Identifiabilité paramétrique

F. Anstett-Collin*, G. Millérioux**

* Laboratoire MIPS - Université de Haute Alsace
floriane.collin@uha.fr

** CRAN - Nancy Université
https://sites.google.com/site/gillesmillerioux/

Pourquoi ? - Problématique

- Choix de la structure d'un modèle
- Le modèle dépend de paramètres à estimer

Problème

Peut-on déterminer les paramètres de façon unique à partir des données entrée/sortie ?

Paramètres identifiables ?

Cadre idéalisé

- Mesures non bruitées
- Entrées et temps de mesures choisis librement

Sommaire

Sommaire

C'est quoi ? - Définitions

Système à temps continu

$$\Sigma_\theta \begin{cases} \dot{x}(t) = f_\theta(x(t), m(t)) \\ y(t) = h_\theta(x(t), m(t)) \end{cases}$$

Système à temps discret

$$\Sigma_\theta \begin{cases} x(k+1) & = f_\theta(x(k), m(k)) \\ y(k) & = h_\theta(x(k), m(k)) \end{cases}$$

- $x(t)$ (resp. $x(k)$) $\in \mathbb{R}^n$: états
- $m(t)$ (resp. $m(k)$) $\in \mathbb{R}^m$: entrées
- $y(t)$ (resp. $y(k)$) $\in \mathbb{R}^p$: sorties
- $\theta \in \Theta \subset \mathbb{R}^l$: paramètres

- Définitions analytiques
- Définitions algébriques

C'est quoi ? - Définitions

Système à temps continu

$$\Sigma_\theta \begin{cases} \dot{x}(t) = f_\theta(x(t), m(t)) \\ y(t) = h_\theta(x(t), m(t)) \end{cases}$$

Système à temps discret

$$\Sigma_\theta \begin{cases} x(k+1) & = f_\theta(x(k), m(k)) \\ y(k) & = h_\theta(x(k), m(k)) \end{cases}$$

- $x(t)$ (resp. $x(k)$) $\in \mathbb{R}^n$: états
- $m(t)$ (resp. $m(k)$) $\in \mathbb{R}^m$: entrées
- $y(t)$ (resp. $y(k)$) $\in \mathbb{R}^p$: sorties
- $\theta \in \Theta \subset \mathbb{R}^l$: paramètres

- Définitions analytiques
- Définitions algébriques

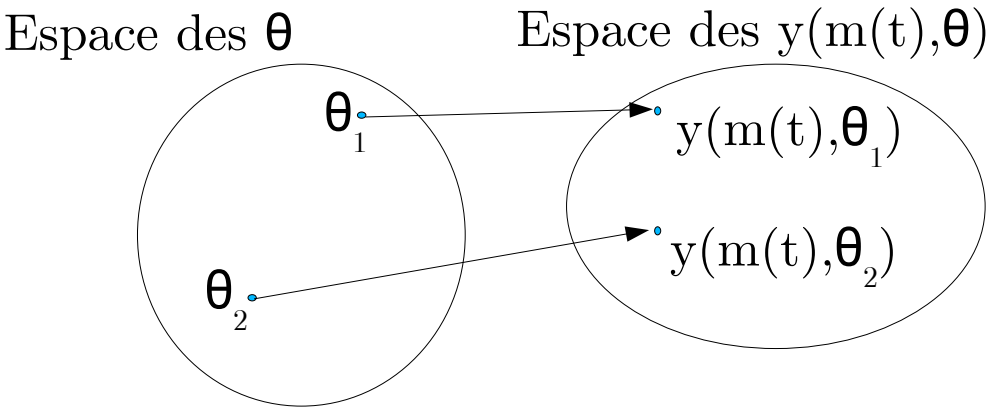
C'est quoi ? - Définitions analytiques

Identifiabilité structurelle globale (s.g.i.)

