PREPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTAIRE DE L'ENSEIGNEMENT SUPERIEUR ET DE
LA RECHERCHE SCIENTIFIQUE
UNIVERSITE ABOU BEKR BELKAID TLEMCEN
DEPARTEMENT DE TELECOMMUNICATIONS

FACULTE DES
SCIENCES DE
L'INGENIEUR

LABORATOIRE DE
TELECOMMUNICATIONS
DE TLEMCEN

Thèse de magister en Télécommunications

Thème :

Systèmes chaotiques et hyperchaotiques pour la transmission sécurisée de données

Présentée par :

M^{me} AZIB née BENZEMAM Djamila

Soutenue devant le jury:

Président: CHIKH BLED Mohammed	Pr. à l'université de Tlemcen
Examinateur: BOUKLI HACENE Noureddine	M.C. à l'université de Tlemcen
Examinateur: MERIAH	M.C. à l'université de Tlemcen
Examinatrice: BENSGHIR née LAZOUNI Sihem	M.C. à l'université de Tlemcen
Encadrant: Mme BENMANSOUR F.Z.	M.C. à l'université de Tlemcen

Année universitaire
2009-2010

REMERCIEMENT

Ce travail a été réalisé au Laboratoire de Télécommunications (LTC), de la Faculté des Sciences de l'Ingénieur à l'Université Abou Bekr Belkaid de Tlemcen, dirigée par Monsieur le Professeur *BENDIMERAD F.T*, que je remercie énormément son humanité et ça compréhension.

Je remercie très chaleureusement ma directrice de thèse, Mme *BENMANSOUR F.Z*, Maitre de conférences à l'Université Abou Baker Belkaid de Tlemcen, pour avoir dirigé mes travaux. Merci pour vos échanges scientifiques, vos conseils et votre rigueur. Merci pour votre soutien scientifique et humain. Je voudrais aussi vous remercier d'avoir cru en mes capacités et de m'avoir fourni d'excellentes conditions me permettant d'aboutir à la production de cette thèse. Cette thèse n'aurait vu le jour sans votre confiance et votre générosité.

J'exprime également mes remerciements aux membres du jury, qui ont accepté d'évaluer mon travail de thèse. Merci à Monsieur CHIKH BLED M, d'avoir accepté d'être le président du jury de cette thèse, à Messieurs *BOUCLI HACENE N* , MERIAH et Mme BENSGHIR S pour avoir accepté d'examiner ce manuscrit et de faire partie de mon jury de thèse.

J'adresse mes vifs remerciements à tous mes amis, pour leur sympathie et leur encouragement, surtout dans les moments difficiles. Je n'oublie pas non plus, tous les membres du Laboratoire de Télécommunications.

Toute ma gratitude et mes chaleureux remerciements vont à ma famille et à ma belle famille.

Enfin, je ne remercierai sans doute jamais assez mon cher époux, qui a su faire preuve d'une grande patience, de compréhension et m'a accompagné et soutenu de façon permanente dans les moments difficiles.

Et surtout je remercie ALLAH le tout puissant de m'avoir donné le courage et la volonté de mener à ce terme ce présent travail.

A mon cher époux Toufik
A ma famille et ma belle famille
A tout ce qui comptent pour moi

TABLE DES MATIAIRES

TABLE DES FIGURES

TABLE DES TABLEAUX

INTRODUCTION GENERALE

L'explosion des communications personnelles de ces quinze dernières années a grandement modifié le paysage contemporain des systèmes de communication. Les objets communiquant, tels que les téléphones portables, les ordinateurs et autres périphériques informatiques usant des systèmes réseaux sans fils mais aussi plus récemment, les capteurs sans fils (wireless sensor) et les systèmes d'identification Radio Fréquence (RFID), envahissent peu à peu notre quotidien et sont le sujet d'un essor commercial grandissant.

Les contraintes de conception de ces systèmes deviennent de plus en plus strictes. Elles incluent aussi bien des couts financiers et temps de développement limités, que des performances nécessaires en termes de débit d'information élevé et d'encombrement spectral réduit autour de fréquences porteuses élevées, ainsi qu'une faible consommation électrique et sans oublier la miniaturisation des dispositifs d'´emission/réception, mêlant sur de mêmes puces, un segment numérique, organe de traitement de l'information à l'état binaire et un segment analogique, centre de transposition de l'information entre basses et hautes fréquences.

La vulgarisation des échanges de données via ce type de systèmes de communication amène le problème actuel de la sécurité de l'information. Ainsi plusieurs moyens ont été développés, partant d'un système classique vers des systèmes numériques. L'utilisation des caractéristiques chaotique et hyperchaotique a permis aussi le chiffrage des informations échangées entre un émetteur et un récepteur. Les deux entités communicantes doivent être synchronisées. Ce phénomène, évoqué par Pecora en 1990, offre la possibilité de développer de nouveaux systèmes de transmission sécurisés. Ces nouveaux systèmes peuvent être vus comme une alternative aux méthodes de cryptographie traditionnelles, mais aussi comme des systèmes apportant un niveau supplémentaire de confidentialité puisque la sécurisation de la transmission peut s'effectuer uniquement par l'intermédiaire des étages de modulation et de démodulation des systèmes de communication [1].

Cette thèse a pour objet l'étude de la synchronisation des systèmes dynamiques chaotiques. Il est donc partagé en quatre parties :

Dans le premier chapitre on va citer les propriétés des systèmes dynamiques en général, et les systèmes chaotiques en particulier. On va parler des notions de stabilité, de bifurcation. Ainsi, on va présenter les systèmes dissipatifs en passant par l'étude du voisinage du point d'équilibre, les systèmes entretenus et la section de Poincaré. En suite, des exemples les plus trouvés dans la littérature, vont être évoqué. A la fin de ce chapitre, les systèmes hyperchaotiques ont été brièvement présentés.

Le deuxième chapitre sera consacré à la cryptographie chaotique, l'utilisation la plus souhaitée du signal chaotique. On commence donc d'abord par une classification des crypto-systèmes ainsi que leurs relations avec le chaos. Enfin on va donner un état de l'art sur les différentes techniques de cryptage en utilisant le chaos.

Dans le troisième chapitre, on va parcourir les différents types de la synchronisation du chaos : la synchronisation identique, la synchronisation généralisée, la synchronisation de phase, et en dernier la synchronisation de retard.

Dans le dernier chapitre, une étude complète du système chaotique de Chen va être réalisée.

CHAPITRE 1

Systèmes dynamiques et chaos

1.1 INTRODUCTION

Les systèmes dynamiques étranges (chaotiques) sont depuis longtemps connus dans le domaine des mathématiques mais c'est seulement au cours de la dernière décennie que les applications concrètes se sont multipliées. Notre étude va se focaliser sur l'usage du chaos pour transmettre de l'information.

1.2 SYSTEMES DYNAMIQUES

Du point de vue mathématique la notion générale de système dynamique est définie à son tour à partir d'un ensemble de variables qui forment le vecteur d'état $x = \{x_i \to R\}, i = 1..n$ où n représente la dimension du vecteur.

Ce jeu de variables a la propriété de caractériser complètement l'état instantané du système dynamique générique. En associant en plus un système de coordonnées on obtient l'espace d'état qui est appelé également l'espace de phase. Conjointement avec l'espace d'état, un système dynamique est défini aussi par une loi d'évolution, généralement désignée par dynamique, qui caractérise l'évolution de l'état du système dans le temps. La notion de déterminisme provient du fait que le système considéré est complètement caractérisé par son état initial et sa dynamique [2].

1.2.1 Définition

Un système dynamique en temps continu est décrit par un système d'équations différentielles, alors qu'en temps discret on parle d'un système d'équations aux différences finies:

1.2.1.1 Temps continu

$$\dot{x}(t) = F(x(t), t) \tag{1.1}$$

où $F: R^n \times R^+ \to R^n$ désigne la dynamique du système.

Si on associe à cette dynamique un état initial $x_0 = x(t_0)$, pour chaque couple choisi (x_0, t_0) on peut identifier une solution unique $\Phi(.; x_0, t_0): R^+ \to R^n$ telle que :

$$\Phi_F(t_0; x_0, t_0) = x_0 \quad \text{et} \quad \Phi_F(t; x_0, t_0) = F(\Phi_F(t; x_0, t_0), t) \tag{1.2}$$

Cette solution unique déterminée à l'aide des équations (1.2), et qui fournit l'ensemble d'états successifs occupés par le système à chaque instant *t*, s'appelle généralement la trajectoire du système dynamique [2].

On considère l'exemple du célèbre système de Lorenz donné par les équations suivantes :

$$\begin{aligned} \frac{dx}{dt} &= \sigma(y - x) \\ \frac{dy}{dt} &= x(\rho - z) - y \\ \frac{dz}{dt} &= xy - bz \end{aligned} \tag{1.3}$$

Les paramètres pour l'exemple de trajectoire donné dans la figure (1.1) ont été choisis de la manière suivante : $\sigma = 10$, $\rho = 28$, $b = 8/3$ avec la condition initiale (x_0, y_0, z_0) = (2, 5, 20).

On observe que la dynamique du système de Lorenz donnée par les équations (1.3) est indépendante de l'instante t considérée. Généralement ce type de système est qualifié d'autonome. La dynamique, dans ce cas particulier, a la forme suivante :

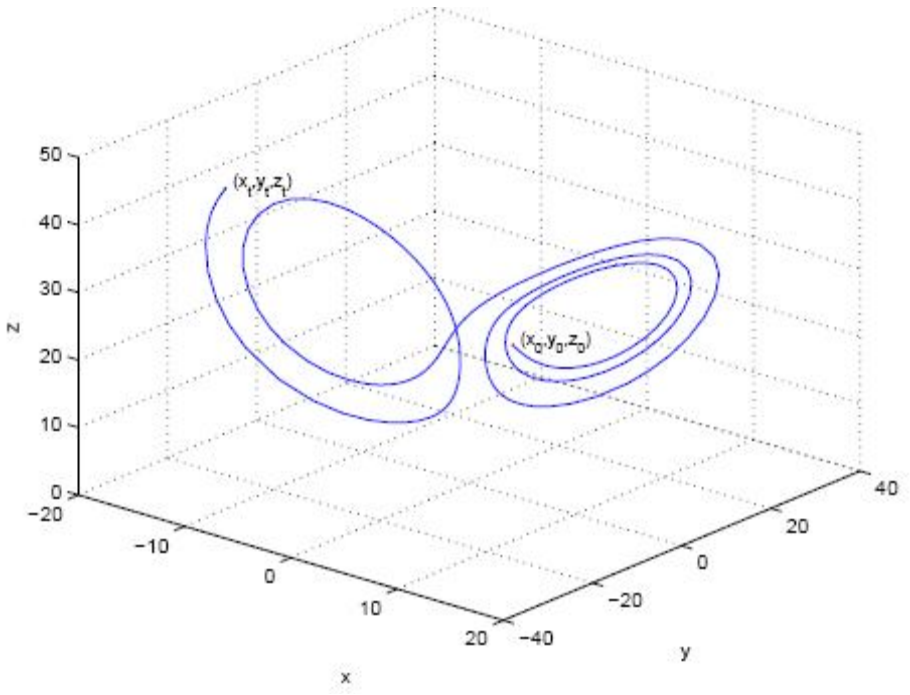


Figure 1.1: Exemple de trajectoire du le système Lorenz [2].

1.2.2.2 Temps discret

$$\dot{x}(t) = F(x(t)) \tag{1.4}$$

Comme il a été déjà précisé, le système dynamique est, dans ce cas, représenté par des équations aux différences finies, avec le modèle général suivant :

$$x(k+1) = G(x(k), k) \tag{1.5}$$

où $G : : R^n \times Z^+ \rightarrow R^n$ désigne la dynamique du système en temps discret.

De même qu'en temps continu, si on associe à cette dynamique un état initial $x_0 = x(k_0)$, pour chaque couple choisi (x_0, k_0) on peut identifier une solution unique $\Phi_G(.; x_0, k_0) : Z^+ \rightarrow R^n$ telle que :

$$\Phi_G(k_0; x_0, k_0) = x_0 \quad \text{et} \quad \Phi_G(k+1; x_0, k_0) = G(\Phi_G(k; x_0, k_0), k) \tag{1.6}$$

En temps discret on définit aussi le système autonome comme une dynamique qui ne dépend pas de l'instant *k*.

$$x(k+1) = G(x(k)) \tag{1.7}$$

1.2.2 Comportement des systèmes dynamiques

A partir d'un état initial x_0 et après un régime transitoire, la trajectoire d'un système dynamique atteint une région limitée de l'espace des phases. Ce comportement asymptotique, obtenu quand t et k tendent vers l'infini, est une des caractéristiques les plus importantes à étudier pour tout système dynamique. Dans le cas d'un système linéaire, si la solution asymptotique est indépendante de la condition initiale et unique, en présence de non-linéarités, il existe donc une plus grande variété de régimes permanents, parmi lesquelles on trouve, par ordre de complexité: points d'équilibre, solutions périodiques, solutions quasi-périodiques et chaos, respectivement. Il faut préciser que cette fois, le comportement développé par un système dynamique particulier est fortement dépendant de la condition initiale choisie [2].

Pour la suite, on va définir et illustrer les comportements évoqués ci-dessus, en utilisant une dynamique très connue dans la théorie des systèmes non-linéaires. Il s'agit de l'équation logistique définie par l'expression suivante:

$$x_{k+1} = f(x_k) = r x_k (1 - x_k) \tag{1.8}$$

Dans les figures 1.2 on montre la dynamique propre à l'équation logistique ainsi que certains modes asymptotiques particuliers. Le mécanisme de construction d'une séquence est tout d'abord montré sous la forme d'un diagramme en toile. Cette méthode permet la génération de la séquence choisie, graphiquement en utilisant la projection des états successifs par rapport à la diagonale principale (fig. 1.2 a) ; r = 3.9).

Dans la partie b) est présenté le diagramme de bifurcation qui montre la distribution des états limites pour différents choix du paramètre *r*. On appelle cette représentation diagramme de bifurcation parce que le comportement asymptotique subit, pour des valeurs du paramètre *r* bien déterminées, une bifurcation de l'ensemble des états limites. Dans le cas continu la bifurcation se manifeste comme une multiplication

des trajectoires possibles. Pour cette représentation on a choisi pour chaque valeur r $\in$ [1, 4] une séquence de 500 échantillons avec une période de transition de 50 échantillons. Par la suite pour chaque type de régime permanent on a [2] :

1.2.2.1 Point d'équilibre

Dans ce cas, la solution asymptotique est représentée par un point, sa valeur étant déterminée en fonction de la condition initiale choisie. Ainsi, pour des conditions initiales différentes on peut retrouver plusieurs points d'équilibres. De même ces points peuvent être stables ou instables suivant que les trajectoires voisines convergent ou divergent entre elles. Dans le cas de la dynamique logistique, on observe que pour toute valeur $r \in [1, 3]$, le régime permanent est formé par un point limite stable, sa valeur étant dépendante du choix de paramètre *r*. La figure 1.2 c) nous donne un aperçu d'une telle trajectoire pour $r = 2$. Ainsi on observe qu'après une période de transition relativement courte, la séquence se stabilise autour du point fixe qui cette fois est $x_\infty = 0.5$.

1.2.2.2 Régime périodique

Le régime permanent périodique correspond à une trajectoire dont les répliques d'une portion élémentaire sont espacées à des intervalles nT, $n \in N^+$, T désignant la période. Pour la fonction logistique, on a choisi deux exemples pour le paramètre r = 3.2 puis r = 3.55. Pour le premier cas, ce choix nous garantit que l'ensemble des états limites est formé par deux points, et la période correspond à deux échantillons (figure 1.2 d). La deuxième solution nous permet d'augmenter la dimension de l'ensemble des états limites et la période de répétition à 8 (figure 1.2 e) [2].

1.2.2.3 Régime quasi-périodique

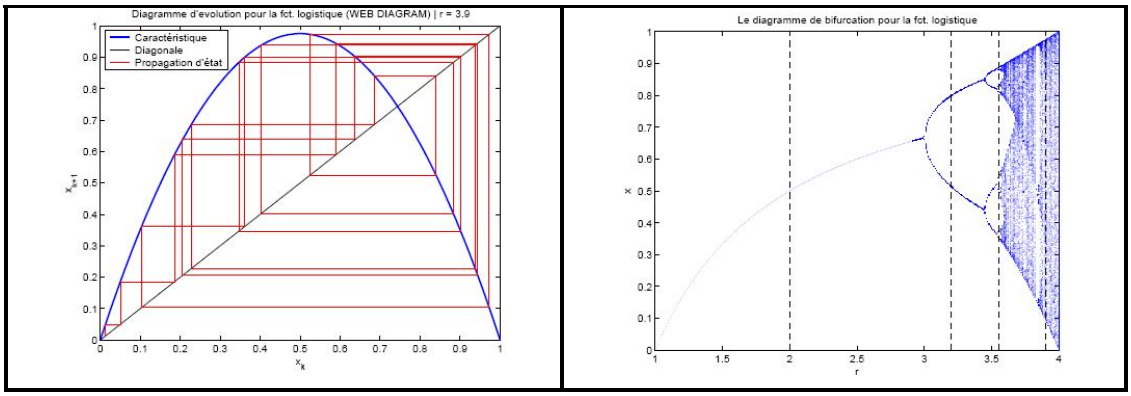
Il correspond à une somme de solutions périodiques, dont le rapport des périodes est un nombre irrationnel. Un régime quasi-périodique peut être représenté dans l'espace d'état par un tore.

1.2.2.4 Régime chaotique

Le régime chaotique est par définition, tout régime permanent qui n'appartient à aucune des classes présentées antérieurement. Une telle solution a une trajectoire asymptotique bornée avec une extrême sensibilité aux conditions initiales. Ainsi deux trajectoires générées à partir de CI (conditions initiales) très proches, vont diverger très vite l'une par rapport à l'autre. Cette sensibilité par rapport aux CI traduit aussi le comportement, en apparence stochastique, des générateurs chaotiques, de telle sorte qu'une prévision à long terme du comportement du système est impossible.

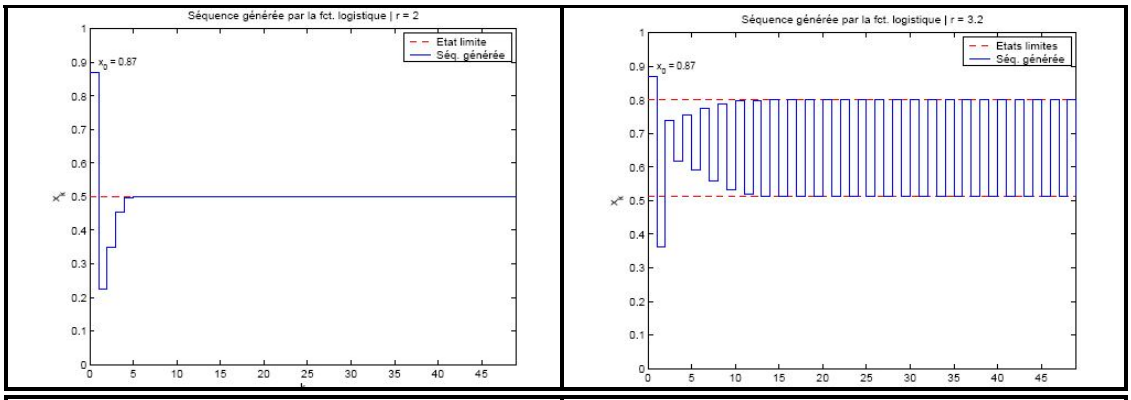
Dans la figure 1.2 f, un exemple est donné pour deux CI espacées par une valeur de 10^{-4}. On peut observer que juste après quelques itérations les deux trajectoires divergent et deviennent non corrélées.

Généralement, l'ensemble des solutions asymptotiques stables décrites ci-dessus est qualifié d'attracteur. Il représente la région de l'espace d'état au voisinage de laquelle les trajectoires restent confinées lorsque t et k tendent vers l'infini. En parallèle, avec la définition de l'attracteur apparaît la notion de bassin d'attraction qui est défini comme la région de l'espace d'état formée par l'ensemble des CI à partir desquelles l'attracteur sera atteint.



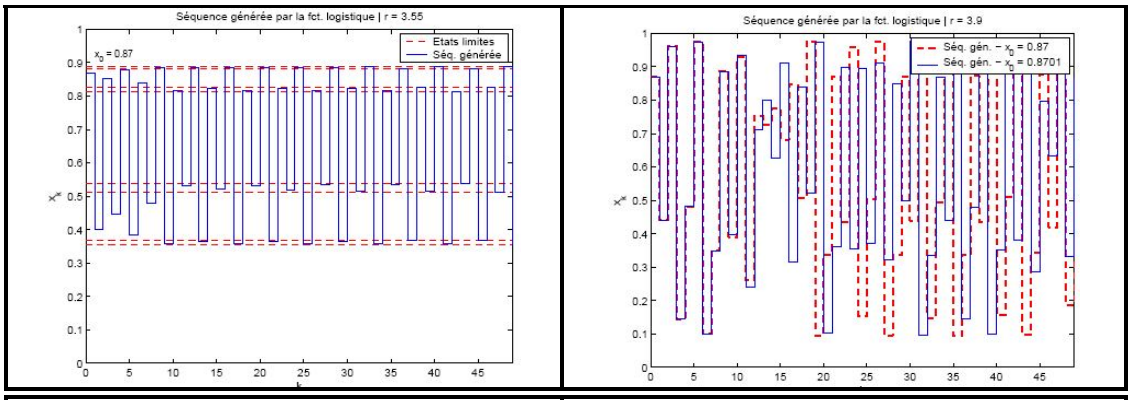
(a) Génération de la séquence récursive (*web diagram*)

(b) Diagramme de bifurcation



(c) Séquence générée et états limites pour $r = 2$

(d) Séquence générée et états limites pour $r = 3.2$



(e) Séquence générée et états limites pour $r = 3.55$

(f) séquences générées et sensibilité aux CI pour $r = 3.9$ (comportement chaotique)

Figure 1.2: Étude du comportement dynamique pour la fonction logistique (eq. 1.8) [2].

1.2.3 Evaluation du comportement dynamique

La présence d'un comportement chaotique pour un système dynamique quelconque, peut être déterminée par élimination de comportements introduits auparavant : si son comportement asymptotique n'est pas un point fixe, périodique ou quasi-périodique on conclut qu'il est chaotique. Mais dans le cas où la dynamique employée pour générer la séquence observée n'est pas connue et si en plus un bruit affecte les observations une telle méthode n'est pas envisageable. Par conséquence, la communauté scientifique a proposé des solutions avec une approche statistique du problème comme le calcul de la dimension de corrélation, l'entropie de Kolmogorov ou les exposants de Lyapunov [2].

La dimension de corrélation est un outil qui offre la possibilité de déterminer la dimension de l'attracteur reconstruit à partir d'une série temporelle observée, tandis que l'entropie ou les exposants de Lyapunov sont employés pour l'évaluation de l'instabilité propre au phénomène chaotique. Dans la pratique ces exposants se sont imposés comme des outils performants, même dans le cas de séries temporelles courtes, avec un coût de calcul relativement réduit par rapport à la dimension de corrélation ou l'entropie de Kolmogorov [2].

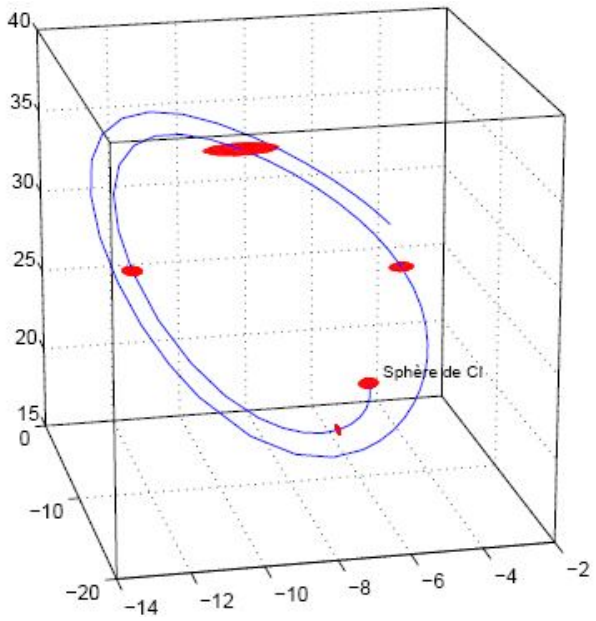


Figure 1.3: Sensibilité aux CI - système de Lorenz [2].

Dans ce chapitre, on se limite à la description des exposants de Lyapunov, la solution la plus pertinente dans le contexte des systèmes à dimension d'état réduite destinés aux communications numériques. Ainsi les exposants de Lyapunov se définissent comme une mesure invariante propre à un système dynamique qui caractérise la séparation exponentielle en temps de deux trajectoires proches. Cette propriété est aussi qualifiée de sensibilité aux CI, mais elle se réfère généralement à la divergence de trajectoires à n'importe quel instant temporel. Ainsi dans le cas d'un attracteur chaotique, deux trajectoires initialement voisines vont diverger à une vitesse exponentielle quantifiée par l'exposant de Lyapunov. Géométriquement, cela se traduit par le fait que si on choisit un ensemble de CI situées dans une sphère infiniment petite (de diamètre δ (0)) dans le bassin d'attraction du système dynamique de dimension *n ;* Sous l'effet de la dynamique cette sphère va se déformer pour se transformer en ellipsoïde.

Le $i^{ème}$ exposant de Lyapunov se définit alors en fonction de la déformation subie sur la $i^{ème}$ direction comme :

$$\lambda_i = \lim_{t\to\infty} \frac{1}{t} \ln \frac{\delta_i(t)}{\delta_i(0)}, i = 1..n \qquad (1.9)$$

L'ensemble $\{\lambda_i\}_{i=1...n}$ constitue le spectre de Lyapunov. D'habitude les exposants sont classés par ordre décroissant: $\lambda_i \geq \lambda_{i+1},\ i = 1..n-1.$

Dans la figure 1.3 on montre l'exemple d'un ensemble de CI choisies dans le voisinage d'une valeur située dans le bassin d'attraction pour le système de Lorenz.

On observe par la suite les déformations de cette sphère initiale à des instants différents. De cette façon on remarque que les déformations ne sont pas uniformes dans toute la région qui définit l'attracteur. Pour caractériser ce comportement, Abarbanel a défini le spectre de Lyapunov associé localement à un point dans l'attracteur.

Il faut noter que l'existence d'un attracteur nécessite que la dynamique de ce système soit globalement dissipative. Cela signifie que le système doit être caractérisé par une stabilité globale qui correspond à la condition suivante sur le spectre de Lyapunov :

$$\sum_{i=1}^{n} \lambda_i < 0 \qquad (1.10)$$

Si le spectre de Lyapunov reste une des plus robustes méthodes pour évaluer le comportement dynamique d'un système quelconque, le spectre de fréquence peut donner aussi des indices sur le régime permanent.

Les divers critères permettant de caractériser la dynamique d'un système quelconque sont regroupés dans le tableau 1.1.

Régime permanent	**Attracteur**	**Spectre**	**Exposants Lyapunov**
Point d'équilibre	Point	Composante continue	$0> \lambda_1 \geq \ldots \geq \lambda_n$
périodique	Courbe fermée	Fréquence Fondamentale + harmoniques entières	$\lambda_{1=0}$ $0 > \lambda_2 \geq \ldots \geq \lambda_n$
Quasi-périodique	tore	Composantes fréquentielles en rapport irrationnel	$\lambda_1 = \ldots = \lambda_i = 0$ $0 > \lambda_{i+1} \geq \ldots \geq \lambda_n$
chaotique	fractale	Spectre large	$\lambda_1>0$ $0 \geq \lambda_2 \geq \ldots \geq \lambda_n$

Tableau 1.1: Classification des régimes permanents en fonction du spectre Lyapunov

1.3 SYSTEMES CHAOTIQUES

1.3.1 Définition

Le chaos est défini généralement comme un comportement particulier d'un système dynamique déterministe non-linéaire.

1.3.2 Caractérisation globale du chaos

Quelques systèmes physiques se comportent de manière chaotique. Parmi ces systèmes, on peut citer l'atmosphère, un robinet qui goutte, un pendule excité dans un champ

magnétique... Ces quelques systèmes se démarquent par leurs dimensions et l'origine de leurs mouvements. Il existe plusieurs définitions possibles du chaos. Ces définitions ne sont pas toutes équivalentes, mais elles convergent vers certains points communs caractérisant ainsi le chaos [24] [25].

Par la suite, on va présenter quelques caractéristiques qui permettent de comprendre qualitativement les points marquants d'un système chaotique [3].

