à partir de la définition de T et de T' donnée dans (3.2), on a

$$T_{\sigma_{s_1}} = T_{\sigma_{s_2}} \quad et \quad T'_{\sigma_{s_1}} = T'_{\sigma_{s_2}}$$

ce qui implique que

$$\Omega_{\sigma_{s_2}}((T_{\sigma_{s_1}} - T_{\sigma_{s_2}})u_{k-h,k} + (T'_{\sigma_{s_1}} - T'_{\sigma_{s_2}})) = \boldsymbol{0}$$

Par conséquent, à partir de (3.40) et (3.41), on en déduit que la Proposition 16 du Chapitre 3 n'est pas satisfaite et la séquence σ_{s_1} n'est pas $(0,1)$–discernable de σ_{s_2}. Cela achève la preuve.

4.3.2.3 (λ)–discernabilité arrière

Proposition 29 *Si U_k reste constant entre deux instants consécutifs k et $k+1$, le système (4.6) n'est pas $(\lambda = 1)$–discernable en arrière.*

Preuve 33 *Considérons la séquence $\sigma_{s_3} = \sigma^{h-\lambda}i(0,0)$ et $\sigma_{s_4} = \sigma^{h-\lambda}j(0,0)$ de longueur $h+1$ avec $\sigma^{h-\lambda} = (0,0)(0,0)\cdots(0,0)$, $i = (0,0)$ et $j = (0,1)$. Il suffit de montrer que les conditions (3.56) et (3.57) de la Proposition 23 du Chapitre 3 ne sont pas vérifiées pour σ_{s_3} et σ_{s_4}.*
Pour les deux séquences σ_{s_3} et σ_{s_4}, il s'avère que $\tau(k) = 0$ pour tout $k \in \mathbb{N}$. Puisque la matrice d'observabilité $\mathcal{O}_{\sigma_{[k-h,k]}}$ dépend exclusivement de $\tau(k)$, $\mathcal{O}_{\sigma_{s_3}} = \mathcal{O}_{\sigma_{s_4}}$ et donc $ker(\mathcal{O}_{\sigma_{s_3}}) = ker(\mathcal{O}_{\sigma_{s_4}})$ ce qui implique que

$$\Omega_{\sigma_{s_4}}\mathcal{O}_{\sigma_{s_3}} = \boldsymbol{0} \tag{4.9}$$

D'autre part, il s'avère que $A_{(0,0)} = A_{(0,1)}$, $D_{(0,0)} = D_{(0,1)}$ *et* $E_{(0,0)} = E_{(0,1)}$ *ne dépendent pas de* $\tau'(k)$. *À partir de la définition de* T *et* T' *donnée dans (3.2), on trouve que* $T'_{\sigma_{s_3}} = T'_{\sigma_{s_4}}$. *L'équation (3.29) devient*

$$\Omega_{\sigma_{s_4}}((T_{\sigma_{s_3}} - T_{\sigma_{s_4}})u_{k-h,k}) \neq \boldsymbol{0} \tag{4.10}$$

avec

$$T_{\sigma_{s_3}} - T_{\sigma_{s_4}} = \begin{bmatrix} \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} \\ \vdots & \vdots & \vdots \\ \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} \\ \boldsymbol{0} & C(B_{(0,0)} - B_{(0,1)}) & \boldsymbol{0} \end{bmatrix}$$

En tenant compte de la structure des matrices C *et* $B_{\sigma(k)}$, *nous obtenons*

$$T_{\sigma_{s_3}} - T_{\sigma_{s_4}} = \begin{bmatrix} \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} \\ \vdots & \vdots & \vdots & \vdots \\ \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} \\ \boldsymbol{0} & \mathcal{CB} & -\mathcal{CB} & \boldsymbol{0} \end{bmatrix}$$

En remplaçant $T_{\sigma_{s_3}} - T_{\sigma_{s_4}}$ *dans (4.10) nous obtenons*

$$\Omega_{\sigma_{s_4}} \begin{bmatrix} \boldsymbol{0} & \mathcal{CB}U_{k-1} - \mathcal{CB}U_{k-2} \end{bmatrix}^T \neq \boldsymbol{0} \tag{4.11}$$

Par conséquent, si $U_{k-1} = U_{k-2}$, *à partir de* (4.9) *et* (4.11), *nous en déduisons que ni (3.56) ni (3.57) de la Proposition 23 du Chapitre 3 n'est satisfaite et la séquence* σ_{s_3} *n'est pas* $(\lambda = 1)$*–discernable arrière de* σ_{s_4}. *Cela achève la preuve.*

Il est intéressant de souligner que les considérations sur l'entrée pour décider de la discernabilité sont conformes au concept d'"observabilité active" comme souligné dans la Remarque 8 du Chapitre 3.

4.3.3 Procédure globale d'estimation de retard

1. Formulation hybride

– Réécriture du système (4.6) sous la forme (3.1).

2. Estimation du retard $\tau(k)$

– Les étapes sont résumées dans la Section 3.7 du Chapitre 3. Cependant, il a été démontré à la Section 4.3.2 que (4.6) n'est pas
  – discernable, $\mathcal{R}$–discernable ni discernable en arrière
  – $(0,1)$–discernable
  – (1)–discernable en arrière lorsque l'entrée reste constante entre deux instants consécutifs k et $k+1$

  Par conséquent, l'estimation du retard $\tau(k)$, et donc du mode $\sigma(k)$, est effectuée grâce à la procédure globale donnée dans la Section 3.7 excepté que l'Étape 2, l'Étape 3, l'Étape 6 et l'Étape 7 avec $\lambda = 1$ peuvent être ignorées. L'algorithme correspondant est donné sur la Figure 4.4.

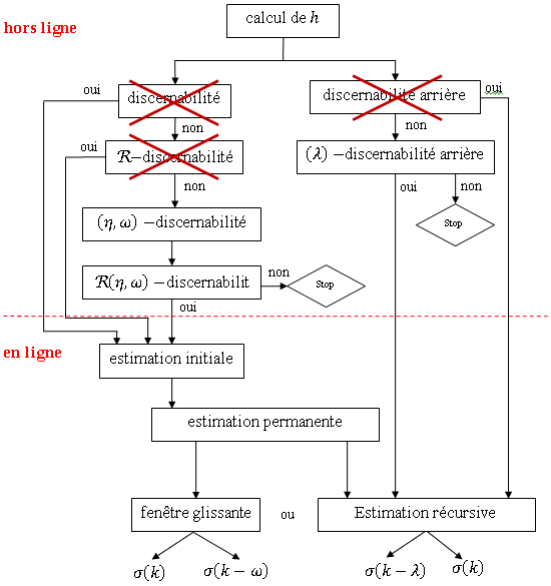


FIGURE 4.4 – Procédure d'estimation de modes pour les systèmes à retards

4.3.4 Exemple illustratif

Considérons le système donné par (4.6) avec

$$\mathcal{A} = \begin{bmatrix} -0.21 & 0.1 \\ 0 & 1; \end{bmatrix}, \quad \mathcal{G} = \begin{bmatrix} 0.25 & 0 \\ 0 & -0.21 \end{bmatrix}, \quad \mathcal{B} = \begin{bmatrix} 1.5 & 0 \\ 1 & 0.8 \end{bmatrix}, \quad \mathcal{C} = \begin{bmatrix} 1 & 3 \\ 2.5 & 0 \end{bmatrix},$$

$$\mathcal{E} = \begin{bmatrix} 1 \\ 0.3 \end{bmatrix}, \quad \mathcal{D} = \mathbf{0}$$

Les retards vérifient $\tau(k) \in \{0, 1, 2\}$, $\alpha' = 0$.