Définition 1 [Walter, Pronzato] - Paramètre θ_i

Le paramètre θ_i est *s.g.i.* si, pour presque tout $\theta \in \Theta$:

$$y(m(t), \theta) = y(m(t), \hat{\theta}) \Rightarrow \theta_i = \hat{\theta}_i$$



Définition 2 [Walter, Pronzato] - Système Σ_θ

Le système Σ_θ est *s.g.i* si tous les θ_i, $i = 1, \ldots, l$, sont *s.g.i.*

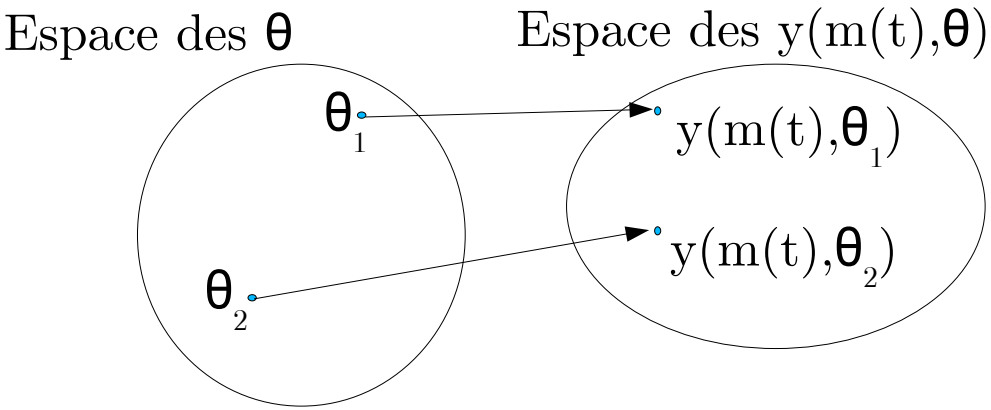
C'est quoi ? - Définitions analytiques

Identifiabilité structurelle globale (s.g.i.)

Définition 1 [Walter, Pronzato] - Paramètre θ_i

Le paramètre θ_i est *s.g.i.* si, pour presque tout $\theta \in \Theta$:

$$y(m(t), \theta) = y(m(t), \hat{\theta}) \Rightarrow \theta_i = \hat{\theta}_i$$



Définition 2 [Walter, Pronzato] - Système Σ_θ

Le système Σ_θ est *s.g.i* si tous les θ_i, $i = 1, \ldots, l$, sont *s.g.i.*

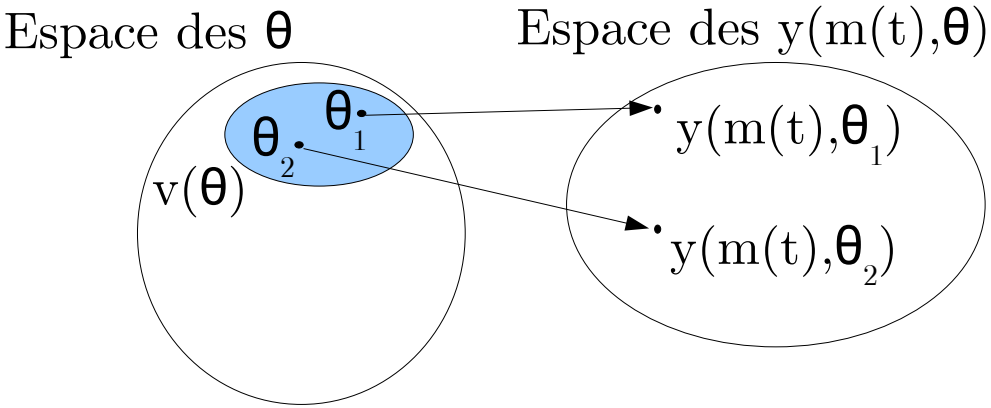
C'est quoi ? - Définitions analytiques

Identifiabilité structurelle locale (s.l.i.)