1.3.2.1 Sensibilité aux conditions initiales (SCI)

Tout d'abord, les systèmes chaotiques sont extrêmement sensibles aux perturbations. On peut illustrer ce fait par *l'effet papillon*, popularisé par le météorologue *Edward Lorenz*. L'évolution d'un système dynamique chaotique est imprédictible dans le sens qu'elle est sensible aux conditions initiales. Ainsi, deux trajectoires de phases initialement voisines s'écartent toujours l'une de l'autre, et ceci quelle que soit leur proximité initiale. Il est clair que la moindre erreur ou simple imprécision sur la condition initiale empêche de décider à tout temps qu'elle sera la trajectoire effectivement suivie et, par conséquence, de faire une prédiction autre que statistique sur le devenir à long terme du système. Ainsi, bien que l'on traite de systèmes déterministes, il est impossible de prévoir à long terme leurs comportements. La seule manière est d'opérer effectivement l'évolution du système. Si cette simulation se fait informatiquement, un problème de précision sur les conditions initiales se pose alors : de petites erreurs d'arrondissement dues à la précision du type de la variable codant ces conditions initiales peuvent exponentiellement s'amplifier de telle sorte que la trajectoire de phases obtenue n'est pas représentative de la réalité.

Illustrons ce phénomène de SCI par une simulation numérique. On affecte à un système chaotique deux conditions initiales très proches. Dans un premier temps, les deux systèmes évoluent de la même manière; mais, très vite, leur comportement devient différent. Ceci est illustré dans la figure suivante [3] :

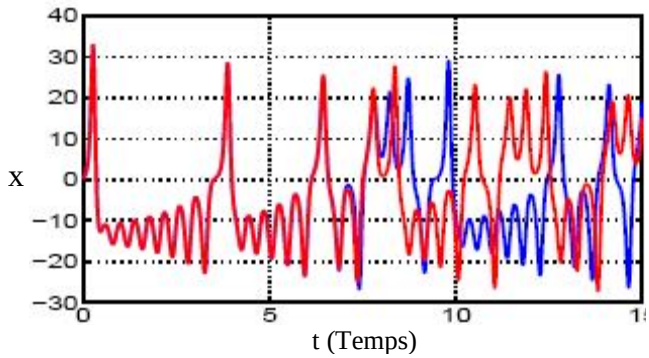


Figure 1.4: Evolution dans le temps pour deux conditions initiales très proches [3].

1.3.2.2 Aspect aléatoire

Les courbes précédentes (figure. 1.4) illustrent la sensibilité aux conditions initiales. Cependant, une autre caractéristique des systèmes chaotiques peut être observée sur les courbes précédentes. En effet, un système chaotique évolue d'une manière qui semble aléatoire. La courbe suivante permet de comparer une évolution simple, périodique et donc prédictible d'un système classique avec l'évolution plus complexe, non périodique et non prédictible d'un système chaotique.

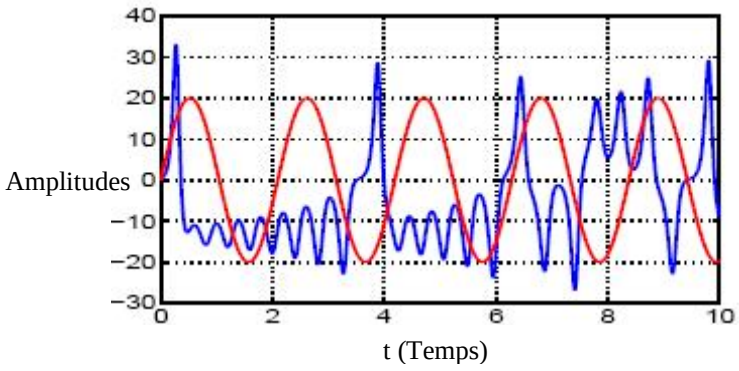


Figure 1.5: Evolution dans le temps d'un système chaotique, comparé à une sinusoïde [4].

Ainsi, les systèmes chaotiques semblent évoluer de manière aléatoire. En tout cas, on ne peut pas prévoir facilement quelle sera leur évolution dans le temps.

Notons que les systèmes chaotiques obéissent tout de même aux lois de la physique. Si on se place dans l'approximation de la physique classique, on peut affirmer que le système est totalement déterministe. Il ne faut donc pas se laisser abuser par le caractère a priori aléatoire qui ne dénote qu'une complexité du système [3].

1.3.3 Espace de phase

La sensibilité aux conditions initiales est le problème majeur du chaos, elle empêche toute prédiction sur l'évolution du système au delà d'un certain temps. Une erreur $\varepsilon_0 > 0$ sur la condition initiale va évoluer exponentiellement. L'erreur à un instant *t*, aura l'expression suivante: $|\varepsilon(t)| = \varepsilon e^{\lambda t}$. On peut calculer la valeur de λ, appelé *exposant de Lyapunov*, grâce aux méthodes développées par Alexandre Lyapunov.

Une façon de contourner ce problème est d'éliminer le temps entre les équations. C'est le rôle de *l'espace des phases* (ou espace des états), il s'agit d'un espace de dimension 2 ou 3 dans lequel chaque coordonnée est une variable d'état du système considéré [4].

1.3.3.1 Exemple

Le pendule libre n'est pas chaotique et cependant l'équation différentielle vérifiée par l'angle θ que fait la tige du pendule avec la normale est non linéaire. Un système non linéaire n'est donc pas forcément chaotique alors que la réciproque est toujours vraie. Le problème du pendule simple est très souvent résolu pour de petits angles en posant $\sin\theta \sim \theta$ dans son équation :

$$\ddot{\theta} + 2\hat{\alpha}\,\dot{\theta} + \omega_0^2 \sin(\hat{\theta}) = 0$$

Dans le portait de phase du pendule, la vitesse angulaire est uniquement en fonction de la position. Afin d'obtenir une équation du premier ordre, on pose : $x = \theta$ et $y = \dot{\theta}$. L'équation devient donc un système que l'on peut résoudre numériquement.

Le système obtenu s'écrit aussi de façon vectorielle :

$$\begin{pmatrix} \dot{x} \\ \dot{y} \end{pmatrix} = \begin{pmatrix} y \\ -\omega_0^2 \sin(x) - 2\alpha y \end{pmatrix} \Leftrightarrow \dot{x} = F(x) \quad \text{avec} \quad X = \begin{pmatrix} x \\ y \end{pmatrix} \tag{1.11}$$

À partir des différents portraits de phase du pendule (fig. 1.7) certaines propriétés peuvent être dégagées :

- Dans l'espace des phases une sinusoïde est représentée par une ellipse (ou un cercle).
- Une grandeur périodique y est représentée par une courbe fermée.
- Si le système est dissipatif, la trajectoire est *attirée* par le point de repos (angle nul et vitesse angulaire nulle).

Par cette méthode, on peut vérifier que l'approximation faite sur l'angle θ est bien justifiée puisque pour de petits angles (cas du pendule conservatif), on obtient approximativement les mêmes ellipses.

Toutefois, ce qui se passe au voisinage du point de repos mérite d'être approfondi.

1.3.3.2 Attracteur chaotique

Afin de bien rendre compte de ce qui peut être observé dans un espace des phases à trois dimensions, voici la représentation de l'attracteur de Rössler. Il s'agit d'un attracteur chaotique (ou attracteur étrange), c'est-à-dire que cette figure géométrique est la représentation dans l'espace des phases d'un système chaotique [4].

Attracteur de Rössler

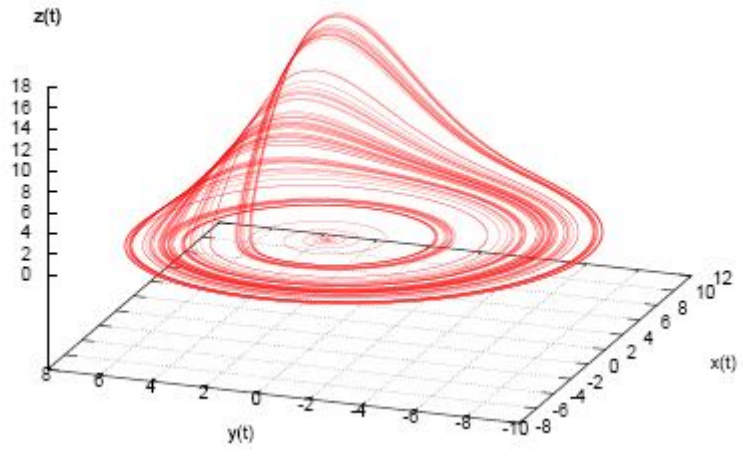


Figure 1.6: Attracteur chaotique de Rössler [4].

Les équations du système de Rössler sont données par le système différentiel suivant (avec pour la figure 1.6 : $a = b = 0.2$ et $c = 5$) :

$$\begin{cases} \dot{x} = -(y+z) \\ \dot{y} = x + ay \\ \dot{z} = b - cz + xz \end{cases}$$

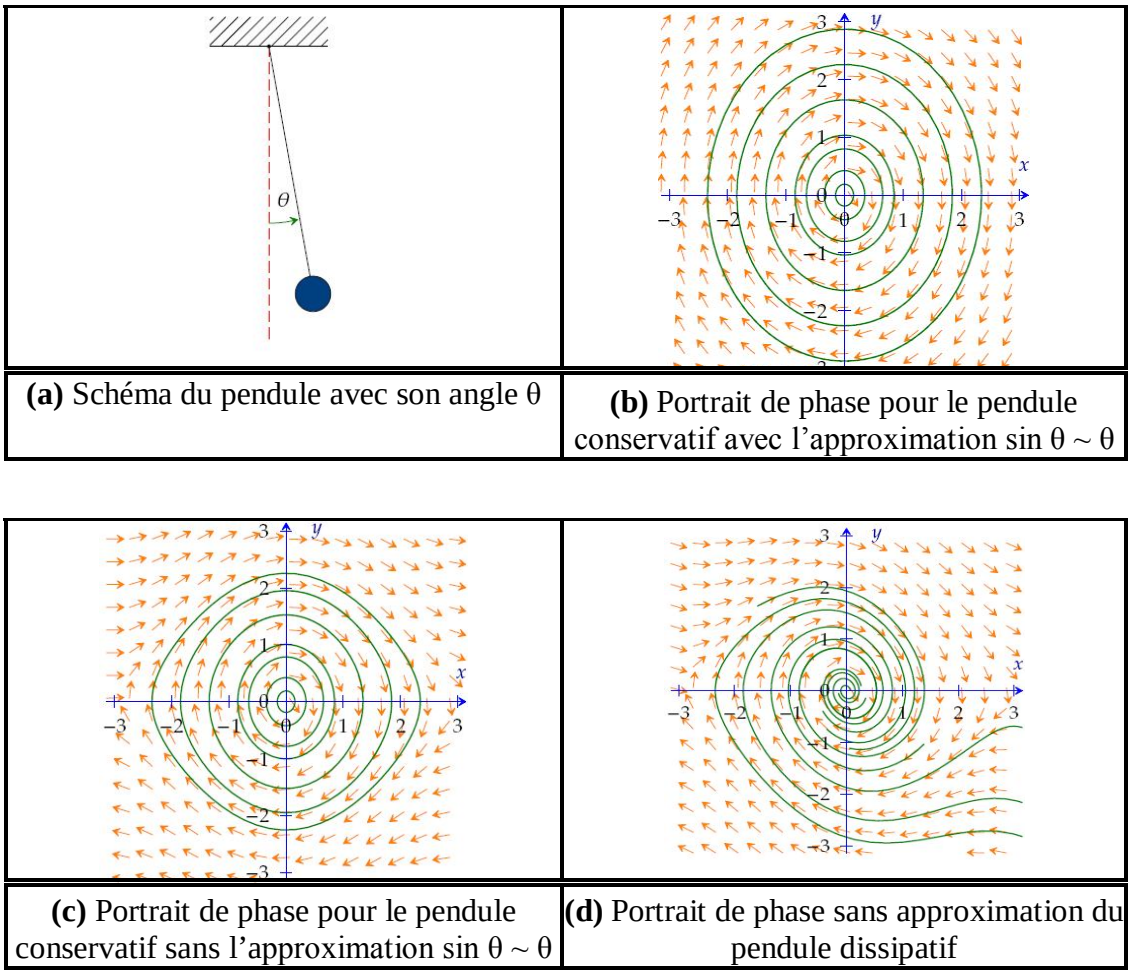
L'objet géométrique observé (fig. 1.6) est relativement complexe et dégage la richesse d'informations que contient le système de Rössler. Un attracteur chaotique possède notamment la propriété remarquable suivante : la trajectoire ne repasse jamais par un même état. Ce qui signifie, entre autres, que cette trajectoire passe par une infinité d'états.

1.3.4 Système dissipatif

L'exemple du pendule dans le cas dissipatif (fig. 1.7) nous montre que, dans l'espace des phases, la trajectoire est *attirée* vers le point de repos. Étudier ce qui se passe au voisinage de ce point, pourrait se révéler être très instructif [4].

1.3.4.1 Etude du voisinage du point d'équilibre

On a pu constater que le pendule obéissait à une équation de la forme $\dot{X} = F(X)$ (équation (1.11)), ceci nous permet d'effectuer un développement limité du premier ordre au voisinage du point d'équilibre.



(a) Schéma du pendule avec son angle θ	**(b)** Portrait de phase pour le pendule conservatif avec l'approximation sin θ ~ θ
(c) Portrait de phase pour le pendule conservatif sans l'approximation sin θ ~ θ	**(d)** Portrait de phase sans approximation du pendule dissipatif

Figure 1.7: Les différents portraits de phase du pendule

À l'aide de la matrice Jacobienne J_F de F et du vecteur X_0 dont les coordonnées sont celles du point d'équilibre, nous pouvons donner une approximation de l'évolution du système lorsqu'il est soumis à une perturbation δX :

$$F(X_{\dot{a}} + \delta X) = F(X_0) + J_F(X_0)\delta X + o(\delta X) \qquad (1.12)$$

Dans le cas du pendule : X_0 est le vecteur nul et F(0) = 0 donc, étant donné que

$J_F(0) = \begin{pmatrix} 0 & 1 \\ -\omega_0^2 - 2\alpha \end{pmatrix}$, on trouve, en prenant $\delta X = \begin{pmatrix} \delta x \\ \delta y \end{pmatrix}$:

$$F\left(\begin{pmatrix} \delta x \\ \delta y \end{pmatrix}\right) = \begin{pmatrix} \delta \dot{x} \\ \delta \dot{y} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -\omega_0^2 - 2\alpha \end{pmatrix} \cdot \begin{pmatrix} \delta x \\ \delta y \end{pmatrix} + 0\left(\begin{pmatrix} \delta x \\ \delta y \end{pmatrix}\right) \qquad (1.13)$$

Avant de diagonaliser la matrice Jacobienne, une remarque s'impose. La trace de la matrice Jacobienne est dans le cas général : $\mathrm{Tr}(\mathrm{J_F}) = \frac{\delta F_x}{\delta x} + \frac{\delta F_y}{\delta y}$.

(ou $\mathrm{Tr}(\mathrm{J_F}) = \frac{\delta F_x}{\delta x} + \frac{\delta F_y}{\delta y} + \frac{\delta F_z}{\delta z}$ en 3 dimensions).

La valeur de la trace de J_F est donc en fait la divergence de F :

$$divF = \mathrm{Tr}(\mathrm{J_F}) \tag{1.14}$$

Dans le cas du pendule : $divF = Tr(J_F(0)) = -2\alpha$, la divergence est négative, cela traduit la dissipation de l'énergie qui fait que la trajectoire tend vers le point de repos.

Cette parenthèse étant terminée, revenons-en à la diagonalisation de J_F. Si J_F est diagonalisable alors, on considère une base de vecteurs propres $\vec{u}_1, \vec{u}_2$ avec λ_1, λ_2 les valeurs propres associées et :

$$\delta X(t) = \mu_1 e^{\lambda_1 t}\vec{u}_1 + \mu_2 e^{\lambda_2 t}\vec{u}_2$$

Remarque :

λ_1 et λ_2 peuvent être complexes conjuguées.

Puisque les valeurs propres peuvent être complexes conjuguées, on distingue les trois cas suivants :

- Une des valeurs propres est à partie réelle positive : la trajectoire s'éloigne exponentiellement du point d'équilibre.
- Les deux valeurs propres sont à partie réelle négative : la trajectoire converge vers le point de repos.
- Si l'une (ou les deux) des valeurs propres est nulle : une des composantes de l'erreur δX (ou les deux) reste constante.

Les valeurs propres évoquées sont appelées *exposants de Lyapunov*.

1.3.4.2 Systèmes entretenus

Pour construire une horloge, il faut palier au problème de la perte d'énergie du pendule en concevant un dispositif qui pourrait entretenir les oscillations. On ne s'intéresse pas ici à la manière dont est réalisé ce dispositif mais plutôt à ses effets. Nous étudions donc un pendule forcé de manière sinusoïdale dont l'équation est :

$$\ddot{\theta} + 2\alpha\dot{\theta} + \omega_0^2 \sin(\theta) = \gamma\omega_0^2 \cos(\omega t) \tag{1.15}$$

La matrice Jacobienne du système n'a pas changé, le système est toujours dissipatif, il est attiré par le point de repos. Cependant, expérimentalement le pendule ne s'arrête jamais d'osciller, il n'atteint jamais le point de repos.

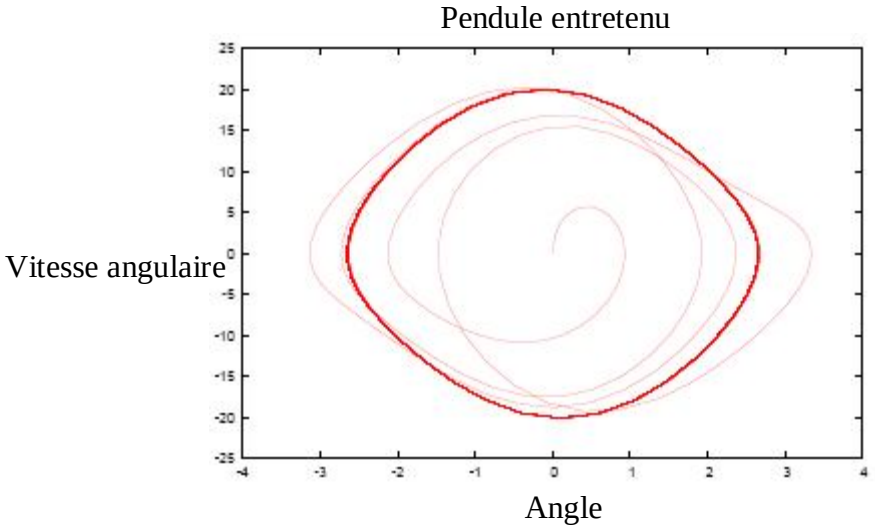


Figure 1.8: Portrait de phase du pendule forcé pour: $\omega = \pi$, $\alpha = \omega_0 / 4$ [4].

On observe (fig. 1.8) que, partant du point de repos, la trajectoire finit par se stabiliser sur une courbe fermée, on a alors un signal périodique en sortie de l'oscillateur. Cette convergence de la trajectoire vers une courbe fermée, similaire au second cas de la figure 1.7, est appelée *cycle limite*. Il faut en fait regarder ce qui se passe sur un temps infini pour observer la courbe fermée, d'où la notion de limite.

1.3.4.3 Section de Poincaré

Henri Poincaré a apporté une contribution très utile pour l'étude des systèmes chaotiques. Parmi ces contributions on trouve les *sections de Poincaré*. Faire une section de Poincaré revient à couper la trajectoire dans l'espace des phases, afin d'étudier les intersections de cette trajectoire (en dimension trois, par exemple), avec un plan. On passe alors d'un système dynamique à temps continu à un système dynamique à temps discret. Les mathématiciens ont bien sûr démontré que les propriétés du système sont conservées après la réalisation d'une section de Poincaré judicieusement choisie. Dans un premier temps nous allons voir quelles sont les différentes sections de Poincaré utilisées en général.

1.3.4.3.1 Exemples de sections de Poincaré

La section de Poincaré la plus naïve est de couper la trajectoire dans l'espace des phases par un plan (en dimension trois) ou par une droite (en dimension deux).

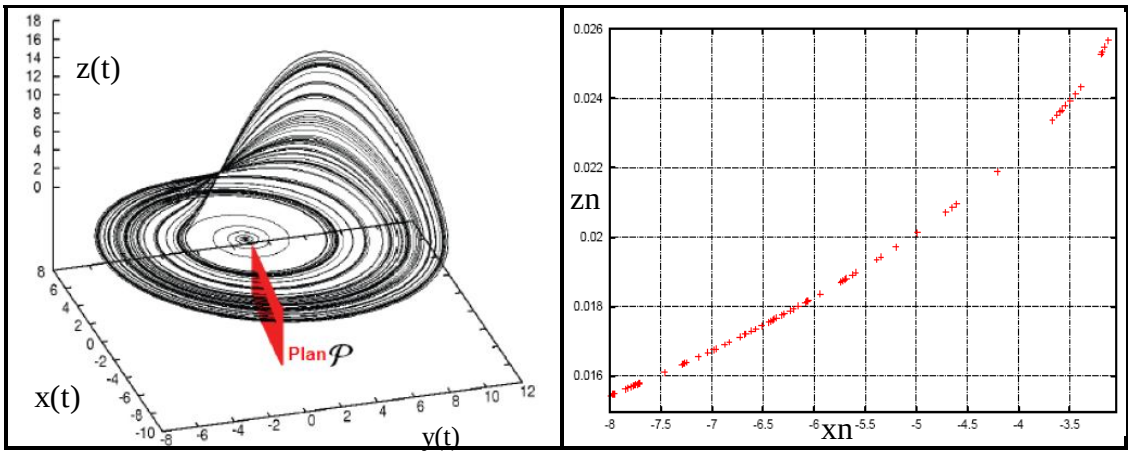
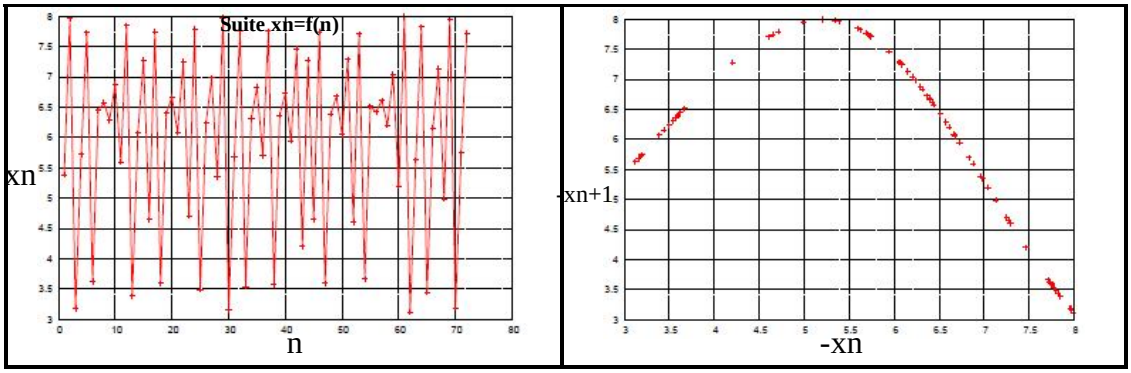


Figure 1.9: Intersections de la trajectoire de l'attracteur de Rössler avec un plan φ d'équation $y = 0$ $(x \leq 0)$ [4].

Sur la figure 1.9, on voit clairement que si on observe l'intersection de la trajectoire du système Rössler avec le plan φ il faut alors étudier les deux suites $(x_n)_{n\in N}$ et $(z_n)_{n\in N}$.

On peut se restreindre à l'étude de la suite $(-x_n)_{n\in N}$ l'opposée de la suite $(x_n)_{n\in N}$ car toutes les valeurs de $(x_n)_{n\in N}$ sont négatives.

La figure 1.10 montre que l'évolution de la suite $(-x_n)_{n\in N}$ est clairement chaotique. Pourtant, on observe que la caractéristique $(-x_{n+1})_{n\in N} = f\ (-x_n)_{n\in N}$ semble dégager une certaine régularité, on dirait en effet que cette caractéristique est assimilable à une parabole. Ou du moins, la fonction qui a x_n associe x_{n+1} semble pouvoir être approximée par une fonction polynomiale, ce qui peut quand même paraître étonnant étant donné le comportement de la suite $(-x_n)_{n\in N}$. Nous voyons que cette section de Poincaré conserve les propriétés du système d'origine :



(a) $-x_n = f\,(n)$ **(b)** $-x_{n+1} = f\,(-x_n)$.

Figure 1.10: La suite $(-x_n)_{n\in N}$ [4]

La suite $(-x_n)_{n\in N}$ est effectivement chaotique.

Une autre façon de réaliser une section de Poincaré, toute aussi intéressante, consiste à regarder la suite des maximums de l'une des grandeurs du système (surface d'équation $\dot{x} = 0$) .

Prenons par exemple la grandeur $y(t)$ du système de Rössler, et observons la suite des maximums successifs correspondantes, notée U_n. La figure 1.11 montre la caractéristique $U_{n+1} = f\,(U_n)$, celle-ci a les mêmes propriétés que la caractéristique donnée en figure 1.10 (à droite).

Cependant, la courbe n'est pas exactement la même, il faut chercher leurs similitudes au delà de leurs apparences, le calcul de leur pente moyenne (moyenne géométrique), nous montrerait que ces deux fonctions ont la même pente moyenne. C'est parce que la valeur de la pente moyenne de ces fonctions est liée à l'exposant de Lyapunov de la grandeur y(t).

Les deux techniques que nous venons d'exposer sont surtout valables pour des systèmes autonomes, c'est-à-dire des systèmes qui ne sont pas forcés. Qu'en est-il pour le pendule forcé par exemple ? Et bien pour les systèmes entretenus, et en particulier pour le pendule, on étudie l'une des grandeurs du système, par exemple $\theta(t)$ pour le pendule, et l'on regarde les valeurs de cette grandeur à des temps multiples de la période T_e d'excitation (phase constante). Pour le pendule, on étudie les valeurs prises par la suite $(u_n)_{n\in N}$ telle que $u_n = \theta(nT_e)$.

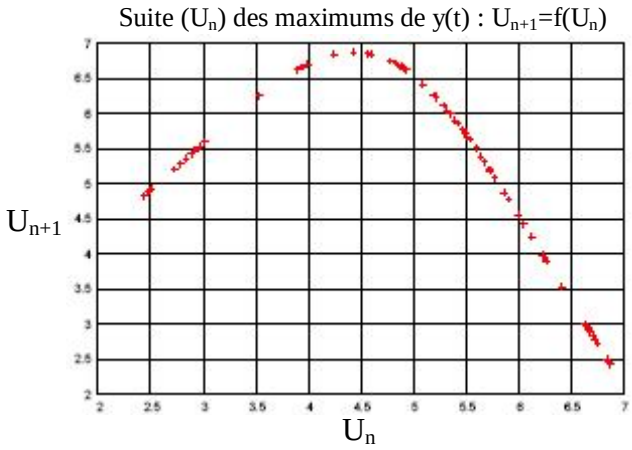


Figure 1.11: La suite $(U_n)_{n\in N}$ des maximums de la grandeur $y(t)$ du système de Rössler [4]

Cette figure montre la caractéristique $U_{n+1} = f(U_n)$). Pour l'instant, l'intérêt des sections de Poincaré n'est pas évident, cependant il est énorme. On va donc, à travers un exemple, étudier l'une des utilisations des sections de Poincaré.

1.3.4.3.2 Application logistique

La figure 1.12 montre que la suite logistique u_{n+1} admet un comportement chaotique.

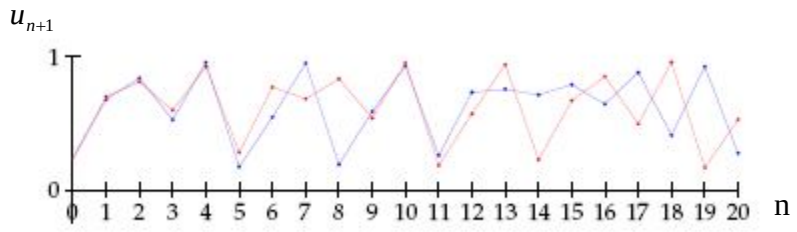


Figure 1.12: Exemple de suite à comportement chaotique : $u_{n+1} = 3.82u_n(1-u_n)$ [4]

Pour deux conditions initiales différentes de 10^{-2}, l'erreur augmente de façon exponentielle durant les huit premières itérations.

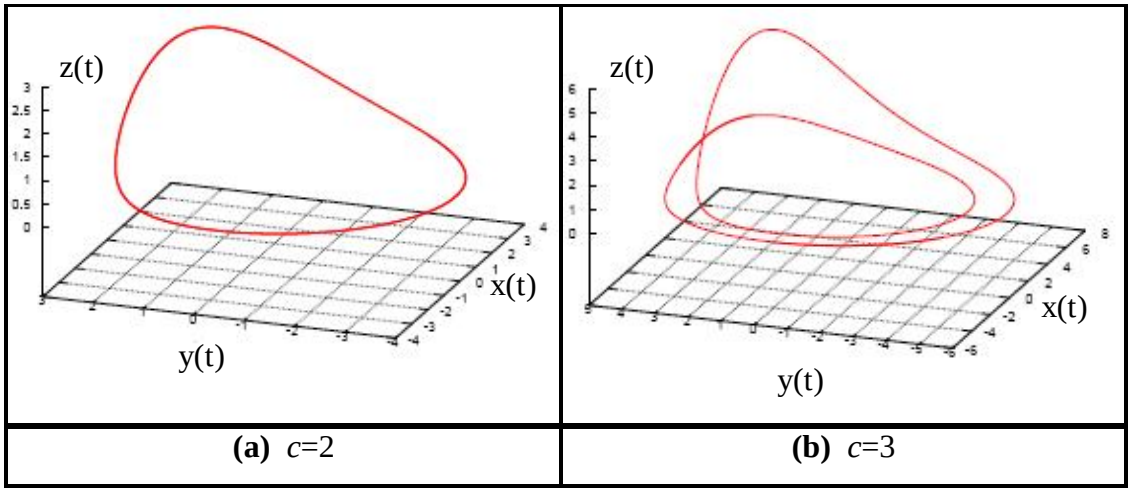
La suite définie par $x_{n+1} = 3.82x_n(1-x_n)$ admet un comportement chaotique et pourtant la suite définie par $x_{n+1} = x_n(1-x_n)$ est clairement convergente car minorée par 0 et décroissante ($\text{car}\, x_{n+1} - x_n = -x_n^2 \leq 0$). Cette conséquence nous amène à définir l'application logistique de la manière suivante :

$$f_r : \begin{cases} [0;1] \to [0;1] \\ x_n \to f_r(x_n) = x_{n+1} = rx_n(1-x_n) \end{cases} \qquad (1.16)$$

L'application logistique dépend d'un *paramètre r* et pour que f_r soit bien de [0 ; 1] dans lui-même, on choisit : $r \in [0; 4]$.