1. Formulation hybride

Ce système linéaire à retard à temps discret est réécrit sous la forme (3.1) avec

$$x_k = \begin{bmatrix} X_k \\ X_{k-1} \\ X_{k-2} \end{bmatrix}, \quad u_k = U_k, \quad y_k = Y_k$$

et la loi de commutation σ a 3 modes.

$$A_0 = \begin{bmatrix} \mathcal{A}+\mathcal{G} & \mathbf{0} & \mathbf{0} \\ \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} \end{bmatrix}, \; A_1 = \begin{bmatrix} \mathcal{A} & \mathcal{G} & \mathbf{0} \\ \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} \end{bmatrix}, \; A_2 = \begin{bmatrix} \mathcal{A} & \mathbf{0} & \mathcal{G} \\ \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} \end{bmatrix}$$

$$B_i = \begin{bmatrix} \mathcal{B} \\ \mathbf{0} \\ \mathbf{0} \end{bmatrix}, E_i = \begin{bmatrix} \mathcal{E} \\ \mathbf{0} \\ \mathbf{0} \end{bmatrix},$$

$$C_i = \begin{bmatrix} \mathcal{C} & \mathbf{0} & \mathbf{0} \end{bmatrix}, \; D_i = 0 \quad i \in \{0, 1, 2\}$$

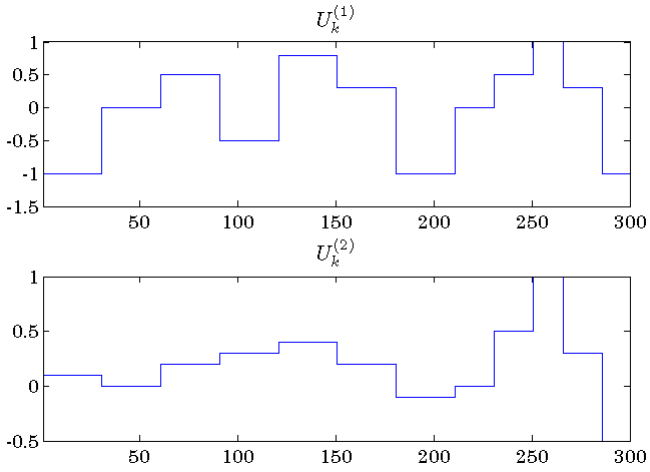


FIGURE 4.5 – Séquence d'entrée u_k

2. Estimation du retard $\tau(k)$

Étape 1 : horizon de détection

Le plus petit horizon de détection h qui satisfait (3.26) est $h = 3$.

– Estimation initiale

Étant donné que la discernabilité et la $\mathcal{R}$–discernabilité ne sont pas vérifiées pour (4.6), comme précédemment indiqué dans la Section 4.3.3, l'Étape 2 et l'Étape 3 de la procédure globale sont ignorées et la séquence $\sigma^*_{[0,3]}$ ne peut pas être estimée dans sa totalité.

Étape 4 : (η, ω)–discernabilité

La propriété de (η, ω)–discernabilité est vérifiée à l'aide de (3.40) ou (3.41) de la Proposition 16 du Chapitre 3. Après avoir effectué le test, il s'avère que (3.40) ou (3.41) sont satisfaites pour $\eta = 2$ et $\omega = 1$ ce qui signifie que la $(2, 1)$–discernabilité est vérifiée. Par conséquent, à l'instant $k = 3$, le détecteur est en mesure de fournir $\sigma^*(2)$. La première sous-séquence $\sigma_{[0,1]}$ ne peut pas être estimée.

Étape 5 : $\mathcal{R}(\eta, \omega)$–discernabilité

La propriété de $\mathcal{R}(\eta, \omega)$–discernabilité est vérifiée à l'aide de (3.44). Après avoir effectué le test, il s'avère que (3.44) est satisfaite pour $\eta = 1$ et $\omega = 1$ ce qui signifie que la $\mathcal{R}(1, 1)$–discernabilité est vérifiée. Par conséquent, à l'instant $k = 3$, le détecteur est en mesure de fournir la sous-séquence active $\sigma^*_{[1,2]}$ plus longue qu'avec la (η, ω)–discernabilité conformément à la Remarque 13. Le premier mode $\sigma(0)$ ne peut pas être estimé, ce qui explique l'erreur au début de l'estimation comme le montre la Figure 4.6.

– Estimation permanente

Étape 7 : (λ)–discernabilité arrière

Les conditions (3.56) et (3.57) sont testées. Puisque au moins une des conditions est vérifiée, car il s'avère en effet que (3.56) est satisfaite pour $\lambda = 1$, l'estimation permanente peut être effectuée. Le détecteur peut délivrer le mode actif $\sigma^*(k-1)$ lorsque $k > h + \omega + \eta - \lambda - 1 = 3$.

Finalement, le détecteur récupère avec succès le retard inconnu pour $k > 0$ comme représenté sur la Figure 4.6, la séquence d'entrées u_k étant donné dans la Figure 4.5.

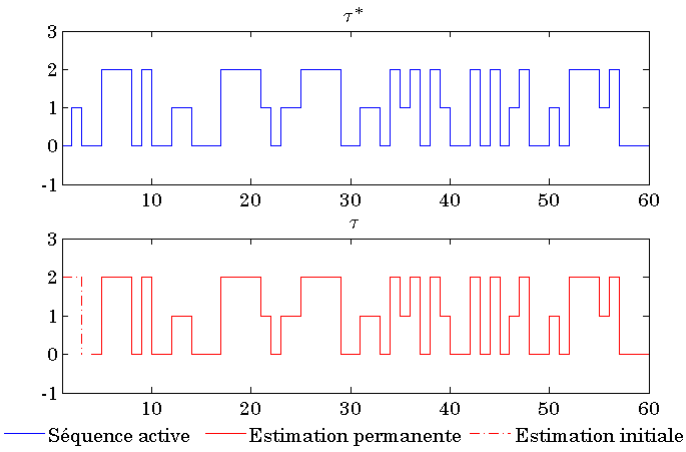


FIGURE 4.6 – Séquence active τ^* et séquence estimée τ

4.4 Estimation de retards variables pour les systèmes affines à commutation

On montre dans cette section que l'estimation de retards variables traitée dans la Section 4.3 pour les systèmes affines peut être étendue aux systèmes affines à commutation. Cette extension est importante car elle permet d'apporter une solution au problème de la récupération de l'information dans le cadre du chiffrement chaotique par injection du retard. Soulignons en effet qu'un système linéaire, même à retard ne peut pas exhiber de dynamique chaotique et ne peut donc pas être utilisé pour le chiffrement. Un exemple illustratif sera proposé dans cette section.

4.4.1 Formulation hybride de l'estimation

Considérons le système affine à commutation à retard à temps discret donné par

$$\begin{cases} X_{k+1} = \mathcal{A}_{\gamma(k)} X_k + \mathcal{G}_{\gamma(k)} X_{k-\tau(k)} + \mathcal{B}_{\gamma(k)} U_{k-\tau'(k)} + \mathcal{E}_{\gamma(k)} \\ Y_k = \mathcal{C} X_k + \mathcal{D} U_k \end{cases} \tag{4.12}$$

où $k \in \mathbb{N}$ est le nombre naturel représentant le temps discret, $X_k \in \mathbb{R}^N$ est le vecteur d'état, $Y_k \in \mathbb{R}^M$ est la sortie, $U_k \in \mathbb{R}^P$ est l'entrée. Les matrices $\mathcal{A}_{\gamma(k)} \in \mathbb{R}^{N\times N}$, $\mathcal{G}_{\gamma(k)} \in \mathbb{R}^{N\times N}$, $\mathcal{B}_{\gamma(k)} \in \mathbb{R}^{N\times P}$, $\mathcal{C} \in \mathbb{R}^{M\times N}$, $\mathcal{D} \in \mathbb{R}^{M\times P}$ et $\mathcal{E}_{\gamma(k)} \in \mathbb{R}^{N\times 1}$ sont les matrices états. La quantité $\gamma(k)$ est la loi de commutation appartenant à l'ensemble fini $\gamma(k) \in \mathcal{J}' = \{1, \cdots, J'\}$. Les quantités $\tau(k)$ et $\tau'(k)$ sont les retards variant dans le temps associés respectivement au vecteur d'état et à l'entrée. Elles prennent des valeurs dans les ensembles finis respectifs $\mathcal{T} = \{0, 1, \cdots, \alpha\}$ et $\mathcal{T}' = \{0, 1, \cdots, \alpha'\}$. La variation de $\tau(k)$ et $\tau'(k)$ est supposée arbitraire. Le cas où $\gamma(k)$, $\tau(k)$ et $\tau'(k)$ ne sont pas directement accessibles est considéré. Par conséquent, l'objectif est d'estimer $\gamma(k)$, $\tau(k)$ et $\tau'(k)$ tandis que le modèle et les séquences U_k et Y_k sont supposées être connus et accessibles en ligne.