Définition 3 [Walter, Pronzato] - Paramètre θ_i

Le paramètre θ_i est *s.l.i.* si, pour presque tout $\theta \in \Theta$, il existe un voisinage $v(\theta)$ de θ, tel que:

$$\hat{\theta} \in v(\theta), \quad y(m(t), \theta) = y(m(t), \hat{\theta}) \Rightarrow \theta_i = \hat{\theta}_i$$



Définition 4 [Walter, Pronzato] - Système Σ_θ

Le système Σ_θ est *s.l.i* si tous les θ_i, $i = 1, \ldots, l$, sont *s.l.i.*

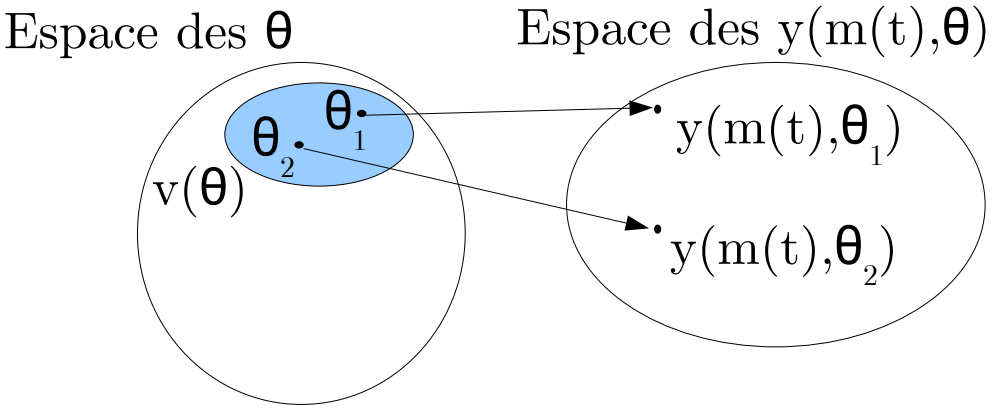
C'est quoi ? - Définitions analytiques

Identifiabilité structurelle locale (s.l.i.)

Définition 3 [Walter, Pronzato] - Paramètre θ_i

Le paramètre θ_i est *s.l.i.* si, pour presque tout $\theta \in \Theta$, il existe un voisinage $v(\theta)$ de θ, tel que:

$$\hat{\theta} \in v(\theta), \quad y(m(t), \theta) = y(m(t), \hat{\theta}) \Rightarrow \theta_i = \hat{\theta}_i$$



Définition 4 [Walter, Pronzato] - Système Σ_θ

Le système Σ_θ est *s.l.i* si tous les θ_i, $i = 1, \ldots, l$, sont *s.l.i.*

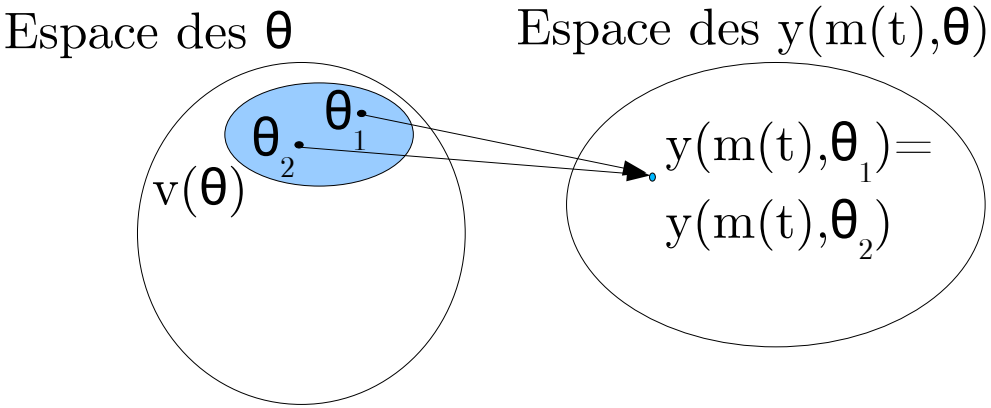
C'est quoi ? - Définitions analytiques

Non identifiabilité structurelle (s.n.i.)