On peut parfaitement imaginer que l'application logistique soit le résultat d'une section de Poincaré faite sur un attracteur chaotique comme celui de Rössler, il suffit de constater que les deux courbes s'apparentent effectivement à des paraboles. On peut même concevoir que les paramètres *c* (ou *a* ou *b*) du système de Rössler et le paramètre *r* de l'application logistique sont liés.

Observons l'effet que peut avoir la modification du paramètre *c* du système de Rössler sur la structure de son attracteur. La figure 1.13 montre bien que pour certaines valeurs de *c* le système de Rössler n'a pas un comportement chaotique.



(a) *c*=2 **(b)** *c*=3

Figure 1.13: Allure de l'attracteur de Rössler pour deux valeurs différentes du paramètre c [4]

Le régime transitoire a été supprimé.

Dans le cas où c = 2, la trajectoire est une courbe fermée, ce qui signifie que les grandeurs de sortie du système de Rössler sont périodiques. On dit alors que l'on se trouve sur une orbite périodique. Pour le second cas, il s'agit toujours d'une orbite périodique, seulement, la période est deux fois plus longue, il y a eu un doublement de période. Pour la suite logistique le comportement est similaire, pour r = 3.2 la suite est périodique ($x_{n+2} = x$) et pour r = 3.5 la période a doublé ($x_{n+4} = x_n$).

Afin de déterminer avec précision les différents comportements possibles de la suite logistique en fonction du paramètre r, on construit un diagramme de bifurcation. Après un certain nombre d'itérations de la suite pour une certaine valeur de r, on place les points correspondants aux p itérations suivantes en abscisses, l'opération est renouvelée pour plusieurs valeurs de r allant de 2.5 à 4. On obtient le diagramme de bifurcation, qui est aussi appelé diagramme de Feigenbaum (fig. 1.14).

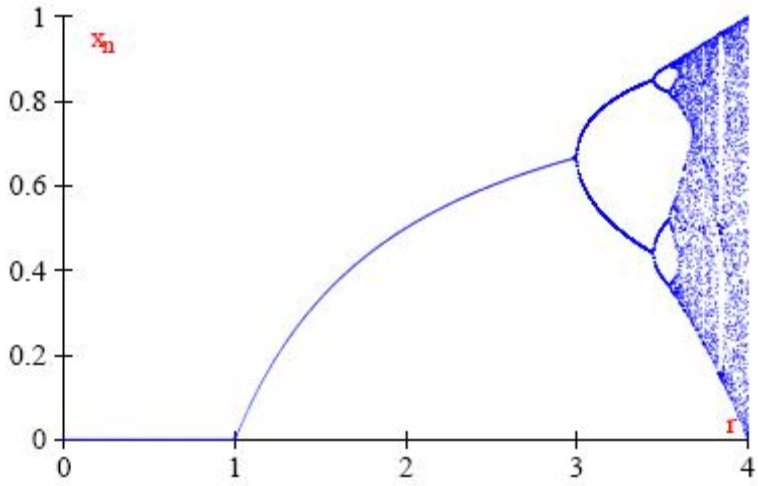


Figure 1.14: Diagramme de bifurcation de la suite logistique [4].

Ce diagramme permet de connaître tous les comportements de la suite logistique en fonction de *r*.

En particulier, pour r = 3 on observe un doublement de période appelé ici bifurcation. Avant de basculer dans le chaos il y une cascade de doublements de période. Après un doublement de période l'orbite périodique précédente est toujours présente mais instable, ce qui explique qu'elle n'est pas visible sur le diagramme de bifurcation, un système chaotique a donc une infinité d'orbites périodiques.

1.3.5 Exemples de systèmes chaotiques

En 1963, Lorenz a donné le premier système dynamique chaotique autonome de dimension trois. Plusieurs modèles sont issus à partir du modèle de Lorenz; parmi ces derniers, on distingue une classe des systèmes chaotiques qu'on appelle les systèmes généralisés, ceux-ci englobent plusieurs modèles : les systèmes de Chen, Chua, Lorenz, Lü.

Ci-dessous, quelques exemples de systèmes chaotiques vont être exposés :

1.3.5.1 Systèmes à temps continu

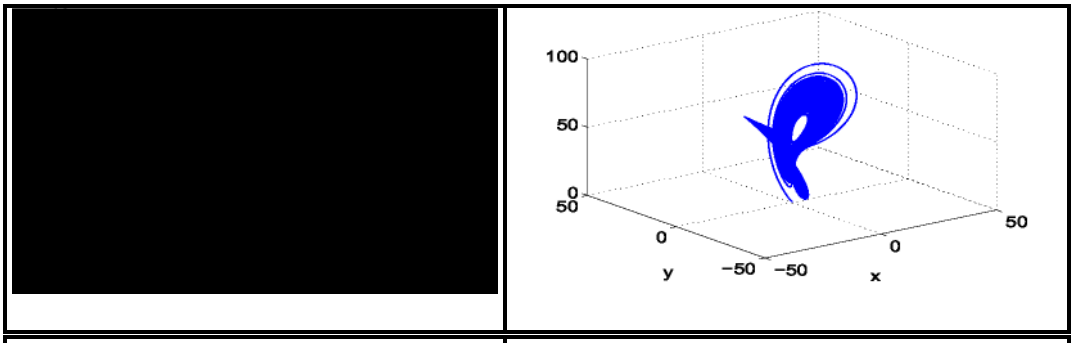
Les exemples considérés sont: le système de Lorenz, le système de Rössler et le système de Chua.

1.3.5.1.1 Système de Lorenz

Le système de Lorenz est un exemple célèbre de système différentiel au comportement chaotique, pour certaines valeurs de paramètres. Ce système est défini par les équations suivantes :

$$\begin{cases} \dot{x} = \sigma(y - x) \\ \dot{y} = -rx - y - xz \\ \dot{z} = -bz + xy \end{cases} \tag{1.17}$$

Ci-dessous l'attracteur de *Lorenz* (l'espace des phases) et la coordonnée x obtenus à partir des valeurs numériques $\sigma = 10, r = \frac{8}{3}$ et b = 28.



(a) La première coordonnée, x.	**(b)** Attracteur chaotique de *Lorenz*.

Figure 1.15: Système chaotique de *Lorenz* [3].

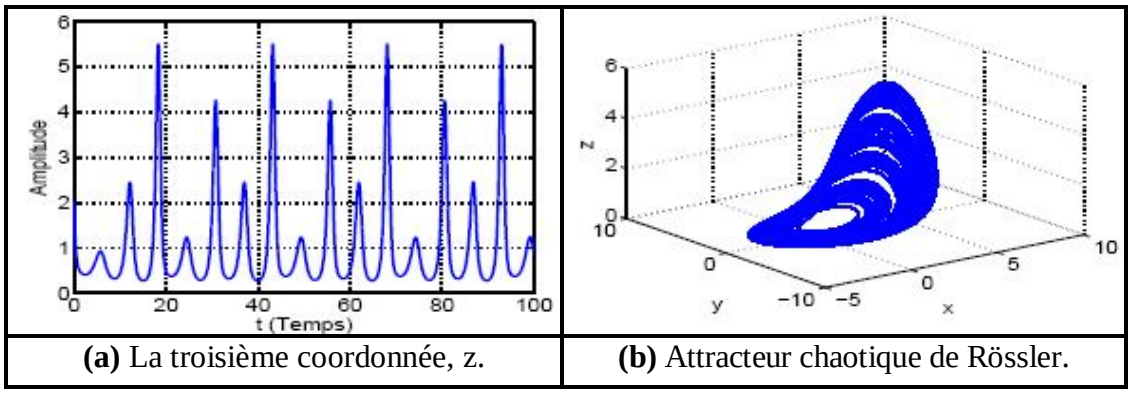
1.3.5.1.2 Système de Rössler

Les équations de ce système sont les suivantes :

$$\begin{cases} \dot{x} = -(y+z) \\ \dot{y} = x + ay \\ \dot{z} = b - cz + xz \end{cases} \qquad (1.18)$$

avec a, b et c des constantes.

Ce système, qui a été 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. Pour une simulation numérique, nous prenons a = 0.398, b = 2 et c = 4. Nous obtenons l'évolution dans le temps de la coordonné z et l'attracteur de Rössler dans la figure ci-dessous [3]:



(a) La troisième coordonnée, z. **(b)** Attracteur chaotique de Rössler.

Figure 1.16: Système chaotique Rössler [3].

1.3.5.1.3 Système de Chua

Le système de *Chua* est à la base un circuit électrique dont le schéma est donné dans la figure 1.17

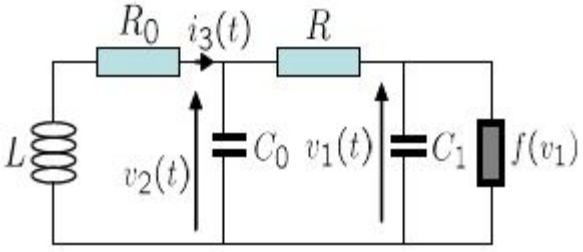


Figure 1.17: Le circuit électrique de Chua [3].

Ce circuit est composé d'éléments passifs (L, C_0, C_1, R_0, R) et d'un élément actif non-linéaire (une diode). Ce simple circuit électrique, développé par *Leon Chua,* possède une dynamique chaotique [3].

La dynamique de ce circuit peut être décrite par les équations d'états suivantes :

$$\begin{cases} \dot{x}_1 = -\dfrac{1}{C_0 R}(x_1 - x_2) + \dfrac{1}{C_0} f(x_1) \\ \dot{x}_2 = \dfrac{1}{C_1 R}(x_1 - x_2) + \dfrac{1}{C_1} x_3 \\ \dot{x}_3 = \dfrac{1}{L} x_2 + \dfrac{R_0}{L} x_3 \end{cases} \qquad 1.19$$

avec

$$f(x_1) = g_b x_1 + \frac{1}{2}(G_a - G_b)\left(|x_1 + E| - |x_1 - E|\right)$$

et

$$x = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} v_1 \\ v_2 \\ i_3 \end{bmatrix}.$$

Le portrait de phases de ce système est donné sur la figure 1.8 :

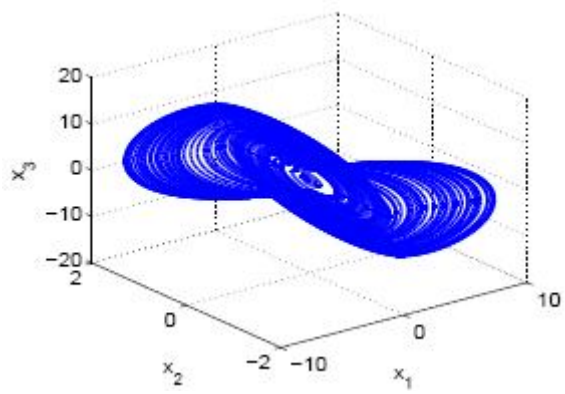


Figure 1.18: L'attracteur chaotique de Chua [3].

Après quelques transformations simples, ce système peut s'écrire sous une autre forme, appelée *forme sans dimension* du circuit de Chua:

$$\begin{cases} \dot{x} = \alpha\left(y - x - f(x)\right) \\ \dot{y} = x - y + z \\ \dot{z} = -\beta y - \gamma z \end{cases} \qquad (1.20)$$

où α, β et γ sont des constantes et f représente la fonction caractéristique de la diode de Chua, qui est donnée par :

$$f(x) = bx + \frac{1}{2}(a-b)\left(|x+1| - |x-1|\right)$$

avec a < b < 0, des constantes.

1.3.5.2 Système à temps discret

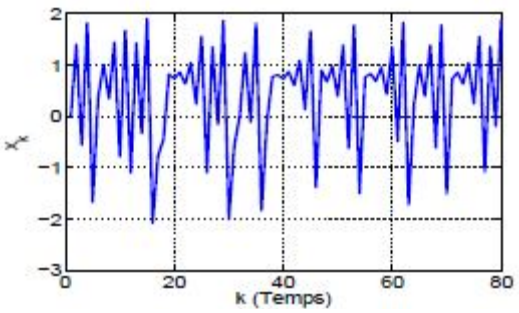
1.3.5.2.1 Système de Henon

Le système de Hénon est un modèle proposé en 1976 par le mathématicien Michel Hénon. Il s'agit d'un système qui introduit des itérations dans le plan. Ces itérations sont définies par les relations suivantes [3]:

$$\begin{cases} x_{k+1} = a - x_k^2 + by_k \\ y_{k+1} = x_k \end{cases}$$

avec k, le nombre d'itérations.

Le portrait de phases (l'attracteur) ainsi que la première coordonnée, x, du système sont représentées sur la figure 1.18 pour a = 1.4 et b = 0,3.



(a) La première coordonnée, x. **(b)** Attracteur chaotique de Henon.

Figure 1.19: Système chaotique de Henon [3].

Il existe d'autres systèmes chaotiques discrets. Nous citons le système de Lozi qui consiste en le système de Henon pour lequel la non-linéarité x_k^2 est remplacée par $\left|x_k^2\right|$.

1.4 SYSTEMES HYPERCHAOTIQUES

1.4.1 Définition

Un attracteur hyperchaotique est généralement défini, comme étant un comportement chaotique avec au moins deux exposants de Lyapunov positifs, combiné avec un exposant nul le long de l'écoulement et un exposant négatif pour garantir la reliée de la solution.

La dimension minimale d'un système hyperchaotique (continu) est 4 [5].

1.4.2 Premier système hyperchaotique

Le premier système hyperchaotique à 4 dimensions a été proposé en 1979 par Rössler. Ce système est défini par les équations suivantes :

$$\begin{cases} \dot{x} = -(y+z) \\ \dot{y} = x + ay + w \\ \dot{z} = b + xz \\ \dot{w} = -cz + dw \end{cases} \tag{1.21}$$

Le système suit un comportement hyperchaotique (fig.1.20), quand les paramètres a, b, c et d prennent les valeurs suivantes : a=0.25, b=3, c=0.5 et d=0.05.

Les conditions initiales peuvent prendre les valeurs suivantes : $x_0 = -10,\ y_0 = -6;$ $z_0 = 0,\ w_0 = 10.0.$

Les quatre exposants de Lyapunov correspondants sont $\lambda_1 = 0.112,\ \lambda_2 = 0.119,$ $\lambda_3 = 0$ et $\lambda_4 = -25.118.$

On constate bien que ce système répond aux conditions de passage du chaos vers l'hyperchaos déjà prédéfinies.

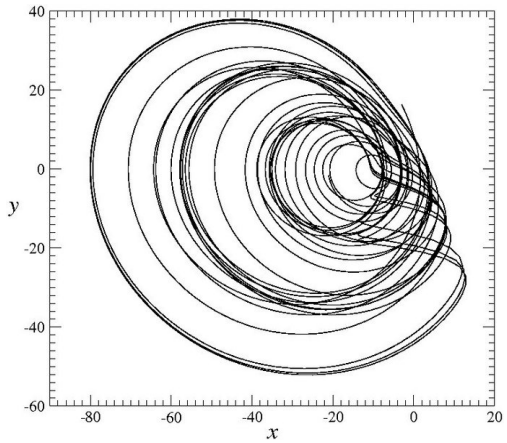


Figure 1.20: Projection plane de l'attracteur hyperchaotique de Rössler de 4D [5].

Le caractère hyperchaotique de ce comportement n'est pas si évident à partir de cette projection d'avion, qui ressemble un peu à un attracteur chaotique "bruyant" [5].

1.4.3 Modèle 9D pour une transition d'hyperchaos du chaos

Un modèle de 9 dimensions, pour une convection Rayleigh-Bénard dans une cellule carrée a été proposé par Reiterer en 1998. Il est défini ainsi :

$$\dot{C}_1 = -\sigma b_1 C_1 - C_2 C_4 + b_4 C_4^{\,2} + b_3 C_3 C_5 - \sigma b_2 C_7$$

$$\dot{C}_2 = -\sigma C_2 + C_1 C_4 - C_2 C_5 + C_4 C_5 - \sigma C_9 / 2$$

$$\dot{C}_3 = -\sigma b_1 C_3 + C_2 C_4 - b_4 {C_2}^2 - b_3 C_1 C_5 + \sigma b_2 C_8$$

$$\dot{C}_4 = -\sigma C_4 - C_2 C_3 - C_2 C_5 + C_4 C_5 + \sigma C_9 / 2$$

$$\dot{C}_5 = -\sigma b_5 C_5 - {C_2}^2 / 2 - {C_4}^2 / 2$$

$$\dot{C}_6 = -b_6 C_6 + C_2 C_9 - C_4 C_9$$

$$\dot{C}_7 = -b_1 C_7 - R C_1 + 2 C_5 C_8 - C_4 C_9$$

$$\dot{C}_8 = -b_1 C_8 + R C_3 - 2 C_5 C_7 + C_2 C_9$$

$$\dot{C}_9 = -C_9 - R C_2 + R C_4 - 2 C_2 C_6 + 2 C_4 C_6 + C_4 C_7 - C_2 C_8$$

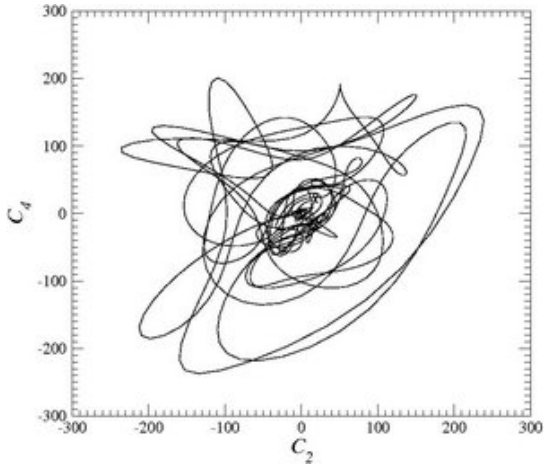


Figure 1.21: Comportement hyperchaotique 9D [5].

Où :

Les paramètres constants b_i sont une mesure de la géométrie de la cellule carrée, définie par :

$$b_1 := 4\frac{1+a^2}{1+2a^2}, \quad b_2 := \frac{1+2a^2}{2(1+a^2)}, \quad b_3 := 2\frac{1+a^2}{1+a^2},$$

$$b_4 := \frac{a^2}{1+a^2}, \qquad b_5 := \frac{8a^2}{1+2a^2}, \qquad b_6 := \frac{4}{1+2a^2}$$

et R=43.3.

Dans les études précédentes, ce système a fait l'objet d'une enquête avec a=0.25 pour laquelle la route vers le chaos est une cascade doublant la période. La transition du chaos à

l'hyperchaos (Figue 1.21) est observée autour de R=43.3, où un deuxième exposant de Lyapunov devient positif (voir l'évolution du spectre de Lyapunov montré dans la Figue 1.22) [5].

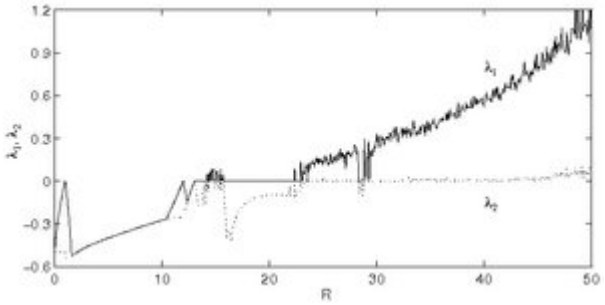


Figure 1.22: Évolution des deux premiers exposants de Lyapunov les plus grands contre la valeur R [5].

Le deuxième exposant de Lyapunov devient positif pour R environ 43.3 suggestion d'une transition lisse de chaotique au comportement hyperchaotique

1.4.5 Comportements hyperchaotiques expérimentaux

Très peu de comportements hyperchaotiques expérimentaux ont été identifiés à ce jour. Comme les systèmes hyperchaotiques (continus) sont minimum de quatre dimensions nécessairement, l'effet de la fonction de mesure h : $R^m \rightarrow R$ devient de plus en plus critique que pour les systèmes chaotiques tridimensionnel (continu chaotique).

En particulier, quand l'exposant positif de Lyapunov λ_1 est suffisamment plus grand que le deuxième exposant positif λ_2, il y a deux différentes échelles de temps dans la dynamique hyperchaotique. En conséquence, il devient tout à fait difficile de reconstruire d'une façon adéquate le signal du départ.

Ainsi, seulement peu de comportements hyperchaotiques expérimentaux ont été identifiés. L'occurrence du comportement hyperchaotique a été trouvée dans un circuit électronique (Matsumoto et Al, 1986), le laser de NMR (le Perron et Al, 1988), dans un système de semi-conducteur (le Perron et Al, 1989) et dans un système de réaction chimique (Eiswirth et Al, 1992). Dans le modèle 9D, la notabilité est de façon significative réduite dans le régime hyperchaotique quand le premier exposant positif de Lyapunov est plus grand que le deuxième exposant de Lyapunov positif [5].

1.5 CONCLUSION

Ce chapitre avait comme objectif, l'introduction de quelques notions élémentaires des systèmes dynamiques chaotiques. Dans la première section les définitions des systèmes dynamiques non-linéaires en temps continu et discret, ainsi que leurs particularisations pour le cas de systèmes chaotiques ont été données. Et pour une meilleure compréhension du chaos déterministe, on a présenté par la suite, les systèmes dissipatifs en passant par l'étude de voisinage du point d'équilibre, les systèmes entretenus ainsi que la section de Poincaré. Ensuite, les exemples les plus célèbres des systèmes chaotiques à temps continus et discrets ont été exposés. Et finalement on a fait une brève présentation des systèmes hyperchaotiques, puisque le reste de ce travail est orienté plutôt vers les systèmes chaotiques.

Dans le chapitre suivant, on étudiera l'application du chaos dans le domaine des télécommunications, et on donnera l'état de l'art des méthodes employées pour les transmissions à porteuse chaotique.

CHAPITRE 2 Cryptographie chaotique

2.1 INTRODUCTION

Dans le domaine des télécommunications, où les échanges d'informations multimédias se développent rapidement, il est indispensable de pouvoir disposer de systèmes sécurisés pour protéger les données à caractère personnel ou confidentiel et assurer la sécurité des transferts de données. Il est donc nécessaire de développer un outil efficace de protection des données transférées et des communications contre les intrusions arbitraires. Le cryptage des données est très souvent le seul moyen efficace pour répondre à ces exigences [6].

2.2 HISTORIQUE

Depuis les années 1990, le chaos est utilisé au cœur des systèmes de transmissions sécurisées, ou crypto-systèmes. Bien que purement déterministe, un signal chaotique présente une forte ressemblance avec un bruit. Par conséquent, les techniques de cryptage chaotique consistent à cacher, à noyer l'information dans un signal porteur chaotique. Cette révolution dans l'étude du chaos a été rendue possible grâce à la découverte de la capacité de synchronisation des systèmes chaotiques, qui semblait a priori impossible [7].

La prolifération des terminaux d'accès à l'information ainsi que l'usage croissant des télécommunications (mettant en œuvre des transferts de données électroniques imposent de disposer de techniques fiables, sécurisées et communément acceptées.

En fait, l'utilisation d'un réseau de communication expose les échanges à certains risques, qui nécessitent l'existence de mesures de sécurité adéquates. Par exemple, les images à transmettre peuvent être enregistrées et copiées durant leur parcours sans pertes de qualité. Les images piratées peuvent être par la suite le sujet d'un échange de données et de stockage numérique illégal. D'après Shannon, les techniques de bases pour un système décryptage peuvent être classées en deux catégories principales : transformation des valeurs (confusion) et permutation des positions (diffusion). La combinaison entre les deux classes est aussi possible. Dans la littérature, plusieurs algorithmes ont été développés et analysés.

Ces algorithmes sont inutilisables sous leurs formes classiques, à cause des contraintes de la vitesse et de la perte de l'information qui peuvent être causées par un crypto-système classique.

Ainsi, des travaux récents pour la sécurisation des données ont été orientés vers la conception des nouveaux algorithmes qui assurent une sécurité fiable tout en minimisant le coût de temps de calcul ainsi que la perte d'information. Nous citons par exemple, les algorithmes qui sont basés sur les signaux chaotiques. Un signal chaotique ressemble à un bruit, mais qui est totalement reproductible du fait qu'il est généré par des modèles mathématiques déterministes. Ce signal est sensible aux conditions initiales, rendre ainsi difficile sa reproduction si le modèle de génération demeure inconnu.

Cependant, ses inconvénients résident principalement dans la nécessité d'effectuer des calculs avec une grande précision et dans le risque d'avoir réussir d'obtenir la clef initiale, après plusieurs tentatives de lancement, et de ce fait, l'attaque du crypto-système devient facile [6].

2.3 LES CRYPTO-SYSTEMES

Un crypto-système a pour but de chiffrer un message clair en un message codé (Cryptogramme) suivant des techniques complexes, incompréhensible par toute personne curieuse (Cryptanalyse ou décrypteur) différente du destinataire légitime [6].

2.3.1 Classification des crypto-systèmes

Les crypto-systèmes peuvent être classés conformément aux différentes caractéristiques. Ainsi, selon les types des clefs utilisées, on a la catégorie suivante des crypto-systèmes : *systèmes symétriques, systèmes asymétriques et systèmes hybrides.* Une autre catégorie des crypto-systèmes est basée sur les techniques de chiffrement : *chiffrement par bloc ou chiffrement par flot.* La notion de sécurité est une autre caractéristique qui peut être utilisée pour classes les crypto-systèmes. Ainsi, on a *les systèmes à sécurité parfaite ou inconditionnelle, les systèmes à sécurité sémantique et les systèmes à sécurité calculatoire* liée à la quantité de ressources informatiques. Cette classification a été inspire à partir de la référence [6].

2.3.2 Relation entre le chaos et les crypto-systèmes

Tout d'abord, nous notons qu'il y a une forte ressemblance entre les systèmes chaotiques et les crypto-systèmes symétriques à chiffrement par bloc.

Pour commencer, un crypto-système est dit bon, s'il satisfera les trois caractéristiques suivantes :

1. Transformation aléatoire des données nettes aux données chiffrées sans garder aucune information sur les données nettes.

2. Soit fortement sensible aux données nettes de telle sorte qu'un plus petit changement dans les données nettes engendre des données chiffrées complètement différentes.

3. Soit aussi fortement sensible à la clef de telle sorte qu'un plus petit changement dans la clef donne une naissance à des nouvelles données chiffrées complètement différentes. Une autre caractéristique importante des crypto-systèmes symétriques et qu'ils utilisent quelques fonctions de chiffrage en mode itératif qui est une condition pratique pour certains crypto-systèmes populaires.

En ce qui concerne les caractéristiques particulières des systèmes chaotiques, notons qu'un système chaotique est constitué de quelques fonctions de base *f* qui sont itérées sur un ensemble *X*. Le fonctionnement d'un tel système consiste à remplir les conditions suivantes :

1. Soit un mélangeur, ceci signifie que l'ensemble *X* devrait être aléatoirement mélangé par la répétition de l'action de *f*.

2. Soit sensible à l'état initial de telle sorte qu'une légère modification dans les états initiaux engendra des états complètement différents.

3. Soit sensible aux certains paramètres de contrôle et un léger changement dans ces paramètres causera un changement dans les propriétés de la carte chaotique.

En comparant entres les particularités d'un crypto-système et les caractéristiques d'un système chaotique, il est évident que le chiffrage et le chaos montrent des similarités remarquables, si nous considérons que les données nettes correspond à un état initial, la clef correspond à l'ensemble des paramètres, et la fonction de chiffrage correspond à la fonction de base *f*.

Cependant, il y a une différence importante entre ces deux concepts. En fait, le crypto-système travaille sur des ensembles finis (discrets), alors que le système chaotique est conçu pour travailler sur des ensembles infinis (continus). C'est probablement la raison principale pour laquelle la relation entre le chaos et le chiffrage a été restée inaperçue [6].