La même approche que celle proposée en Section 4.3 pour les systèmes affines peut être utilisée. Il suffit de redéfinir la loi de commutation comme suit.

Soit σ une fonction $\sigma : \mathbb{N} \to \mathcal{J}$ qui, à chaque instant k, identifie de manière unique $(\gamma(k), \tau(k), \tau'(k)) \in \mathcal{J}' \times \mathcal{T} \times \mathcal{T}'$ en fonction de la correspondance suivante : $(\gamma(k), \tau(k), \tau'(k)) = (0,0,0) \leftrightarrow \sigma(k) = 1$, $(\gamma(k), \tau(k), \tau'(k)) = (0,0,1) \leftrightarrow \sigma(k) = 2$, $\ldots$, $(\gamma(k), \tau(k), \tau'(k)) = (0,0,\alpha') \leftrightarrow \sigma(k) = \alpha' + 1$, $(\gamma(k), \tau(k), \tau'(k)) = (0,1,0) \leftrightarrow \sigma(k) = \alpha' + 2$, $(\gamma(k), \tau(k), \tau'(k)) = (1,0,0) \leftrightarrow \sigma(k) = \alpha \cdot \alpha' + 1$, $\ldots$, $(\gamma(k), \tau(k), \tau'(k)) = (J', \alpha, \alpha') \leftrightarrow \sigma(k) = J' \cdot (\alpha + 1) \cdot (\alpha' + 1)$. On peut écrire sans aucune confusion une séquence de mode $\sigma_s = \sigma(k)\sigma(k+1)\ldots\sigma(k+h)$ et une séquence de triplets $\sigma_s = (\gamma(k), \tau(k), \tau'(k))(\gamma(k+1), \tau(k+1), \tau'(k+1))\ldots(\gamma(k+h), \tau(k+h), \tau'(k+h))$. Finalement, on définit

$$x_k = \begin{bmatrix} X_k \\ X_{k-1} \\ X_{k-2} \\ \vdots \\ X_{k-\alpha} \end{bmatrix}, \quad u_k = \begin{bmatrix} U_k \\ U_{k-1} \\ U_{k-2} \\ \vdots \\ U_{k-\alpha'} \end{bmatrix}, \quad y_k = Y_k \tag{4.13}$$

Le système (4.12) peut être réécrit, d'une manière équivalente, sous la forme du système affine à commutation donné par (3.1) avec $n = (\alpha+1)N$, $p = (\alpha'+1)P$, $m = M$, une loi de commutation σ avec $J = J'(\alpha+1)(\alpha'+1)$ modes et les matrices d'état obéissant à la construction suivante

$$A_{\sigma(k)} = \begin{bmatrix} \mathcal{A}_{\gamma(k)} + \kappa(\tau(k))\mathcal{G}_{\gamma(k)} & \psi_1(\gamma(k), \tau(k)) & \cdots & \psi_\alpha(\gamma(k), \tau(k)) \\ \mathbf{1} & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \cdots & \mathbf{0} \\ \vdots & & \cdots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots\ \mathbf{1} & \mathbf{0} \end{bmatrix}$$

$$B_{\sigma(k)} = \begin{bmatrix} \psi'_0(\gamma(k), \tau'(k)) & \psi'_1(\gamma(k), \tau'(k)) & \cdots & \psi'_\alpha(\gamma(k), \tau'(k)) \\ \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} \end{bmatrix}$$

$$E_{\sigma(k)} = \begin{bmatrix} \mathcal{E}_{\gamma(k)} \\ \mathbf{0} \end{bmatrix}, C_{\sigma(k)} = \begin{bmatrix} \mathcal{C} & \mathbf{0} \end{bmatrix}, D_{\sigma(k)} = \begin{bmatrix} \mathcal{D} & \mathbf{0} \end{bmatrix}$$

où κ est défini comme

$$\kappa(\tau(k)) = \begin{cases} 1 & \text{si } \tau(k) = 0 \\ 0 & \text{si } \tau(k) \neq 0 \end{cases}$$

ψ_i est défini pour $i = 1, \ldots, \alpha$ comme

$$\psi_i(\gamma(k), \tau(k)) = \begin{cases} \mathcal{G}_{\gamma(k)} & \text{si } \tau(k) = i \\ \mathbf{0} & \text{si } \tau(k) \neq i \end{cases}$$

Finalement, ψ'_i est défini pour $i = 0, \ldots, \alpha$ comme

$$\psi'_i(\gamma(k), \tau'(k)) = \begin{cases} \mathcal{B}_{\gamma(k)} & \text{si } \tau'(k) = i \\ \mathbf{0} & \text{si } \tau'(k) \neq i \end{cases}$$

Ainsi, il est à présent clair que l'estimation de $\gamma(k)$, $\tau(k)$ et $\tau'(k)$ de (4.12) revient à estimer le mode $\sigma(k)$ de (3.1).

Les démonstrations sur la discernabilité, la $\mathcal{R}$–discernabilité, la (η, ω)–discernabilité et la (λ)–discernabilité arrière sont identiques et donnent le même résultat. Les preuves ne sont donc pas détaillées.

4.4.2 Unicité : spécificité des systèmes à retards

4.4.2.1 Discernabilité

Proposition 30 *Pour le système* (4.12)*, la discernabilité, la $\mathcal{R}$–discernabilité et la discernabilité arrière ne sont pas vérifiées.*

Preuve 34 *La preuve suit le même raisonnement que celui de la Preuve 31 de la Proposition 27 avec $\sigma_{s_1} = \sigma_{s[k-h,k-1]}i$ et $\sigma_{s_2} = \sigma_{s[k-h,k-1]}j$ $i \neq j \in \mathcal{J}$.*

4.4.2.2 $(0,1)$–Discernabilité

Proposition 31 *Le système* (4.12) *n'est pas* $(0,1)$*–discernable.*

Preuve 35 *La preuve suit le même raisonnement que celui de la Preuve 32 de la Proposition 28 avec $\sigma_{s_1} = (1,0,0)(1,0,0)\cdots(1,0,0)$ et $\sigma_{s_2} = (1,1,0)\ (1,0,0)\cdots(1,0,0)$ $i \neq j \in \mathcal{J}$.*

4.4.2.3 (λ)–discernabilité arrière

Proposition 32 *Si U_k reste constant entre deux instants consécutifs k et $k+1$, le système* (4.12) *n'est pas* $(\lambda = 1)$*–discernable en arrière.*

Preuve 36 *La preuve suit le même raisonnement que celui de la Preuve 33 de la Proposition 29 avec $\sigma_{s_3} = \sigma^{h-\lambda}i(1,0,0)$ et $\sigma_{s_4} = \sigma^{h-\lambda}j(1,0,0)$ et $\sigma^{h-\lambda} = (1,0,0)(1,0,0)\cdots(1,0,0)$, $i = (1,0,0)$ et $j = (1,0,1)$.*

4.4.3 Procédure globale d'estimation de retard

La procédure globale reste inchangée par rapport au cas des systèmes affines. Elle est rappelée néanmoins ci-dessous.

1. Formulation hybride

– Réécriture du système (4.12) dans la forme (3.1).

2. Estimation du retard $\tau(k)$

– Les étapes sont résumées dans la Section 3.7 du Chapitre 3. Cependant, il a été démontré à la Section 4.4.2 que (4.12) n'est pas
  – discernable, $\mathcal{R}$–discernable ni discernable en arrière
  – $(0,1)$–discernable
  – (1)–discernable en arrière lorsque l'entrée reste constante entre deux instants consécutifs k et $k+1$

  Par conséquent, l'estimation du retard $\tau(k)$, et donc du mode $\sigma(k)$, est effectuée grâce à la procédure globale donnée dans la Section 3.7 excepté que l'Étape 2, l'Étape 3, l'Étape 6 et l'Étape 7 avec $\lambda = 1$ peuvent être ignorées.

Cette extension est particulièrement intéressante pour examiner la méthode par injection de retard comme illustré dans l'exemple suivant.