Définition 5 [Walter, Pronzato] - Paramètre θ_i

Le paramètre θ_i est *s.n.i.* si, pour presque tout $\theta \in \Theta$, il n'existe pas de voisinage $v(\theta)$ de θ, tel que :

$$\hat{\theta} \in v(\theta), \quad y(m(t),\theta) = y(m(t),\hat{\theta}) \Rightarrow \theta_i = \hat{\theta}_i$$



Définition 6 [Walter, Pronzato] - Système Σ_θ

Le système Σ_θ est *s.n.i* s'il existe au moins un θ_i *s.n.i.*

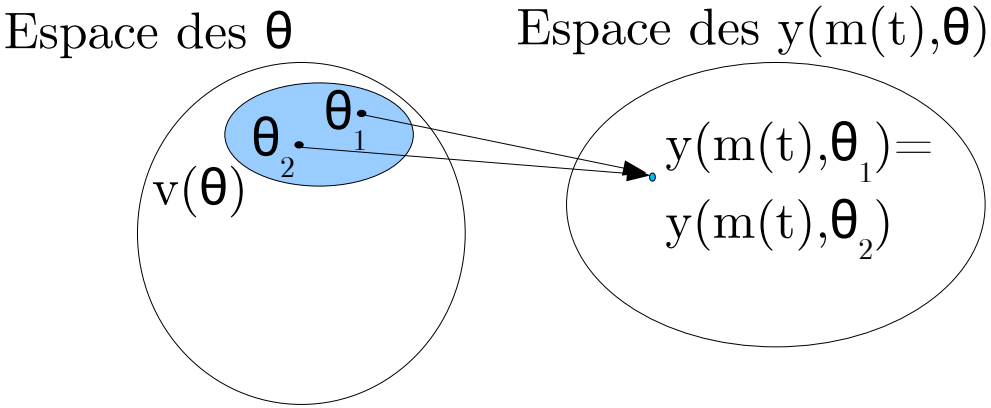
C'est quoi ? - Définitions analytiques

Non identifiabilité structurelle (s.n.i.)

Définition 5 [Walter, Pronzato] - Paramètre θ_i

Le paramètre θ_i est *s.n.i.* si, pour presque tout $\theta \in \Theta$, il n'existe pas de voisinage $v(\theta)$ de θ, tel que :

$$\hat{\theta} \in v(\theta), \quad y(m(t), \theta) = y(m(t), \hat{\theta}) \Rightarrow \theta_i = \hat{\theta}_i$$



Définition 6 [Walter, Pronzato] - Système Σ_θ

Le système Σ_θ est *s.n.i* s'il existe au moins un θ_i *s.n.i.*

C'est quoi ? - Définitions

- Extension aux systèmes à temps discret [Nõmm, Moog]

Système à temps continu	Système à temps discret
$\Sigma_\theta \begin{cases} \dot{x}(t) = f_\theta(x(t), m(t)) \\ y(t) = h_\theta(x(t), m(t)) \end{cases}$	$\Sigma_\theta \begin{cases} x(k+1) = f_\theta(x(k), m(k)) \\ y(k) = h_\theta(x(k), m(k)) \end{cases}$

- f_θ : polynôme en $x(t)$, $m(t)$ (resp. $x(k)$, $m(k)$)
- h_θ : polynôme en $x(t)$, $m(t)$ (resp. $x(k)$, $m(k)$)
- Identifiabilité algébrique

C'est quoi ? - Définitions

- Extension aux systèmes à temps discret [Nõmm, Moog]

Système à temps continu	Système à temps discret
$\Sigma_\theta \begin{cases} \dot{x}(t) = f_\theta(x(t), m(t)) \\ y(t) = h_\theta(x(t), m(t)) \end{cases}$	$\Sigma_\theta \begin{cases} x(k+1) = f_\theta(x(k), m(k)) \\ y(k) = h_\theta(x(k), m(k)) \end{cases}$

