UNIVERSITAT DE BARCELONA

Facultat de Matemàtiques
i Informàtica

GRAU DE MATEMÀTIQUES

Treball final de grau

Sistema de Lorenz i criptosistemes caòtics

Autor: Pol Arévalo Soler

Directors:	**Dr. Arturo Vieiro Yanes**
	Dr. Marina Gonchenko
Realitzat a:	**Departament de Matemàtiques i Informàtica**
Barcelona,	**24 de gener de 2023**

Abstract

In this work we study the Lorenz system and its application in the field of cryptography. Initially, from a theoretical point of view, we describe the most important properties and basic concepts of the system, in particular, we study the symmetry of the system, the invariance of the z axis, the existence of a global attractor, the stability of the equilibrium points, bifurcations and we present basic notations of chaos theory in order to understand the main features of the behavior of the Lorenz system and its strange attractor. To do this, we use analytical and numerical tools. Later, from a more practical point of view, we present the synchronization of chaos that will allow us to introduce the concept of chaotic cryptography. Finally, we implement algorithms (in C) to encrypt and decrypt signals using the Lorenz system and analyze the dependence that exists between the error committed when recovering the original signal and the same signal.

Resum

En aquest treball estudiem el sistema de Lorenz i la seva aplicació en l'àmbit de la criptografia. Inicialment, des d'un vessant teòric descrivim les propietats més importants i conceptes bàsics del sistema, en particular, estudiem la simetria del sistema, la invariància de l'eix z, l'existència d'un atractor global, l'estabilitat dels punts d'equilibri, bifurcacions. Presentem una breu introducció a la teoria del caos per tal d'entendre millor les propietats més rellevants del comportament del sistema de Lorenz i del seu atractor estrany. Per fer-ho, utilitzem eines analítiques i numèriques. Posteriorment, des d'un vessant més pràctic, presentem la sincronització del caos que ens permetrà introduir el concepte de criptografia caòtica. Finalment, presentem algorismes (en C) per xifrar i desxifrar senyals usant el sistema de Lorenz i analitzem la dependència que existeix entre l'error comès en recuperar el senyal original i el mateix senyal.

2020 Mathematics Subject Classification. 11G05, 11G10, 14G10

Agraïments

M'agradaria donar les gràcies a totes aquelles persones sense les quals ni aquest treball ni els meus estudis haguessin estat possibles.

Primer de tot, vull agrair als meus tutors, Arturo i Marina, per tota la seva dedicació a aquest projecte i la seva comprensió i paciència durant aquests mesos, per acompanyar-me en aquest treball i per tots els consells que m'han donat. Sempre han mostrat disponibilitat per atendre els meus dubtes, per orientar-me i guiar-me en el projecte. Tot això ha fet que sempre em sentís ajudat.

També m'agradaria donar les gràcies a la meva família i amics pel suport al llarg de la carrera, tant els de sempre com els que he conegut al grau, especialment a l'Aleix i el Guillem.

Índex

1 Introducció

1.1 Motivació

El sistema d'equacions diferencials, conegut com a sistema de Lorenz, fou descobert pel meteoròleg i matemàtic del Massachusetts Institute of Technology (MIT) Edward N. Lorenz.

L'any 1963, Lorenz publicà un article [1] en el qual, seguint els passos de Saltzman (1962) [2], construí un model matemàtic molt simplificat que intentava reproduir el comportament de convecció a l'atmosfera. De manera general, podem definir la convecció com el transport de calor entre zones amb diferents temperatures mitjançant un fluid. En el cas de l'atmosfera, el moviment és degut a la força gravitacional a conseqüència de la diferència de densitat entre les masses d'aire fred i calent. Les masses d'aire fred, més pesades per la seva major densitat, descendeixen, al contrari que les masses d'aire calent, menys pesades per la seva menor densitat que ascendeixen.

Considerem un fluid comprès entre dues capes d'amplada h en el pla $x - z$. La capa inferior s'escalfa mentre que la capa superior es refreda, creant una diferència de temperatura constant ΔT, aquest fet crea una força externa sobre el fluid que genera la convecció. L'any 1962 Saltzman obtingué les equacions darrere d'aquest problema físic. El treball de Lorenz fou desenvolupar aquestes equacions utilitzant la teoria de l'aproximació per obtenir un sistema molt simplificat, l'anomenat sistema de Lorenz. Una anàlisi més profunda sobre la derivació original d'aquest model es pot trobar a [1]. Seguint la notació original presentem el sistema de Lorenz

$$\begin{aligned} \dot{x} &= \sigma(y - x), \\ \dot{y} &= -xz + rx - y, \\ \dot{z} &= xy - bz, \end{aligned}$$

on σ, r, $b > 0$ són paràmetres, σ s'anomena *número de Prandlt*, r s'anomena *número de Rayleigh* i b no té nom.

Lorenz, en integrar numèricament aquestes equacions en un ordinador, descobrí que aquest sistema determinista presentava dinàmiques extremadament erràtiques. Tot i disposar d'un ordinador personal al seu despatx, excepcional per l'època, a causa de la precarietat dels ordinadors d'aquells temps i l'elevat temps de computació, decidí prendre condicions inicials de tan sols tres decimals. Aquest fet, aparentment no hauria de suposar un gran canvi en el resultat, ja que l'experiència deia que canviar lleugerament les condicions inicials produïa que les solucions canviessin lleugerament també. La sorpresa fou quan veié que les solucions obtingudes eren totalment diferents. Aquest fenomen és el que avui en dia anomenem *sensibilitat respecte les condicions inicials*.

El més sorprenent, però, fou que per un ampli rang de paràmetres, en particular Lorenz estudià el cas $\sigma = 10$, $b = \frac{8}{3}$ i $r = 28$, les solucions oscil·laven irregularment sense repetir, però sempre dins d'una regió acotada en l'espai de fases. Quan representà les trajectòries en tres dimensions, descobrí que romanien en un conjunt complicat, un *atractor estrany*. A diferència dels punts fixos estables o cicles límit, l'atractor estrany no és ni un punt ni una corba, sinó un *fractal* de dimensió aproximadament 2.06.

Aquest descobriment donà lloc a la popular denominació de *teoria del caos*, una branca de les matemàtiques que estudia sistemes dinàmics molt sensibles a les variacions de les condicions inicials.

1.2 Objectius

Els objectius d'aquest treball final de grau són entendre les propietats bàsiques i l'estructura de l'espai de fases del sistema de Lorenz, ser capaç d'implementar mètodes numèrics simples per a la integració numèrica d'equacions diferencials i usar-los per explorar propietats dinàmiques del sistema, així com per resoldre el sistema i usar coneixements previs per donar una bona reflexió sobre els resultats obtinguts. També entendre el funcionament dels sistemes caòtics i utilitzar el sistema de Lorenz en l'àmbit de la comunicació privada per poder xifrar i desxifrar senyals. Finalment, es pretén analitzar com es comporta l'error d'encriptació d'un senyal.

1.3 Estructura de la Memòria

La memòria s'ha estructurat en dos capítols: un primer capítol on s'inclou una descripció matemàtica del sistema de Lorenz i un segon capítol on es discuteix l'ús d'aquest sistema en l'àmbit de la criptografia.

Així en el capítol 2, descrivim algunes propietats del sistema de Lorenz, en particular, la no-linealitat, la simetria que presenta i la invariància de l'eix z. Presentem i demostrem l'existència d'un atractor global i estudiem les característiques més importants de l'espai de fases. En particular, oferim resultats bàsics sobre l'estabilitat dels seus punts d'equilibri, varietats invariants i òrbites homoclíniques, heteroclíniques i periòdiques que sorgeixen en variar els paràmetres del sistema. També donem una introducció a la teoria del caos i els conceptes més rellevants com la dependència respecte a les condicions inicials i els exponents de Lyapunov per entendre millor el comportament del sistema de Lorenz i del seu atractor estrany.

En el capítol 3, donem una breu introducció a la criptografia i introduïm el concepte de sincronització del caos, en concret, provem la sincronització en el sistema de Lorenz. Aquest fet, ens permet presentar la idea de criptografia caòtica, en particular, estudiarem l'emmascarament caòtic usant el sistema de Lorenz. Posteriorment, implementem un algorisme en C per xifrar i desxifrar senyals emprant el sistema de Lorenz i analitzem la dependència que existeix entre l'error comès en recuperar el senyal original i el mateix senyal. Finalment, posem en context l'estat actual de la criptografia caòtica i els mètodes que s'estan utilitzant en l'actualitat per a millorar la seguretat en l'àmbit de la comunicació privada.