2.4 TRANSMISSION A PORTEUSE CHAOTIQUE

Les signaux chaotiques peuvent être utilisés pour la transmission de l'information, principalement dans deux objectifs : Le premier est de protéger l'information transmise. Dans ce cas, les applications réalisées sont en compétition avec les méthodes de cryptographie classiques. Un deuxième objectif est d'étaler le signal informationnel avec tous les avantages des techniques à étalement de spectre. Dans ce deuxième cas, les méthodes développées doivent être comparées aux systèmes classiques à étalement de spectre [2].

Si on regarde du point de vue de la structure d'un tel système de transmission, on peut définir deux approches : La première, est représentée dans la figure 2.1. Elle remplace le signal porteur sinusoïdal par un modulateur chaotique contrôlé d'une manière quelconque par le signal informationnel. Cette solution a l'avantage d'être très simple à implémenter mais par contre nécessite un système chaotique avec des contraintes fortes sur les paramètres intrinsèques. En plus, celui-ci doit travailler à des hautes fréquences.

En pratique, il est difficile de trouver des circuits permettant un tel fonctionnement et donc, pour le moment, cette solution est surtout considérée dans un cadre théorique.

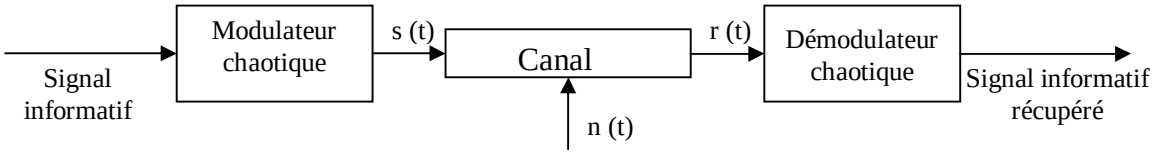


Figure 2.1: Modulation directe du signal informationnel par une porteuse haute fréquence chaotique

Une deuxième solution est de moduler le signal informationnel par celui chaotique en bande de base, et après d'appliquer une transposition en haute-fréquence par l'intermédiaire d'une porteuse sinusoïdale. Ce schéma est présenté dans la figure 2.2. Son avantage principal consiste dans une simplification importante du modulateur chaotique, mais avec une complexité générale du système plus importante.

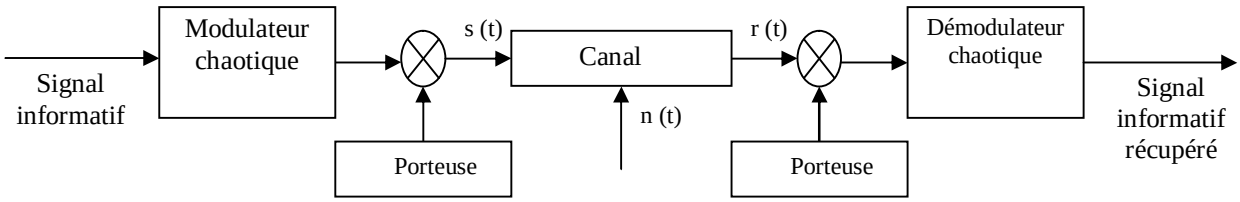


Figure 2.2: Modulation en bande de base du signal informationnel par le signal chaotique, combinée avec une mise sur porteuse classique.

2.4.1 Exemple d'un système de cryptographie chaotique

Cet exemple, exploite les dynamiques chaotiques produites par des lasers à semi-conducteurs pour réaliser des communications optiques sécurisées. Ce type de cryptographie est intéressant pour des utilisations commerciales et militaires. Pour pouvoir être déployées à grande échelle, il est nécessaire que les communications chaotiques apportent un niveau de sécurité plus élevé, soient capables de véhiculer de très grands débits de données et, enfin, qu'elles soient compatibles avec l'infrastructure existante des télécommunications optiques.

Actuellement, les principes utilisés dans les télécommunications classiques ont recours à la théorie linéaire. En particulier, des efforts considérables sont déployés pour faire en sorte que les émetteurs et les récepteurs conventionnels opèrent dans un régime linéaire. Au lieu d'essayer d'éviter les non-linéarités, nous proposons d'exploiter les dynamiques complexes qui sont produites naturellement par des systèmes dynamiques optiques non-linéaires. Ces dynamiques complexes, qui ont longtemps été considérées comme nuisibles, peuvent aussi être une source d'améliorations dans les systèmes de télécommunications. En effet, les dynamiques complexes et imprévisibles peuvent être exploitées pour masquer physiquement un message [8].

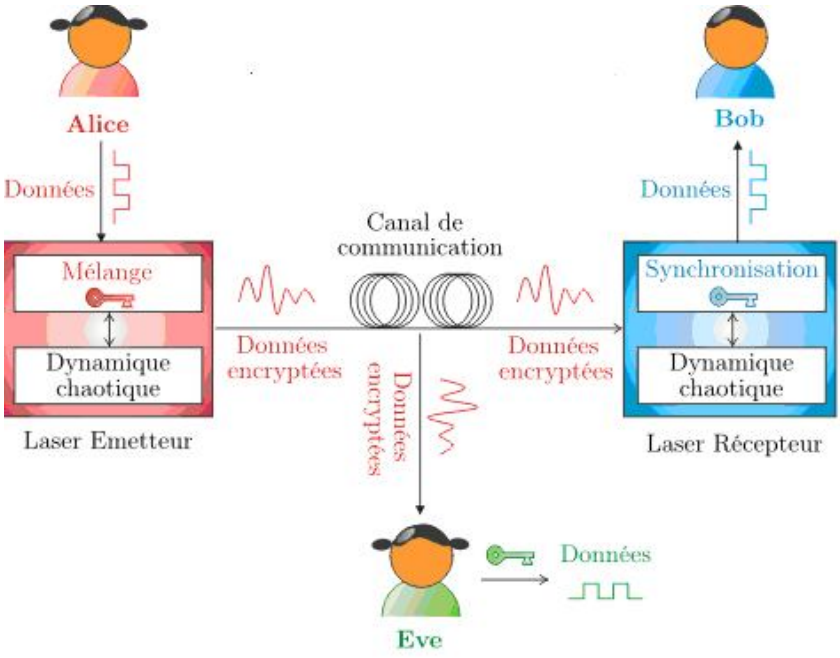


Figure 2.3: Description d'un système de communication par chaos (exemple d'un lazer)

Alice encrypte des données en utilisant la dynamique chaotique d'un laser, les informations sont transmises à Bob qui les décrypte par synchronisation. Une espionne, Eve, peut pirater la ligne et décrypter les informations si elle parvient à identifier le laser d'Alice.

Les systèmes dynamiques non-linéaires peuvent aussi présenter une grande efficacité, étant donné qu'ils réagissent fortement à de faibles perturbations, et peuvent donc être contrôlés et produire des signaux en réponse à une faible énergie de commande. Ils présentent aussi une grande capacité de transport d'information, car la variété d'états complexes produits offre de nombreuses possibilités d'encodage compact de l'information. Enfin, comme les communications optiques non-linéaires ne doivent pas se conformer à la division classique du spectre en bandes de fréquences, le nombre de canaux utilisables pourrait être plus grand que dans le cas de systèmes linéaires. Le nombre de canaux disponibles est en effet uniquement limité par la capacité des récepteurs à distinguer des états chaotiques différents.

Des crypto-systèmes optiques peuvent être construits en utilisant des lasers à semi-conducteurs soumis à une rétroaction optique ou à l'injection optique d'un autre laser. Ce type de système possède un riche comportement dynamique. Dans certaines conditions opératoires, l'intensité optique du laser peut fluctuer de façon chaotique. Ces fluctuations chaotiques peuvent être utilisées pour masquer ou encoder physiquement un message utile en temps réel.

Le décryptage du message est possible en utilisant comme récepteur une copie de l'émetteur, qui se synchronise avec l'émetteur et permet d'extraire le message utile [8].

2.4.2 Masquage chaotique

La méthode de masquage chaotique a été la première solution proposée dans la littérature comme application du chaos aux communications. L'idée est d'additionner directement le signal informationnel s (t) au signal chaotique y (t) et de le récupérer ensuite par synchronisation chaotique (fig.2.4). Le même système est utilisé à la fois à l'émetteur et au récepteur, avec la différence que le récepteur est contrôlé par le signal émis pour obtenir la synchronisation. Il est démontré que grâce à la synchronisation chaotique, à la sortie du système dynamique récepteur, le signal sera plus proche du signal

chaotique original $y(t)$ que de la somme $y(t)+s(t)$. Ainsi avec une simple différence on peut obtenir une approximation $\hat{s}(t)$ du signal informationnel initial. Il est évident que la présence d'un bruit important dans le canal de communication va affecter fortement les performances du système.

Même si cette méthode n'a pas trouvé d'applications directes sur des canaux radio-fréquence, elle est envisagée comme solution de cryptage sur des canaux à fort *SNR*, comme c'est le cas dans la fibre optique [2].

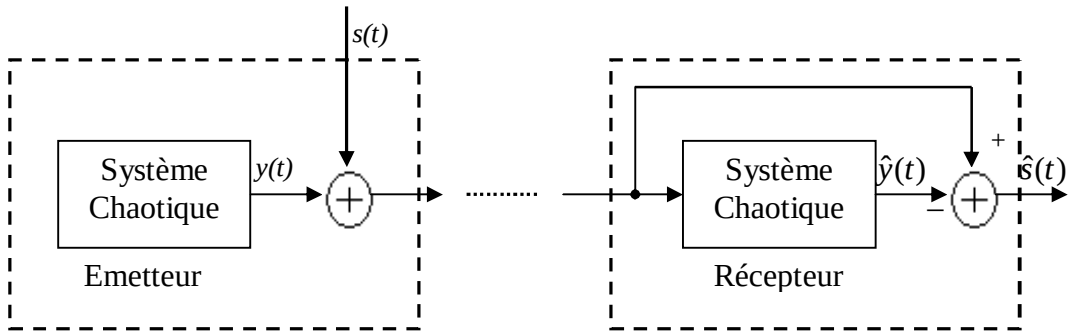


Figure 2.4: Modulation par masquage chaotique

2.4.2.1 Chaos Shift Keying (CSK)

La technique CSK est définie comme une modulation numérique qui associe à chaque symbole informationnel un attracteur ou une somme d'attracteurs différents, en se plaçant dans une période de symbole de durée *T*. Cette définition générale peut être développée analytiquement avec la supposition que chaque attracteur va générer une fonction de base $g_j(t)$ et que l'ensemble des signaux porteurs de l'information s'exprime alors, sur l'intervalle $t \in [iT, (i+1)T]$, comme:

$$s_i(t) = \sum_{j=1}^{N} s_{ij} g_j(t), \quad i=1,2,\ldots,M \qquad (2.1)$$

où $N \leq M$ est le nombre de fonctions de base et M est la dimension de l'espace de symboles.

Dans la figure 2.5 on présente le schéma générique pour un système de communication CSK en bande de base. Du côté de l'émetteur la construction de la forme d'onde courante, associée au symbole *i*, est définie par l'équation (2.1). Ainsi on suppose une commutation des coefficients s_{ij} aux instants multiples de la durée symbole *T*. Si dans le cas d'un système de transmission classique les formes d'onde des fonctions de base ont un caractère périodique, dans le cas du CSK cette condition ne reste plus valable à cause du caractère chaotique des attracteurs utilisés pour la génération de ces fonctions de base.

A la réception on suppose que la forme du signal reçu $r_i(t)$, associée au symbole *i*, est donnée par la version du signal émis $s_i(t)$ affectée par un bruit additif $n(t)$:

$$r_i(t) = s_i(t) + n(t) \tag{2.2}$$

La structure usuelle d'un récepteur CSK repose sur une batterie de corrélateurs, en fonction du nombre de fonctions de base *N* utilisées par l'émetteur. Les fonctions $\{y_j(t)\}_{j=1..N}$ forment l'ensemble des fonctions de base utilisées pour mettre en place le mécanisme de corrélation [2].

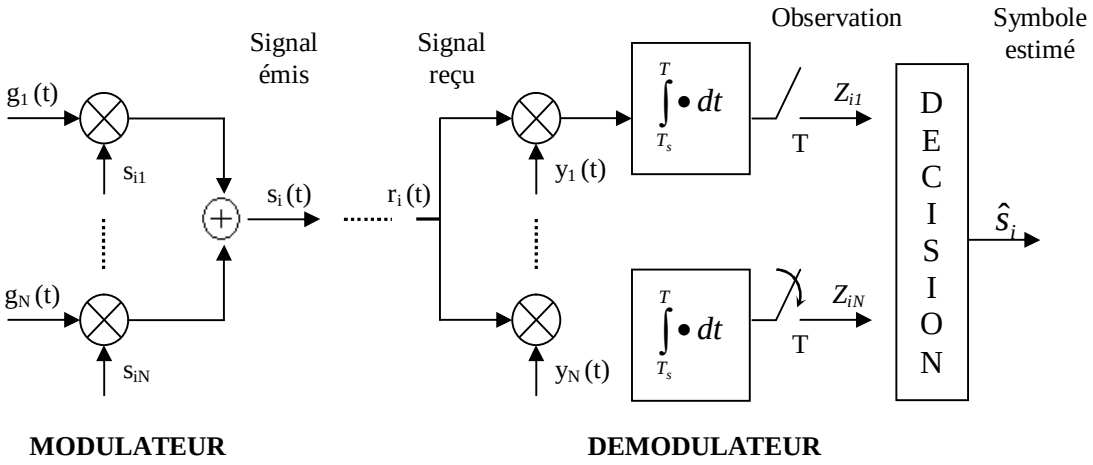


Figure 2.5: Système générique de communication CSK

Le choix de ces fonctions est fait par rapport à une structure particulière du récepteur. Après corrélation, le vecteur d'observation $z_i = [z_{i1},...,z_{iN}]^T$ est utilisé pour faire la décision du symbole transmis $\hat{s}_i$.

Pour cette configuration de récepteur, comme dans le cas des communications numériques classiques, on peut considérer les quatre cas suivants [2] :

2.4.2.1.1 Récepteur cohérent qui utilise une méthode de synchronisation chaotique

Dans ce cas, les références $\{y_j(t)\}$ correspondent aux fonctions de base originales $\{g_j(t)\}$ reconstruites à partir du signal reçu à l'aide d'une méthode de synchronisation chaotique (fig. 2.6).

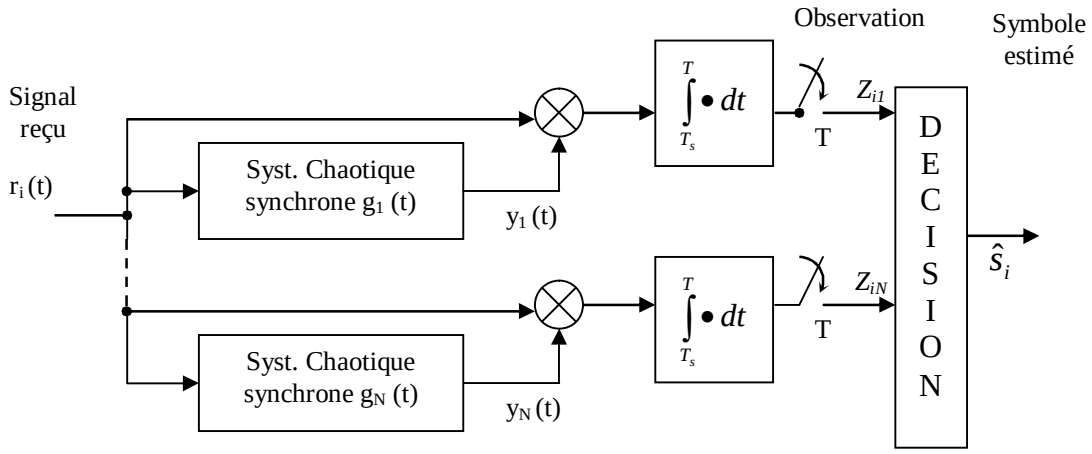


Figure 2.6: Récepteur cohérent CSK

Dans cette structure le signal reçu va essayer de synchroniser tous les systèmes chaotiques, ainsi en supposant que le signal transmis est $s_i(t) = g_j(t)$, à la sortie du $j^{ème}$ circuit chaotique synchrone, on va avoir une convergence de $y_j(t)$ vers $g_j(t)$. T_s est le temps nécessaire pour que la synchronisation soit réalisée.

En contraste avec la synchronisation de ce système, tous les autres vont avoir un caractère divergent par rapport au $j^{ème}$ attracteur. La prise de décision sera alors faite à partir de l'erreur de synchronisation, en sortie des corrélateurs. Ainsi, on peut affirmer sans doute que la convergence de $y_j(t)$ vers $g_j(t)$ sur l'intervalle $[T_s, T]$ va nous donner une

observation $z_{ij} > z_{ik}, \forall k = 1...N, k \neq j$. Avec une telle conclusion l'étape de décision consiste à prendre la valeur caractérisée par l'énergie maximale.

Analytiquement on peut écrire que la valeur du coefficient d'observation z_{ij} est donnée par :

$$\begin{aligned} z_{ij} &= \int_{T_s}^{T} r_i(t) y_j(t) dt \\ &= \int_{T_s}^{T} [s_i(t) + n(t)] y_j(t) dt \\ &= \int_{T_s}^{T} g_j(t) y_j(t) dt + \int_{T_s}^{T} n(t) g_j(t) dt \end{aligned} \tag{2.3}$$

Ceci nous montre que z_{ij} est une variable aléatoire, dont la valeur moyenne va dépendre de l'énergie par élément binaire et de la qualité de synchronisation.

L'inconvénient important présenté par cette méthode est que la synchronisation est perdue et ensuite récupérée chaque fois que le symbole informationnel change. Ainsi, le temps nécessaire pour la transmission d'un seul symbole est donné par le temps de synchronisation plus le temps d'estimation, dont le vecteur d'observation est calculé. Par conséquence le débit de transmission possible est limité par l'inverse du temps de synchronisation [2].

2.4.2.1.2 Récepteur cohérent de type filtre adapté

Dans le cas des transmissions classiques, si cette solution est équivalente aux structures cohérentes de type corrélateur, elle n'est pas utilisable dans le cas des transmissions à porteuse chaotique. L'impossibilité vient du fait que les formes d'ondes employées dans la modulation doivent être connues en avance, contrairement aux systèmes chaotiques où ces formes d'ondes changent d'un symbole à l'autre [2].

2.4.2.1.3 Récepteur non-cohérent

Dans le cas de la détection non-cohérente, la référence côté récepteur ne sera plus obtenue par l'intermédiaire d'une synchronisation chaotique, mais par contre elle va correspondre à une partie du signal reçu (fig 2.7).

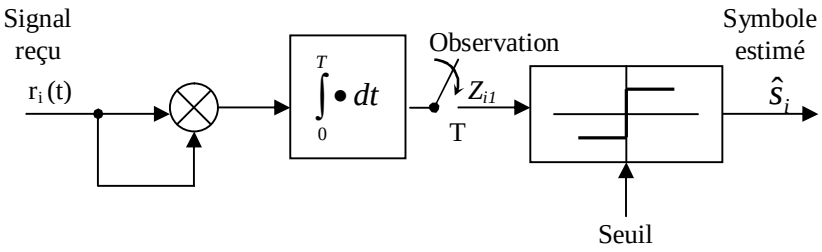


Figure 2.7: Récepteur non-cohérent CSK/COOK

Dans la littérature deux systèmes CSK non-cohérents sont proposés :

2.4.2.1.3.1 Système COOK (Chaotic on-off keying):

Ce système offre la plus simple solution, le signal informationnel binaire est directement multiplié par le signal chaotique. Ce principe est équivalent à associer le signal $s_1(t) = g_1(t)$ au mot binaire "1", et le signal $s_2(t) = 0$ au mot binaire "0". Dans ce cas, le récepteur présenté dans la figure 2.7, va évaluer l'énergie par bit transmis et va prendre la décision en utilisant un comparateur à seuil [2].

2.4.2.1.3.2 Système CSK non cohérent

Il utilise des propriétés qui peuvent différencier les différentes formes d'onde associées aux symboles transmis, au niveau statistique par exemple. La structure présentée dans la figure 2.7 reste la même avec la prise décision cette fois effectuée sur les paramètres d'intérêt.

Généralement, ces solutions sont envisageables, étant donné que les propriétés statistiques entre les différents attracteurs chaotiques sont différentiables. Par exemple, dans les fonctions de base sont deux signaux chaotiques caractérisés par des fréquences moyennes différentes. Côté récepteur les signaux peuvent être identifiés en mesurant la valeur moyenne de la fréquence quand le signal change de signe.

D'autres méthodes de modulation considèrent, par exemple, l'évaluation de la fonction d'auto-corrélation qui est modifiée selon le symbole à transmettre [2].

2.4.2.1.4 Récepteur cohérent différentiel (DCSK : Differential Chaos Shift Keying)

Dans le cas du récepteur cohérent CSK, les fonctions de base $g_i(t)$ doivent être récupérées avant que toute démodulation soit possible. Il existe des situations pour

lesquelles, cette approche est impossible, à cause des mauvaises conditions de propagation.

Dans ce cas, la seule solution cohérente disponible est une solution différentielle, ainsi on va transmettre sur une partie de la durée du symbole une référence, et le reste est associé à la transmission de l'information.

Par exemple, pour la modulation DCSK binaire, le symbole "1" est représenté par un signal de référence, de durée *T*/2, suivi d'une réplique exacte de celui-ci retardée bien sûr avec la même durée *T*/2. Pour le bit "0" on transmet le même signal référence suivi cette fois par sa copie inversée. On peut exprimer alors le signal produit par le modulateur pour le $i^{\text{ème}}$ symbole comme [2]:

$$s_i(t) = \begin{cases} x(t) & t_i \le t < t_i + \dfrac{T}{2} \\ b_i x\left(t - \dfrac{T}{2}\right) & t_i + \dfrac{T}{2} \le t < t_i + T \end{cases} \qquad (2.4)$$

où $x(t)$ désigne le signal issu d'une source chaotique et $b_i \in \{-1,+1\}$, représente le $i^{\text{ème}}$ symbole informationnel à transmettre.

Côté récepteur, la démodulation est réalisée en utilisant une structure similaire au CSK non-cohérent.

Ainsi, on introduit dans ce cas une cellule à retard, qui permet au signal de référence et à celui porteur de l'information d'être en phase (fig. 2.8).

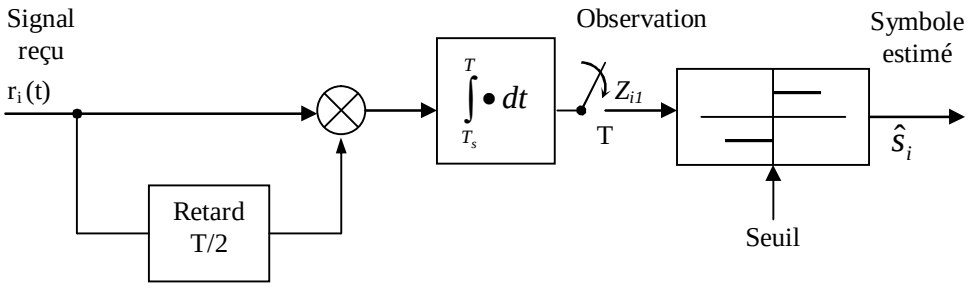


Figure 2.8: Récepteur non-cohérent DCSK

Analytiquement la valeur z_i observée est donnée par la relation suivante :

$$z_i = \int_{T/2}^{T} r_i(t) r_i\left(t - \frac{T}{2}\right) dt$$

$$= \int_{T/2}^{T} [s_i(t) + n(t)]\left[s_i\left(t - \frac{T}{2}\right) + n\left(t - \frac{T}{2}\right)\right] dt$$

$$= \int_{T/2}^{T} [x(t) + n(t)]\left[b_i x(t) + n\left(t - \frac{T}{2}\right)\right] dt$$

$$= b_i \int_{T/2}^{T} x^2(t) dt + \int_{T/2}^{T} x(t) n\left(t - \frac{T}{2}\right) dt +$$

$$b_i \int_{T/2}^{T} x(t) n(t) dt + n(t) n\left(t - \frac{T}{2}\right) dt$$

Avec l'hypothèse que le bruit présent dans le canal est blanc, le récepteur devient un estimateur non biaisé, avec un seuil de décision nul, indépendant de la variance du bruit présent dans le canal. Une autre observation doit être faite sur le terme associé à l'inter-corrélation avec le bruit, qui va influencer de façon négative les performances. En plus de ce fait, étant donné que l'énergie associée à chaque symbole varie, à cause de la séquence chaotique utilisée, une incertitude doit être encore prise en compte pour déterminer le taux d'erreur binaire. Une solution à ce problème est d'employer une modulation FM qui va nous permettre de garder une énergie constante sur la durée du symbole.

Dans les dernières années, les solutions DCSK ont reçues plus d'attention, étant donné que des systèmes à accès multiple sont proposés avec une évaluation des performances sur des canaux à trajets multiples [2].

2.5 CONCLUSION

Dans ce chapitre, après une introduction à la cryptographie chaotique, une classification des crypto-systèmes a été effectuée ainsi que leurs relations avec le chaos. Pour arriver en dernier à la transmission à porteuse chaotique toute en donnant l'état de l'art sur les différentes techniques de cryptage en utilisant le chaos. Dans le chapitre suivant, nous allons voir les différentes méthodes de synchronisation.

CHAPITRE 3

Synchronisation des systèmes chaotiques

3.1 INTRODUCTION

Le problème majeur soulevé par un système de cryptographie chaotique est clairement explicité par le phénomène de la bille de billard : un joueur de billard est incapable de renvoyer sa bille d'où elle vient. Par conséquent, reproduire exactement le même signal chaotique va devenir une opération très complexe voir impossible [9].

Une découverte surprenante a été effectuée dans ce domaine en 1996 par Thomas Caroll et Louis Pecora, lorsqu'ils sont parvenus à reproduire à l'identique un signal électrique chaotique et à le mettre en phase avec le signal original. Ils ont pour ainsi dire réussi à renvoyer la bille de billard exactement sur sa trajectoire. C'est la synchronisation des signaux chaotiques [9].

3.2 HISTOIRE DE LA SYNCHRONISATION

....Pendant que j'étais obligé de garder la chambre durant quelques jours, j'étais occupé de faire des observations sur mes deux horloges du nouvel atelier ; j'ai remarqué un effet admirable auquel personne n'aurait jamais penser : C'est que ces deux horloges, accrochées l'une à côté de l'autre avec une distance d'un ou deux pieds l'une de l'autre gardent entre elles une précision si exacte, que les deux pendules battent toujours ensemble sans jamais varier ; ce que j'avais fort admiré pendant un certain temps. J'ai finalement constaté que ceci s'est produit en raison d'une sorte de sympathie : quand j'ai fait balancer les pendules à un rythme différent, j' ai constaté qu'une demi-heure plus tard, ils sont toujours revenus à la synchronisation ....cette fois je les ai mis

l'une plus loin de l'autre, accrochant une d'un côté de la salle et l'autre à une quinzaine de pieds plus loin, j'ai vu qu'après un jour, il y a eu une différence de cinq secondes entre elles et, par conséquent, leur accord plus tôt était seulement dû à de la sympathie... A mon avis, cela ne peut pas être provoqué par n'importe quoi, si ce n'est que par une agitation imperceptible de l'aire dû au mouvement du pendule....

C'est par cette lettre qui a été écrite le 26 février 1665 [10], par le scientifique hollandais Cristiaan Huygens, destinée à son père Constantyn Huygens, que le phénomène de la synchronisation a été évoqué pour la première fois. Ce phénomène était un sujet de recherche active depuis les jours les plut tôt de la physique [11].

Christian Huygen aurait constaté que deux de ses horloges à balancier, placée cote à cote, convergeaient rapidement vers un mouvement identique en phase et en fréquence; c'est à dire que les deux horloges avaient une parfaite synchronisation. S'il les perturbait, elles se resynchronisaient en une demi-heure, et s'il les éloignait, la synchronisation cessait. Dans la terminologie moderne, cela signifie que les deux horloges ont été synchronisées dans l'antiphase du à l'accouplement par le support mural.

Au milieu du dix-neuvième siècle, Sir John William Strutt (Lord Rayleigh) a décrit un phénomène intéressant de la synchronisation dans les systèmes acoustiques. Ainsi, Rayleigh a observé non seulement le phénomène de la synchronisation, mais également l'effet relatif d'oscillation.

Le phénomène de la synchronisation chaotique, était probablement le plus ancien effet non linéaire qui a été étudié, mais il a été appliqué seulement dans les années 20, lorsqu' E.V.Appleton et B.Van Der Pol ont étudié des générateurs de triode. Cette nouvelle étape dans la recherche sur la synchronisation a été liée au développement de la physique électrique.

Le 17 février 1920, W.H.Eccles et J.H.Vincent se sont approprié la découverte de la synchronisation d'un générateur de triode basé sur un tube à vide qui produit un courant électrique périodiquement alternatif. Dans leurs expériences Eccles et Vincent ont couplé

deux générateurs fonctionnant a des fréquences légèrement différentes, et ont démontré que l'accouplement a forcé les systèmes pour vibrer avec une fréquence commune [10].

Quelques années après E.Appleton et B.Van Der Pôl ont prolongé les expériences d'Eccles et de Vincent et ont fait la première étape dans l'étude théorique. Ils ont prouvé que la fréquence d'un générateur peut être entrainée, ou synchronisée par un signal externe faible d'une fréquence légèrement différente. La synchronisation a été employée pour stabiliser la fréquence d'un générateur puissant à l'aide d'un signal faible mais très précis.