- f_θ : polynôme en $x(t)$, $m(t)$ (resp. $x(k)$, $m(k)$)
- h_θ : polynôme en $x(t)$, $m(t)$ (resp. $x(k)$, $m(k)$)
- Identifiabilité algébrique

C'est quoi ? - Définitions algébriques

Définition 7 [Diop, Fliess] - Paramètre θ

θ est *algébriquement identifiable* si et seulement s'il existe une équation algébrique de la forme :

$$\mathcal{L}(\theta, y(t), \dot{y}(t), \ldots, m(t), \dot{m}(t), \ldots) = 0$$

- Pas unicité de la valeur de θ
- Unicité de la valeur de θ $->$ *rationnellement identifiable*, équivalente à:

Définition 8 [Ljung] - Système Σ_θ

Le système Σ_θ est *globalement identifiable* si et seulement s'il peut être réécrit sous forme de régression linéaire telle que, pour $i = 1, \ldots, l$:

$$P_i(y(t), \dot{y}(t), \ldots, m(t), \dot{m}(t), \ldots)\theta_i - Q_i(y(t), \dot{y}(t), \ldots, m(t), \dot{m}(t), \ldots) = 0$$

où P_i et Q_i polynômes de $y(t)$, de $m(t)$ et de leurs dérivées.

- Extension aux systèmes à temps discret [Nõmm, Moog]

C'est quoi ? - Définitions algébriques

Définition 7 [Diop, Fliess] - Paramètre θ

θ est *algébriquement identifiable* si et seulement s'il existe une équation algébrique de la forme :

$$\mathcal{L}(\theta, y(t), \dot{y}(t), \ldots, m(t), \dot{m}(t), \ldots) = 0$$

- Pas unicité de la valeur de θ
- Unicité de la valeur de θ $->$ *rationnellement identifiable*, équivalente à:

Définition 8 [Ljung] - Système Σ_θ

Le système Σ_θ est *globalement identifiable* si et seulement s'il peut être réécrit sous forme de régression linéaire telle que, pour $i = 1, \ldots, l$:

$$P_i(y(t), \dot{y}(t), \ldots, m(t), \dot{m}(t), \ldots)\theta_i - Q_i(y(t), \dot{y}(t), \ldots, m(t), \dot{m}(t), \ldots) = 0$$

où P_i et Q_i polynômes de $y(t)$, de $m(t)$ et de leurs dérivées.

- Extension aux systèmes à temps discret [Nõmm, Moog]

Sommaire

Comment ? - Approche égalité des sorties

Identifiabilité analytique

Système à temps discret : $\Sigma_\theta \begin{cases} x(k+1) & = f_\theta(x(k), m(k)) \\ y(k) & = h_\theta(x(k), m(k)) \end{cases}$

Théorème

Le système Σ_θ est *s.g.i.* pour presque tout $\theta \in \Theta$ si $\forall x(0)$, $\forall m(k)$, il existe $T > 0$, tel que :

$$\{y(x(0), m(k), \theta)\}_0^T = \{y(x(0), m(k), \hat{\theta})\}_0^T \Rightarrow \theta = \hat{\theta}$$

- Condition suffisante d'identifiabilité
- Système à temps continu

  Développement en série de Taylor

  Test sur l'égalité des coefficients du développement en série de Taylor

Comment ? - Approche égalité des sorties

Identifiabilité analytique

Système à temps discret : $\Sigma_\theta \begin{cases} x(k+1) & = f_\theta(x(k), m(k)) \\ y(k) & = h_\theta(x(k), m(k)) \end{cases}$

Théorème

Le système Σ_θ est *s.g.i.* pour presque tout $\theta \in \Theta$ si $\forall x(0)$, $\forall m(k)$, il existe $T > 0$, tel que :

$$\{y(x(0), m(k), \theta)\}_0^T = \{y(x(0), m(k), \hat{\theta})\}_0^T \Rightarrow \theta = \hat{\theta}$$