4.4.4 Exemple illustratif : estimation en ligne de retards variables pour un système de chiffrement par injection de retard

Le principe de chiffrement chaotique par injection de retard est rappelé sur la Figure 4.7. Côté émetteur, considérons la "'Tent map"' retardée donnée par :

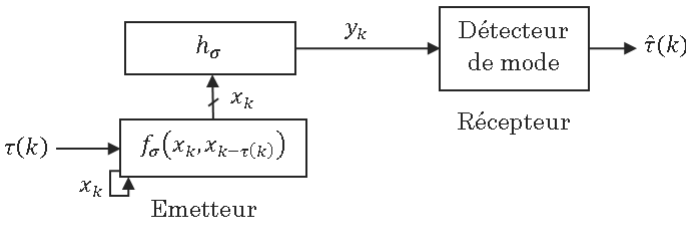


FIGURE 4.7 – Détection de mode pour l'estimation de retards variables

$$X(k+1) = \begin{cases} \mu X(k) + 0.1X(k-\tau(k)) & \text{si } X(k) < 0.5 \\ \mu - \mu X(k) + 0.2X(k-\tau(k)) & \text{si } X(k) \geq 0.5 \end{cases} \tag{4.14}$$

où $\mu = 1.5$, $\tau(k) \in \{0,\ 1,\ 2\}$ représente l'information conformément au principe décrit à la Section 1.4.5 du Chapitre 1.
L'attracteur chaotique correspondant est donné sur la Figure 4.8.

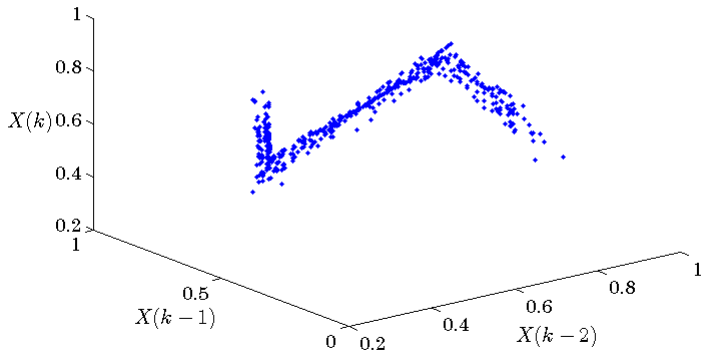


FIGURE 4.8 – Attracteur chaotique de la fonction Tent avec retard variable

Le système (4.14) admet la forme (4.12) avec

$$\mathcal{A}_1 = \mu,\ \mathcal{A}_2 = -\mu, \mathcal{G}_1 = 0.1,\ \mathcal{G}_2 = 0.2,\ \mathcal{C} = 3,\ \mathcal{E}_1 = 0,\ \mathcal{E}_2 = -\mu$$

1. Formulation hybride

Ce système affine à commutation à retard à temps discret est réécrit sous la forme (3.1) avec

$$x_k = \begin{bmatrix} X_k \\ X_{k-1} \\ X_{k-2} \end{bmatrix},\quad y_k = Y_k$$

et la loi de commutation σ a 6 modes.

$$A_{(i,0,0)} = \begin{bmatrix} \mathcal{A}_i + \mathcal{G}_i & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, A_{(i,1,0)} = \begin{bmatrix} \mathcal{A}_i & \mathcal{G}_i & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \; A_{(i,2,0)} = \begin{bmatrix} \mathcal{A}_i & 0 & \mathcal{G}_i \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

$$B_{(i,1,0)} = B_{(i,2,0)} = B_{(i,3,0)} \begin{bmatrix} \mathbf{0} \\ \mathbf{0} \\ \mathbf{0} \end{bmatrix}, E_{(i,1,0)} = E_{(i,2,0)} = E_{(i,3,0)} = \begin{bmatrix} \mathcal{E}_i \\ 0 \\ 0 \end{bmatrix}$$

$$\mathcal{C}_{(i,1,0)} = \mathcal{C}_{(i,2,0)} = \mathcal{C}_{(i,3,0)} = \begin{bmatrix} C & 0 & 0 \end{bmatrix}, \quad D_{(i,1,0)} = D_{(i,2,0)} = D_{(i,3,0)} = 0 \quad i \in \{0,1,2\}$$

2. Estimation du retard $\tau(k)$ côté récepteur
L'estimation du retard $\tau(k)$ constitue ici le déchiffrement côté récepteur et s'effectue en ligne.
Étape 1 : horizon de détection
Le plus petit horizon de détection h qui satisfait (3.26) est $h = 3$.

– Estimation initiale

Étant donné que la discernabilité et la $\mathcal{R}$–discernabilité ne sont pas vérifiées pour (4.12), comme indiqué précédemment dans la Section 4.3.3, l'Étape 2 et l'Étape 3 de la procédure globale sont ignorées et la séquence $\sigma^*_{[0,3]}$ ne peut pas être estimée dans sa totalité.
Étape 4 : (η,ω)–discernabilité
La propriété de (η,ω)–discernabilité est vérifiée à l'aide de (3.40) ou (3.41) de la Proposition 16 du Chapitre 3. Après avoir effectué le test, il s'avère que (3.40) ou (3.41) sont satisfaites pour $\eta = 2$ et $\omega = 1$ ce qui signifie que la $(2,1)$–discernabilité est vérifiée. Par conséquent, à l'instant $k = 3$, le détecteur est en mesure de fournir le premier mode actif $\sigma^*(2)$. La première sous-séquence $\sigma_{[0,1]}$ ne peut pas être estimée.
Étape 5 : $\mathcal{R}(\eta,\omega)$–discernabilité
La propriété de $\mathcal{R}(\eta,\omega)$–discernabilité est testée à l'aide de (3.44). Après avoir effectué le test, il s'avère que (3.44) est satisfaite pour $\eta = 2$ et $\omega = 1$ ce qui signifie que la $\mathcal{R}(2,1)$–discernabilité est vérifiée. Par conséquent, à l'instant $k = 3$, le détecteur est en mesure de fournir le premier mode actif $\sigma^*(2)$. Ici la $\mathcal{R}(\eta,\omega)$–discernabilité n'apporte pas d'amélioration quant à la longueur de la première sous-séquence à estimer par rapport à la (η,ω)–discernabilité. La sous-séquence $\sigma_{[0,1]}$ ne peut pas être estimée.

– Estimation permanente

Étape 7 : (λ)–discernabilité arrière
Les conditions (3.56) et (3.57) sont testées. Puisque au moins une des conditions est vérifiée, car il s'avère que (3.56) est satisfaite pour $\lambda = 1$, l'estimation permanente peut être effectuée par le détecteur qui délivre le mode actif $\sigma^*(k-1)$ lorsque $k > h + \omega + \eta - \lambda - 1 = 4$.

Finalement, le détecteur récupère avec succès la loi de commutation et le retard inconnu pour $k > 1$ comme représenté sur la Figure 4.9 et la Figure 4.10.

4.5 Conclusion

Dans ce chapitre, nous avons présenté des applications de la détection de mode. D'abord, une démarche a été détaillée pour la synchronisation des systèmes chaotiques affines à commutation,