Finalment, en el capítol 4 s'exposen les conclusions del treball i s'inclouen dos annexos. El primer annex un breu apunt sobre integració numèrica d'equacions diferencials i el segon annex inclou una explicació del càlcul dels exponents de Lyapunov de sistemes dinàmics continus.

2 Propietats del sistema de Lorenz

En aquest capítol, presentem les propietats més rellevants del sistema de Lorenz. Acabem el capítol provant l'existència d'un conjunt atractor global. Aquesta propietat requereix conceptes previs i d'una anàlisi matemàtica molt detallada. La demostració completa i rigorosa és una tasca molt complexa que durant molts anys fou un repte per a tots els matemàtics.

2.1 Camps vectorials i equacions diferencials autònomes. Flux.

Sigui $f : U \to \mathbb{R}^n$ un camp vectorial de classe $C^r (r \geq 1)$ en l'obert U. Li associem l'equació diferencial autònoma $\dot{x} = f(x)$ en $\Omega = \mathbb{R} \times U$.

Aleshores, definim l'aplicació

$$\begin{aligned} \phi : D \subset \mathbb{R} \times U &\longrightarrow \quad U, \\ (t; x_0) &\longrightarrow \phi(t;\ 0,\ x_0), \end{aligned}$$

on $D = \left\{(t; x_0) \in \mathbb{R} \times U \mid t \in I(x_0)\right\}$, $\big((I(x_0)$ interval de definició de les solucions$\big)$. Llavors,

1. $D \subset \mathbb{R} \times U$ és obert.
2. Per a tot $x_0 \in U, s \in I(x_0)$:
   (a) $0 \in I(x_0)$ i $\phi(0; x_0) = x_0$.
   (b) $t \in I\left(\phi(s;\ x_0)\right)$ si, i només si, $t + s \in I(x_0)$, i $\phi\left(t;\ \phi(s;\ x_0)\right) = \phi(t + s;\ x_0)$.
3. ϕ és derivable respecte a t i la seva derivada parcial $\frac{\partial \phi}{\partial t} : D \to \mathbb{R}^n$ és C^r, $r \geq 1$.

Es diu que ϕ és el flux (local) associat al camp vectorial f. Per a cada $t \in \mathbb{R}$, definim $U_t = \{x \mid t \in I(x)\}$ i la immersió difeomòrfica $\phi_t : U_t \to U$ per $\phi_t(x) = \phi(t, x)$ (suposant que $U_t \neq \emptyset$). A més, les propietats (a) i (b) es tradueixen com $\phi_0 = id_{|U}$ i $\phi_{t+s} = \phi_t \circ \phi_s$. En particular, es té $\phi_t^{-1} = \phi_{-t}$.

2.2 Notació i no-linealitat

Primerament, introduïm notació que utilitzarem al llarg del capítol per tal de facilitar-ne la lectura.

D'ara endavant, considerarem el sistema autònom

$$\begin{aligned} \dot{x} &= f(x), \\ x(0) &= x_0, \end{aligned} \tag{2.1}$$

on assumirem que $f \in C^r(U, \mathbb{R}^n)$, $r \geq 1$ i U subconjunt obert de $\mathbb{R}^n$. Sovint anomenem (2.1) com problema de valor inicial (P.V.I) o problema de Cauchy.

Considerem el sistema d'equacions diferencials de Lorenz

$$\begin{aligned} \dot{x} &= \sigma(y - x), \\ \dot{y} &= -xz + rx - y, \\ \dot{z} &= xy - bz, \end{aligned} \tag{2.2}$$

on $\sigma, r, b > 0$. Aquí el punt denota la derivada respecte del temps. Donat que el sistema d'equacions és autònom, introduint $w(t) = (x(t), y(t), z(t))$ podem reescriure (2.2) de la següent manera

$$\dot{w}(t) = f(w(t)), \tag{2.3}$$

on $f : \mathbb{R}^3 \to \mathbb{R}^3$ és el camp vectorial.

Encara que sembli un sistema d'equacions molt simple, és molt complicat de resoldre analíticament, ja que presenta dues no-linealitats, els termes quadràtics xy i xz.

2.3 Existència i unicitat

Quan se'ns presenta un sistema d'equacions diferencials, sembla natural començar per provar l'existència i unicitat de solucions.

La matriu jacobiana del sistema (2.2) ve donada per

$$\begin{pmatrix} -\sigma & \sigma & 0 \\ r - z & -1 & -x \\ y & x & -b \end{pmatrix} \tag{2.4}$$

Com que totes les components són contínues, és a dir, el camp f de (2.3) és $C^1(\mathbb{R}^3)$ el teorema de Picard garanteix l'existència i unicitat de solucions per qualsevol problema de Cauchy amb $t_0 \in \mathbb{R}$ i $w_0 \in \mathbb{R}^3$.

2.4 Simetria

El sistema de Lorenz és invariant sota la transformació $(x, y, z) \mapsto (-x, -y, z)$. Aquesta simetria persisteix per qualsevol valor dels paràmetres. És a dir, si $(x(t), y(t), z(t))$ és solució del sistema, aleshores $(-x(t), -y(t), z(t))$ també ho és.

A continuació, provem aquesta propietat.

Proposició 2.1. *Sigui $\varphi(t) = (x(t), y(t), z(t))$ una solució del sistema de Lorenz, aleshores $\hat{\varphi}(t) = (-x(t), -y(t), z(t))$ també ho és.*

Demostració. Sigui $\varphi(t) = (x(t), y(t), z(t))$ solució del sistema (2.2). Volem provar que $\hat{\varphi}(t) = (-x(t), -y(t), z(t))$ també és solució, és a dir, volem veure que $\frac{d}{dt}\hat{\varphi}(t) = f(\hat{\varphi}(t))$. Sigui $(X, Y, Z) = (-x, -y, z)$. Per provar que $\hat{\varphi}(t) = (-x(t), -y(t), z(t))$ és solució, n'hi ha prou en comprovar que (X, Y, Z) verifica (2.2).

$$\begin{aligned}
\dot{X} &= (-\dot{x}) = -\dot{x} = -\sigma(y - x) = \sigma(-y - (-x)) = \sigma(Y - X), \\
\dot{Y} &= (-\dot{y}) = -\dot{y} = -(-xz + rx - y) = -(-x)z + r(-x) - (-y) = -XZ + rX - Y, \\
\dot{Z} &= \dot{z} = (-x)(-y) - bZ = XY - bZ.
\end{aligned}$$

Per tant, el sistema de Lorenz és invariant sota la transformació $(x, y, z) \mapsto (-x, -y, z)$. □

2.5 Eix z

L'eix z és invariant. Totes les trajectòries que comencen en aquest eix hi romanen i tendeixen a l'origen $(0, 0, 0)$ quan $t \to +\infty$. La següent proposició mostra aquesta propietat.

Proposició 2.2. *L'eix z és invariant.*

Demostració. L'eix z ve determinat pels punts $x = y = 0$. Si inicialment prenem un punt de l'eix z, $(0, 0, z_0)$, i restringim el sistema de Lorenz (2.2) a aquest eix, obtenim

$$\dot{x} = 0,\ \dot{y} = 0,\ \dot{z} = -bz.$$

Integrant aquest sistema i aplicant la condició inicial obtenim que $x = y = 0$ per tot a temps futur t i $z(t) = z_0 e^{-bt}$. Clarament, $z(t) = z_0 e^{-bt} \to 0$ quan $t \to +\infty$.

Per tant, l'eix z és un conjunt invariant i totes les solucions que comencen en aquest eix tendeixen a l'origen quan $t \to +\infty$, és a dir, tenim que $\{x = y = 0\} \subset W^s(0, 0, 0)$ i és invariant. □

La Figura 1 mostra la invariància de l'eix pels valors clàssics $\sigma = 10,\ b = \frac{8}{3}$ i dos valors de r, $r = 15,\ r = 28$.