- Condition suffisante d'identifiabilité
- Système à temps continu

  Développement en série de Taylor

  Test sur l'égalité des coefficients du développement en série de Taylor

Comment ? - Approche égalité des sorties

Identifiabilité analytique

Système à temps discret : $\Sigma_\theta \begin{cases} x(k+1) & = f_\theta(x(k), m(k)) \\ y(k) & = h_\theta(x(k), m(k)) \end{cases}$

Théorème

Le système Σ_θ est *s.g.i.* pour presque tout $\theta \in \Theta$ si $\forall x(0)$, $\forall m(k)$, il existe $T > 0$, tel que :

$$\{y(x(0), m(k), \theta)\}_0^T = \{y(x(0), m(k), \hat{\theta})\}_0^T \Rightarrow \theta = \hat{\theta}$$

- Condition suffisante d'identifiabilité
- Système à temps continu

  Développement en série de Taylor

  Test sur l'égalité des coefficients du développement en série de Taylor

Comment ? - Approche relation entrée/sortie

Identifiabilité algébrique

Système à temps discret : $\Sigma_\theta \begin{cases} x(k+1) & = f_\theta(x(k), m(k)) \\ y(k) & = h_\theta(x(k), m(k)) \end{cases}$

f_θ, h_θ polynômes en $x(k)$ et $m(k)$

- Relation entrée/sortie

$$\mathcal{L}_1(\theta, y(k), \ldots, y(k+s), m(k), \ldots, m(k+s)) = 0$$

Eliminer $x(k)$ inconnu

Méthodes algébriques d'élimination (bases de Gröbner, ...)

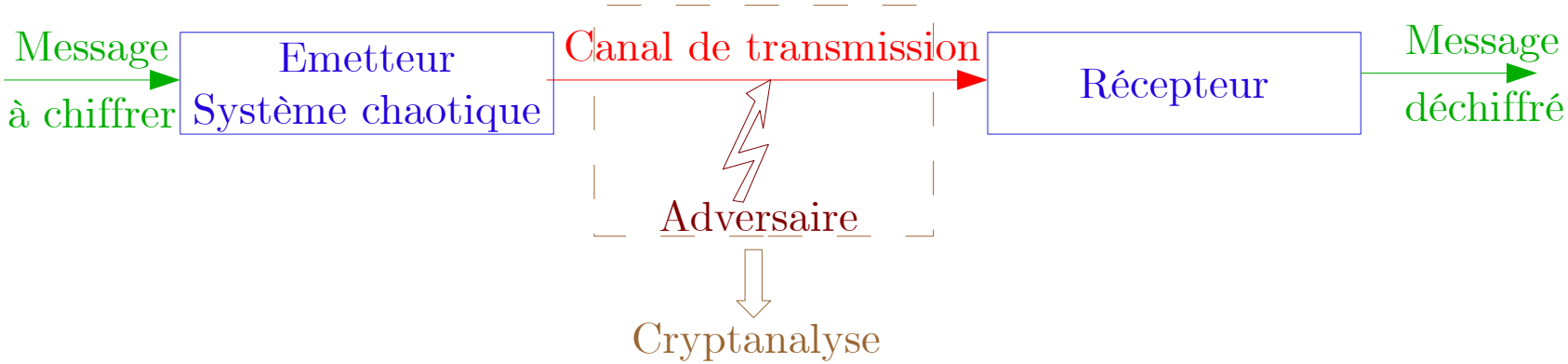
- Test de l'unicité de θ à partir de la relation entrée/sortie

θ_i *globalement identifiable* si :

$$\theta_i = \frac{Q_i(y(k), \ldots, y(k+N), m(k), \ldots, m(k+N))}{P_i(y(k), \ldots, y(k+N), m(k), \ldots, m(k+N))}$$