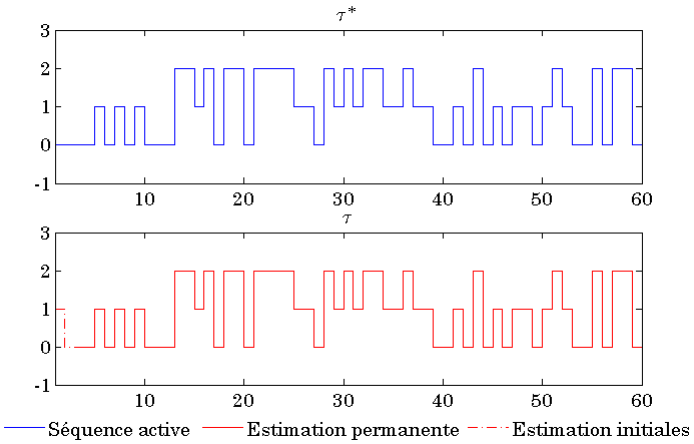


FIGURE 4.9 – Séquence active τ^* et séquence estimée τ

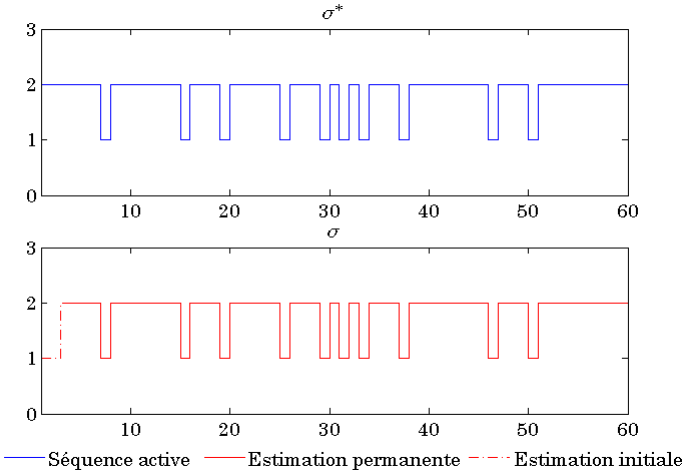


FIGURE 4.10 – Séquence active σ^* et séquence estimée σ

lorsque l'état discret n'est pas accessible, situation rencontrée pour la modulation paramétrique, la commutation chaotique ou encore la transmission à deux canaux. Ensuite, une approche pour estimer les retards variant dans le temps des systèmes affines et affines à commutation à temps discret a été proposée. Le problème a été transformé en un problème de détection de mode équivalent pour les systèmes affines à commutation. Les conditions sur la discernabilité ont été particularisées à ce contexte particulier. Pour les systèmes affines, les résultats présentent un intérêt dans le cadre général de l'Automatique. Pour les systèmes affines à commutation, ils constituent en plus une solution pour résoudre le problème de l'estimation de retard pour le chiffrement par injection de retard. Cette estimation peut être considérée comme une méthode de déchiffrement si le retard contient l'information claire. Elle peut être également considérée comme un moyen de cryptanalyse si le retard constitue la clé secrète.

Conclusion Générale

Le travail développé dans ce manuscrit a porté sur la synchronisation des systèmes chaotiques. Il est articulé autour de deux axes principaux : la synthèse d'observateur et la détection de mode.

Dans un premier temps, quelques rappels sur le chaos et les principales architectures de systèmes de chiffrement chaotiques proposés depuis les années 90 dans la littérature ont été effectués. Ensuite, nous avons rappelé comment les systèmes chaotiques à non linéarité polynomiale ou affines à commutation peuvent se réécrire sous forme LPV polytopique. Une revue des principaux résultats sur la synthèse d'observateurs LPV polytopiques reposant sur l'utilisation des LMI a été effectuée. Le principe de la synthèse garantissant la stabilité, en particulier polyquadratique, dans le contexte non bruité puis les performances en termes d'ISS, de gain crête-à-crête et de gain $\mathcal{L}_2$ dans le contexte avec perturbation ou incertitude a été rappelé. Une extension des résultats aux observateurs polytopiques à entrées inconnues, à la fois dans le cas déterministe, bruité ou incertain, a été proposée. On a montré comment ces observateurs pouvaient assurer la synchronisation du chaos et donc le déchiffrement dans les systèmes de chiffrement "modulation paramétrique", "commutation chaotique", "transmission à deux canaux". Pour le "chiffrement par inclusion", on a recours à des observateurs polytopiques à entrées inconnues.

Pour les systèmes affines à commutation, on a considéré la situation où l'état discret n'est pas connu, car dépendant de composantes du vecteur d'état non accessibles ou dépendant de l'information qui, par définition, n'est pas non plus accessible. La connaissance de l'état discret étant nécessaire pour assurer le déchiffrement côté récepteur, nous nous sommes intéressés au problème de la détection de mode. Une présentation unifiée des méthodes fondées sur les espaces de parité proposées dans la littérature pour les systèmes linéaires et affines à commutation à temps discret a été réalisée. On a procédé à une étude comparative, et les conditions relatives à l'existence de détecteurs ont été assouplies. Le problème de discernabilité a fait l'objet d'une étude approfondie, et de nouvelles conditions relatives à la propriété de discernabilité ont été introduites. Une approche globale étape-par-étape pour la détection de mode a été détaillée comme solution complète y compris pour les systèmes non discernables.
Ensuite, nous avons présenté deux applications de la détection de mode. D'abord, une démarche a été détaillée pour la synchronisation des systèmes chaotiques affines à commutation, lorsque l'état discret n'est pas accessible, situation rencontrée pour la modulation paramétrique, la commutation chaotique ou encore la transmission à deux canaux. Puis, une approche pour estimer les retards variant dans le temps des systèmes affines et affines à commutation à temps discret a été proposée. En effet, le problème a été transformé en un problème de détection de mode équivalent pour les systèmes affines à commutation. Les conditions sur la discernabilité ont été particularisées à ce contexte. Pour les systèmes affines, les résultats présentent un intérêt dans le cadre général de l'Automatique. Pour les systèmes affines à commutation, ils constituent en plus une solution pour résoudre le problème de l'estimation de retard pour le chiffrement par

injection de retard. Cette estimation peut être considérée comme une méthode de déchiffrement si le retard contient l'information claire. Elle peut être également considérée comme un moyen de cryptanalyse si le retard constitue la clé secrète.

Le travail réalisé dans ce manuscrit s'ouvre vers des contributions futures. Nous citerons deux perspectives ci-dessous.

- Robustesse des notions de discernabilité dans le cas stochastique ou incertain.

- L'unicité de la solution délivrée par une détection de mode est une question importante. Nous avons fait une revue dans ce manuscrit des principales propriétés de discernabilité. Cependant, ces conditions reposent sur la structure des détecteurs et nécessitent la connaissance du modèle. Lorsque le modèle n'est pas connu, on peut avoir recours à des approches fondées sur les données utilisant des techniques d'identification [Vidal et al., 2003] [Venkatasubramanian et al., 2003a]. Il serait alors intéressant d'étudier comment la discernabilité se traduit pour ces approches.

- Dans les systèmes cyber-physiques, les réseaux peuvent engendrer l'apparition de retards, parfois variables et inconnus. Il faudrait donc s'intéresser au problème de l'intégration de l'estimation des retards dans les schémas de commande. Les problèmes de stabilité et de performances devront être examinés.

Bibliographie

[Alessandri et al., 2005] Alessandri, A., Baglietto, M., and Battistelli, G. (2005). Receding-horizon estimation for switching discrete-time linear systems. *IEEE Transactions on Automatic Control*, 50(11).

[Allison and Noga, 1997] Allison, D. C. S. and Noga, M. T. (1997). Computing the three-dimensional convex hull. *Computer Physics Communications*, 103(1) :74–82.

[Alvarez and Li, 2006] Alvarez, G. and Li, S. (2006). Some basic cryptographic requirements for chaos-based cryptosystems. *International Journal of Bifurcation and Chaos*, 16(8) :2129–2151.

[Amigó et al., 2007] Amigó, J. M., Kocarev, L., and Szczepanski, J. (2007). Theory and practice of chaotic cryptography. *Physics Letters A*, 366 :211–216.

[Anstett et al., 2004] Anstett, F., Millerioux, G., and Bloch, G. (2004). Global adaptive synchronization based upon polytopic observers. *In Proceedings of IEEE International Symposium on Circuits and Systems ISCAS'04*, 4 :IV –728–31.

[Apkarian et al., 1995] Apkarian, P., Gahinet, P., and Becker, G. (May 1995). A convex characterization of gain-scheduled H_∞ Controllers. *IEEE Transactions on Automatic Control*, 40(5) :853–864.

[Babaali and Egerstedt, 2003] Babaali, M. and Egerstedt, M. (2003). Pathwise observability and controllability are decidable. In *In Proceeding of the 42nd IEEE Conference on Decision and Control (CDC'03)*, volume 6, pages 5771–5776, Maui, Hawaii.

[Babaali and Egerstedt, 2004] Babaali, M. and Egerstedt, M. (2004). Observability of switched linear systems. *Hybrids Systems : Computation and Control*, pages 48–63.

[Babaali and Egerstedt, 2005] Babaali, M. and Egerstedt, M. (2005). Asymptotic observers for discrete-time switched linear systems. In *In Proceeding of the 16th IFAC World Congress*, Czech Republic.

[Baglietto et al., 2007] Baglietto, M., Battistelli, G., and Scardovi, L. (2007). Active mode observability of switching linear systems. *Automatica*, 43(11) :1442–1449.