Jusqu'a ce jour là, il paraissait impossible de synchroniser le chaos, mais dans la littérature plusieurs concepts de synchronisation chaotique ont été proposés. Tout d'abord avec les travaux de Yamada et Fujisaka qui ont utilisé une approche locale de la synchronisation chaotique [2].

Par la suite, Afraimovich et Al ont développé les concepts importants liés à la synchronisation chaotique et ultérieurement Pecora et Carroll ont défini la synchronisation chaotique connue sous le nom de synchronisation identique, développée sur la base de circuits chaotiques couplés, avec l'un appelé maître et l'autre esclave. Ces travaux ont ouvert la voie à des applications du chaos aux télécommunications [2] [22].

Une autre solution plus récente est la méthode de synchronisation généralisée, dont Rulkov et Al ont posé les bases. Cette approche considère aussi une paire de systèmes configurés en maître-esclave, mais cette fois le couplage n'est pas réservé à l'identité.

En parallèle avec ces études, est apparue la notion de synchronisation de phases entre deux circuits chaotiques couplés, dans ce cas la synchronisation vise à réaliser une cohérence de phases entre les variables d'état des systèmes considérés [2] [23]..

3.3 METHODES DE SYNCHRONISATION CHAOTIQUE

3.3.1 Synchronisation identique

Pour illustrer la méthode de synchronisation par couplage entre deux systèmes chaotiques, on a choisi de présenter la synchronisation identique proposée par Pecora et Carroll. Celle-ci a l'avantage de représenter une solution simple et performante de

synchronisation, dont l'objectif est que l'esclave reproduise le plus fidèlement possible l'état du maître, après un régime transitoire [2].

Considérons un système dynamique autonome, en temps continu, de dimension *n*, représenté par la relation suivante :

$$\dot{x}(t) = F(x(t)) \tag{3.1}$$

Où $x = [x_1, ..., x_n]^T$.

Par la suite on divise le système initial en deux sous-systèmes $\{S_1, S_2\}$:

$$\begin{cases} S_1 : \dot{x}^{\{1\}} = F^{\{1\}}(x^{\{1\}}, x^{\{2\}}) \\ S_2 : \dot{x}^{\{2\}} = F^{\{2\}}(x^{\{1\}}, x^{\{2\}}) \end{cases} \tag{3.2}$$

avec les états et les dynamiques définis conformément aux relations suivantes :

$$\begin{aligned} x &= \left[x^{\{1\}}, x^{\{2\}}\right]^T \\ x^{\{1\}} &= \left[x_1, ..., x_m\right]^T \\ x^{\{2\}} &= \left[x_{m+1}, ..., x_n\right]^T \end{aligned} \tag{3.3}$$

$$F(x) = \left[F^{\{1\}}(x); F^{\{2\}}(x)\right] \tag{3.4}$$

Bien sûr, cette opération peut être réalisée de manière arbitraire avec une réorganisation des variables d'état dans un ordre quelconque. On considère maintenant un deuxième sous-système S_2^1 caractérisé par une dynamique identique $F^{\{2\}}$, et un vecteur d'état $\hat{x}^{\{2\}}$ [2]:

$$S_2^1 : \dot{\hat{x}}^{\{2\}} = F^{\{2\}}(x^{\{1\}}, \hat{x}^{\{2\}}) \tag{3.5}$$

On peut dire que ce sous-système réplique S_2^1, est un candidat susceptible de se synchroniser avec la dynamique complète initiale. Pecora et Carroll ont démontré que la condition nécessaire et suffisante pour que cette proposition soit vraie, est que le sous-système S_2^1 soit stable. Cette hypothèse qui est équivalente à la condition de l'ensemble des coefficients Lyapunov du sous-système S_2^1 qui sont négatifs [2] [23].

Une synchronisation parfaite peut alors être accomplie; les trajectoires étant asymptotiquement convergentes :

$$\lim_{t\to\infty} = \left\| \hat{x}^{\{2\}}(t) - x^{\{2\}}(t) \right\| = 0 \tag{3.6}$$

Dans la figure 3.1 on représente graphiquement le processus de décomposition en sous-systèmes, cette fois avec la notation $\mathrm{y} = \mathrm{x}^{\{1\}} + \mathrm{n}$ de la variable d'état qui commande le système S_2^1 où n est un éventuel bruit additif associé au canal de communication. Dans le cas pratique où la variance de ce bruit d'observation est significative, l'équation 3.6 qui traduit la convergence asymptotique ne reste plus valable. Dans ce cas on doit utiliser une approche de synchronisation généralisée [2].

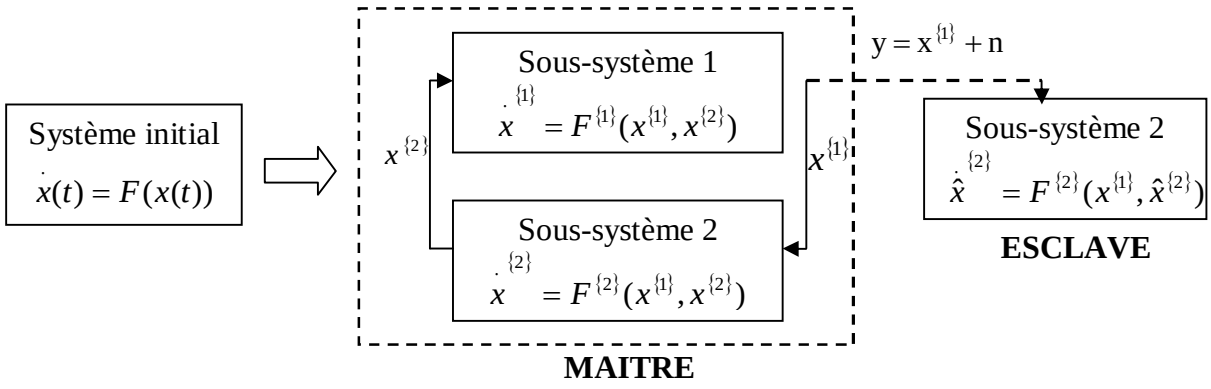
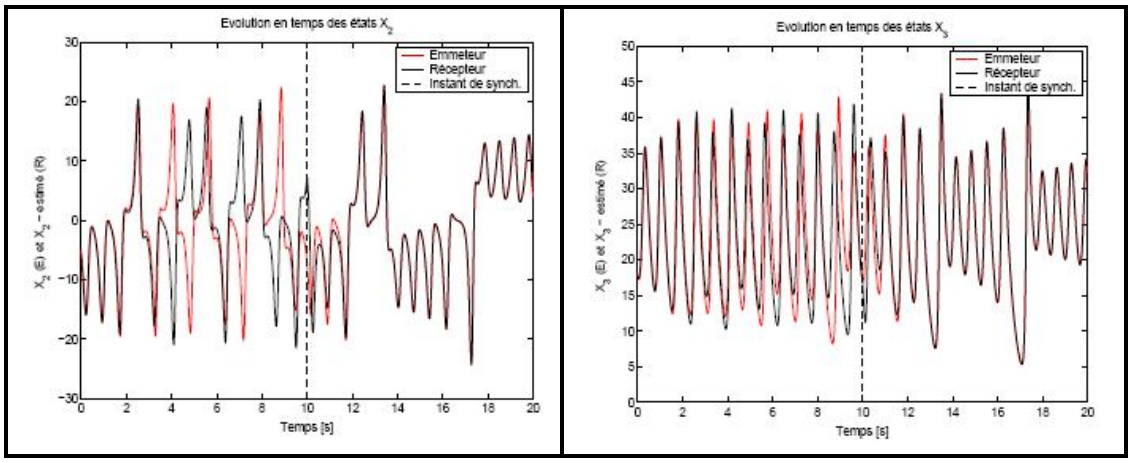


Figure 3.1 Synchronisation Maître-Esclave en utilisant la décomposition en sous-systèmes

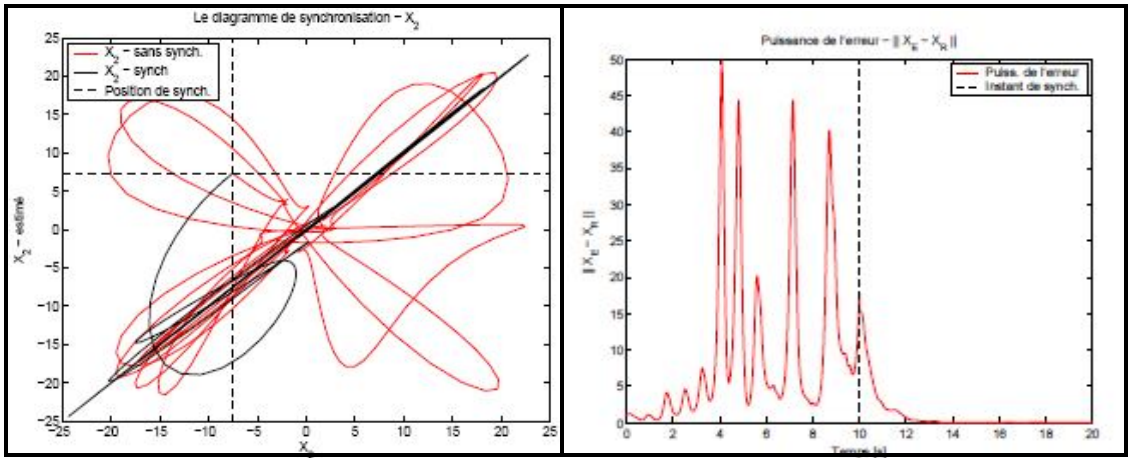
Pour illustrer ce mécanisme de synchronisation on considère de nouveau le système dynamique de Lorentz, donné par les équations (1.3), avec l'ensemble de paramètres : $\{\sigma = 10, \rho = 28, \mathrm{b} = 8/3\}$. L'émetteur et le récepteur sont initialisés séparément avec des conditions initiales proches. Pour une durée de 10 secondes, on les laisse fonctionner indépendamment, ainsi on observe que les trajectoires des deux systèmes deviennent assez vite divergentes. A l'instant *t* = 10 *s* on supprime la dimension *x* du système récepteur et

on le remplace par l'état correspondant côté émetteur. Cette opération va forcer les états *y* et *z* du système esclave à converger asymptotiquement vers les états correspondants du système maître. La garantie de cette convergence est donnée par les valeurs négatives des exposants de Lyapunov (λ_2^1, $\lambda_3^1 \leq 0$) associés au système esclave [2].

Dans les figures 3.2 ce comportement est démontré graphiquement par les représentations des états $y = X_2$ et $z = X_3$. Le diagramme de synchronisation montré pour l'état $y = X_2$ ainsi que la puissance de l'erreur nous confirment encore une fois qu'après une période de transition, le système esclave converge asymptotiquement vers l'état de l'émetteur (maître).



(a) $y = X_2$ **(b)** $z = X_3$



(c) Diagramme de synchronisation pour l'état $y = X_2$ **(d)** Puissance de l'erreur de synchronisation

Figure 3.2: Évolution des états du système maître et de l'esclave avant et après synchronisation [2].

3.3.2 Synchronisation par filtre de Kalman Etendu

La méthode de synchronisation chaotique par filtrage de Kalman Étendu a été introduite comme une généralisation des méthodes de synchronisation à couplage unidirectionnel, telles que la synchronisation identique [2]

L'estimation récursive des états, pour un système chaotique a été proposée pour la première fois par Fowler, avec des aspects sur l'optimalité et la stabilité d'une telle synchronisation.

Plusieurs applications ont été développées par la suite pour des structures de systèmes de communication avec l'emploi dans la démodulation et même l'égalisation du canal. L'objet de cette étude est de proposer des structures de filtrage non-linéaire innovantes, dans la continuité des travaux précités [2].

Par exemple on considère un système en temps discret, autonome défini par la relation générale :

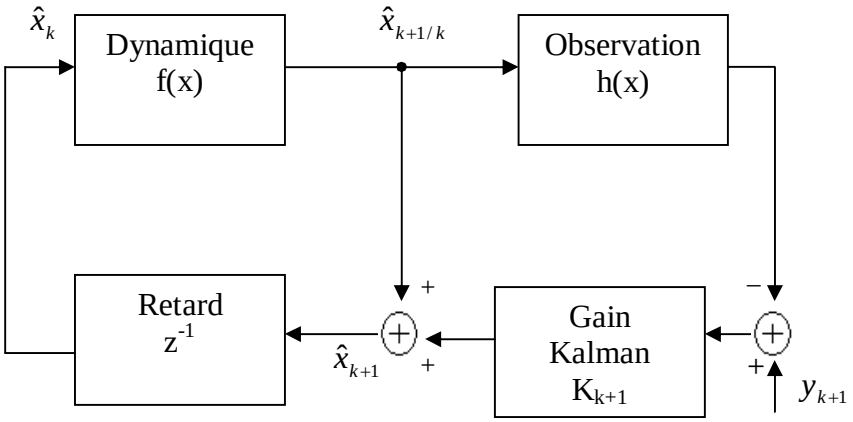


Figure 3.3: Structure de l'estimateur récursif EKF

$$x_{k+1} = f(x_k) \tag{3.7}$$

où $x_k \in R^n$ est le vecteur d'état et $f(\cdot)$ est la dynamique non-linéaire associée.

Pour une efficacité maximale, on a intérêt à transmettre entre l'émetteur et le récepteur un nombre d'état le plus réduit possible, nous supposerons que le signal de contrôle est un scalaire donné par l'équation suivante :

$$y_k = h^T x_k + n_k \tag{3.8}$$

Où $\mathrm{h} = [\mathrm{h}_1, ..., \mathrm{h}_n]^{\mathrm{T}}$, et $\mathrm{n}_k = \mathrm{N}(0, \mathrm{R})$ représente l'éventuel bruit supposé gaussien centré, de variance *R*, associé aux imperfections du canal de communication. Généralement, dans le cadre d'un filtrage récursif de Kalman les équations (3.7) et (3.8) sont appelées modèle de processus et modèle d'observation [2].

L'interprétation dans le cas général d'un tel modèle, est donnée dans la figure 3.3 comme une structure à rétroaction qui permet l'estimation de l'état à partir des observations bruitées. On note que le modèle d'observation dans ce cas ne doit pas respecter forcément une fonction linéaire. Ainsi, dans la partie gauche du schéma on effectue une projection de l'estimation courante $\hat{x}_k$ pour obtenir la valeur a priori du nouvel état estimé $\hat{x}_{k+1/k}$.

Dans la partie droite, ce nouvel état va incorporer l'information apportée par la nouvelle mesure y_{k+1} pour obtenir la valeur estimée a posteriori $\hat{x}_{k+1}$ [2].

Le coefficient de pondération K_{k+1}, appelé aussi gain de Kalman, est calculé par rapport à la dynamique du système. Il donne une évaluation de la confiance accordée aux observations à chaque étape de filtrage.

Cette dualité présentée par la structure de l'algorithme de filtrage se retrouve dans le développement des équations employées :

- Equations de mise à jour temporelle, destinées à évaluer la statistique, d'ordre deux de l'état prédit :

$$\begin{aligned} \hat{x}_{k+1/k} &= f(\hat{x}_k) \\ P_{k+1/k} &= F_k P_k F_k^T \end{aligned} \tag{1.9}$$

Où $F_k \overset{\Delta}{=} f\big|_{\hat{x}k}$ et $P_{k+1/k}$ représente la covariance des erreurs prédite.

- Equations de mise à jour par des observations, donnant la valeur estimée en utilisant la connaissance de l'état observé :

$$\begin{aligned} \hat{x}_{k+1} &= \hat{x}_{k+1/k} + K_{k+1}(y_k - h^T \hat{x}_{k+1/k}) \\ P_{k+1} &= (I_n - K_{k+1}h)P_{k+1/k} \end{aligned} \tag{3.10}$$

Où I_n : la matrice unité $n \times n$,

P_{k+1} : la covariance des erreurs,

et K_{k+1} : le gain de Kalman s'exprimant comme :

$$K_{k+1} = K_{k+1/k} h^T (hP_{k+1/k}h^T + R)^{-1} \tag{3.11}$$

Ainsi par l'unification des relations 3.9 et 3.10 on obtient la solution récursive suivante :

$$\hat{x}_{k+1} = f(\hat{x}_k) + K_{k+1}(y_k - h^T f(\hat{x}_k)) \tag{1.12}$$

En utilisant la décomposition du vecteur d'état sous la forme $x_k = \left[x_k^{\{1\}}, x_k^{\{2\}}\right]^T$, comme en synchronisation identique, on peut écrire la dynamique du système sous la forme :

$$f(x_k) = \left[f^{\{1\}}(x_k^{\{1\}}, x_k^{\{2\}}), f^{\{2\}}(x_k^{\{1\}}, x_k^{\{2\}})\right]^T \tag{3.13}$$

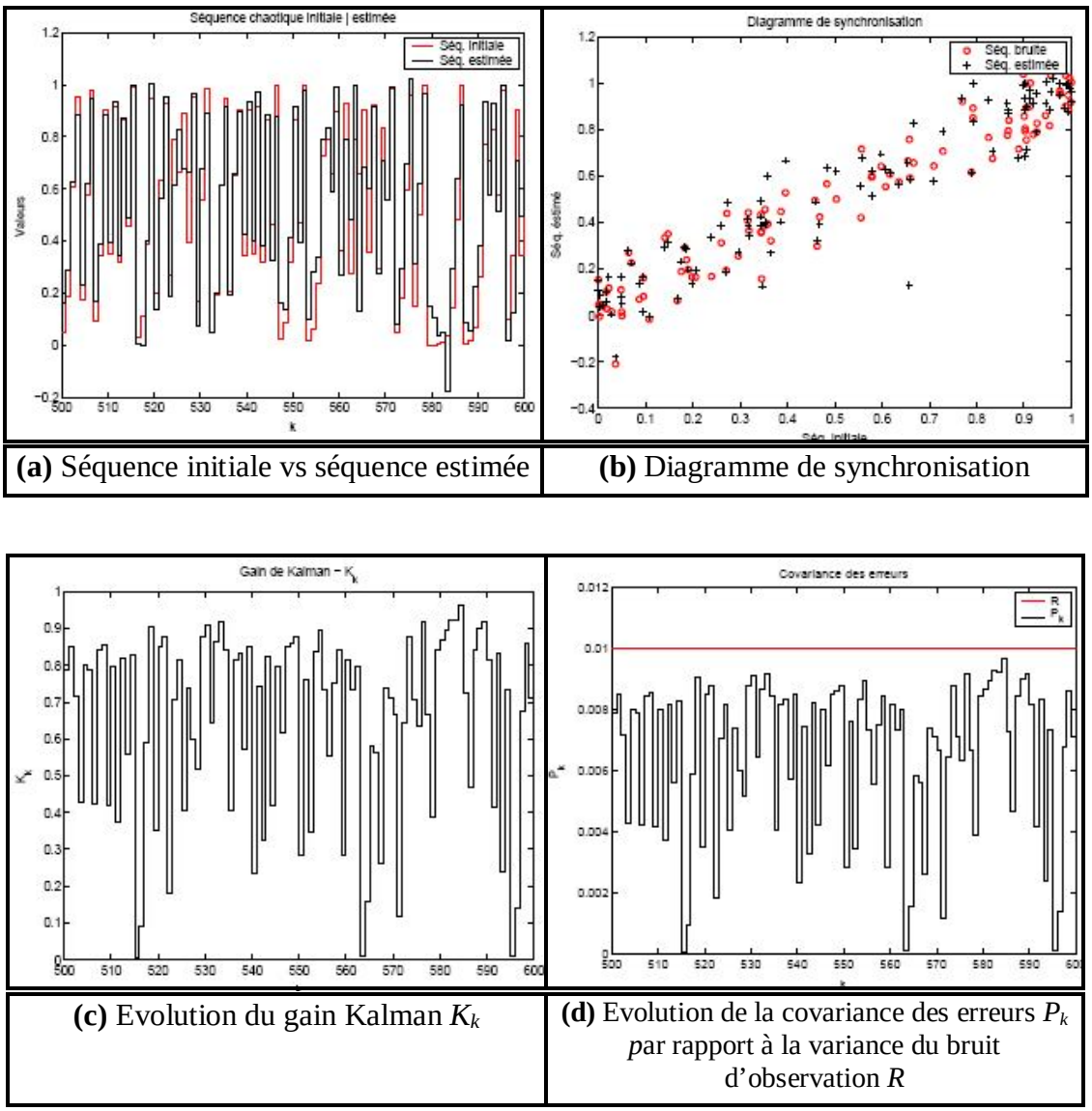
Avec cette relation, le parallèle avec la synchronisation identique est immédiat.

En considérant le système esclave caractérisé par la dynamique $f^{\{2\}}(y_k, \hat{x}_k^{\{2\}})$ ou $y_k = x_k^{\{1\}} + n_k$ est le signal de synchronisation, et avec $\mathrm{h} = [1, 0, ..., 0]\mathrm{T}$, $\mathrm{K_k} = [1, 0, ..., 0]^{\mathrm{T}}$ nous obtenons :

$$\begin{aligned} \hat{x}_{k+1}^{\{1\}} &= y_{k+1} \\ \hat{x}_{k+1}^{\{2\}} &= f^{\{2\}}(\hat{x}_k, \hat{x}_k^{\{2\}}) \end{aligned} \tag{3.14}$$

Nous voyons ainsi, que la méthode de synchronisation en utilisant le filtrage de Kalman, est une généralisation de la méthode de synchronisation identique, présentée antérieurement [2].

Il est intéressant de mentionner que si généralement, le gain de Kalman converge vers une valeur fixe, des oscillations apériodiques du gain seront obtenues, dans le cas de systèmes chaotiques. Le même phénomène est constaté au niveau de la covariance des erreurs P_k [2].



(a) Séquence initiale vs séquence estimée

(b) Diagramme de synchronisation

(c) Evolution du gain Kalman K_k

(d) Evolution de la covariance des erreurs P_k par rapport à la variance du bruit d'observation R

Figure 3.4: Exemple de synchronisation chaotique par filtrage de Kalman Etendu [2]

Dans les figures 3.4, on considère le cas de la synchronisation chaotique appliquée à une dynamique non linéaire monodimensionnelle représentée par la fonction logistique (eq. 1.8), avec le paramètre $r = 4$. Ainsi on a généré une séquence chaotique avec une longueur de

600 échantillons, affectée par un bruit d'observation gaussien additif de variance $R = 10^{-2}$. Après une période de transition de 500 échantillons on représente l'évolution de la séquence estimée, le diagramme de synchronisation, le comportement du gain de Kalman K_k ainsi que la covariance des erreurs estimées P_k [2].

Si on parle qualitativement de performances de synchronisation, on observe que l'introduction du bruit de mesure dans le modèle va entraîner l'impossibilité d'obtenir une synchronisation parfaite. Cela signifie que le vecteur d'état du système maître et le vecteur d'état du système esclave ne seront jamais égaux. Dans ce cas la synchronisation chaotique peut être définie au sens d'une erreur d'estimation bornée. Une autre remarque peut être faite par rapport à l'évolution comparative entre le gain de Kalman et la covariance des erreurs, qui suivent une relation de proportionnalité. Analytiquement il est facile de prouver que dans le cas monodimensionnel cette relation est valide, avec un coefficient de proportionnalité égal à la variance du bruit d'observation considéré [2]:

$$P_k = RK_k \tag{3.15}$$

Le modèle d'estimation employé reste assez sensible aux perturbations introduites par le bruit de canal ainsi qu'aux approximations fait par le filtre de Kalman Etendu. Une solution généralement utilisée pour compenser ces approximations, est de considérer la présence d'un bruit de processus associé au système dynamique chaotique mais un paramétrage optimal de la valeur de ce bruit est difficile à faire.

3.3.3 Synchronisation généralisée

Dans le concept de la synchronisation identique sous l'effet d'accouplement unidirectionnel il a été indiqué que le système récepteur est identique ou presque identique au système émetteur. Cependant, on va essayer d'imaginer la situation pratique intéressante où le système récepteur est différent du système émetteur [12].

En général, quand il existe une différence essentielle entre les systèmes couplés, on ne peut pas être sûr du premier coup d'œil d'affirmer que les systèmes chaotiques non identiques peuvent être synchronisés, mais plusieurs travaux ont démontré que ce type de synchronisation chaotique peut exister en généralisant le concept de la synchronisation pour

inclure la non identification entre les systèmes couplés, et on a appelé ce phénomène la synchronisation généralisée [12].

Pour définir la synchronisation généralisée pour deux systèmes chaotiques couplés unidirectionnelement, on va travailler avec des systèmes non-linéaires composés d'un système émetteur autonome avec les variables dynamiques x dans un espace de phase X couplé à un système récepteur avec des variables dynamiques y dans l'espace d'état Y .
La dynamique des systèmes émetteur et récepteur est donnée par :

$$\dot{x} = F(x(t)) \tag{3.16}$$

$$\dot{y} = G(y(t), g, x(t)) \tag{3.17}$$

avec g une constante qui caractérise la force d'accouplement unidirectionnel.

Définition:

Quand $g \neq 0$, on dit que les deux systèmes chaotiques (3.16), et (3.17) sont synchronisés dans un sens généralisé, s'il y a une transformation $\phi : X \rightarrow Y$ qui prend les trajectoires de l'attracteur de l'espace X dans les trajectoires de l'attracteur de l'espace Y, pour que $y(t) = \phi(x(t))$, et si cette transformation ne dépend pas des conditions initiales du système récepteur y(0) dans le bassin d'attraction de l'attracteur synchronisé.

Remarque:

On souligne que dans cette définition de synchronisation généralisée que l'existence de transformation ϕ est exigée seulement pour les trajectoires sur l'attracteur.

La transformation n'est pas exigée d'exister pour les trajectoires passagères. Plusieurs méthodes ont été proposées pour détecter et étudier la stabilité de la synchronisation généralisée, mais on va proposer une de ces méthodes qui est connue sous le nom de *"système auxiliaire approché"* [12].

3.3.3.1 Méthode du système auxiliaire approché

Le principe de cette méthode est basé sur le fait que, si le même système émetteur x(t) conduit deux systèmes récepteurs identiques y(t) et z(t) qui commencent par des conditions

initiales différentes dans le bassin d'attraction, alors l'analyse de stabilité de la synchronisation dans l'espace X ⊕ Y , qui peut en général avoir une forme très compliquée y(t) = ϕ(x(t)), peut être remplacée par l'analyse de la stabilité tout à fait simple z(t) = y(t) dans l'espace Z ⊕ Y [12].

A cet effet on va supposer le système auxiliaire suivant :

$$\dot{z} = G(z(t), g, x(t)) \tag{3.18}$$

qui est identique au système récepteur (3.17). Clairement, quand le système récepteur (3.17) et son auxiliaire (3.18) ont le même signal émetteur x(t), alors les champs (domaines) vectoriels dans les espaces de phase du récepteur et des systèmes auxiliaires sont identiques, et les systèmes peuvent se développer sur des attracteurs identiques [12].

Il est facile de montrer que la stabilité linéaire du collecteur z(t) = y(t) est équivalente à la stabilité linéaire du collecteur des mouvements synchronisés dans X ⊕ Y, qui est déterminé par ϕ(.). Les équations linéarisées qui dirigent l'évolution des quantités $\zeta_y(t)$ telle que $\zeta_y(t) = y(t)-\phi(x(t))$ et $\zeta_z(t) = z(t)-\phi(x(t))$, sont [12]:

$$\dot{\varsigma}_y(t) = DG(\phi(x(t), g, x(t)) \cdot \dot{\varsigma}_y(t) \tag{3.19}$$

$$\dot{\varsigma}_z(t) = DG(\phi(x(t), g, x(t)) \cdot \dot{\varsigma}_z(t) \tag{3.20}$$

avec

$$DG(w, h_u(t)) = \frac{\partial G(w, h_u(t))}{\partial w} \tag{3.21}$$

Puisque les équations linéarisées pour $\zeta_y(t)$ et $\zeta_z(t)$ sont identiques, les équations linéarisées pour $\zeta_z(t)$ - $\zeta_y(t)$ = z(t) - y(t) ont la même matrice Jacobienne DG(., g, x(t)) que dans l'équation précédente. Donc, si le collecteur des mouvements synchronisés dans X ⊕ Y ⊕ Z est linéairement stable pour z(t) - y(t), alors il est linéairement stable pour $\zeta_y(t) = y(t) - \phi(x(t))$ et vice versa. Notons que l'équation linéarisées pour z(t) - y(t) est identique à l'équation qui définit les exposants de Lyapunov conditionnels pour le système récepteur. Ainsi, quand le collecteur z = y est linéairement stable, les exposants de Lyapunov conditionnels pour le

système émetteur, conditionnés sur la valeur du système récepteur x(t), sont tous négatifs [12].