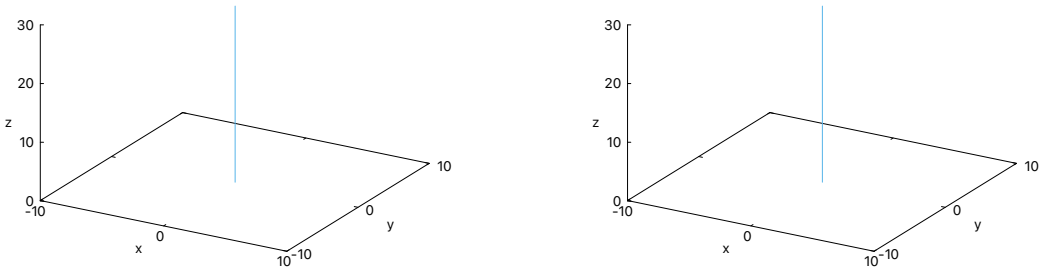

Figura 1: A l'esquerra, solució del P.V.I per $r = 15$ i condicions inicials $x_0 = (0,\ 0,\ 30)$. A la dreta, solució del P.V.I per $r = 28$ i condicions inicials $x_0 = (0,\ 0,\ 30)$.

2.6 Existència d'un atractor global

El sistema de Lorenz és dissipatiu

L'objectiu d'aquesta secció és descriure l'evolució del volum d'un subconjunt de $\mathbb{R}^n$ sota el flux. En particular, veiem que el sistema de Lorenz és de naturalesa dissipativa, és a dir, el volum en l'espai de fases es contrau sota el flux. Aquest fet té conseqüències sobre les possibles solucions del sistema de Lorenz, i ens servirà per demostrar més endavant que l'*atractor estrany* té mesura de Lebesgue 0.

A continuació, enunciem un seguit de resultats que ens ajudaran a comprovar que el sistema de Lorenz és dissipatiu.

Lema 2.3. ***(Fórmula de Liouville).*** *Considerem l'equació lineal $\dot{x} = A(t)x$ i sigui $N(t)$ una matriu fonamental de solucions. Aleshores per a tot $t_0 \in I$,*

$$\det(N(t)) = \det\left(N(t_0)\right) exp\left(\int_{t_0}^{t} Tr\left(A(s)\right)\, ds\right), \tag{2.5}$$

on $Tr\,(A(t))$ denota la traça de la matriu $A(t)$.

Demostració. Veure[3].

Lema 2.4. *Sigui $\dot{x} = f(x)$ un sistema dinàmic en $\mathbb{R}^n$ amb el flux corresponent $\phi(t, x)$. Sigui U un subconjunt obert acotat de $\mathbb{R}^n$ i $V = \int_U dx$ el seu volum. Abreviem $U(t) = \phi(t, U)$, respectivament, $V(t) = \int_{U(t)} dx$. Aleshores*

$$\dot{V}(t) = \int_{U(t)} div\,(f(x))\; dx \tag{2.6}$$

Demostració. Per la fórmula del canvi de variables en $\mathbb{R}^n$ tenim que

$$V(t) = \int_{U(t)} dx = \int_U \det\,(D\phi(t, x))\; dx,$$

on $D\phi(t, x)$ denota el Jacobià del flux.

Com que per definició $\Pi(t, x) = D\phi(t, x)$ satisfà la primera equació variacional,

$$\dot{\Pi}(t, x) = D_x f\,(\phi(t, x))\,\Pi(t, x),$$

aplicant la fórmula de Liouville (2.3) i tenint en compte que $Tr(Df(x)) = \mathrm{div}(f(x))$ obtenim

$$\det(D\phi(t, x)) = exp\left(\int_0^t \mathrm{div}(f(\phi(s, x)\,ds\right).$$

Si derivem respecte el temps ens queda

$$\begin{aligned}\frac{d}{dt}\det(D\phi(t, x)) &= \mathrm{div}\,(f(\phi(t, x))\,exp\left(\int_0^t \mathrm{div}\,(f(\phi(s, x))\,ds\right)\\ &= \mathrm{div}\,(f(\phi(t, x))\det\,(D\phi(t, x))\,.\end{aligned}$$

Per tant, quan derivem el volum respecte el temps

$$\dot{V}(t) = \int_U \mathrm{div}(f(\phi(t, x)\det(D\phi(t, x))\,dx,$$

i un segon canvi de variable finalitza la prova aconseguint el resultat desitjat. □

Definició 2.5. *Un camp f és conservatiu $\iff$ $div(f) = 0$.*

Teorema 2.6. *El sistema de Lorenz és dissipatiu, $\forall \sigma,\ b,\ r > 0$.*

Demostració. Sigui V(t) un volum arbitrari acotat, aplicant el lema (2.4) al sistema de Lorenz obtenim

$$\dot{V}(t) = \int_V \mathrm{div}(f(x))\,dx.$$

Per això, hem de calcular la divergència

$$\mathrm{div}(f(x)) = \frac{\partial f}{\partial x} + \frac{\partial f}{\partial y} + \frac{\partial f}{\partial z}.$$

En el sistema (2.2) la divergència és constant i ve donada per

$$\mathrm{div}\,(f(x)) = -(\sigma + 1 + b),$$

aleshores la variació del volum ve descrita per l'equació diferencial

$$\dot{V}(t) = -(\sigma + 1 + b)V.$$

Resolent l'equació diferencial anterior, obtenim

$$V(t) = e^{-(\sigma+1+b)}V(0),$$

on V(0) denota el volum inicial del conjunt de partida. Com que els paràmetres σ i b són positius resulta que $-(\sigma + 1 + b) < 0$ i concloem que qualsevol volum en l'espai de fases es redueix de manera exponencial fins a un conjunt atractor de volum 0. □

Més endavant veurem si aquest atractor és un punt fix, un cicle límit o per alguns valors dels paràmetres, un atractor estrany.

La contracció del volum imposa fortes restriccions sobre les possibles solucions del sistema de Lorenz (2.2).

Lema 2.7. *No hi ha punts d'equilibri totalment repulsors ni òrbites periòdiques repulsores.*

Demostració. Els repulsors són incompatibles amb la contracció del volum perquè són fonts de volum. Suposem que englobem un repulsor amb una superfície tancada de condicions inicials properes a l'espai de fases. En particular, escollim una esfera al voltant d'un punt fix, o un tub al voltant d'una òrbita tancada. Poc temps després, la superfície s'haurà expandit a mesura que s'allunyen les trajectòries corresponents. Així augmentaria el volum dins de la superfície. Això contradiu el fet que tots els volums es contrauen. □

L'origen és globalment estable quan $r < 1$

Notem que en l'apartat (2.7) provarem que l'origen és linealment estable. En aquest apartat provem que l'origen és globalment estable quan $r < 1$. Aquesta propietat requereix la introducció del mètode de Lyapunov que serveix per determinar l'estabilitat de punts fixos. Tot seguit, presentem el concepte d'estabilitat asimptòtica i les idees que hi ha al darrere del mètode de Lyapunov per tal de poder demostrar l'estabilitat de l'origen.

Sigui $x(t)$ una solució de (2.1). Conceptualment, $x(t)$ és *estable* si les solucions que comencen "a prop" de $x(t)$ en un temps donat, es mantenen a prop de $x(t)$ per a tot temps futur. I, és *asimptòticament estable* si les solucions properes convergeixen a $x(t)$ quan $t \to +\infty$. Formalment, suposem que f té un punt d'equilibri x^*, és a dir $f(x^*) = 0$, aleshores definim:

Definició 2.8. *Un punt d'equilibri x^* de* (2.1) *s'anomena* ***estable en el sentit de Lyapunov*** *si per a tot $U_0 \subset U$ entorn de x^*, existeix $U_1 \subset U$ entorn de x^*, tal que per a tot $x_1 \in U_1$*

$I_+(x_1) = [0, +\infty)$, *interval de definició de la solució maximal del PVI* $\dot{x} = f(x)$, $x(0) = x_1$, $\phi(t, x_1) \in U_0$, *per a tot* $t \geq 0$.