[Baglietto et al., 2009] Baglietto, M., Battistelli, G., and Scardovi, L. (2009). Active mode observation of switching linear systems based on set-valued estimation on the continuous state. *International Journal Robust Nonlinear Control*, 19 :1521–1540.

[Bako, 2011] Bako, L. (2011). Identification of switched linear systems via sparse optimization. *Automatica*, 47(4) :668–677.

[Balluchi et al., 2002] Balluchi, A., Benvenuti, L., Benedetto, M. D. D., and Sangiovanni-Vincentelli, A. L. (2002). Design of Observers for Hybrid Systems. In *In Proceeding of the 5th International Workshop on Hybrid Systems*, volume 2289, pages 76–89, Stanford, Calif, USA.

[Bara et al., 2001] Bara, G. I., Daafouz, J., Kratz, F., and Ragot, J. (2001). Parameter-dependent state observer design for affine LPV systems. *International Journal of Control*, 74(16) :1601–1611.

[Barata and Hussein, 2012] Barata, J. C. A. and Hussein, M. S. (2012). The Moore-Penrose Pseudoinverse : A Tutorial Review of the Theory. *Brazilian Journal of Physics*, 42 :146–165.

[Belkoura et al., 2009] Belkoura, L., Richard, J.-P., and Fliess, M. (2009). Parameters estimation of systems with delayed and structured entries. *Automatica*, 45(5) :1117–1125.

[Bemporad et al., 2005] Bemporad, A., Garulli, A., Paoletti, S., and Vicino, A. (2005). A bounded-error approach to piecewise affine system identification. *IEEE Trans. on Automatic Control*, 50(10) :1567–1580.

[Bjorklund and Ljung, 2003] Bjorklund, S. and Ljung, L. (2003). A review of time-delay estimation techniques. In *In Proceeding of the 42nd IEEE Conference on Decision and Control.*

[Borges et al., 2005] Borges, J., Verdult, V., Verhaegen, M., and Botto, M. A. (2005). A switching detection method based on projected subspace classification. In *In Conference on Decision and Control-European Control Conference*, Seville, Spain.

[Boutat-Baddas et al., 2004] Boutat-Baddas, L., Barbot, J. P., Boutat, D., and Tauleigne, R. (2004). Sliding mode observers and observability singularity in chaotic synchronization. *Mathematical Problems in Engineering*, 1 :11–31.

[Boutayeb et al., 2002] Boutayeb, M., Darouach, M., and Rafaralahy, H. (2002). Generalized state-space observers for chaotic synchronization and secure communications. *IEEE Transactions on Circuits and Systems I : Fundamental Theory and Applications*, 49(3) :345–349.

[Bruzelius, 2004] Bruzelius, F. (2004). Linear Parameter-Varying Systems : an approach to gain scheduling. *PhD thesis, Department of Signals and Systems, Chalmers University of Technology, Goteborg, Sweden.*

[Carroll and Pecora, 1991] Carroll, T. L. and Pecora, L. M. (1991). Synchronizing chaotic circuits. *IEEE Transactions on Circuits and Systems*, 38(4) :453–456.

[Chatterjee and Chatterjee, 1990] Chatterjee, S. and Chatterjee, S. (1990). A note of finding extreme points in multivariable space. *Computational Statistics and Data Analysis*, 10(1) :87–92.

[Cuomo et al., 1993] Cuomo, K. M., Oppenheim, A. V., and Strogatz, S. H. (1993). Synchronization of Lorenz based chaotic circuits with applications to communications. *IEEE Transactions on Circuits and Systems II*, 40(10) :626–633.

[Daafouz et al., 2002] Daafouz, J., Millérioux, G., and Iung, C. (November 2002). A poly-quadratic stability based approach for switched systems. *International Journal of Control*, 75 :1302–1310.

[Darouach et al., 1994] Darouach, M., Zazadinski, M., and Xu, S. J. (March 1994). Full-order observers for linear systems with unknown inputs. *IEEE Transactions on Automatic Control*, 4(39) :606–609.

[Datcu et al., 2012] Datcu, O., Fridman, L., and Barbot, J.-P. (2012). A third-order sliding-mode observer for a continuous delay chaotic system.

[Dedieu et al., 1993] Dedieu, H., Kennedy, M. P., and Hasler, M. (1993). Chaos shift keying : modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits. *IEEE Transactions on Circuits and Systems II : Analog and Digital Signal Processing*, 40 :634–642.

[Dedieu and Ogorzalek, 1997] Dedieu, H. and Ogorzalek, M. (1997). Identification of chaotic systems based on adaptive synchronization. *In Proc. ECCTD'97, Budapest*, pages 290–295.

[Devaney, 1989] Devaney, R. L. (1989). An introduction to chaotic dynamical systems. *Redwood City, CA : Addison-Wesley.*

[Domlan et al., 2007] Domlan, E. A., Ragot, J., and Maquin, D. (2007). Switching systems mode estimation using a model-based diagnosis method. In *In 8th Conference on Diagnostics of Processes and Systems*, Slubice, Poland.

[Douglas, 1992] Douglas, E. (1992). Internetworking with TCP/IP : principles, protocols, architecture. *Prentice-Hall International, New Jersey, USA.*

[Eckmann and Ruelle, 1992] Eckmann, J. P. and Ruelle, D. (1992). Fundamental limitations for estimating dimensions and Lyapunov exponents in dynamical systems. *Physica D*, 56 :185–187.

[Eddy, 1977] Eddy, W. F. (1977). A new convex hull algorithm for planar sets. *ACM Transactions on Mathematical Software*, (3) :398–403.

[Farhood and Dullerud, 2010] Farhood, M. and Dullerud, G. (2010). Control of nonstationary LPV systems. *Automatica*, (44) :2108–2119.

[Feldmann et al., 1996] Feldmann, U., Hasler, M., and Schwarz, W. (1996). Communication by chaotic signals :the inverse system approach. *International Journal of Circuit Theory and Applications*, 24 :551–579.

[Ferrari-Trecate et al., 2003] Ferrari-Trecate, G., M.Muselli, Liberati, D., and Morari, M. (2003). A clustering technique for the identification of piecewise affine systems. *Automatica*, 39(2) :205–217.

[Fradkov and Markov, 1997] Fradkov, A. L. and Markov, A. Y. (1997). Adaptive synchronization of chaotic systems based on speed-gradient method and passification. *IEEE Transactions on Circuits and Systems I : Fundamental Theory and Applications*, 44(10) :905–912.

[Frank, 1990] Frank, P. M. (1990). Fault diagnosis in dynamic systems using analytical and knowledge-based redundancy : A survey and some new results. *Automatica*, 26(3) :459–474.

[Ghaoui et al., 2000] Ghaoui, L. E., Niculescu, S.-I., and editors (2000). *Advances in Linear Matrix Inequality Methods in Control. SIAM's Advances in Design and Control.*

[Graham, 1973] Graham, R. L. (1973). An efficient algorithm for determining the convex hull of a finite planar set. *Information Processing Letters*, 2(1) :132–133.

[Grassi and Mascolo, 1997] Grassi, G. and Mascolo, S. (1997). Nonlinear observer design to synchronize hyperchaotic systems via a scalar signal. *IEEE Transactions on Circuits and Systems I : Fundamental Theory and Applications*, 44(10) :1011–1014.

[Halimi et al., 2013] Halimi, M., Millérioux, G., and Daafouz, J. (2013). Polytopic observers for LPV discrete-time systems. 437 :97–124.

[Hasler, 1998] Hasler, M. (1998). Synchronization of chaotic systems and transmission of information. *International Journal of Bifurcation and Chaos*, 8(4).

[Heemels et al., 2010] Heemels, M., Daafouz, J., and Millérioux, G. (September 2010). Observer-based control of discrete-time LPV systems with uncertain parameters. *IEEE Transactions on Automatic Control*, 55(9) :2130–2135.

[Hetel et al., 2008] Hetel, L., Daafouz, J., and Iung, C. (2008). Equivalence between the Lyapunov-Krasovskii functional approach for discrete delay systems and the stability conditions for switched systems. *Nonlinear Analysis : Hybrids Systems*, pages 697–705.