3.3.4 Synchronisation de phase

3.3.4.1 Phase d'un système chaotique

La phase d'un système chaotique est un peu difficile à calculer par rapport à celle d'un système périodique. Une définition directe compte sur le fait que, si l'attracteur du système chaotique suit une rotation appropriée dans l'espace de phase, il est possible de trouver un plan dans lequel la projection d'une trajectoire de l'attracteur suit une rotation appropriée aussi (ces systèmes sont appelés des systèmes avec une phase bien définit). Dans ce cas on peut donner cette définition [12]:

Définition : Soit Un système dynamique chaotique,

$$\dot{x} = f(x) \tag{3.22}$$

Et soit le plan cartésien (u, v), dans lequel la projection de l'attracteur du système (3.22) suit une rotation appropriée.
On peut définir la phase du système (3.22) par la fonction continue suivante :

$$\phi :]-\infty,+\infty[\longrightarrow [0,\Pi]$$

tel que

$$\phi(t) = \arctan\frac{u(t)-u_0(t)}{v(t)-v_0(t)} \tag{3.23}$$

avec (u_0, v_0) représente le centre de la rotation de l'attracteur projeté.

La dynamique de la phase est :

$$\phi(\mathrm{t}) = \phi_0 \pm \Omega t + \xi(t) \tag{3.24}$$

avec ϕ_0 une constante donnée par la condition initiale. Cette constante, quand elle est positive, définit une dérivée constante de la phase et représente la fréquence moyenne du système, $\xi(t)$ une petite fluctuation chaotique limitée ayant un zéro moyen [12].

La phase d'un système chaotique peut aussi être définie sur une section de Poincaré appropriée avec laquelle l'orbite chaotique se croise une fois, pour chaque rotation. Le croisement successif avec la section de Poincaré peut être associé à une augmentation de phases de. Ces dernières peuvent être calculées, au milieu, avec une interpolation linéaire [12].

c'est-à-dire :

$$\phi(t) = 2\pi k + 2\pi \frac{t - \tau_k}{\tau_{k+1} - \tau_k} \qquad \tau_k < t < \tau_{k+1} \tag{3.25}$$

Où τ_k est le temps du croisement de k^{ième} tour de l'attracteur avec la section de Poincaré.

La troisième façon de définir la phase d'un système chaotique, consiste à considérer le signal analytique suivant:

$$\xi(t) = x(t) + JH[x] = A(t)\exp(i\phi(t)) \tag{3.26}$$

avec H[x] : une fonction qui représente la transformé d'Hilbert de x(t)

$$H[x] = \frac{1}{\pi} v.p. \int_{-\infty}^{+\infty} \frac{x(\tau)}{t - \tau} d\tau$$

v.p. signifie la valeur principale de l'intégrale, tandis que ϕ(t) et A(t) représentent, respectivement, la phase et l'amplitude du système chaotique.

Synchronisation de phase :

Un cas fréquemment étudié dans la littérature, est quand une force périodique externe faible est appliquée à un système chaotique autonome. Ce phénomène peut être décrit par le système d'équations différentielles d'ordre n suivant [12]:

$$\dot{x}(t) = f(x) + p(t) \tag{3.27}$$

avec $p(t) = A_1 \cos(\omega t + \delta_1), A_2 \cos(\omega t + \delta_2), \ldots, A_n \cos(\omega t + \delta_n)$, la force périodique appliquée de fréquence ω, dont l'intensité est mesurée par l'amplitude A_i, i = 1, .., n.

Dans ces circonstances il est possible d'observer le phénomène connu comme la synchronisation de phase. Cela signifie que le système reste chaotique mais sa dynamique est modifiée d'une telle façon que la phase de l'attracteur chaotique rencontre celui de la force appliquée. La présence d'une synchronisation de phase d'un système chaotique à une force agissante de fréquence ω est représentée par la relation suivante [12] :

$$\psi(t) = \phi(t) \pm \frac{m}{n} wt \tag{3.28}$$

avec

m et n : des nombres entiers, comme le cas quand il y a deux nombres réels, ε_1 et ε_2, qui vérifient $\varepsilon_1 < \varepsilon_2$ et $\varepsilon_2 - \varepsilon_1 < 2\pi$, tel que $\varepsilon_1 < \psi(t) < \varepsilon_2$ pour tout t.

$\phi(t)$: la phase de l'oscillateur chaotique.

$\Psi(t)$: la différence entre la phase de l'oscillateur chaotique et celle de la force agissante.

Cette condition peut être réécrite, en utilisant l'équation (3.24), comme [12]:

$$\left| n\Omega - m\omega \right| = 0 \tag{3.29}$$

pour que la synchronisation de phase signifie que la phase de l'oscillateur reste toujours assez près de la phase de la force (m = n = 1), ou à une de ses harmoniques (m > n), ou bien la fréquence de l'oscillateur, Ω, est près d'une harmonie de la fréquence de la force (m < n) [12].

La synchronisation de phase peut être obtenue ou non, selon les propriétés de la force appliquée: sa fréquence ω, amplitude A_i et les angles δ_i, i = 1..n, à cause des approches différentes à la phase de l'oscillateur présenté dans la subdivision précédente; la synchronisation de phase peut être contrôlée de plusieurs façons [12].

3.3.5 Synchronisation de retard

Après la synchronisation complète et généralisée, les chercheurs ont découvert que deux systèmes dynamiques chaotiques non identiques peuvent exposer un phénomène de synchronisation dans lequel les variables dynamiques des deux systèmes deviennent synchronisées, mais avec un retard dans temps, de l'un par rapport à l'autre. Ils s'agit de la synchronisation de retard [12].

A cet effet, considérons deux systèmes chaotiques légèrement différents : $\dot{x}_1 = F_1(x_1)$ et $\dot{x}_2 = F_2(x_2)$, accrochés par un accouplement unidirectionnel définit par la force d'accouplement ε. On s'attend donc, a ce que $x_1(t)$ soit synchronisé avec $x_2(t+\tau)$, dans une gamme de valeurs de ε, où $\tau \neq 0$ est le retard de temps qui dépend beaucoup plus de ε que du paramètre caractérisant la différence entre les deux oscillateurs [12].

Pour évaluer quantitativement la synchronisation de retard, nous utilisons la fonction de similitude suivante :

$$s(\tau) = \sqrt{\frac{< (x_2(t-\tau) - x_1(t))^2 >}{(< (x_1^2(t) >< x_2^2(t))^2 >)^{1/2}}} \tag{3.30}$$

où τ est le temps de retard. Soit s_{min} la valeur minimale de $s(\tau)$ et soit τ_{min} la quantité (somme) de retard où s_{min} est réalisé. On désigne par $<\cdot>$ le produit scalaire définit sur l'espace de phases [12].

La synchronisation de retard entre les deux oscillateurs est caractérisée par les conditions

$$s_{min} = 0 \text{ et } \tau_{min} \neq 0 \tag{3.31}$$

tandis que la synchronisation complète est caractérisée par les conditions

$$s_{min} = 0 \text{ et } \tau_{min} = 0 \tag{3.32}$$

3.4 CONCLUSION

Dans ce chapitre, et après avoir abordé l'histoire de la synchronisation chaotique et ces principaux acteurs, on a essayé d'expliquer au mieux ce phénomène tout en parcourant les méthodes, les plus connues dans la littérature, on cite: la synchronisation identique, celle réalisée par le filtre de Kalman étendu, la généralisée, de phase et de retard.

Par la suite, on va présenter une des méthodes, pour établir éventuellement une synchronisation entre deux systèmes chaotiques, dans le but de transmettre un signal informatif.

CHAPITRE 4

Application : étude de système de Chen

4.1 INTRODUCTION

Dans ce chapitre on va s'intéresser seulement à étudier les propriétés mathématiques du système de Chen.

4.2 SYSTEME DE CHEN

4.2.1 Historique

Le système de Chen a été découvert grâce à la chaotication (anti-contrôle) du système de Lorenz contrôlé, c'est-à-dire à partir d'un système non chaotique on va essayer de créer un système chaotique, en employant la méthode de la rétroaction d'état (state feedback).

Le système de Lorenz contrôlé est donné par :

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = cx - xz - y + u \\ \dot{z} = xy - bz \end{cases} \tag{4.1}$$

Avec a, b, c sont des constantes, et u le contrôleur linéaire de rétroaction de la forme suivante :

$$u = k_1 x + k_2 y + k_3 z$$

avec k_1, k_2, k_3 des constantes à déterminer.

On souhaite que le système (4.1) devienne chaotique, donc il suffit que k_1, k_2, k_3 prennent des valeurs de sorte que ce système ait un comportement chaotique.

Les points d'équilibre du système (4.1) sont donnés par: $P_1 = (0,0,0), P_{2,3} = (\alpha, \alpha, \alpha)$, avec :

$$\alpha = \frac{k_3}{2} \pm \frac{1}{2}\sqrt{k_3^2 + 4b(c + k_1 - k_2 - 1}$$

- La matrice Jacobienne du système (4.1) au point (x_0, y_0, z_0), est donnée par :

$$J_{(x_0,y_0,z_0)} = \begin{pmatrix} -a & a & 0 \\ c + k_1 - z_0 & k_2 - 1 & k_3 - x_0 \\ y_0 & x_0 & -b \end{pmatrix}$$

On remarque qu'au point d'équilibre $P_1 = (0,0,0)$, la matrice Jacobienne associée est :

$$J_{(0,0,0)} = \begin{pmatrix} -a & a & 0 \\ c + k_1 & k_2 - 1 & k_3 \\ 0 & 0 & -b \end{pmatrix}$$

k_3 ne contribue pas à ces valeurs propres, donc il ne contribue pas aux exposants de Lyapunov. Alors, pour simplifier, Chen a choisi $k_3 = 0$.

Pour avoir un comportement chaotique, il faut, aux moins, avoir une valeur propre instable pour chacun des deux autres points d'équilibre. En appliquant les critères de Routh-Herwitz (voir glossaire), on peut prendre $k_1 = -a$, $k_2 = 1 + c$ comme un choix simple parmi plusieurs autres.

Alors, le contrôleur de rétroaction va prendre la forme suivante:

$$u = -ax + (1 + c)y$$

donc le système (4.1) devient :

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = (c - a)x + cy - xz \\ \dot{z} = xy - bz \end{cases} \tag{4.2}$$

C'est le système de Chen.

4.2.2 Analyse du système

4.2.2.1 Propriétés mathématiques

Le système (4.2) est un système autonome. Son espace de phase est tridimensionnel. Il est invariable par la transformation suivante :

$$(x, y, z) \rightarrow (-x, -y, -z)$$

On peut noter cette transformation par P, tel que :

$$\begin{aligned} P : \Re^3 &\rightarrow \Re^3 \\ X &\rightarrow MX \end{aligned}$$

qui satisfait $f(PX) = Pf(X)$

avec $M = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, et X = (x, y, z).

4.2.2.2 Dissipation et existence de l'attracteur

Pour le système de Chen, la divergence de champ de vitesse est donnée par :

$$divf = \frac{\partial \dot{x}}{\partial x} + \frac{\partial \dot{y}}{\partial y} + \frac{\partial \dot{z}}{\partial z}$$

ce qui donne :

$$divf = -a + c - b$$

Pour que le système soit dissipatif, il faut que :

$$divf < 0$$

Pour les paramètres (a, b, c) = (35, 3, 28), le système de Chen est dissipatif. Ainsi, le volume de n'importe quel attracteur du système doit être nul, quand t tend vers ∞.

4.2.3 Etude des points d'équilibre

Pour calculer les points d'équilibre il suffit de résoudre le système suivant :

$$\begin{cases} a(y-x)=0 \\ (c-a)x+cy-xz=0 \\ xy-bz=0 \end{cases}$$

Après un simple calcul, on trouve les points d'équilibres suivants :

$$C_1(0,0,0), C_2\left(+\sqrt{b(2c-a)},+\sqrt{b(2c-a)},2c-a\right), C_3\left(-\sqrt{b(2c-a)},-\sqrt{b(2c-a)},2c-a\right)$$

On constate que les deux points C_2 et C_3 apparaissent lorsque $c > \frac{a}{2}$.

Donc :

- Si $c \le \frac{a}{2}$, il y a un seul point d'équilibre ($C_2 = C_3 = 0$).
- Si $c > \frac{a}{2}$, il y a trois points d'équilibre.

4.2.3.1 Stabilité des points d'équilibre

Pour étudier la stabilité au voisinage des points d'équilibre, on va utiliser la méthode de Lyapunov. Il suffit donc, d'étudier les signes des valeurs propres de la matrice Jacobienne associée à chaque point d'équilibre.

a. A l'origine (le point d'équilibre C1) :

La matrice Jacobienne associée est :

$$J_{(0,0,0)} = \begin{pmatrix} -a & a & 0 \\ c-a & c & 0 \\ 0 & 0 & -b \end{pmatrix} \qquad (4.3)$$

Le polynôme caractéristique est donné par :

$$p(\lambda) = -(b+\lambda)(\lambda^2 + (a-c)\lambda + a^2 - 2ac \qquad (4.4)$$

Les valeurs propres de la matrice (4.3) sont les solutions du polynôme (4.4). Ce qui nous donne :

$$\lambda_1 = -b$$
$$\lambda_2 = \frac{c - a - \sqrt{(a-c)^2 + 4a(2c-a)}}{2}$$
$$\lambda_3 = \frac{c - a + \sqrt{(a-c)^2 + 4a(2c-a)}}{2}$$

Pour (a, b, c) = (35, 3, 28), $\lambda_1 = -b = -3$ est toujours négative. Il ne reste donc qu'à étudier le signe de λ_2 et λ_3 :

- Si $0 < c < (2\sqrt{3} - 3).a$ donc on a $0 < c < 16{,}24$.

λ_2 et λ_3 sont deux valeurs propres complexes de parties réelles: $\frac{c-a}{2} = -3{,}5 < 0$, donc l'origine est un foyer asymptotiquement stable (un puits).

- Si $(2\sqrt{3} - 3).a < c < \frac{a}{2}$, donc on a $16{,}24 < c < 17{,}5$.

λ_2 et λ_3 sont deux valeurs propres réelles négatives, l'origine est alors un nœud impropre asymptotiquement stable.

- Si $c > 16.24$ et $c < \frac{a}{2}$, donc on a $c > 16{,}24$ et $c < 17{,}5$.

λ_2 et λ_3 sont deux valeurs propres réelles positives, donc l'origine est un point selle.

- Si $c = \frac{a}{2}$, les valeurs propres deviennent :

$$\lambda_1 = -b, \lambda_2 = -\frac{a}{2}, \lambda_3 = 0$$

Dans ce cas, on utilise le théorème de la variété centrale (voir glossaire), pour étudier la stabilité de l'origine :

Les vecteurs propres associés aux valeurs propres $\lambda_1 = -b, \lambda_2 = -\frac{a}{2}, \lambda_3 = 0$ sont :

$$v_1(1,1,0)^T, v_2(2,1,0)^T, v_3(0,0,1)^T$$

Dans cette partie on doit imposer sur le système de Chen une petite perturbation. Pour cela on pose $c = \frac{a}{2} + \varepsilon$.

Le système (4.2) devient :

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = (-\frac{a}{2} + \varepsilon)x + (\frac{a}{2} + \varepsilon)y - xz \\ \dot{z} = xy - bz \end{cases}$$

Ensuite, on passe à la base des vecteurs propres :

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 & 2 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} u \\ v \\ w \end{pmatrix}$$

La transformation inverse nous donne :

$$\begin{pmatrix} u \\ v \\ w \end{pmatrix} = \begin{pmatrix} -1 & 2 & 0 \\ 1 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

Alors :

$$\begin{cases} u = -x + 2y \\ v = x - y \\ w = y + z \end{cases}$$

Ce qui donne :

$$\begin{cases} \dot{u} = (u + 2v)(2\varepsilon + 2w) + (u + v)2\varepsilon \\ \dot{v} = -\frac{a}{2}v + (u + 2v)(-\varepsilon + w) + (u + v)(-\varepsilon) \\ \dot{w} = -bw + (u + 2v)(u + v) \\ \dot{\varepsilon} = 0 \end{cases}$$

donc :

$$\begin{pmatrix}\dot{u}\\ \dot{v}\\ \dot{w}\\ \dot{\varepsilon}\end{pmatrix}=\begin{pmatrix}0 & 0 & 0 & 0\\ 0 & -\frac{a}{2} & 0 & 0\\ 0 & 0 & -b & 0\\ 0 & 0 & 0 & 0\end{pmatrix}\begin{pmatrix}u\\ v\\ w\\ \varepsilon\end{pmatrix}+(u+2v)\begin{pmatrix}2\varepsilon-2w\\ w-\varepsilon\\ u+v\\ 0\end{pmatrix}+(u+v)\begin{pmatrix}2\varepsilon\\ -\varepsilon\\ 0\\ 0\end{pmatrix}$$

Dans ce cas, la variété centrale est définie par des équations de la forme :

$$v=h_1(u,\varepsilon), w=h_2(u,\varepsilon)$$

Ce qui donne :

$$\dot{v}=\dot{u}Dh_1(u,\varepsilon), \dot{w}=\dot{u}Dh_2(u,\varepsilon)$$

Alors

$$-\frac{a}{2}v+(u+2v)(-\varepsilon+w)+(u+v)(-\varepsilon)=[(u+2v)(2\varepsilon-2w)+(u+v)2\varepsilon]Dh_2(u,\varepsilon) \qquad (4.5)$$

D'autre part :

$$h_1(u,\varepsilon)=b_{11}\varepsilon^2+b_{12}u\varepsilon+a_{12}u^2+.....$$
$$h_2(u,\varepsilon)=b_{21}\varepsilon^2+b_{22}u\varepsilon+2a_{22}u^2+.....$$

Alors

$$Dh_1(u,\varepsilon)=b_{12}\varepsilon+2a_{12}u+.... \qquad (4.6)$$
$$Dh_2(u,\varepsilon)=b_{22}\varepsilon+2a_{22}u+....$$

de (4.5) et (4.6), on obtient que :

$$b_{11}=0, b_{21}=0, a_{12}, a_{22}=\frac{1}{b}, b_{12}=-\frac{4}{a}, b_{22}=0$$

ce qui nous donne :

$$v=h_1(u,\varepsilon)=-\frac{4}{a}u\varepsilon+....$$
$$w=h_2(u,\varepsilon)=\frac{1}{b}u^2+....$$

Finalement on trouve le système suivant :

$$\begin{cases}\dot{u}=4u\varepsilon+...\\ \dot{\varepsilon}=0\end{cases}$$

Le seul point d'équilibre pour ce système est u = 0, il est stable pour $\varepsilon > 0$, et instable pour $\varepsilon < 0$

b. Stabilité des points fixes C_2, C_3 :

Au voisinage de ces points d'équilibre, la matrice Jacobienne associée est :

$$J_{C_{2,3}} = \begin{pmatrix} -a & a & 0 \\ -c & c & \mp\sqrt{b(2c-a)} \\ \pm\sqrt{b(2c-a)} & \pm\sqrt{b(2c-a)} & -b \end{pmatrix}$$

Son polynôme caractéristique est donné par :

$$P(\lambda) = \lambda^3 + A_1\lambda^2 + A_2\lambda + A_3 \tag{4.7}$$

D'où:

$$\begin{cases} A_1 = a + b - c \\ A_2 = bc \\ A_3 = 2ab(2c-a) \end{cases}$$

D'autre part, si λ_1, λ_2, λ_3 sont des racines du polynôme caractéristique précédant, alors on peut l'écrire sous la forme :

$$P(\lambda) = (\lambda - \lambda_1)(\lambda - \lambda_2)(\lambda - \lambda_3)$$

Après un simple calcul, on arrive à trouver les relations suivantes :

$$\begin{cases} \lambda_1 + \lambda_2 + \lambda_3 = -(a + b - c) \\ \lambda_1\lambda_2 + \lambda_1\lambda_3 + \lambda_2\lambda_3 = bc \\ \lambda_1\lambda_2\lambda_3 = -2ab(2c-a) \end{cases}$$

Dans cette partie, on à $\frac{a}{2} < c < a + b$. Il existe donc, une racine réelle négative $\lambda_1 < 0$.

Calculons les deux autres valeurs propres du polynôme (4.7):

par le changement de variable $\lambda_1 = \alpha - \frac{A_1}{3}$, on peut ramener le polynôme (4.7) à la forme suivante :

$$F(\alpha) = \alpha^3 + (A_2 - \frac{A_1^2}{3})\alpha + \frac{2A_1^3}{27} - \frac{A_1 A_2}{3} + A_3$$

Cardan a donné une méthode pour résoudre ce genre d'équations: (N'oublions pas que $a = 35, b = 3$ et $17.5 = \frac{a}{2} < c < a + b = 38$).

On calcule le discriminant

$$\Delta = q^2 + \frac{4}{27} p^3$$

avec

$$q = \frac{- A_1^2}{3} + A_2 \ , \ p = \frac{2A_1^3}{27} - \frac{A_1 A_2}{3} + A_3$$

puis, on étudie son signe.

Après un simple calcul on arrive à donner à Δ sa formule :

$$\Delta = (-0.0001c^4 + 0{,}0091c^3 \ 0.2644c^2 + 2.5159c - 5{,}7270).10^6 \qquad (4.8)$$

Le polynôme (4.8) a quatre solutions réelles, mais la seule solution qu'on peut considérer est: c = 17,5872.

donc :

- Si $\Delta < 0 \Rightarrow 17.5 < c < 17.5872$, le polynôme (4.7) possède trois solutions réelles et négatives, donc les deux points d'équilibre sont deux nœuds impropres asymptotiquement stables.

- Si $\Delta > 0 \Rightarrow c > 17.5872$, le polynôme (4.7) possède une solution réelle et deux solutions complexes et conjuguées :

$$\lambda_1 = (u+v) + \frac{38-c}{3}$$

$$\lambda_1 = -\frac{1}{2}(u+v) + \frac{38-c}{3} \pm i\frac{\sqrt{3}}{2}(u+v)$$

avec

$$u = \sqrt[3]{\frac{-q+\sqrt{\Delta}}{2}}, v = \sqrt[3]{\frac{-q-\sqrt{\Delta}}{2}}$$

La partie réelle de ces deux valeurs propres est négative, d'où C_2 et C_3 sont deux foyers asymptotiquement stables.

Au point c = 20,07, la partie réelle de λ_2, λ_3 va devenir zéro. Physiquement ce résultat donne naissance à deux cycles limites autours des points C_2 et C_3. On appelle ce phénomène une bifurcation de Hopf (voir annexe A).

Si c continue à croître, la bifurcation des cycles limites engendre ce qu'on appelle : *« l'attracteur étrange de Chen »*, qui va apparaître clairement pour c = 28.

4.2.4 Etude numérique

4.2.4.1 L'attracteur étrange

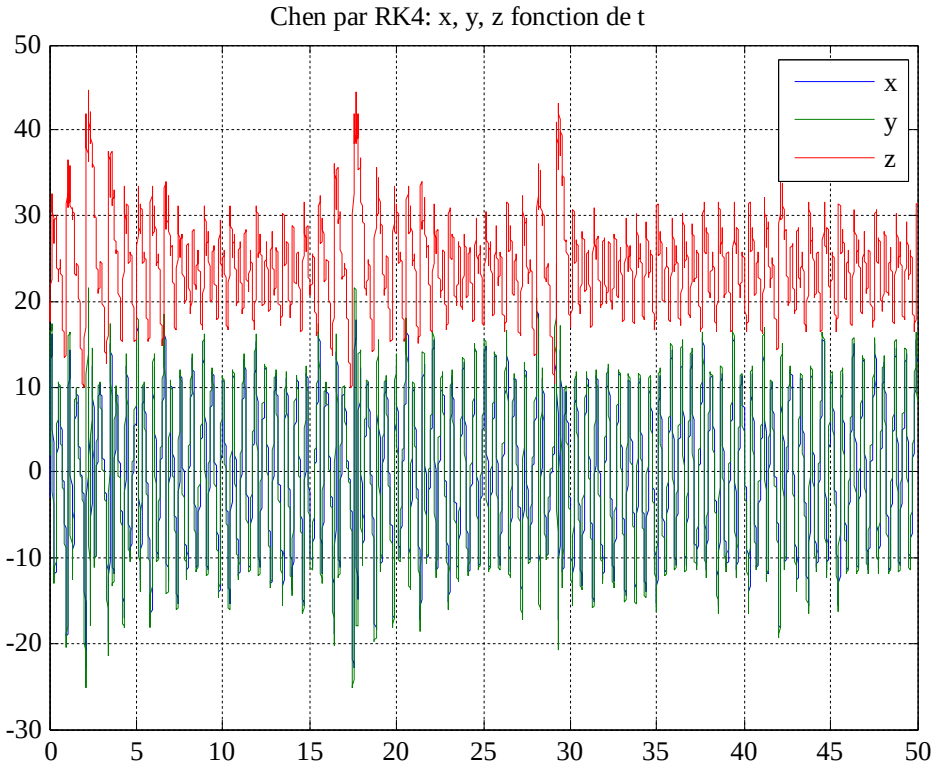


Figure 4.1: L'attracteur étrange de Chen

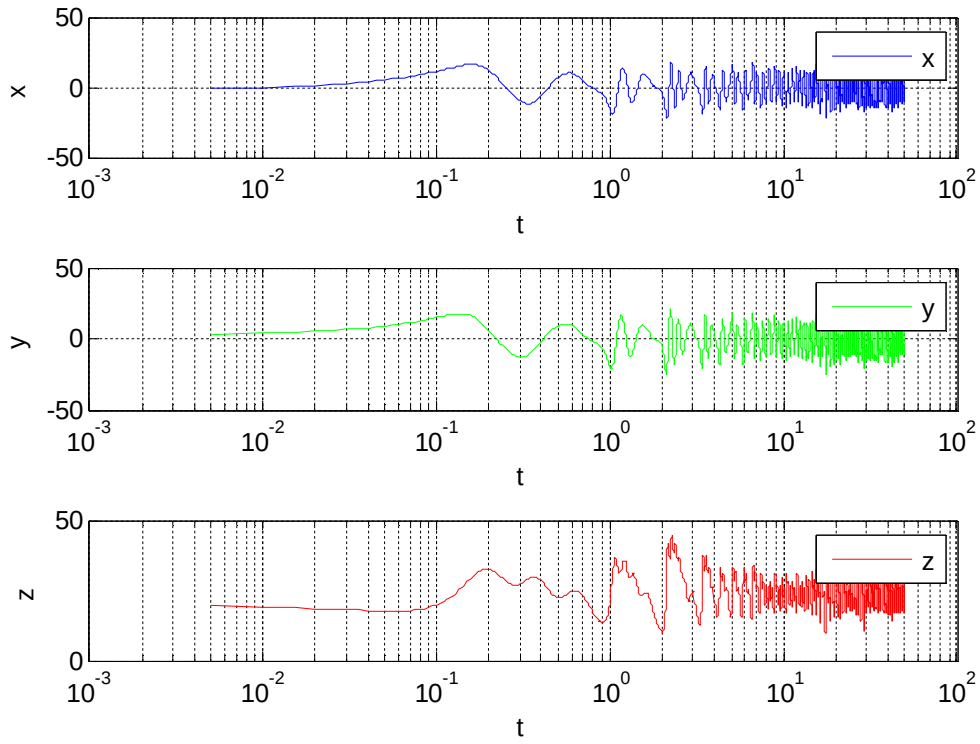
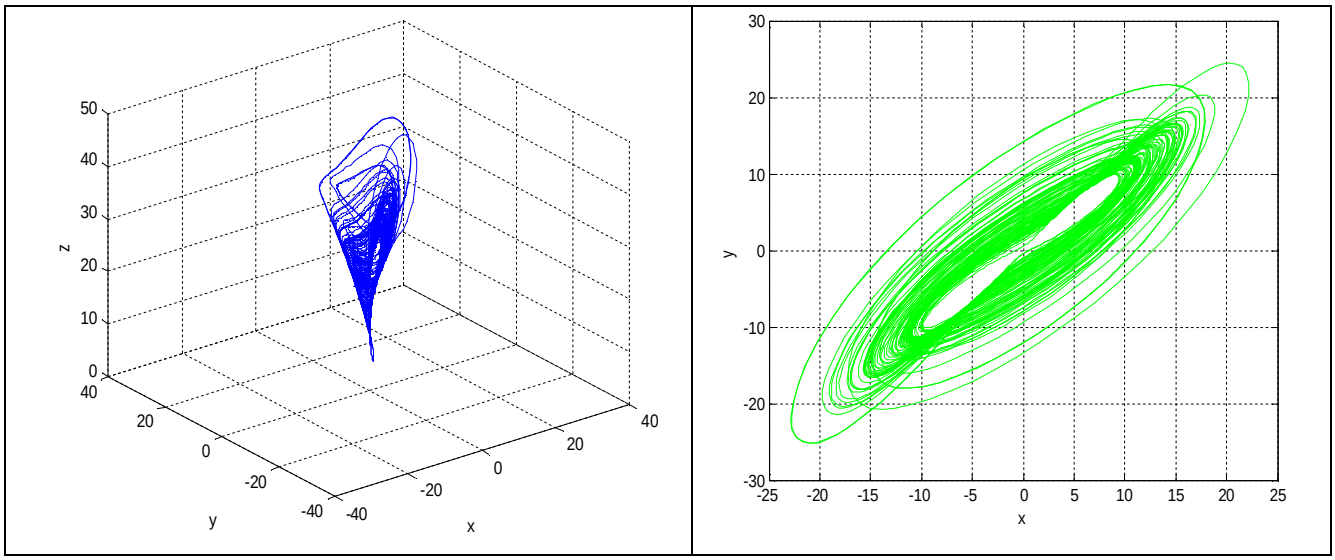


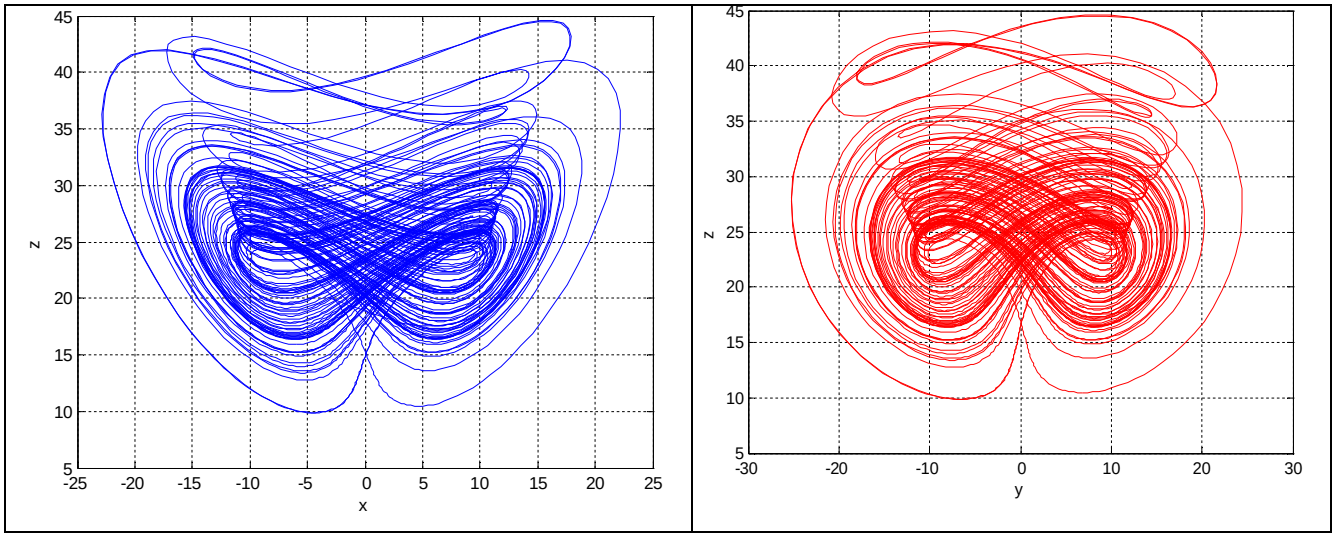
Figure 4.2: La projection de l'attracteur de Chen sur les axes (x, y, z)

4.2.4.2 Comportement du système

Pour une même condition initiale (-3; 2; 20) et pour plusieurs valeurs de c, le pas de temps est 0.005, 10000 itérations, on obtient les résultats représentés par les figures suivantes :



1ère itération	2ème itération



3ème e itération	4ème itération

Figure 4.3: Comportement du système de Chen

4.2.4.3 Transition vers le chaos

Dans ce modèle, il y a trois points fixes, dont deux se transforment en solutions périodiques, après une série de bifurcations fourche et de bifurcations de Hopf, qui apparaissent en changeant les valeurs du paramètre de contrôle c.