Definició 2.9. *Un punt d'equilibri x^* de* (2.1) *s'anomena* ***asimptòticament estable*** *si és estable en el sentit de Lyapunov i per a tot $x_1 \in U_1$, $\phi(t, x_1) \to x^*$ quan $t \to +\infty$.*

Definició 2.10. *Un punt d'equilibri x^* de* (2.1) *s'anomena* ***globalment asimptòticament estable*** *si tota solució del sistema convergeix a ell quan $t \to +\infty$.*

Passem a explicar el mètode de Lyapunov. Aquest mètode, sovint s'utilitza per determinar l'estabilitat dels punts fixos quan són no hiperbòlics, és a dir, quan la part real d'algun valor propi de $Df(x)_{|x=x^*}$ és zero, ja que aleshores no podem utilitzar la teoria general de linealització.

Intuïtivament, el mètode de Lyapunov funciona de la següent manera. Donat un sistema autònom (2.1) amb un punt d'equilibri x^*, volem determinar si és estable o no. Seguint les definicions (2.8) (2.9) d'estabilitat, n'hi ha prou en trobar un entorn tal que totes les òrbites que comencen en aquest entorn s'hi mantinguin per tot temps futur. Aquí no distingim entre estable i asimptòticament estable. Per verificar aquesta condició, hauríem de provar que, o bé el camp vectorial és tangent a la frontera de $U(x^*)$, o bé apunta a l'interior de $U(x^*)$. Per això, cal que la frontera sigui C^1. Aquest fet s'hauria de complir a mesura que reduïm l'entorn $U(x^*)$ en direcció cap a x^*.

El mètode de Lyapunov ens dona una manera de dur a terme aquest raonament de forma precisa, mitjançant l'anomenada funció de Lyapunov. En particular, trobar aquesta funció és equivalent a trobar una *regió de captura*. Un dels inconvenients, però, és que no hi ha una forma sistemàtica per trobar aquesta funció. Sovint és convenient provar expressions que involucrin sumes de quadrats.

Definició 2.11. *Un conjunt obert E amb adherència compacta s'anomena **regió de captura** per al flux $\phi(t,x)$ si $\phi(t,E) \subset E$ per a tot $t \geq 0$.*

Definició 2.12. *Sigui x^* un punt d'equilibri del sistema (2.1) i $U(x^*)$ un entorn obert de x^*. Anomenem **funció de Lyapunov** a la funció contínua*

$$V : U\left(x^*\right) \to \mathbb{R},$$

tal que $V(x) > 0$ per a tot $x \neq x^*$ i $V(x^*) = 0$, és a dir, és una funció definida positiva i satisfà

$$V\left(x\left(t_0\right)\right) \geq V\left(x\left(t_1\right)\right), \quad t_0 < t_1, \quad x\left(t_j\right) \in U\left(x^*\right) \setminus \{x^*\}, \tag{2.7}$$

*per qualsevol solució $x(t)$. S'anomena **funció estricte de Lyapunov** si la igualtat de (2.7) no passa mai.*

Observació 2.13. La majoria de funcions de Lyapunov són diferenciables. En aquest cas, la condició descrita en (2.7) és equivalent a comprovar que

$$\frac{d}{dt}V(x(t)) = \sum_{i=1}^{n} \frac{\partial V}{\partial x_i} f_i(x) = \nabla V \cdot f(x) \leq 0. \tag{2.8}$$

Teorema 2.14. ***(Estabilitat / Estabilitat asimptòtica).*** *Considerem el sistema autònom (2.1). Siguin x^* un punt d'equilibri i $V: U(x^*) \to \mathbb{R}$ una funció de classe C^1 definida en un entorn $U(x^*)$ de x^*. Aleshores,*

1. *Si hi ha una funció de Lyapunov V, aleshores x^* és estable en el sentit de Lyapunov.*
2. *Si a més és estricte, és a dir, $\frac{d}{dt}V(x) < 0$, $\forall x \in U(x^*) \setminus \{x^*\}$, aleshores x^* és asimptòticament estable.*
3. *Si a més, a més, $\lim_{||x|| \to +\infty} V(x) = +\infty$, llavors x^* és globalment asimptòticament estable. Aquesta propietat s'anomena infinitat radial.*

Demostració. Veure [4]. □

Per què necessitem la propietat de la infinitat radial en el teorema 2.14? Aquesta propietat ens assegura que el conjunt de nivell $\Omega_c = \{x \in \mathbb{R}^n |\ V(x) \leq c\}$ és acotat per a tot $c > 0$. Sense aquesta propietat el conjunt Ω_c podria no ser acotat per alguns valors de c. El següent exemple mostra aquesta necessitat.

Exemple 2.15. Considerem la funció

$$V(x, y) = \frac{x^2}{1 + x^2} + y^2.$$

Fixem $y = 0$, i fem tendir $x \to +\infty$. Per provar la propietat d'infinitat radial hauríem de tenir $V(x, y) \to +\infty$ per qualsevol combinació x, y tal que $\|(x, y)\| \to +\infty$. Aquest fet val per qualsevol norma, però considerem la norma Euclídia $\|\cdot\|_2$ per simplicitat. Com que $x \to +\infty$ i $y = 0$, tenim $\|(x, y)\|_2 = \sqrt{x^2 + y^2} = \sqrt{+\infty^2 + 0^2} \to +\infty$. En canvi, per $V(x, y)$ obtenim

$$\lim_{x\to+\infty} V(x, 0) = 1 \neq 0.$$

Per tant $V(x, y)$ no té la propietat d'infinitat radial. Per $c \geq 1$ el conjunt $\Omega_c = \{(x, y) \in \mathbb{R}^2 |\ V(x, y) \leq c\}$ no és acotat.

Un cop introduïts tots els conceptes previs necessaris, ja podem demostrar l'objectiu d'aquesta secció.

Teorema 2.16. *Per $r < 1$, l'origen del sistema de Lorenz és globalment estable.*

Demostració. Considerem la funció $V\colon \mathbb{R}^3 \to \mathbb{R}$ definida com

$$V(x, y, z) = \frac{1}{\sigma}x^2 + y^2 + z^2.$$

Les superfícies de nivell $V_c = \{x \in \mathbb{R}^3 |\ V(x) = c\}$ són el·lipsoides centrats a l'origen. Intuïtivament, volem provar que quan $r < 1$ i $(x, y, z) \neq (0, 0, 0)$, aleshores $\dot{V} < 0$ al llarg de les trajectòries. Això, implica que les trajectòries continuen movent-se cada cop a el·lipsoides més i més petits quan $t \to +\infty$. La propietat clau, per provar l'estabilitat global, és comprovar la propietat d'infinitat radial, ja que ens assegura que les superfícies de nivell són compactes per a qualsevol $c > 0$.
Passem a comprovar les hipòtesis del teorema 2.14.

1. L'origen és un punt fix. Efectivament $V(0, 0, 0) = (0, 0, 0)$.

2. La funció V és definida positiva en $\mathbb{R}^3\backslash\{0\}$. Si $(x, y, z) \neq (0, 0, 0)$, aleshores $V(x, y, z) > 0$, ja que és suma de termes estrictament positius.

3. $\dot{V}$ és definida negativa en $\mathbb{R}^3\backslash\{0\}$. Per tant, hem de demostrar que és estrictament decreixent al llarg de les solucions del sistema de Lorenz.

$$\begin{aligned}\frac{1}{2}\dot{V} &= \frac{1}{\sigma}x\dot{x} + y\dot{y} + z\dot{z} = x(y - x) + y(-xz + rx - y) + z(xy - bz)\\ &= (yx - x^2) + (ryx - y^2 - xyz) + (zxy - bz^2) = (r + 1)xy - x^2 - y^2 - bz^2.\end{aligned}$$

   Completem quadrats dels dos primers termes i obtenim la següent expressió

$$\frac{1}{2}\dot{V} = -\left[x - \left(\frac{1 + r}{2}\right)y\right]^2 - \left[1 - \left(\frac{1 + r}{2}\right)\right]y^2 - bz^2. \tag{2.9}$$

   Vegem que $\dot{V} < 0$ quan $r < 1$ i $(x, y, z) \neq (0, 0, 0)$. En efecte, no és positiu perquè és resta de quadrats. Per tant, hem reduït el problema a comprovar que $1 - \left(\frac{1+r}{2}\right) > 0$ i això és cert

si i només si $r < 1$.
Queda provar que no es pot donar el cas $\dot{V} = 0$. Aquest fet, implicaria que els termes de la dreta de la igualtat (2.9) fossin iguals a 0, és a dir, $y = 0$ i $z = 0$. El primer terme, es redueix a $-x^2$ que és zero només si $x = 0$.
En conclusió, $\dot{V}$ és definida negativa en $\mathbb{R}^3 \backslash \{0\}$.