[Huang et al., 2004] Huang, K., Wagner, A., and Ma, Y. (2004). Identification of hybrid linear time-invariant systems via subspace embedding and segmentation. In *Proc. of 43rd conference on Decision and Control (CDC 2004)*, Bahamas.

[Huijberts et al., 2000] Huijberts, H. J. C., Nijmeijer, H., and Willems, R. (2000). System identification in communication with chaotic systems. *IEEE Transactions on Circuits and Systems I : Fundamental Theory and Applications*, 47(6) :800–808.

[Inoue and Ushio, 2001] Inoue, E. and Ushio, T. (2001). Chaos communication using unknown input observers. *Electronics and communication in Japan part III : Fundamental Electronic Science*, 84(12) :21–27.

[Itoh et al., 1997] Itoh, M., Wu, C. W., and Chua, L. O. (1997). Communications systems via chaotic signals from a reconstruction viewpoint. *International Journal of Bifurcation and Chaos*, 7(2) :275–286.

[Jaluski et al., 2002] Jaluski, A., Heemels, M., and Weiland, S. (2002). Observer design for a class of piecewise affine systems. In *Proc. of 41st conference on Decision and Control (CDC 2002)*, Las Vegas.

[Jiang, 2002] Jiang, Z. P. (2002). A note on chaotic secure communication systems. *IEEE Transactions on Circuits and Systems I : Fundamental Theory and Applications*, 49(1) :92–96.

[Jiang and Wang, 2001] Jiang, Z.-P. and Wang, Y. (2001). Input-to-state stability for discrete-time nonlinear systems. *Automatica*, (37) :857–869.

[Kerkhoff, 1883] Kerkhoff, A. (1883). La cryptographie militaire. *Journal des Sciences Militaires*, 9(5) :161–191.

[K.Ikeda, 1979] K.Ikeda (1979). Multiple-valued stationary state and its instability of the transmitted light by a ring cavity system. *Optics Communications*, 30(2) :257–261.

[Kolumban et al., 1998] Kolumban, G., Kennedy, M. P., and Chua, L. O. (1998). The role of synchronization in digital communications using chaos - part ii : Chaotic modulation and chaotic synchronization. *IEEE Transactions on Circuits and Systems I : Fundamental Theory and Applications*, 45 :1129–1140.

[Lavrov et al., 2010] Lavrov, R., Jacquot, M., and Larger, L. (2010). Nonlocal non-linear electro-optic phase dynamics demonstrating 10 gb/s chaos communications. *IEEE Journal of Quantum Electronics*, 46(10) :1430–1435.

[Lee and Park, 2007] Lee, S. M. and Park, J. H. (2007). Output feedback model predictive control for LPV systems using parameter-dependent Lyapunov-function. *Applied Mathematics and Computation*, (190) :671–676.

[Leith and Leithead, 2000] Leith, D. and Leithead, W. (2000). Survey of gain scheduling analysis and design. *International Journal of Control*, (73) :1001–1025.

[Lian and Liu, 2000] Lian, K. Y. and Liu, P. (2000). Synchronization with message embedded for generalized Lorenz chaotic circuits and its error analysis. *IEEE Transactions on Circuits and Systems I : Fundamental Theory and Applications*, 47(9) :1418–1424.

[Lunze and Richter, 2008] Lunze, J. and Richter, J. H. (2008). Reconfigurable fault-tolerant control : a tutorial introduction. *European Journal of Control*, 14(5) :359–386.

[Matthews, 1989] Matthews, R. (1989). On the derivation of a chaotic encryption algorithm. *Cryptologia*, 13 :29–41.

[May, 1976] May, R. (1976). Simple mathematical models with complicated dynamics. *Nature*, 261 :459–470.

[Menezes et al., 1996] Menezes, A. J., Oorschot, P. C., and Vanstone, S. A. (1996). Handbook of Applied Cryptography. *CRC Press*.

[Millerioux et al., 2005] Millerioux, G., Anstett, F., and Bloch, G. (February 2005). Considering the attractor structure of chaotic maps for observer-based synchronization problems. *Mathematics and Computers in Simulation*, 68(1) :67–85.

[Millérioux and Bloch, 2013] Millérioux, G. and Bloch, G. (2013). Scalable decay factor and iss gain for disturbed linear polytopic discrete-time systems. In *In Proceeding of 12th European Control Conference (ECC'13)*, Zurich, Swiss.

[Millérioux and Daafouz, 2009] Millérioux, G. and Daafouz, J. (March 2009). Flatness of switched linear discrete-time systems. *IEEE Transactions on Automatic Control*, 54(3) :615–619.

[Millérioux and Daafouz, 2004] Millérioux, G. and Daafouz, J. (May 2004). Performances of unknown input observers for chaotic LPV maps in a stochastic context.

[Millérioux and Daafouz, 2001] Millérioux, G. and Daafouz, J. (October 2001). Global chaos synchronization and robust filtering in noisy context. *IEEE Transactions on Circuits and Systems I : Fundamental Theory and Applications*, 48(10) :1170–1176.

[Millérioux et al., 2004] Millérioux, G., Rosier, L., Bloch, G., and Daafouz, J. (August 2004). Bounded state reconstruction error for LPV systems with estimated parameters. *IEEE Transactions on Automatic Control*, 49(8) :1385 – 1389.

[Millérioux, 1997] Millérioux, G. (1997). Chaotic synchronization conditions based on control theory for systems described by discrete piecewise linear maps. *International Journal of Bifurcation and Chaos*, 7(7) :1635–1649.

[Millérioux et al., 2008] Millérioux, G., Amigó, J. M., and Daafouz, J. (2008). A connection between chaotic and conventional cryptography. *IEEE Transactions on Circuits and Systems I : Regular Papers*, 55(6).

[Millérioux and Daafouz, 2003] Millérioux, G. and Daafouz, J. (2003). An observer-based approach for input independent global chaos synchronization of discrete-time switched systems. *IEEE Transactions on Circuits and Systems I : Fundamental Theory and Applications*, 50(10) :1270–1279.

[Millérioux and Daafouz, 2004] Millérioux, G. and Daafouz, J. (2004). Unknown input observers for message-embedded chaos synchronization of discrete-time systems. *International Journal of Bifurcation and Chaos*, 14(4) :1357–1368.

[Millérioux and Daafouz, 2006] Millérioux, G. and Daafouz, J. (2006). Chaos in automatiControl-theoretical concepts in the design of symmetric cryptosystems control. *Boca Raton, FL : CRC Press.*

[Millérioux and Mira, 1998] Millérioux, G. and Mira, C. (1998). Coding scheme based on chaos synchronization from noninvertible maps. *International Journal of Bifurcation and Chaos*, 8(10) :2019–2029.

[Mirasso et al., 1996] Mirasso, C. R., Colet, P., and Garcia-Fernadez, P. (1996). Synchronization of chaotic semiconductor lasers : application to encoded communications. *IEEE Photonics Technology Letters*, 8(2) :299–301.

[Nijmeijer and Mareels, 1997] Nijmeijer, H. and Mareels, I. M. Y. (1997). An observer looks at synchronization. *IEEE Transactions on Circuits and Systems I : Fundamental Theory and Applications*, 44 :882–890.

[Nikolakopoulos et al., 2005] Nikolakopoulos, G., Panousopoulou, A., Tzes, A., and Lygeros, J. (2005). Multi-hopping induced gain scheduling for wireless networked controlled systems. In *In Proceeding of the 44th IEEE Conference on Decision and Control (CDC'05)*, Seville.

[Ogorzalek, 1993] Ogorzalek, M. J. (1993). Taming chaos - part I : synchronization. *IEEE Transactions on Circuits and Systems I : Fundamental Theory and Applications*, 40(10) :693–699.

[Ohlsson and Ljung, 2013] Ohlsson, H. and Ljung, L. (2013). Identification of switched linear regression models using sum-of-norms regularization. *Automatica*, 49(4).

[Packard and Balas, 1997] Packard, A. and Balas, G. (1997). Theory and application of linear parameter-varying control techniques.

[Palaniyandi and Lakshmanan, 2001] Palaniyandi, P. and Lakshmanan, M. (2001). Secure digital signal transmission by multistep parameter modumation and alternative driving of transmitter variables. *International Journal of Bifurcation and Chaos*, 11(7) :2031–2036.