Sommaire

Application : cryptanalyse de cryptosystème chaotique



- Emetteur : système chaotique

$$\Sigma_\theta \begin{cases} x(k+1) & = f_\theta(x(k), m(k)) \\ y(k) & = h_\theta(x(k), m(k)) \end{cases}$$

- Hypothèse de Kerckhoff : tout connu sauf θ = clé secrète
- Problème : reconstructibilité de la clé ?
- Problème lié à l'identifiabilité

Application : Approche relation entrée/sortie

Emetteur

$$\begin{cases} x_1(k+1) &= (1+\theta_1)x_1(k) + x_1(k)x_2(k) + m(k) \\ x_2(k+1) &= (1-\theta_2)x_2(k) - (x_1(k))^2 m(k) \\ y(k) &= x_1(k) \end{cases}$$

- Relation entrée/sortie : élimination de $x_2(k)$ inconnu

$$\theta_1\theta_2 y(k)y(k+1) + \theta_2(-y(k+1)^2 + y(k)y(k+1) + m(k)y(k+1)) - y(k+2)y(k)$$

$$+y(k+1)^2 - y(k)^3 y(k+1)m(k) - m(k)y(k+1) + m(k+1)y(k) = 0$$

- Itération de la relation entrée/sortie

$$\theta_1\theta_2 y(k+1)y(k+2) + \theta_2(-y(k+2)^2 + y(k+1)y(k+2) + m(k+1)y(k+2))$$

$$-y(k+3)y(k+1) + y(k+2)^2 - y(k+1)^3 y(k+2)m(k+1) -$$

$$m(k+1)y(k+2) + m(k+2)y(k+1) = 0$$

Application : Approche relation entrée/sortie

Emetteur

$$\begin{cases} x_1(k+1) &= (1+\theta_1)x_1(k) + x_1(k)x_2(k) + m(k) \\ x_2(k+1) &= (1-\theta_2)x_2(k) - (x_1(k))^2 m(k) \\ y(k) &= x_1(k) \end{cases}$$

- Relation entrée/sortie : élimination de $x_2(k)$ inconnu

$$\theta_1\theta_2 y(k)y(k+1) + \theta_2(-y(k+1)^2 + y(k)y(k+1) + m(k)y(k+1)) - y(k+2)y(k)$$

$$+y(k+1)^2 - y(k)^3 y(k+1)m(k) - m(k)y(k+1) + m(k+1)y(k) = 0$$

- Itération de la relation entrée/sortie

$$\theta_1\theta_2 y(k+1)y(k+2) + \theta_2(-y(k+2)^2 + y(k+1)y(k+2) + m(k+1)y(k+2))$$

$$-y(k+3)y(k+1) + y(k+2)^2 - y(k+1)^3 y(k+2)m(k+1) -$$

$$m(k+1)y(k+2) + m(k+2)y(k+1) = 0$$

Application : Approche relation entrée/sortie

Emetteur

$$\begin{cases} x_1(k+1) &= (1+\theta_1)x_1(k) + x_1(k)x_2(k) + m(k) \\ x_2(k+1) &= (1-\theta_2)x_2(k) - (x_1(k))^2 m(k) \\ y(k) &= x_1(k) \end{cases}$$

- Relation entrée/sortie : élimination de $x_2(k)$ inconnu

$$\theta_1\theta_2 y(k)y(k+1) + \theta_2(-y(k+1)^2 + y(k)y(k+1) + m(k)y(k+1)) - y(k+2)y(k)$$

$$+y(k+1)^2 - y(k)^3 y(k+1)m(k) - m(k)y(k+1) + m(k+1)y(k) = 0$$

- Itération de la relation entrée/sortie

$$\theta_1\theta_2 y(k+1)y(k+2) + \theta_2(-y(k+2)^2 + y(k+1)y(k+2) + m(k+1)y(k+2))$$

$$-y(k+3)y(k+1) + y(k+2)^2 - y(k+1)^3 y(k+2)m(k+1) -$$

$$m(k+1)y(k+2) + m(k+2)y(k+1) = 0$$

Application : Approche relation entrée/sortie

$$\begin{cases} x_1(k+1) &= (1+\theta_1)x_1(k) + x_1(k)x_2(k) + m(k) \\ x_2(k+1) &= (1-\theta_2)x_2(k) - (x_1(k))^2 m(k) \\ y(k) &= x_1(k) \end{cases}$$