4. Per definició de V, tenim que
$$\lim_{||x|| \to +\infty} V(x) = +\infty.$$

Concloem pel teorema 2.14 que l'origen és globalment asimptòticament estable quan $r < 1$ i, per tant, tota solució del sistema de Lorenz convergeix a ell quan $t \to +\infty$. □

La Figura 2 mostra com l'origen és un atractor global quan $r < 1$. En particular, considerem els valors clàssics $\sigma = 10,\ b = \frac{8}{3}$.

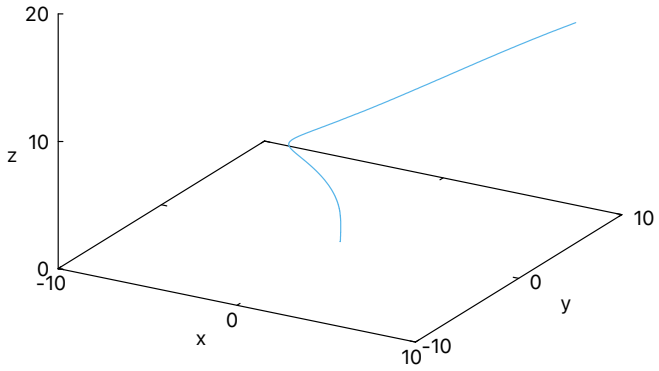

Figura 2: Origen globalment estable. Solució del P.V.I per $r = 0.7$ i condicions inicials $x_0 = (8,\ 9,\ 15)$.

Construcció de l'atractor global

Per valors de r superiors a 1, la propietat anterior no és certa. De fet, com veurem més endavant, per $r > 1$, l'origen esdevé linealment inestable. Tot i això, per qualsevol valor dels paràmetres, podem demostrar l'existència d'una regió positivament invariant on totes les trajectòries entren i no en surten mai. Prèviament, enunciem els resultats i definicions que ens permetran definir el concepte de *conjunt d'atracció* i *atractor*.

Definició 2.17. *Un conjunt invariant tancat $\Lambda \subset \mathbb{R}^n$ s'anomena* ***conjunt d'atracció*** *pel flux $\phi(t, x)$ si existeix un entorn $\Lambda \subset U \subset \mathbb{R}^n$ tal que*

$$\forall x \in U,\ \forall t \geq 0,\ \phi(t, x) \to \Lambda,\ \textit{quan } t \to +\infty.$$

A la pràctica, una manera de trobar els conjunts d'atracció és trobant primer una regió de captura 2.11, ja que aleshores tindrem

$$\Lambda = \bigcap_{t \geq 0} \phi(t, E).$$

Desafortunadament, la definició de conjunt d'atracció de vegades no és suficientment bona. Per això, és convenient introduir la següent definició.

Definició 2.18. *Un conjunt invariant tancat Λ s'anomena* ***topològicament transitiu*** *si per qualssevol subconjunts oberts $W, V \subseteq \Lambda$, existeix $t \in \mathbb{R}$ tal que $\phi(t, V) \cap W \neq \emptyset$. És a dir, si donats dos punts $y_1,\ y_2 \in \Lambda$ i entorns qualssevol $U_1,\ U_2$ de $y_1,\ y_2$ respectivament, existeix una corba solució que comença en U_1 i més endavant passa per U_2.*

Per motivar la definició d'atractor en lloc de conjunt d'atracció, considerem el següent exemple:

Exemple 2.19. Considerem el camp vectorial autònom en el pla xy de $\mathbb{R}^2$

$$\begin{cases} \dot{x} = x - x^3, \\ \dot{y} = -y. \end{cases} \tag{2.10}$$

El camp vectorial (2.10) té un punt de sella $(0, 0)$ i dos nodes atractors $(\pm 1, 0)$, veure Figura 3. L'eix y és la varietat estable de l'origen. Triem una el·lipse, E, que conté els tres punts d'equilibri. Observem que E delimita una regió de captura i l'interval tancat a $\mathbb{R}^2$ $\{(x, y) : x \in [-1, 1], y = 0\} = \bigcap_{t \geq 0} \phi(t, E)$ és el conjunt d'atracció.

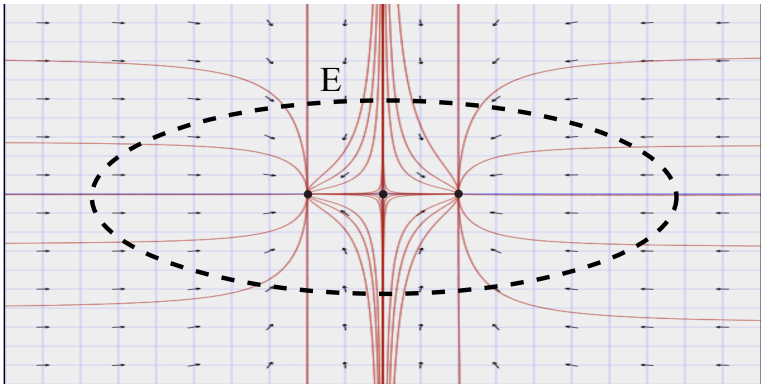

Figura 3: L'interval de l'eix x entre els dos nodes no és un atractor per a aquest sistema, malgrat que totes les solucions entrin en U.

L'exemple 2.19 ressalta una possible deficiència de la definició 2.17. En l'exemple 2.19, quasi tots els punts del pla acabaran a prop d'un dels dos punts $(\pm 1,\ 0)$. El conjunt d'atracció conté dos atractors $(\pm 1,\ 0)$. Per tant, si estem interessats a descriure on van a parar finalment els punts de l'espai de fases la idea del conjunt d'atracció no és del tot precisa.

Observem que en l'exemple 2.19 aquesta definició 2.18 no es verifica perquè cap solució passa per ambdós punts $(\pm 1,\ 0)$. Per tant, no podem considerar $[-1,\ 1]$ com atractor.

És important ressaltar que no hi ha una definició universal de què és o no un atractor.

Definició 2.20. *Un conjunt Λ s'anomena* ***atractor*** *per ϕ si és un conjunt d'atracció topològicament transitiu.*

Passem ara a trobar l'atractor global del sistema de Lorenz. Per trobar la regió de captura, farem ús altre cop de les funcions de Lyapunov.

Teorema 2.21. *Existeix una regió acotada E tal que qualsevol solució que comenci fora de E, finalment hi entra i hi queda atrapada per a tot instant futur.*

Demostració. En aquesta ocasió, considerarem la funció

$$V(x, y, z) = \frac{1}{2}\left(x^2 + y^2 + (z - \sigma - r)^2\right). \tag{2.11}$$

Notem que existeixen altres funcions de Lyapunov que també van bé per provar el resultat, com per exemple la funció

$$V(x, y, z) = rx^2 + \sigma y^2 + \sigma\,(z - 2r)^2\,,$$

però escollim (2.11) perquè ens facilita els càlculs.

$$\dot{V}(x, y, z) = \frac{d}{dt}V(x, y, z) = x\dot{x} + y\dot{y} + (z - \sigma - r)\,\dot{z} = -\sigma x^2 - y^2 - bz^2 + bz(\sigma + r).$$

Clarament, el conjunt de punts que satisfà $\dot{V} \geq 0$ és acotat i la seva frontera és un el·lipsoide. Denotem per D la regió acotada on $\dot{V}$ és no-negativa, és a dir, $D = \{(x, y, z) \in \mathbb{R}^3 |\ \dot{V} \geq 0\}$. Com que D és compacta, V té un màxim en D. Sigui $M = \max_{(x,y,z)\in D} V(x, y, z)$, podem considerar la regió $E = \{(x, y, z) \in \mathbb{R}^3 |\ V(x, y, z) < M + 1\}$. Observem que $D \subset E$, llavors per qualsevol punt $x \in \mathbb{R}^3 \backslash E$ tenim que $x \in \mathbb{R}^3 \backslash D$. Per tant, per aquests punts $\dot{V} \leq -\delta < 0$, és a dir, el valor de V és estrictament decreixent al llarg de les trajectòries i en conseqüència, ha d'entrar a E després d'un temps finit.