[Paoletti et al., 2008] Paoletti, S., Garulli, A., Roll, J., and Vicino, A. (2008). A necessary and sufficient condition for Input realization of switched affine state space models. In *In Proceeding of the 47th IEEE conference on decision and control*, Cancun, Mexico.

[Pardalos et al., 1995] Pardalos, P. M., Li, Y., and Hager, W. W. (1995). Linear programming approaches to the convex hull problem in $\mathbb{R}^m$. *Computers and Mathematics with Applications*, 7(29) :23–29.

[Park and Verriest, 1990] Park, B. P. and Verriest, E. I. (1990). Canonical forms for linear time-varying multivariable discrete systems.

[Parlitz et al., 1993] Parlitz, U., Chua, L. O., Kocarev, L., Halle, K. S., and Shang, A. (1993). Transmission of digital signals by chaotic synchronization. *International Journal of Bifurcation and Chaos*, 3(2) :973–977.

[Pecora and Caroll, 1990] Pecora, L. and Caroll, T. (1990). Synchronization in chaotic systems. *Physical Review Letters*, 64(8) :821–824.

[Peitgen et al., 1992] Peitgen, H. O., Jurgens, H., and Saupe, D. (1992). Chaos and fractals : new frontiers of science. *Springer-Verlag, New York*.

[Pekpe et al., 2004] Pekpe, K. M., Mourot, G., Gasso, K., and Ragot, J. (2004). Identification of switching systems using change detection technique in the subspace framework. In *In Conference on Decision and Control*, Atlantis, Paradise Island, Bahamas.

[Preparata and Shamos, 1985] Preparata, F. P. and Shamos, M. I. (1985). Computational Geometry. *Springer-Verlag*.

[Rössler, 1976] Rössler, O. E. (1976). An equation for continuous chaos. *Physics Letters A*, 57(5) :397–398.

[Sato, 2006] Sato, M. (2006). Filter design for LPV systems using quadratically parameter-dependent lyapunov functions. *Automatica*, 42 :2017–2023.

[Scherer, 2001] Scherer, C. (2001). LPV control and full block multipliers. *Automatica*, 37 :361–375.

[Shannon, 1949] Shannon, C. E. (1949). Communication theory of secrecy systems. *Bell Systems and Technology Journal*, 28 :657–715.

[Silverman, 1969] Silverman, L. M. (June 1969). Inversion of multivariable linear systems. *IEEE Transactions on Automatic Control*, 14(3) :270–276.

[Sontag, 1989] Sontag, E. D. (1989). Smooth stabilization implies coprime factorization. *IEEE Transactions on Automatic Control*, (34) :'435–443.

[Toth et al., 2007] Toth, R., Felici, F., Heuberger, P., and den Hof, P. M. J. V. (2007). Discrete time lpv i/o and state-space representations, differences of behavior and pitfalls of interpolation.

[Tzes et al., 2005] Tzes, A., Nikolakopoulos, G., and Koutroulis, I. (2005). Development and experimental verification of a mobile client-client networked controlled system. *European Journal of Control*, 11(3) :229–241.

[Uchida et al., 2005] Uchida, A., Rogister, F., Garcia-Ojalvoand, J., and Roy, R. (2005). Synchronization and communication with chaotic laser systems. In *Progress in Optics*, volume 48, pages 203–341.

[Venkatasubramanian et al., 2003a] Venkatasubramanian, V., Rengaswamy, R., Kavuri, S. N., and Yin, K. (2003a). A review of process fault detection and diagnosis : Part III : Process history based methods. *Computers and Chemical Engineering*, 27(3) :327–346.

[Venkatasubramanian et al., 2003b] Venkatasubramanian, V., Rengaswamy, R., Yin, K., and Kavuri, S. N. (2003b). A review of process fault detection and diagnosis : Part I : Quantitative model-based methods. *Computers and Chemical Engineering*, 27(3) :293–311.

[Vidal, 2004] Vidal, R. (2004). Identification of pwarx hybrid models with unknown and possibly different orders. In *In Proc. of IEEE American Control Conference*.

[Vidal et al., 2002] Vidal, R., Chiuso, A., and Soatto, S. (2002). Observability and identifiability of jump linear systems. In *In Proceeding of IEEE Conference on Decision and Control*.

[Vidal et al., 2003] Vidal, R., Soatto, S., Ma, Y., and Sastry, S. (2003). An algebraic geometric approach to the identification of a class of linear hybrid systems. In *In Proceeding of the 42nd IEEE Conference on Decision and Control (CDC'03)*, volume 1, pages 167–172.

[Wu and Chua, 1993] Wu, C. W. and Chua, L. O. (1993). A simple way to synchronize chaotic systems with applications to secure communications systems. *International Journal of Bifurcation and Chaos*, 3(6) :1619–1627.

[Wu, 1995] Wu, F. (1995). Control of linear parameter varying systems. *PhD thesis, University of Carlifonia at Berkeley, Mechanical Engineering*.

[Yang, 2004] Yang, T. (2004). A survey of chaotic secure communication systems. *International Journal of Computational Cognition Retrieved from http ://www.YangSky.com/yangijcc.htm*.

[Zheng et al., 2008] Zheng, G., Boutat, D., Floquet, T., and Barbot, J.-P. (2008). Secure data transmission based on multi-input multi-output delayed chaotic system. *International Journal of Bifurcation and Chaos*, 18(7) :2063–2072.

[Zheng et al., 2009] Zheng, G., Woihida, A., and Barbot, J.-P. (2009). Analogue private communication based on hybrid chaotic systems with delays. *2nd IFAC Conference on Analysis and Control of Chaotic Systems*.

Résumé

Le travail développé dans ce manuscrit porte sur la synchronisation des systèmes chaotiques. Il est articulé autour de deux axes principaux : la synthèse d'observateur et la détection de mode. Dans un premier temps, quelques rappels sur le chaos et les principales architectures de systèmes de chiffrement chaotiques sont effectués. Ensuite, nous montrons comment les systèmes chaotiques à non linéarité polynomiale ou affines à commutation peuvent se réécrire sous forme LPV polytopique. Une revue des principaux résultats sur la synthèse d'observateurs LPV polytopiques reposant sur l'utilisation des LMI est faite. Une extension des résultats aux observateurs polytopiques à entrées inconnues, à la fois dans le cas déterministe, bruité ou incertain est proposée. Ces observateurs assurent la synchronisation du chaos et donc le déchiffrement dans les systèmes de chiffrement "modulation paramétrique", "commutation chaotique", "transmission à deux canaux" et "chiffrement par inclusion". Pour les systèmes affines à commutation utilisés en tant que générateur du chaos, le cas où l'état discret n'est pas accessible est considéré. Une présentation unifiée des méthodes fondées sur les espaces de parité, proposées dans la littérature pour les systèmes linéaires et affines à commutation à temps discret, est réalisée. Le problème de discernabilité fait l'objet d'une étude approfondie. Une approche pour estimer les retards variables des systèmes affines et affines à commutation à temps discret, formulée en termes de détection de mode, est proposée en tant que solution à l'estimation de retard pour le chiffrement par injection de retard.

Mots-clés: Synchronisation, systèmes chaotiques, observateurs polytopiques, détection de mode, systèmes à retards

Abstract

The work developed in this manuscript addresses the synchronization of chaotic systems. It is organized around two main axes : the observer synthesis and the mode detection. In a first step, we recall the main architectures of chaotic encryption systems and show how chaotic systems with polynomial nonlinearities or switched affine dynamics can be rewritten in a polytopic LPV form. A review of the main LMI based results for polytopic LPV observers synthesis is made. An extension to polytopic unknown input observers, both in the deterministic case and noisy or uncertain case, is proposed. These observers ensure chaos synchronization and information recovering in the framework of the following encryption systems : "parametric modulation", "chaotic switching", "two channels transmission" and "inclusion encryption". For affine switched systems used as a generator of chaos, the case where the discrete state is not available is considered. A unified presentation of mode detection methods based on parity spaces proposed in the literature for linear and affine switched discrete time systems is proposed. The problem of discernibility is the subject of a complete study. An approach to estimate time varying delays for affine switched discrete time systems, formulated in terms of mode detection, is proposed as a solution for delay injection encryption.

Keywords: Synchronization, chaotic systems, polytopic observers, mode detection, delay systems