Le tableau suivant résume notre étude :

$c < 17.5$	Il y a un seul point d'équilibre
$c = 17.5$	Naissance des deux points d'équilibre : bifurcation de fourche
$17.5 < c < 17.587$	Naissance des cycles limites, les solutions sont périodiques
$c > 20.17$	Naissance de la bifurcation de Hopf
$c > 28$	Il n'y a pas d'attracteur

Tableau 4. 1 : Tableau récapitulatif de la transition vers le chaos

4.3 CONCLUSION

Dans cette dernière partie, on a étudié analytiquement et numériquement le système dynamique chaotique de Chen, on a donné un aperçu historique en indiquant comment Chen a obtenu son modèle à partir du modèle de Lorenz. Ce modèle possède trois points d'équilibre. L'étude de leurs stabilités nous a conduit à faire une étude complète sur les propriétés chaotiques de ce système.

CONCLUSION GENERALE

La théorie du chaos propose pour l'univers un modèle déterministe tout en laissant un espace au hasard, et une dimension à l'imprévisible.

L'objectif principal de cette thèse était d'étudier l'utilisation des signaux chaotiques, pour permettre l'amélioration des systèmes de transmission, soit en terme de sécurité, soit en terme d'efficacité spectrale.

Contributions principales :

La première partie de cette thèse, étudie les propriétés d'un signal chaotique toute en expliquant son comportement dynamique non linéaire et sa stricte dépendance des conditions initiales. Ainsi la propriété hyperchaotique a été évoquée.

Dans **la deuxième partie**, nous récapitulons l'état de l'art des méthodes employées pour les transmissions à porteuse chaotique, dans le but de crypter les messages échangés entre deux entités différentes.

Grace à ça complexité de régénération, le signal chaotique ne cesse d'impressionner les chercheurs, et de prendre une place essentielle dans le codage de l'information. Il s'agit de l'application principale du chaos dans le monde des télécommunications. C'est pour quoi de nouvelles solutions de cryptage sont exposées dans ce chapitre.

Dans **la troisième partie,** nous exposons les méthodes de synchronisation chaotique, les plus croisées dans la littérature, principalement la synchronisation identique. C'est une forme franche de synchronisation qui peut se produire quand deux oscillateurs chaotiques identiques sont mutuellement couplés, ou quand l'un d'entre eux commande l'autre ainsi que d'autres méthodes.

Dans la dernière partie, on étudie le système chaotique de Chen, en montrant que c'est un modèle déduit de celui de Lorenz. Ce système possède trois points d'équilibre. Ainsi, une étude complète de ces propriétés est effectuée.

L'apport principal de cette thèse est d'exposer le passage d'un signal dynamique à un signal chaotique déterministe, utilisé dans la sécurisation des systèmes de communications.

Perspectives :

Les méthodes de contrôle du chaos pourraient être étudiées dans le futur, pour améliorer les performances du codage et décodage itératif. De même, des études plus développée de la synchronisation des systèmes chaotique peuvent être envisagées, ce phénomène qui trouve son utilisation dans des domaines différents, en particulier dans la communication numérique, avec l'essor des nouvelles technologies de cette dernière, et le problème associé de la confidentialité des échanges. Il s'avère que les caractéristiques essentielles du chaos (son caractère erratique et sa grande sensibilité aux conditions initiales), peuvent être mises à profit à des fins de cryptage.

Lors de cette dernière décennie, plusieurs principes de masquage chaotique ont été proposés. Certains utilisent des procédés de modulation. La technique de récupération de l'information claire s'apparente alors à un problème d'identification. D'autres techniques consistent à injecter l'information à coder au sein d'un générateur de chaos : c'est le mélange par inclusion. Pour cette technique, le problème réside dans le décryptage, c'est-à-dire à la récupération de l'information originale. On peut montrer que ce décryptage nécessite la synchronisation de séquences chaotiques générées par l'émetteur et par le récepteur. La phase de synchronisation s'apparente alors à la synthèse d'observateurs de systèmes non linéaires.

NOTATIONS MATHEMATIQUES

$\mathbf{R}$	Ensemble des réels.
$\mathbf{R}^+$	Ensemble des réels positif ou nuls.
$\mathbf{Z}$	Ensemble des entiers.
$\mathbf{Z}^+$	Ensemble des entiers positifs ou nuls.
$\mathbf{N}$	Ensemble des entiers naturels.
$\mathbf{N}^+$	Ensemble des entiers naturels positifs ou nuls.
$\dot{x}$	Dérivée du vecteur d'état x.
$\mathbf{I_N}$	Matrice identité de dimension N
λ_i	Exposant de Lyapunov de rang i.
$\hat{x}$	Vecteur **x** estimé
$\hat{x}_{k+1/k}$	Etat prédit à l'instant k + 1, en sachant la statistique à l'instant k.
$P_{k+1/k}$	Covariance des erreurs prédite à l'instant k+1, en sachant la statistique à l'instant k.
K_k	Gain de Kalman à l'instant k.
$\hat{x}_{k/k}$	Etat estimé à l'instant k
$\nabla_x f$	Gradient de la fonction **f** par rapport au vecteur **x**

LISTE DES ABREVIATIONS

CI: Conditions **I**nitiales

COOK: Chaotic **O**n-**O**ff **K**eying

CSK: Chaos **S**hift **K**eying

DCSK: Differential **C**haos **S**hift **K**eying

EKF: Extended **K**alman **F**ilter

FM: Frequency **Mo**dulation

KF: Kalman **F**ilter

RFID: Radio **F**requency **ID**entification

SCI: Sensibilité aux **C**onditions **I**nitiales

SNR: Signal to **N**oise **R**atio

v. a: variable **a**léatoire

GLOSSAIRE

♣ **Entropie de Kolmogorov :**

L'entropie métrique, ou entropie de Kolmogorov (se dit aussi en anglais measure-theoretic entropy) est un outil développé par Kolmogorov vers le milieu des années 1950 issu du concept probabiliste d'entropie de la théorie de l'information de Shannon. Kolmogorov montra comment l'entropie métrique peut être utilisée pour montrer si deux systèmes dynamiques ne sont pas conjugués. C'est un invariant fondamental des systèmes dynamiques mesurés. En outre, l'entropie métrique permet une définition qualitative du chaos : une transformation chaotique peut être vue comme une transformation d'entropie non nulle [13].

♣ **Scénario de Feigenbaum :**

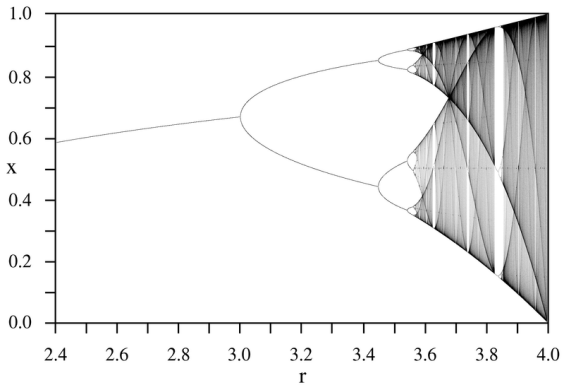
Feigenbaum a proposé un scénario dit : « *par doublement de période* » pour décrire la transition d'une dynamique régulière vers le chaos. Ce scénario trouve son origine dans le comportement de la suite logistique, qui est définie par récurrence par une application du segment [0, 1] dans lui-même :

$$x_{n+1} = \mu x_n (1 - x_n)$$

où $n = 0, 1, \ldots$ dénote le temps discret, x l'unique variable dynamique, et $0 \le \mu \le 4$ un paramètre. La dynamique de cette application présente un comportement très différent selon la valeur du paramètre μ :

- ✓ Pour $0 \le \mu \le 3$, le système possède un point fixe attractif, qui devient instable lorsque $\mu = 3$.
- ✓ Pour $3 \le \mu \le 3.57...$, , l'application possède un attracteur qui est une orbite périodique, de période 2^n où n est un entier qui tend vers l'infini lorsque μ tend vers 3.57…
- ✓ Lorsque $\mu = 3.57...$, l'application possède un attracteur de Feigenbaum fractal (mais non étrange) découvert par le biologiste May (1976).
- ✓ Le cas $\mu = 4$ avait été étudié dès 1957 par Ulam et Von Neumann. À noter qu'on peut dans ce cas précis établir l'expression exacte de la mesure invariante ergodique.

Lorsque le paramètre μ augmente, on obtient donc une succession de bifurcations de la régularité vers le chaos, résumée sur la figure ci-contre [14].



Bifurcation vers le chaos par doublement de période

♣ **Effet papillon**

Ce phénomène est mieux expliquer par l'exemple de la météo. Le chaos impose une limite fondamentale à notre aptitude à prévoir la météo. Cela ne veut pas dire qu'il faut cesser d'écouter le bulletin météorologique. Les prévisions à court terme, sur un ou deux jours, et sur une superficie restreinte comme celle de la France sont assez fiables; en revanche, au-delà de 6 ou 7 jours, les prévisions deviennent spéculatives, voire carrément fausses. Cette limite de la connaissance est incontournable. Même si on couvrait la terre de stations météo se touchant les unes les autres, il y aurait toujours de petites fluctuations dans l'atmosphère, si minuscules qu'elles ne pourraient être détectées, pour s'amplifier et modifier le climat de la planète entière.

C'est pourquoi le chaos a souvent été explicité par ce qu'on appelle l'effet papillon : le battement d'aile d'un papillon aujourd'hui à Pékin engendre dans l'air suffisamment de remous pour influer sur l'ordre des choses et provoquer une tempête le mois prochain à New-York [21].

L'effet papillon prit une désignation technique : *la dépendance sensitive aux conditions initiales.*

Ce que nous apprend le modèle de Lorenz, c'est qu'aucune incertitude initiale, aussi négligeable puisse-t-elle paraître, ne doit être négligée dans un système doté de sensibilité aux conditions initiales, vu ses conséquences à long terme. Cela revient aussi à dire que la prédiction à long terme n'a pas de sens, étant donné le très grand nombre de perturbations

minimes mais incontrôlées présentes non seulement en météorologie, mais aussi dans beaucoup d'autres systèmes.

C'est ce que l'on appelle le " chaos ". Le chaos tel que le scientifique le comprend ne signifie pas " absence d'ordre " ; il se rattache plutôt à une notion d'imprévisibilité, d'impossibilité de prévoir à long terme. Parce que l'état final dépend de manière si sensible de l'état initial, qu'un petit rien peut tout venir modifier, nous sommes fondamentalement limités dans la prédiction de cet état final. En somme, notre connaissance de l'état initial est toujours entachée d'une certaine imprécision, si petite soit-elle. Dans les systèmes dits chaotiques, cette imprécision s'amplifie de manière exponentielle et a pour résultat une non-connaissance de l'état final.

Philosophiquement, la théorie du chaos peut réconforter ceux qui considèrent qu'ils occupent une place sans importance dans le cosmos. Des choses sans importance peuvent avoir une influence immense dans un Univers non linéaire [15].

♣ **Equation de Navier-Stokes**

Navier, ingénieur et mathématicien, découvre les fameuses équations en 1821 et 1822. Elles sont fondamentales dans la description mathématique des fluides. Celles-ci sont correctes mais la méthode pour y aboutir n'est pas correcte. La bonne sera trouvée par Stokes, mathématicien irlandais, quelques années plus tard.

Au XVIIème, les hommes tentent de décrire le mouvement des planètes. Problème : les outils mathématiques sont statiques (point, ligne, nombre…). Comment étudier le mouvement continu d'un objet avec des outils statiques ? Deux savants, Leibniz et Newton, font simultanément et indépendamment une découverte majeure, le calcul différentiel. Pour donner une image familière, si le cinéma donne cette impression de mouvement, c'est parce qu'il la succession de 24 images/seconde. Eh bien, comme au cinéma, le calcul différentiel permet de séquencer une courbe, mais de façon infinitésimale [16].

La dérivation : outil du continu :

L'opération élémentaire, c'est la dérivation. Elle permet de calculer le taux de changement d'une grandeur variable. Les objets mathématiques auxquels elle s'applique sont des fonctions, et le taux de changement est la pente de la courbe associée à la fonction.

Le calcul différentiel peut s'appliquer à plusieurs dimensions. Par exemple 2, l'interprétation géométrique est alors une surface. Pour analyser un mouvement dans cette surface, il va falloir déterminer le taux de variation par rapport à 2 directions. On parle de

dérivées partielles. Enfin, pour un mouvement dans l'espace, il faudra étudier les 3 directions.

Parfois, pour étudier un mouvement, il est même nécessaire de dériver plusieurs fois une fonction.

Bernoulli en 1738, puis Euler un peu plus tard, formulent des équations afin de décrire le mouvement d'un fluide non visqueux soumis à des forces données. Navier et Stokes y ajoutent le paramètre "viscosité" : les fameuses équations sont nées:

- ✓ Equation de bilan de masse : $\frac{\partial \rho}{\partial t} + \vec{\nabla} \cdot (\rho \vec{v}) = 0$
- ✓ Equation de bilan de quantité de mouvement :

$$\frac{\partial (\rho \vec{v})}{\partial t} + \vec{\nabla} \cdot (\rho \vec{v} \otimes \vec{v}) = -\vec{\nabla} p + \vec{\nabla} \cdot \vec{\vec{\tau}} + \rho \vec{f}$$

- ✓ Equation de bilan d'énergie : $\frac{\partial (\rho e)}{\partial t} + \vec{\nabla} \cdot [(\rho e + p)\vec{v}] = \vec{\nabla} \cdot (\vec{\vec{\tau}} \cdot \vec{v}) + \rho \vec{f} \cdot \vec{v} - \vec{\nabla} \cdot \vec{q} + r$

t représente le temps

ρ désigne la masse volumique du fluide

$\vec{v}$ désigne la vitesse eulérienne d'une particule fluide

p désigne la pression

$\vec{\vec{\tau}}$ le tenseur des contraintes visqueuses

$\vec{f}$ est la résultante des forces massiques s'exerçant sur le fluide

e est l'énergie totale par unité de masse

$\vec{q}$ est le flux de chaleur perdu par conduction thermique

r est la perte de chaleur volumique due au rayonnement

Les équations de Navier-Stokes ressemblent à des équations "ordinaires" que l'on pourrait trouver dans un livre d'étudiant. Pourtant on ne sait pas les résoudre, ni même si elles ont une solution ! En tous cas, si une solution existe, elle a de fortes chances de s'appuyer sur des techniques inédites.

On sait par ordinateur résoudre des cas particuliers de ces équations, et les ingénieurs s'en servent pour construire navires et avions. Restent aux maths à rattraper l'ingénierie. D'une part c'est important d'en avoir la connaissance mathématique, fondamentale. Mais surtout, cela permettrait des avancées en physique, en aéronautique et en ingénierie nautique, car ces équations gouvernent les mouvements de l'air de l'atmosphère, les courants

océaniques, l'écoulement de l'eau dans un tuyau, et de nombreux autres phénomènes d'écoulement de fluides… [16]

♣ **Matrice Jacobienne**

La matrice Jacobienne est la matrice des dérivées partielles du premier ordre d'une fonction vectorielle.

Soit F une fonction d'un ouvert de R^n à valeurs dans R^m. Une telle fonction est définie par ses m fonctions composantes à valeurs réelles :

$$F : \begin{pmatrix} x_1 \\ . \\ . \\ x_n \end{pmatrix} \rightarrow \begin{pmatrix} f_1(x_1,...,x_n) \\ . \\ . \\ f_m(x_1,...,x_n) \end{pmatrix}$$

Les dérivées partielles de ces fonctions en un point M, si elles existent, peuvent être rangées dans une matrice à m lignes et n colonnes, appelée matrice Jacobienne de F :

$$\begin{pmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_n} \\ . & & \\ . & & \\ . & & \\ \frac{\partial f_m}{\partial x_1} & \cdots & \frac{\partial f_m}{\partial x_n} \end{pmatrix}$$

Cette matrice est notée :

$$J_F(M),\ \frac{\partial(f_1,...,f_m)}{\partial(x_1,...,x_n)} \text{ ou } \frac{D(f_1,...,f_m)}{D(x_1,...,x_n)}$$

Pour i = 1, ..., m, la $i^{ème}$ ligne de cette matrice est la transposée du vecteur gradient au point M de la fonction y_i. La matrice Jacobienne est également la matrice de la différentielle de la fonction.

Exemple :

La matrice Jacobienne de la fonction $F : \Re^3 \rightarrow \Re^4$ définie par :

$$F(x_1, x_2, x_3) = (x_1, 5x_3, 4x_2^2 - 2x_3, x_3 \sin(x_1))$$

est:

$$J_F = (x_1, x_2, x_3) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 5 \\ 0 & 8x_2 & -2 \\ x_3 \cos(x_1) & 0 & \sin(x_1) \end{pmatrix}$$

Propriétés :

La matrice Jacobienne d'une composée de fonctions est le produit des matrices Jacobienne de ces fonctions : $J_{fog} = J_f \cdot J_g$

La matrice Jacobienne de la réciproque d'une fonction est l'inverse de la matrice Jacobienne de cette fonction.

♣ **Critère de Routh-Hurwitz**

C'est un critère algébrique qui permet la détermination de la stabilité de système sans connaître les pôles.

Soit $H(p) = \frac{N(p)}{D(p)}$ la fonction de transfert d'un système. Les pôles de H(p), c'est les racines de l'équation D(p) = 0. Un examen assez simple de D(p), permet de savoir si certaines de ces racines sont à partie réelle positive ou nulle, rendant le système instable.

On écrit D(p) sous forme polynômiale : $D(p) = a_n p^n + a_{n-1} p^{n-1} + ... + a_1 p + a_0$ avec $a_n > 0$.

Le critère s'énonce alors de la façon suivante :

1er examen :

Si les a_i ne sont pas tous de même signe ou si certains sont nuls, D(p) a des racines à droite dans le plan complexe, donc à partie réelle positive.

Le système est donc instable.

2ème examen :

Si tous les a_i sont positive, on ne peut connaître la place des pôles qu'après examen de la première dont la construction est expliquée ci-après.

Les deux premières lignes du tableau sont écrites à l'aide des coefficients de D(p). Les autres sont formées de termes calculés à partir de ces coefficients.

On pose :

$$\begin{array}{c|c} p^n & \\ p^{n-1} & \\ p^{n-2} & \\ p^{n-3} & \\ \cdot & \\ \cdot & \\ \cdot & \\ p^0 & \end{array} \left| \begin{array}{ccccc} a_n & a_{n-2} & a_{n-4} & \cdot & \cdot \\ a_{n-1} & a_{n-3} & a_{n-5} & \cdot & \cdot \\ A_{11} & A_{12} & A_{13} & \cdot & \cdot \\ A_{21} & A_{22} & A_{23} & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ A_{n1} & A_{n2} & A_{n3} & \cdot & \cdot \end{array} \right. \rightarrow \text{La matrice de Routh}$$

On calcul :

$$A_{11} = \frac{-\det\begin{bmatrix} a_n & a_{n\_2} \\ a_{n-1} & a_{n-3} \end{bmatrix}}{a_{n-1}}, \quad A_{12} = \frac{-\det\begin{bmatrix} a_n & a_{n\_4} \\ a_{n-1} & a_{n-5} \end{bmatrix}}{a_{n-1}}, \quad A_{13} = \frac{-\det\begin{bmatrix} a_n & a_{n\_6} \\ a_{n-1} & a_{n-7} \end{bmatrix}}{a_{n-1}},$$

$$A_{21} = \frac{-\det\begin{bmatrix} a_{n-1} & a_{n-3} \\ A_{11} & A_{12} \end{bmatrix}}{A_{11}}, \quad A_{22} = \frac{-\det\begin{bmatrix} a_{n-1} & a_{n-5} \\ A_{11} & A_{13} \end{bmatrix}}{A_{11}}, \quad A_{23} = \frac{-\det\begin{bmatrix} a_{n-1} & a_{n-7} \\ A_{11} & A_{14} \end{bmatrix}}{A_{11}}.$$

Routh a établi que la condition nécessaire et suffisante de stabilité et que tous les coefficients de la première colonne soient de même signe.

Le critère algébrique de Routh permet de savoir de façon simple et rapide si un système est stable ou non. Il nous renseigne sur la stabilité du système mais non sur la robustesse de cette stabilité. De plus sa mise en œuvre nécessite la connaissance de l'expression de la fonction de transfert du système étudié.

♣ **Théorème de la variété centrale**

Soit

$$\frac{dx}{dt} = f(x, c) \tag{1}$$

Un système dynamique non linéaire, x_0 son point d'équilibre qu'on peut ramener à l'origine par le changement de variable: $\xi = x - x_0$ et soit J la matrice Jacobienne d'ordre n

associé au système (1) après sa linéarisation au voisinage de point fixe (après avoir considéré une petite perturbation ξ au voisinage de point fixe) $\frac{d\xi}{dt} = J \cdot \xi$

Soient :

- ✓ $\lambda_1, \lambda_2, ..., \lambda_s$ les valeurs propres de la matrice Jacobienne J dont la partie réelle est négative.
- ✓ $u_1, u_2, ..., u_i$ les valeurs propres de la matrice J dont la partie réelle est positive.
- ✓ $s_1, s_2, ..., s_c$ les valeurs propres dont la partie réelle est nulle, avec $s + i + c = n$.

Et soient :

- ✓ E^s le sous espace vectoriel de dimension s engendré par $\{\lambda_1, \lambda_2, ..., \lambda_s\}$.
- ✓ E^i le sous espace vectoriel de dimension i engendré par $\{u_1, u_2, ..., u_i\}$.
- ✓ E^c le sous espace vectoriel de dimension c engendré par $\{s_1, s_2, ..., s_c\}$.

avec

$$E^n = E^s \oplus E^i \oplus E^c$$

On a le théorème suivant :

Théorème : *Il existe des variétés de classe C^r: stable W^s; instable W^i, et centrale W^c tangentes respectivement à E^s, E^i et E^c en x_0. Ces variétés sont invariantes, par rapport au flot de système (1)*

Variété centrale dépendant d'un paramètre

On applique une petite perturbation ε sur le système (1), donc le résultat sera un système dynamique dépendant d'un paramètre ε, et supposons que par une certaine transformation on peut ramener le système (1) à un système de la forme :

$$\begin{cases} \dot{x} = A_1 x + f(x, y, z, \varepsilon) \\ \dot{y} = A_2 y + g(x, y, z, \varepsilon) \\ \dot{z} = A_3 z + m(x, y, z, \varepsilon) \\ \dot{\varepsilon} = 0 \end{cases} \quad (2)$$

La variété centrale au voisinage de (0, 0, 0, 0) est alors donnée par :

$$y = h_1(x,\varepsilon),\ \ z = h_2(x,\varepsilon)$$

Après un simple calcul, et après avoir appliqué le développement de Taylor sur h_1 et h_2, on peut donc écrire le système (2) sous la forme :

$$\begin{cases} \dot{x} = A_1 x + f(x, h_1(x,\varepsilon), h_2(x,\varepsilon), \varepsilon) \\ \dot{\varepsilon} = 0 \end{cases} \qquad (3)$$

Le théorème suivant permet de lier la dynamique du système (3) à celle du système (2):

Théorème : *Si l'origine $x_0 = 0$, du système (3) et asymptotiquement stable (instable), alors l'origine du système (2) est aussi asymptotiquement stable (instable).*

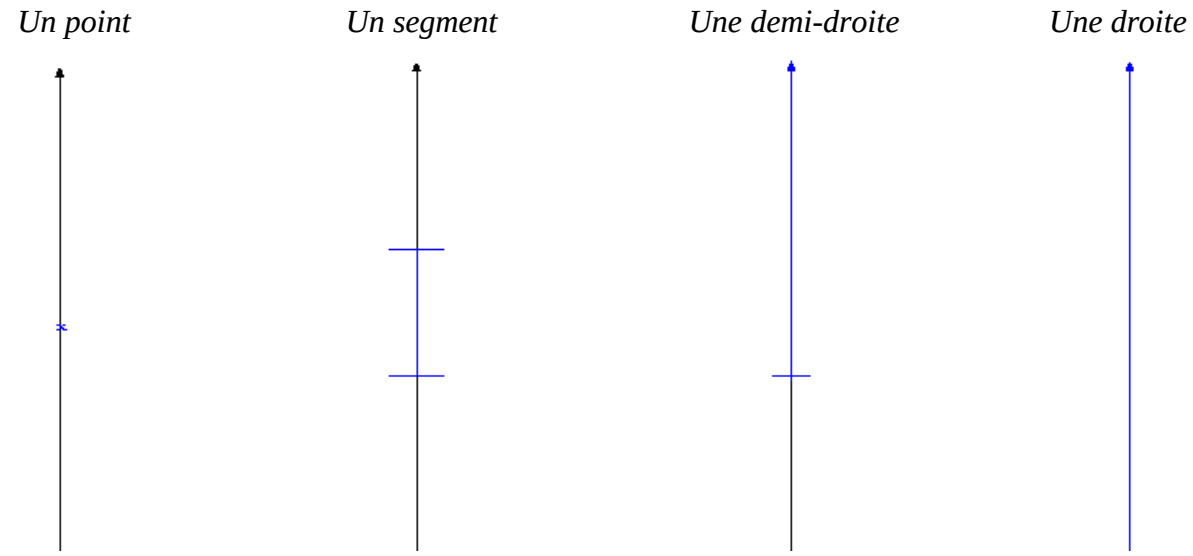
ANNEXE A

BIFURCATIONS EN DIMENSION 1

Considérons le système dynamique suivant, dépendant des paramètres $\vec{\beta} = (\mu, \alpha)$ de l'espace de contrôle E_c, dans un espace des phases E_p de dimension 1.

$$\dot{x} = f_{\vec{\beta}}(x)$$

La figure suivante montre les quatre trajectoires possibles du système:



a. Bifurcation nœud-col ou saddle node :

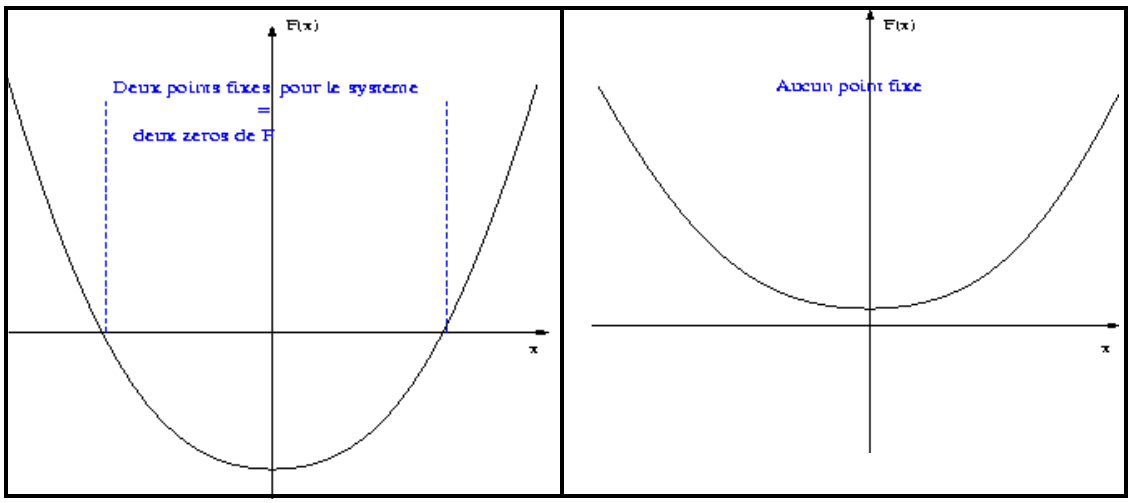
C'est la bifurcation associée à l'équation $\dot{x} = \mu + \alpha x^2$

- ✓ *Recherche des points fixes :*

Recherchons les points de vitesse nulle: $\dot{x} = f_{\vec{\beta}}(x) = \mu + \alpha x^2 = 0$

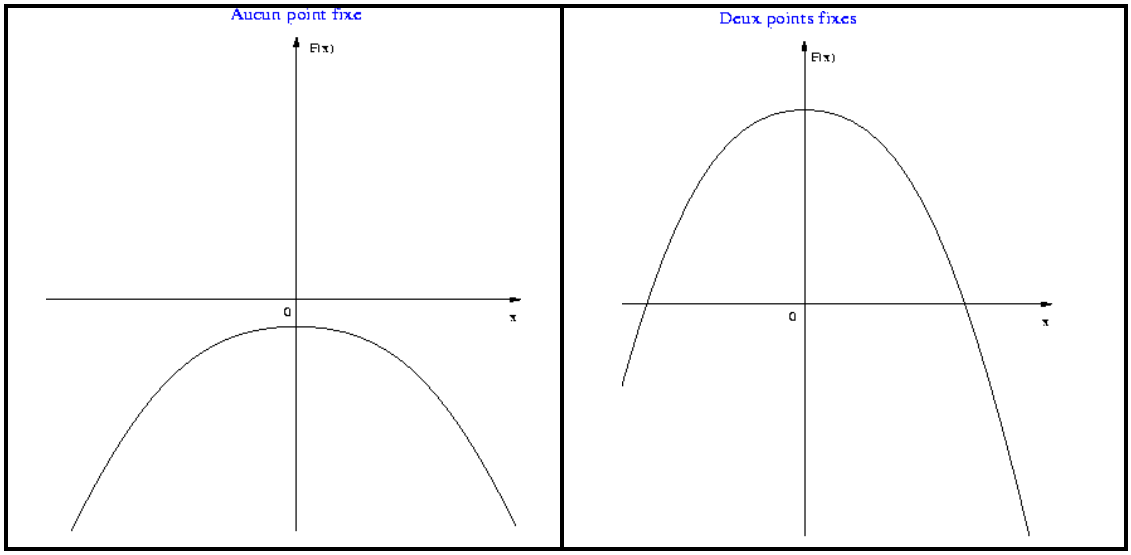
La résolution de l'équation $\dot{x} = \mu + \alpha x^2$, nous conduit à considérer deux cas : $\alpha > 0$ et $\alpha < 0$.