En conclusió, hem trobat una regió de captura E. Si denotem per $\phi(t, \cdot)$ el flux generat pel camp de vectors del sistema de Lorenz, es verifica $\phi(t, E) \subset E$ per a tot temps $t \geq 0$ i podem escriure $\Lambda = \bigcap_{t\geq 0} \phi(t, E)$. Això prova que Λ és un conjunt d'atracció. □

Teòricament, Λ podria ser un conjunt molt gran, potser delimitant una regió oberta de $\mathbb{R}^3$. Tanmateix, pel sistema de Lorenz aquest no és el cas. Com hem vist anteriorment (2.6), el sistema de Lorenz és dissipatiu i per tant Λ té volum 0.

En resum, hem provat que Λ és un conjunt d'atracció global, acotat, de volum 0 i no buit, ja que conté la singularitat (0,0,0). Per provar que Λ és atractor, caldria comprovar que és topològicament transitiu, propietat que s'escapa de l'àmbit d'aquest treball. Efectivament, Λ és un atractor, encara més, és un *atractor estrany*.

A continuació, donem un breu apunt històric sobre la demostració de l'atractor de Lorenz. Lorenz [1] trobà evidències que mostraven que el seu model estava regit per dinàmiques caòtiques, però mancava una demostració rigorosa d'aquest resultat. El següent pas més remarcable fou la creació dels anomenats Models Geomètrics de les equacions de Lorenz. J. Guckenheimer i R. F. Williams [5] provaren l'existència d'un atractor estrany sota certes hipòtesis, però encara hi mancava una demostració general. L'any 1998, Stephen Smale [6] publicà una llista sobre els problemes matemàtics que creia que serien d'interès pel segle XXI, la qual tenia com a catorzena pregunta la demostració de l'existència de l'atractor de Lorenz. Aquest fet fou provat per Warwick Tucker [7], l'any 2002, en una demostració assistida per ordinador.

2.7 Estructura de l'espai de fases. Punts d'equilibri i estabilitat

L'objectiu d'aquest apartat és l'obtenció dels punts d'equilibri del sistema de Lorenz i determinar la seva estabilitat. Per fer-ho, presentem un seguit de definicions i resultats teòrics que són importants per estudiar quins són els punts d'equilibri i estudiar la seva estabilitat.

Punts d'equilibri

Considerem el sistema de Lorenz (2.2), on els paràmetres $\sigma, b, r > 0$, com hem vist en la secció anterior 2.6, els punts d'equilibri venen determinats pels zeros del camp vectorial. Per tant, el càlcul dels punts d'equilibri es redueix a resoldre el sistema $f(w(t)) = 0$.

Sabem que l'origen és un punt d'equilibri 2.6. Per tant, suposem que $(x, y, z) \neq (0, 0, 0)$. Resolem el sistema de Lorenz (2.2) per substitució

$$x = y,\ rx - y - xz = 0,\ -bz + xy = 0. \tag{2.12}$$

Resolent el sistema (2.12) obtenim que els punts fixos venen donats per

$$\begin{aligned} P_1 &= (0,0,0)\,, \\ P_2 &= \left(\sqrt{b(r-1)}, \sqrt{b(r-1)}, r-1\right), \\ P_3 &= \left(-\sqrt{b(r-1)}, -\sqrt{b(r-1)}, r-1\right). \end{aligned} \tag{2.13}$$

Observem que depenent del paràmetre r tenim un o tres punts d'equilibri.

Estabilitat

Per tal d'analitzar l'estabilitat de cada punt d'equilibri, farem ús de la teoria de linealització de sistemes no lineals.

Definició 2.22. *Sigui f un camp vectorial C^1 definit en un obert U de $\mathbb{R}^n$ i sigui $p \in U$ amb $f(p) = 0$ un punt crític. Diem que p és* ***hiperbòlic*** *si $Re\lambda \neq 0$ per tot λ valor propi de $Df(p)$.*

Sigui x^* un punt d'equilibri del sistema autònom (2.1). Per tal de determinar l'estabilitat de x^* hem de comprendre la naturalesa de les solucions a prop de x^*. Per això calculem la linealització del sistema autònom (2.1).

Sigui

$$x(t) = x^* + y(t). \tag{2.14}$$

Substituint (2.14) a (2.1) i calculant la sèrie de Taylor de $f(x(t))$ al voltant de x^* obtenim

$$\dot{x} = \dot{x}^* + \dot{y} = f\left(x^*\right) + Df\left(x^*\right) y + \mathcal{O}\left(|y|^2\right), \tag{2.15}$$

on Df és la matriu jacobiana de f i $|\cdot|$ denota la norma a $\mathbb{R}^n$. Com que x^* és un punt d'equilibri $f(x^*) = 0$ i estem interessats en el comportament de les solucions a prop de x^*, sembla raonable estudiar el sistema lineal associat.

Per tant, l'expressió (2.15) resulta

$$\dot{y} = Df\left(x^*\right) y. \tag{2.16}$$

La solució del sistema (2.16) és $y(t) = x(t) - x^*$, per això, en la nova variable y, l'origen i les seves propietats d'estabilitat, són les mateixes que en el punt d'equilibri x^*.

El següent teorema, posa de manifest la relació entre el retrat de fase a l'entorn d'un punt crític hiperbòlic i la seva part lineal.

Teorema 2.23. ***(Hartman-Grobman).*** *Sigui f un camp vectorial C^1 definit en un obert $U \subset \mathbb{R}^n$ i sigui $p \in U$ amb $f(p) = 0$ un punt crític hiperbòlic. Sigui g el camp lineal definit per $g(x) = Df(p)x$. Aleshores, existeixen entorns V de p i W de 0 tals que $f_{|V}$ i $g_{|W}$ són topològicament conjugats.*

Demostració. Veure [8].

El teorema de Hartman-Grobman dona un resultat molt important en la teoria qualitativa local d'un sistema dinàmic. Aquest teorema mostra que prop d'un punt d'equilibri de tipus hiperbòlic, el sistema no lineal té el mateix comportament qualitatiu (localment) que el sistema linealitzat corresponent.

Considerem el sistema lineal $\dot{x} = Ax$ on A és una matriu real d'ordre $n \times n$. Els subespais generats pels vectors propis dels valors propis corresponents de la matriu A es poden classificar en tres subespais diferents: *estables, inestables* i *centrals*.

Siguin $\lambda_j = \alpha_j \pm i\beta_j$ els valors propis i $w_j = u_j \pm iv_j$, $j = 1, \ldots, k$, els vectors propis de valor propi λ_j de la matriu A. Depenent del signe de α_j els tres subespais es defineixen de la següent manera:

Definició 2.24. ***Subespai estable E^s.*** *El subespai estable E^s és el generat pels vectors propis de valor propi λ_j pels quals $\alpha_j < 0$. Això és, $E^s = span\{u_j, v_j |\ \alpha_j < 0\}$.*

Subespai inestable E^u. *El subespai inestable E^u és el generat pels vectors propis de valor propi λ_j pels quals $\alpha_j > 0$. Això és, $E^s = span\{u_j, v_j |\ \alpha_j > 0\}$.*

Subespai central E^c. *El subespai central E^c és el generat pels vectors propis de valor propi λ_j pels quals $\alpha_j = 0$. Això és, $E^s = span\{u_j, v_j |\ \alpha_j = 0\}$.*

Sigui U un entorn d'un punt d'equilibri hiperbòlic x^*. Definim el següent:

Definició 2.25. ***Varietat local estable:*** $W^s_{loc}(x^*) = \{x \in U |\ \phi_t(x) \to x^* \text{ quan } t \to +\infty,\ \phi_t(x) \in U\ \forall t \geq 0\}$.

Varietat local inestable: $W^u_{loc}(x^*) = \{x \in U |\ \phi_t(x) \to x^* \text{ quan } t \to -\infty,\ \phi_t(x) \in U\ \forall t \leq 0\}$.