- Résolution

$$\theta_1 = \frac{Q_1(y(k),\ldots,y(k+3),m(k),\ldots,m(k+2))}{P_1(y(k),\ldots,y(k+3),m(k),\ldots,m(k+2))}$$

$$\theta_2 = \frac{Q_2(y(k),\ldots,y(k+3),m(k),\ldots,m(k+2))}{P_2(y(k),\ldots,y(k+3),m(k),\ldots,m(k+2))}$$

- θ_1 et θ_2 identifiables $->$ Mauvais pour la sécurité

Sommaire

Conclusion

Résumé

Définitions analytiques	Définitions algébriques
$y(m(k),\hat{\theta}) = y(m(k),\theta) \Rightarrow \hat{\theta} = \theta$	$\theta_i = \frac{Q_i(y(k),\ldots,y(k+N),m(k),\ldots,m(k+N))}{P_i(y(k),\ldots,y(k+N),m(k),\ldots,m(k+N))}$
Approche égalité des sorties	Approche relation entrée/sortie


F. Anstett, G. Millérioux, G. Bloch
Chaotic Cryptosystems: Cryptanalysis and Identifiability
IEEE Trans. on Circuits and Systems : Regular papers, vol. 53, no. 12, pp. 2673-2680, december 2006.


F. Anstett, G. Bloch, G. Millérioux, L. Denis-Vidal
Identifiability of discrete-time nonlinear systems: the local isomorphism approach
Automatica, vol. 44, no. 1, pp. 2884-2889, 2008

Conclusion

Résumé

Définitions analytiques	Définitions algébriques
$y(m(k),\hat{\theta}) = y(m(k),\theta) \Rightarrow \hat{\theta} = \theta$	$\theta_i = \frac{Q_i(y(k),\ldots,y(k+N),m(k),\ldots,m(k+N))}{P_i(y(k),\ldots,y(k+N),m(k),\ldots,m(k+N))}$
Approche égalité des sorties	Approche relation entrée/sortie


F. Anstett, G. Millérioux, G. Bloch
Chaotic Cryptosystems: Cryptanalysis and Identifiability
IEEE Trans. on Circuits and Systems : Regular papers, vol. 53, no. 12, pp. 2673-2680, december 2006.


F. Anstett, G. Bloch, G. Millérioux, L. Denis-Vidal
Identifiability of discrete-time nonlinear systems: the local isomorphism approach
Automatica, vol. 44, no. 1, pp. 2884-2889, 2008

Conclusion

Résumé

Définitions analytiques	Définitions algébriques
$y(m(k),\hat{\theta}) = y(m(k),\theta) \Rightarrow \hat{\theta} = \theta$	$\theta_i = \frac{Q_i(y(k),\ldots,y(k+N),m(k),\ldots,m(k+N))}{P_i(y(k),\ldots,y(k+N),m(k),\ldots,m(k+N))}$
Approche égalité des sorties	Approche relation entrée/sortie


F. Anstett, G. Millérioux, G. Bloch
Chaotic Cryptosystems: Cryptanalysis and Identifiability
IEEE Trans. on Circuits and Systems : Regular papers, vol. 53, no. 12, pp. 2673-2680, december 2006.


F. Anstett, G. Bloch, G. Millérioux, L. Denis-Vidal
Identifiability of discrete-time nonlinear systems: the local isomorphism approach
Automatica, vol. 44, no. 1, pp. 2884-2889, 2008