1er cas : $\alpha > 0$ **:**



(a) Cas $\mu < 0$	**(b)** Cas $\mu > 0$

2ème cas : $\alpha < 0$ **:**



(a) Cas $\mu < 0$	**(b)** Cas $\mu > 0$

✓ <u>Étude de la stabilité de ces points :</u>

Soit une fonction de perturbation u(t), que nous allons rajouter aux points fixes: $x(t) = x_e + u(t)$.

Remarquons tout d'abord que $\dot{x} = \dot{u} = \mu + \alpha x^2 = f_{\bar{\beta}}(x)$. Comme nous sommes au voisinage du point x_e, nous pouvons calculer un développement de Taylor de f à l'ordre 1 :

$$\dot{x} = \dot{u} = f(x_e + u) = f(x_e) + f'(x_e)u + o(u^2)$$

Posons $\lambda = f'(x_e)$, or $f(x_e) = 0$. On aboutit à une équation différentielle linéaire du premier ordre : $\dot{u} = \lambda u$, qui admet des solutions de la forme: $u(t) = u(0)e^{\lambda t}$. La discussion devient alors très simple:

- ✓ Si $\lambda > 0$, u tend vers l'infini, lorsque t devient très grand: le point x_e est instable.
- ✓ Sinon ($\lambda < 0$), le point est stable.

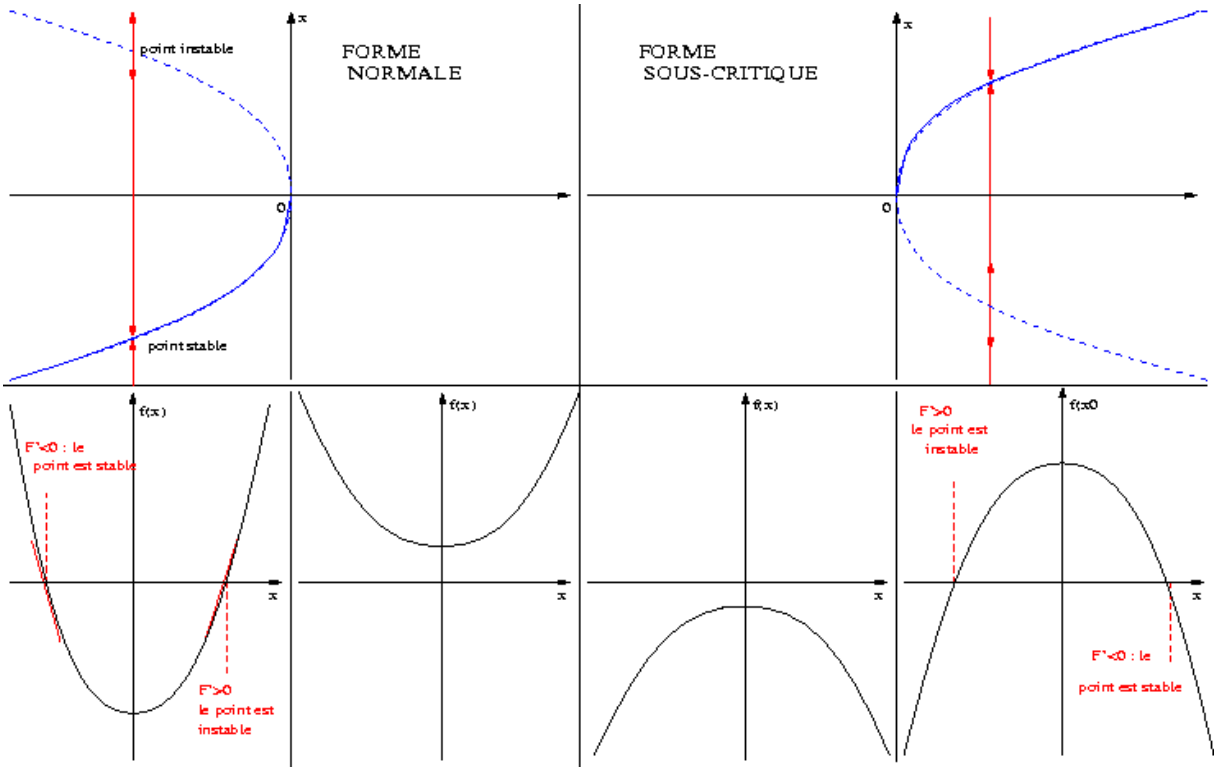
Comme $\lambda = f'(x_e)$, nous en déduisons que la stabilité de point fixe x_e est fonction de la pente de f en x_e.

Remarque: Cette démarche n'est valable que localement i.e. au voisinage des points fixes du système.

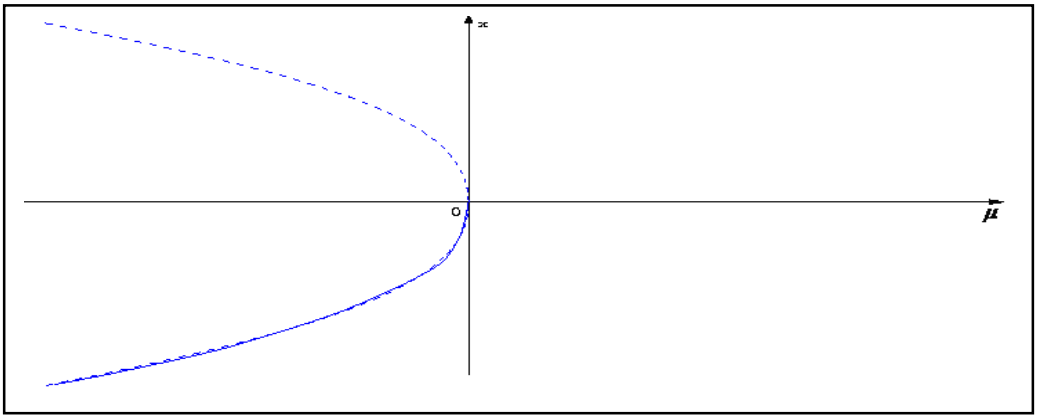
- ✓ *Diagramme de bifurcation et interprétation :*

Toutes les informations peuvent se résumer sur une seule figure, en dessinant:

- en pointillé la trajectoire du point instable
- en trait plein, celle du point stable.



Prenons la figure suivante, qui correspond au cas $\alpha < 0$ et essayons de voir tous les résultats que l'on peut en tirer.



Supposons que l'on possède un potentiomètre qui nous permette de faire varier le paramètre μ. Au départ, le système est placé sur une valeur de μ négative. L'équation $\dot{x} = \mu + \alpha x^2$ admet alors deux points fixes: l'un est stable (attracteur), l'autre est instable. Faisant tendre μ vers 0 sans l'atteindre, on constate que les deux points fixes se rapprochent. Pour $\mu = 0,$ ils fusionnent en un seul point fixe dit semi-stable. Il y a donc eu perte du point attracteur, le système s'est déstabilisé. Augmentant encore μ pour qu'il ne prenne que des valeurs strictement positives, il y purement et simplement disparition de tout point fixe.

b. Bifurcation fourche ou pitchwork

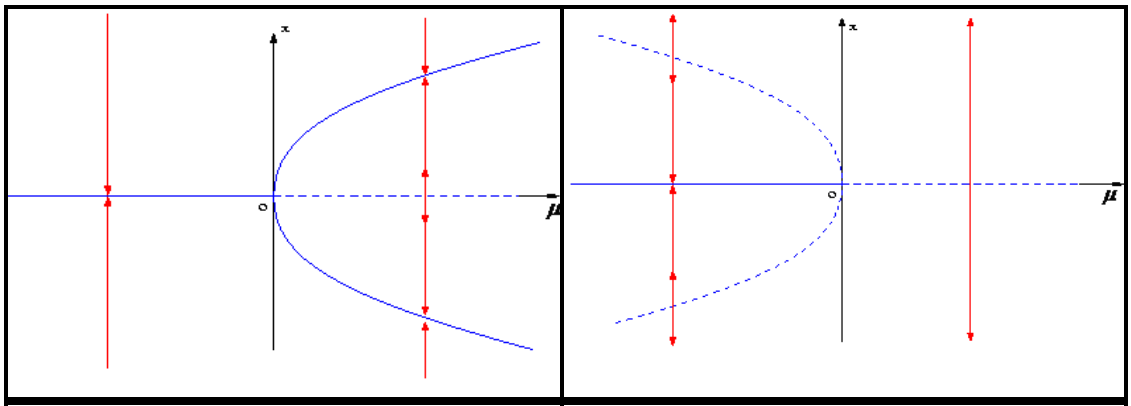
Considérons maintenant l'équation $\dot{x} = \mu x + \alpha x^3$

- *Recherche des points fixes :*

Pour résoudre l'équation $\mu x + \alpha x^3 = 0$ écrivons l'équation sous la forme $x(\mu + \alpha x^2)$. Un premier point fixe apparaît de façon évidente: $x = 0$ valable pour toutes valeurs de μ et de α. Une discussion s'impose, suivant les valeurs du paramètre α.

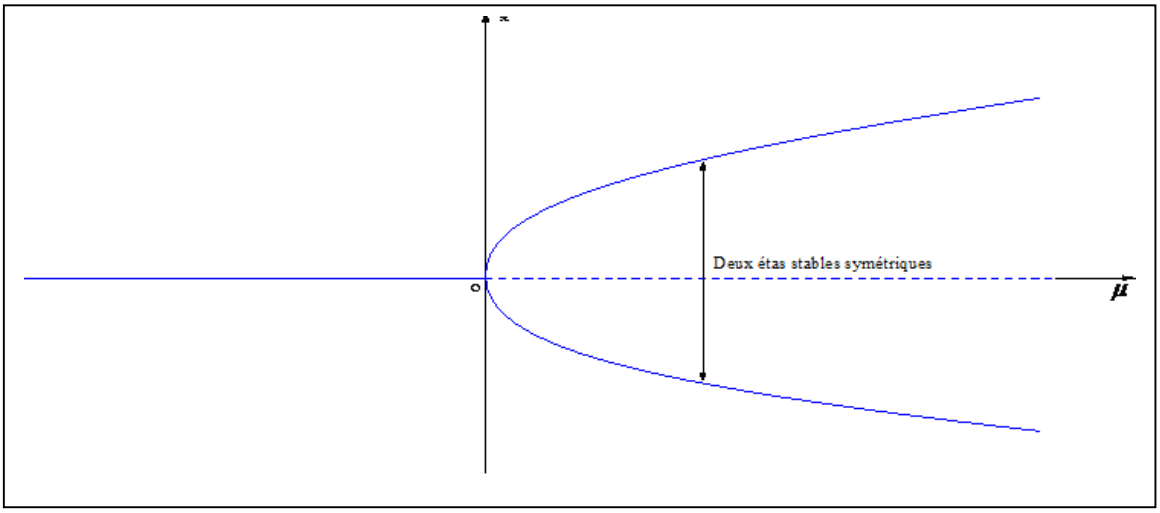
- *Étude de la stabilité de ces points et diagramme de bifurcation :*

Réappliquant la méthode utilisée pour la première bifurcation, nous allons représenter directement le diagramme de bifurcation.



(a) Forme normale ($\alpha < 0$)	**(b)** Forme sous critique ($\alpha > 0$)

Dans un système qui va se déstabiliser par une bifurcation fourche, existe une symétrie ponctuelle, de centre 0 des solutions: si x(t) est une solution du système, alors -x(t) en est une aussi. Cette symétrie apparait de façon évidente sur le diagramme de bifurcation :



Naissance d'une symétrie dans une bifurcation fourche

- *Interprétation (dans le cas où* $\alpha < 0$ *)*

Nous partons donc d'un système où le paramètre μ est négatif: le système possède alors un point fixe stable (un attracteur ponctuel) puis, nous faisons augmenter progressivement μ .

Lorsque μ atteint la valeur 0, le système se déstabilise: le point fixe perd sa stabilité, sa nature topologique change: il y a bifurcation. Augmentant encore le paramètre μ , c'est-à-dire qu'il devient positif, on voit apparaitre alors deux points fixes stables. Il y a eu en quelque sorte dédoublement du point fixe.

c. Bifurcation de Hopf

Considérons l'équation suivante :

$$\dot{Z} = (\lambda + iw)Z - \alpha|Z|^2 Z \qquad \text{(A)}$$

Ou :

Z une variable complexe, qu'on peut sous la forme: $Z = \rho(t)e^{i\theta(t)}$.

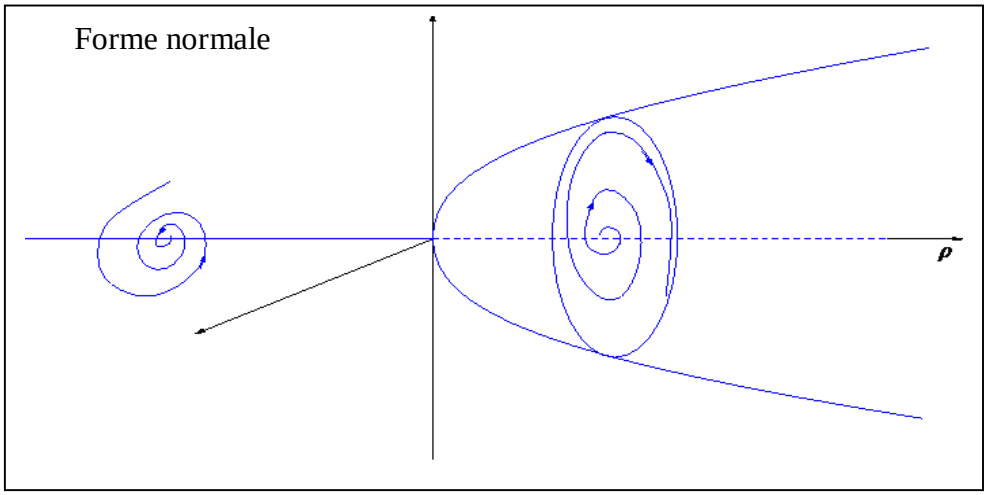
α est un nombre complexe: $\alpha = \alpha_r + i\alpha_i$.

L'équation (1) s'écrit donc sous forme d'un système:

$$\begin{cases} \dot{\rho} = \lambda\rho + \alpha_r\rho^3 & \text{(A.1)} \\ \dot{\theta} = w + \alpha_i\rho^2 & \text{(A.2)} \end{cases}$$

L'équation (A.1) n'est autre qu'une bifurcation fourche étudiée précédemment

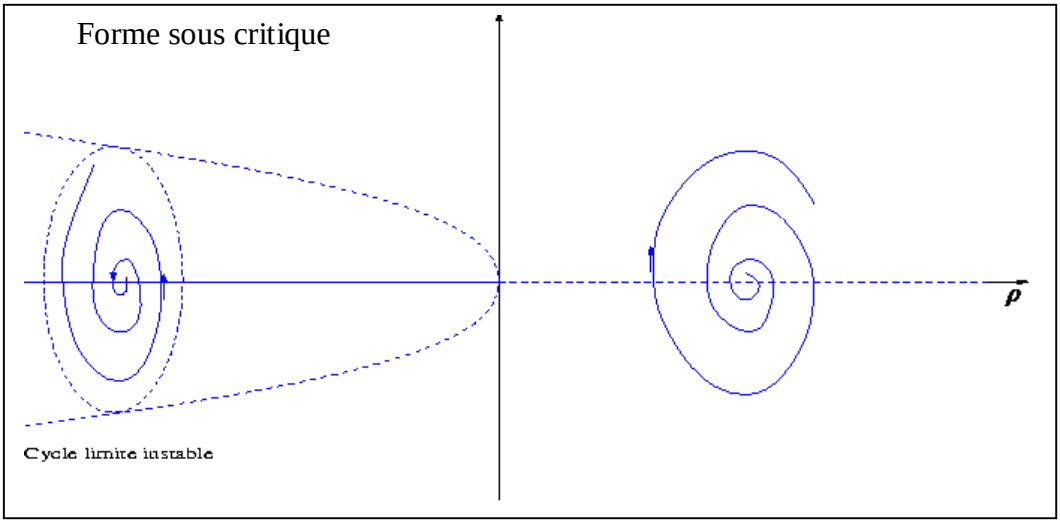
- *Diagramme de bifurcation*

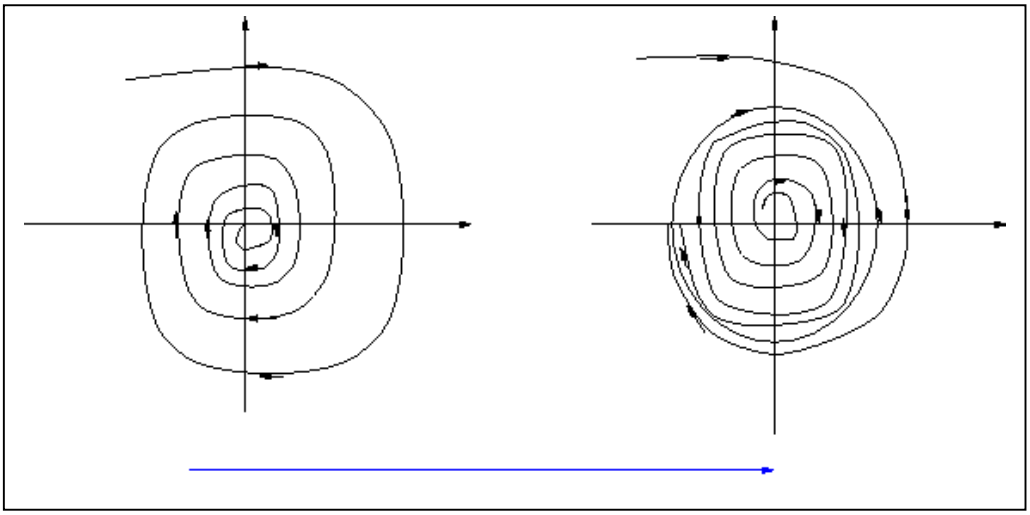


- *Interprétation :*

Le système possède au départ un point fixe attracteur (cas $\lambda < 0$), qui correspond ici, à un point puis: les trajectoires spirales tendent exponentiellement vite vers l'origine. Puis lorsque $\lambda = 0$, ce point fixe perd sa stabilité. Augmentant encore λ (cas > 0), se forme alors un cycle limite stable, c'est-à-dire un attracteur périodique [19].

.





Transformation d'un attracteur ponctuel en un cycle limite

BIBLIOGRAPHIE

[1] A. LAYEC. « Développement de modèles de CAO pour la simulation système des systèmes de communication. Application aux communications chaotiques ». Thèse doctorat 2006.

[2] Mihai Bogdan Luca. « Apports du chaos et des estimateurs d'états pour la transmission sécurisée de l'information ». Thèse doctorat 2006.

[3] A. ZEMOOUCHE. « Sur l'observation de l'état des systèmes dynamiques non linéaires ».Thèse doctorat 2007.

[4] J. ODEN. « Le chaos dans les systèmes dynamiques ». 2007

[5] www.scholarpedia.org/article/Hyperchaos

[6] Z. AMRANI, S. CHITROUB et A. BOUKHARI. « Cryptage d'Images par Chiffrement de Vigenère Basé sur le Mixage des Cartes Chaotiques » 4th International Conference on Computer Integrated Manufacturing CIP'2007 03-04 November 2007.

[7] http://www.greyc.unicaen.fr/auto/seminaires

[8] http://www.umi2958.eu/spip.php?article132&lang=fr

[9] http://www.tout-pour-la-science.com/2284/S%E9curisation+de+l%27information+: +le+cryptage+par+le+chaos.html

[10] Arkady Pikovsky, Michael Rosenblum and Jurgen Kurths « Synchronization: A Universal Concept in Nonlinear Sciences», Cambridge university press 2001.

[11] Jules Haag, «la synchronisation des systèmes oscillants non linéaires». Annales scientifiques de l'E.N.S, 3ème série, tome 67 (1950), p. (321-392).

[12] Dj. KARA ALI. « Synchronisation des systèmes dynamiques chaotiques ». Thèse de magister 2007.

[13] http://fr.wikipedia.org/wiki/Entropie_métrique

[14] http://fr.wikipedia.org/wiki/Théorie_du_chaos

[15] http://www.edelo.net/chaos/chap3.htm

[16] http://www.journaldunet.com/science/science-et-nous/dossiers/07/defis-maths/8.shtml

[17] http://wapedia.mobi/fr/Matrice_Jacobienne

[18] http://www.scribd.com/doc/9933078/LA-STABILITE-DES-SYSTEMES

[19] http://hmf.enseeiht.fr/travaux/CD9598/travaux/optmfn/IH/COURS/BIFURCATIONS/mato/node1.html

[20] http://fr.wikipedia.org/wiki/M%C3%A9thodes_de_Runge-Kutta

[21] Ahmad M. Harb,Wajdi M. Ahmad «Chaotic systems synchronization in secure communication systems. "Electrical Engineering Dept. Jordan Univ. of Science and Technology Irbid, Jordan».

[22] T. Yamada and H. Fujisaka. Stability theory of synchronized motion in coupled-oscillator systems. ii. *Prog. Theor. Phys.*, 70:1240, 1983.

[23] T. Yamada and H. Fujisaka. Stability theory of synchronized motion in coupled oscillator systems. iii. *Prog. Theor. Phys.*, 72:885, 1984.

[24] P. Curran and L. Chua. Absolute stability theory and the synchronization problem. *Int. J. of Bifurcation and Chaos*, 7(6): 1375–1382, 1997.

[25] M. Hasler. Engineering chaos for encryption and broadband communication. *Phil. Trans. Royal Soc. London,* A, 353 :115–126, 1995.

[26] L.M. Pecora and T.L. Carroll. Synchronization in chaotic systems. *Phys. Rev. Lett.*, 64(8): 821–824, 1990.

[27] Paul Manneville, "Dynamique non linéaire et chaos." Laboratoire d'Hydrodynamique, Ecole Polytechnique, Séminaire E2PHY 25 Août 2005.

[28] Peter Stavroulakis, "Chaos applications in telecommunications", CRC 2005.

[29] Serge Dos Santos, "Synchronisation des systèmes : application aux fluctuations de base fréquence des oscillateurs ultra- stables.", Thèse de doctora Université de Besançon France.

[30] S. Boccaletti, J. Kurths, G. Osipov, D.L. Valladares, C.S. Zhou, " The synchronization of chaotic systems.", Physics Reports 366 (2002) 1.101.

[31] T. Carroll et L. Pecora, "Nonlinear dynamics in circuits", World scientific, 1995.

[32] T. L. Carroll and L.M. Pecora, Code 6343, US Naval Research Lab, Washington, DC 20375, "Using multiple attractor chaotic systems for communication."

[33] V. S. Anishchenko," Dynamical chaos- Models and experiments", World scientific 1995.

[34] V. S. Anishchenko, " Nonlinear dynamics of chaotic and stoquatic systems" Springer 2002.

[35] Zeraoulia Elhadj, Hamri Nasr Edine, " A generalized model of some Lorenz Type and Quasi- attractors type strange attractors in three dimensional dynamical systems.", International journal of pur and applied mathematical sciences, vol 2, No 1.2005

[36] Zhigang Zheng, Gang Hu, et Bambi Hu1, "Phase Slips and Phase Synchronization of Coupled Oscillators", volume 81, number 24 physical review letters 14 December 1998.

Résumé :

L’utilisation du chaos pour sécuriser les télécommunications est un thème de recherche récent du début des années 1990. Le chaos est obtenu a partir de systèmes non linéaires; il correspond a un comportement stable, apériodique et éventuellement borné, de ces systèmes, ce qui le fait apparaître comme du « bruit » pseudo-aléatoire. Il peut donc être utilisé pour masquer ou mélanger les informations dans une transmission sécurisée.

L'objectif de cette thèse est de compléter cette étude à la fois sur les aspects théoriques et numériques. Les principaux points abordés sont :

- Les systèmes dynamiques chaotiques et hyperchaotiques.
- Transmission a porteuse chaotique.
- Méthodes de synchronisation chaotique.
- Système chaotique de Chen.

Mots-clés

Systèmes chaotiques, Systèmes hyperchaotiques, théorie du chaos, synchronisation du chaos, cryptographie chaotique.

Abstract:

The use of chaos to reassure telecommunications is the recent research topic of the beginning of 1990s. Chaos is acquired has leave not linear systems; it corresponds has a stable behaviour, periodical and possibly delimited, of these systems, what shows it as pseudo-unpredictable "noise". He can therefore be used to conceal or blend information in a reassured transmission.

The objective of this thesis is to supplement this study at the same time on the theoretical and numerical aspects. The main approached points are:

• The chaotic and hyper-chaotic systems.
• Transmission has chaotic holder.
• Methods of chaotic synchronization.
• System chaotic of Chen.

Key words:

Chaotic systems, hyper-chaotic system, theory of chaos, synchronization of chaos, chaotic cryptography.

الملخص :

إن استعمال الفوضوي في ميدان الاتصالات السلكية و اللاسلكية لحماية المعلومات موضوع حديث درس لأول مرة سنة 1990.

الفوضوي ينشأ من النظم غير الخطية هو إذن استجابة مستقرة غير دورية ومحدودة مما يجعله يشبه الضجيج .

يمكن استعمال الفوضوي لتغطية المعلومة لحمايةالإتصالات.

الهدف من هذه المذكرة هو إكمال الدراسات في هذا المنهج.

أهم النقاط المتداولة:

الأنظمة الدينامكية الفوضوية و الجد فوضوية.

البث على عامل فوضوي.

طرق التزامن الفرضية.

النظام الفوضوي – تشان- .