Teorema 2.26. ***Teorema de la varietat estable.*** *Sigui $f : U \subset \mathbb{R}^n \to \mathbb{R}^n$ una funció diferenciable amb un punt d'equilibri hiperbòlic p. Aleshores,*

- *W^s_{loc} és una varietat diferenciable i el seu espai tangent té la mateixa dimensió que l'espai estable E^s de la linealització de f en el punt p.*
- *W^u_{loc} és una varietat diferenciable i el seu espai tangent té la mateixa dimensió que l'espai inestable E^u de la linealització de f en el punt p.*

Demostració. Veure [9].

Teorema 2.27. ***Teorema de la varietat central.*** *Considerem un sistema no lineal $\dot{x} = f(x)$ on $f \in C^r(U)$, $r \geq 1$, $U \subset \mathbb{R}^n$ és un obert que conté un punt d'equilibri no hiperbòlic, $x^* = 0$ del sistema. Suposem que la matriu jacobiana del sistema $J = Df(0)$, té j valors propis amb part real positiva, k valors propis amb part real negativa i $(m = n - j - k)$ valors propis amb part*

real 0. *Aleshores existeix una varietat estable* $W^s(0)$ *j-dimensional de classe* C^r*, una varietat inestable* $W^u(0)$ *k-dimensional de classe* C^r *i una varietat central* $W^c(0)$ *m-dimensional tangent als subespais* E^s, E^u, E^c *corresponents al sistema lineal* $\dot{x} = Ax$ *a l'origen.*

A més, aquestes varietats són invariants sota el flux ϕ_t *del sistema no lineal. Les varietats* $W^s(0)$ *i* $W^u(0)$ *són úniques, però* $W^c(0)$ *no.*

Demostració. Veure [9].

Donem una classificació de l'estabilitat segons el sentit de Lyapunov dels punts hiperbòlics d'un camp vectorial 3-dimensional. Sigui x^* un punt d'equilibri hiperbòlic d'un camp vectorial 3-dimensional. Aleshores,

- **Node** quan tots els valors propis són reals i tenen el mateix signe. El node és estable (inestable) quan els valors propis són negatius (positius).
- **Sella** quan tots els valors propis són reals i almenys un d'ells és positiu i almenys un és negatiu. Els punts de sella sempre són inestables.
- **Node-focus** quan té un valor propi real i un parell de valors propis conjugats complexos, i tots els valors propis tenen parts reals del mateix signe. L'equilibri és estable (inestable) quan el signe és negatiu (positiu).
- **Sella-focus** quan té un valor propi real amb el signe oposat al signe de la part real d'un parell de valors propis conjugats complexos. Aquest tipus d'equilibri sempre és inestable.

A continuació, classificarem l'estabilitat dels punts hiperbòlics del sistema de Lorenz a partir dels valors propis obtinguts de la matriu jacobiana del sistema (2.16).

Sabem per (2.4) que la matriu Jacobiana ve definida per

$$Df(x,y,z) = \begin{pmatrix} -\sigma & \sigma & 0 \\ r-z & -1 & -x \\ y & x & -b \end{pmatrix}.$$

Tot seguit, estudiarem el caràcter dels punts d'equilibri per a diferents valors del paràmetre r.

1. **Cas $r < 1$.** L'únic punt d'equilibri és l'origen. En el capítol anterior hem provat que l'origen és globalment asimptòticament estable, Teorema 2.16. Com que l'origen és un node atractiu, pel teorema 2.26 té una variable estable $W^s(0,0,0)$ de tres dimensions.
2. **Cas $r = 1$.** De manera similar l'únic punt d'equilibri és l'origen. En aquest punt té lloc una bifurcació de Pitchfork que demostrarem en la secció 2.9. Notem que l'origen és parabòlic, és a dir, té un valor propi real igual a zero.
3. **Cas $r > 1$.** En aquest cas tenim els tres punts d'equilibri definits en (2.13). Fent ús del Teorema 2.23, elaborem una anàlisi detallada de cada un d'ells.

    - $P_1 = (0,0,0)$. Considerem el sistema linealitzat a l'origen, és a dir,

$$Df(0,0,0) = \begin{pmatrix} -\sigma & \sigma & 0 \\ r & -1 & 0 \\ 0 & 0 & -b \end{pmatrix}.$$

A continuació, calculem el seu polinomi característic

$$p_{Df(0,0,0)}(\lambda) = \det\left(\lambda I - Df(0,0,0)\right) = -(b+\lambda)\left[-\sigma - \sigma\lambda - \lambda - \lambda^2 + \sigma r\right].$$

Obtenim tres arrels i, per tant, els tres valors propis següents

$$\lambda_1 = -b,\ \lambda_{2,3} = \frac{1}{2}\Big[-\sigma - 1 \pm \sqrt{(1-\sigma)^2 + 4\sigma r}\Big].$$

Clarament, λ_1 i λ_3 són negatius, però λ_2 és positiu.

$$\begin{aligned}
&\frac{1}{2}\Big[-\sigma - 1 \pm \sqrt{(1-\sigma)^2 + 4\sigma r}\Big] > 0 \iff \sqrt{(1-\sigma)^2 + 4\sigma r} > 1 + \sigma \\
&\iff (1-\sigma)^2 + 4\sigma r > (1+\sigma)^2 \iff 1 + \sigma^2 - 2\sigma + 4\sigma r > 1 + \sigma^2 + 2\sigma \\
&\iff 4\sigma r > 4\sigma \iff r > 1.
\end{aligned}$$

Per tant, l'origen és un punt de sella. Observem a més, que pel teorema de la varietat estable 2.26 l'origen té una varietat inestable $W^u(0,0,0)$ unidimensional i una varietat estable $W^s(0,0,0)$ bidimensional.

- $P_{2,3} = \left(\pm\sqrt{b(r-1)},\ \pm\sqrt{b(r-1)},\ r-1\right)$.
  La raó per la qual tractem els punts P_2 i P_3 de forma simultània és perquè, com veurem més endavant els polinomis característics són iguals. Aquest fet és degut a la simetria que presenta el sistema de Lorenz.
  Considerem els sistemes linealitzats

$$\begin{aligned}
\dot{\zeta} &= Df\left(P_2\right)\zeta, \\
\dot{\xi} &= Df\left(P_3\right)\xi.
\end{aligned}$$

Calculem les matrius jacobianes corresponents

$$Df(P_2) = \begin{pmatrix} -\sigma & \sigma & 0 \\ 1 & -1 & -\sqrt{b(r-1)} \\ \sqrt{b(r-1)} & \sqrt{b(r-1)} & -b \end{pmatrix},$$

$$Df(P_3) = \begin{pmatrix} -\sigma & \sigma & 0 \\ 1 & -1 & \sqrt{b(r-1)} \\ -\sqrt{b(r-1)} & -\sqrt{b(r-1)} & -b \end{pmatrix}.$$

Al ser matrius $3x3$ es veu clarament que a l'hora de calcular els seus polinomis característics, aquests són iguals. Els valors propis de $Df\left(P_{2,3}\right)$ són les arrels del polinomi característic

$$p(\lambda) = \det\left(\lambda I - Df\left(P_{2,3}\right)\right) = \lambda^3 + \lambda^2(\sigma + 1 + b) + \lambda b(\sigma + 1) + 2\sigma b(r-1) = 0. \tag{2.17}$$

El polinomi anterior (2.17) és cúbic amb coeficients reals. Pel Teorema Fonamental de l'àlgebra, sabem que té tres arrels. En particular, com que té coeficients reals, sabem que les tres arrels són reals o té una arrel real i dos de complexes conjugades.

Lema 2.28. *Les arrels reals del polinomi* (2.17) *són negatives.*

Demostració. Primer de tot observem que el polinomi (2.17) és mònic. Aleshores es verifica el següent

$$\lim_{\lambda\to+\infty} p(\lambda) = +\infty, \lim_{\lambda\to-\infty} p(\lambda) = -\infty.$$

D'altra banda, tenim que

$$p'(\lambda) = 3\lambda^2 + 2\lambda(\sigma + b + 1) + b(\sigma + r) > 0, \text{ per a tot } \lambda \geq 0. \tag{2.18}$$

Observem que λ no pot ser positiu, ja que $p(0) > 0$ i el polinomi és estricament creixent (2.18) per a tot $\lambda \geq 0$. Concloem que les arrels reals, quan en tingui, han de ser negatives. □

Com que almenys una arrel és real i sabem que ha de ser negativa pel Lema 2.28, la denotem per λ_1. Les altres dues arrels $\lambda_{2,3}$ sabem que poden ser les dues reals o complexes conjugades $\lambda_{2,3} = \alpha \pm i\beta$. La condició per a que totes les arrels del polinomi (2.17) siguin reals és complicada i poc rellevant. Numèricament es pot comprovar que per $r > r_c$ ($r_c \approx 1.3456$), les arrels tenen part imaginària diferent de zero. Resumint:

- Si $1 < r < r_c$ totes les arrels són reals i els punts $P_{2,3}$ són nodes atractors, perquè com hem vist en el Lema 2.28 els valors propis reals són negatius.
- Si $r > r_c$, tenim un valor propi real, que és negatiu, i dos de complexes conjugats. Per tal d'estudiar l'estabilitat dels punts $P_{2,3}$ hem d'estudiar els signes de $Re(\lambda_{2,3})$.
  - Si $\alpha < 0$, els tres valors propis tenen part real negativa i per tant $P_{2,3}$ són focus atractors.
  - Si $\alpha > 0$, tenim un valor propi negatiu i dos valors propis amb part real positiva, per tant $P_{2,3}$ és un punt de sella-focus. De nou, pel teorema de varietat estable 2.26 $P_{2,3}$ tenen una varietat estable unidimensional i una varietat inestable bidimensional.
  - Si $\alpha = 0$, $\lambda_{2,3}$ són imaginaris purs. En aquest punt tenim el límit d'estabilitat. Anem a estudiar per a quin valor de r tenim $\alpha = 0$.

$$\begin{aligned} p(i\beta) &= (i\beta)^3 + (i\beta)^2(\sigma + 1 + b) + (i\beta)\, b\,(\sigma + 1) + 2\sigma b(r - 1) \\ &= 2b\sigma(r - 1) - (b + \sigma + 1)\beta^2 + i\beta\left(b(\sigma + r) - \beta^2\right) = 0. \end{aligned}$$

Resolent les dues equacions,

$$\begin{aligned} &2b\sigma(r - 1) - (b + \sigma + 1)\beta^2 = 0, \\ &\beta\left(b(\sigma + r) - \beta^2\right) = 0. \end{aligned} \quad \Longrightarrow \; r_H = \frac{\sigma(\sigma + b + 3)}{\sigma - b - 1}.$$

Pels valors típics $\sigma = 10$ i $b = \frac{8}{3}$, $r_H \approx 24.7468$. Aleshores, resumint hem obtingut el següent:

- Pels valors de r tals que $1 < r < r_H$ els punts d'equilibri $P_{2,3}$ són estables. Els tres valors propis de $Df\left(P_{2,3}\right)$ tenen part real negativa.
- Per $r = r_H$ els valors propis creuen l'eix imaginari i donen lloc a una bifurcació subcrítica de Hopf, en la qual els punts $P_{2,3}$ perden la seva estabilitat. Aquesta bifurcació apareix a causa de l'absorció del parell d'òrbites periòdiques que sorgeixen de l'òrbita homoclínica que té lloc pel valor de $r \approx 13.9265$. Estudiarem en més detall aquests casos a les seccions 2.10 i 2.11.

· Pels valors de r tals que $r > r_H$, els punts d'equilibri $P_{2,3}$ són inestables, en particular són punts sella-focus, ja que $Df\left(P_{2,3}\right)$ té un valor propi real negatiu i dos de complexes conjugats amb part real positiva.

En les pròximes seccions estudiarem els diferents tipus de bifurcacions que tenen lloc pels diversos valors del paràmetre r considerant el cas clàssic, en el qual, $\sigma = 10$ i $b = \frac{8}{3}$.

2.8 Bifurcacions

En aquest apartat presentem una introducció breu a les bifurcacions de camps vectorials. Sovint, els sistemes d'interès físic solen tenir paràmetres que apareixen en el sistema d'equacions diferencials. A mesura que aquests paràmetres varien, es produeixen canvis en l'estructura qualitativa o topològica de les solucions per a determinats valors dels paràmetres. Aquests canvis s'anomenen *bifurcacions* i els valors dels paràmetres s'anomenen *valors de bifurcació*. Podem dividir les bifurcacions en dos grans grups: *locals* i *globals*.

Bifurcacions locals. Atès que l'anàlisi d'aquestes bifurcacions es realitza generalment estudiant el camp vectorial a prop del punt d'equilibri o òrbita tancada, i les solucions també es troben en un entorn d'aquest conjunt límit, aquestes bifurcacions s'anomenen locals. Considerem un sistema dinàmic continu descrit per l'equació diferencial ordinària

$$\dot{x} = f(x, \lambda), \text{ on } f : \mathbb{R}^n \times \mathbb{R} \to \mathbb{R}^n \text{ és un camp vectorial de classe } C^1.$$

Una bifurcació local es produeix al punt (x^*, λ^*) quan el jacobià de la matriu Df_{x^*,λ^*} té un valor propi amb part real igual a 0. Si el valor propi és 0 s'anomena *bifurcació estacionària*, però si el valor propi no és 0, sinó que és imaginari pur s'anomena *bifurcació de Hopf*.

A continuació, presentem les bifurcacions que apareixen en el sistema de Lorenz:

1. **Pitchfork.** És una bifurcació local on el sistema passa d'un punt estacionari a tres punts estacionaris. Una bifurcació Pitchfork s'anomena supercrítica si el nou punt estacionari existeix per a valors superiors al valor de la bifurcació. En cas contrari, la bifurcació Pitchfork s'anomena subcrítica. Presentem un model senzill per il·lustrar una bifurcació supercrítica de Pitchfork.

   Considerem $\dot{x} = \mu x - x^3$. Per $\mu < 0$, tenim un únic punt d'equilibri a $x = 0$. Per $\mu > 0$, l'origen és un punt d'equilibri inestable i tenim dos punts d'equilibri estables $x = \pm\sqrt{\mu}$. En el sistema de Lorenz tenim una situació anàloga quan tenim $r = 1$.

2. **Hopf.** És una bifurcació local en la qual un punt d'equilibri de tipus focus canvia l'estabilitat i es pot crear o destruir una òrbita periòdica. Una bifurcació de Hopf es produeix quan un parell de valors propis conjugats complexos creuen l'eix imaginari del pla complex. Una bifurcació de Hopf s'anomena *supercrítica* si un cicle límit estable envolta un punt d'equilibri de focus inestable. En cas contrari, si un cicle límit inestable envolta un punt d'enfocament estable, la bifurcació de Hopf s'anomena a *subcrítica*. Destaquem el cas subcrític, ja que per al sistema de Lorenz, es produeix una bifurcació de Hopf subcrítica per al paràmetre $r_H \approx 24.7468$.

   Considerem el sistema $\dot{r} = r\left(r^2 + \mu\right),\ \dot{\theta} = 1$. Per $\mu < 0$, l'origen és un focus estable i té un cicle límit inestable. Aquest cicle xoca amb l'origen quan $\mu = 0$ i desapareix quan $\mu > 0$ quan l'origen esdevé un focus inestable. Aquesta situació és anàloga al cas del sistema de Lorenz.

Bifurcacions globals. Les bifurcacions globals són aquelles que no són locals, és a dir, les propietats dinàmiques no es poden deduir a partir de la informació local. De fet, les bifurcacions globals impliquen aspectes globals dels fluxos. No hi ha una manera sistemàtica d'estudiar les bifurcacions globals. Algunes d'elles estan associades a canvis globals en la topologia de l'espai de fases, provocats per bifurcacions *homoclíniques* o *heteroclíniques* entre objectes invariants.

Com veurem en l'apartat 2.10 en el sistema de Lorenz tenim una bifurcació global que és clau per a la formació de l'atractor de Lorenz. Aquesta és una bifurcació homoclínica. En tal bifurcació neix un cicle límit fruit d'una connexió homoclínica.

2.9 Anàlisi bifurcació de Pitchfork

Quan $r = 1$, considerant les equacions de Lorenz tenim el punt d'equilibri $(0, 0, 0)$. $Df\,((0, 0, 0))$ té valors propis $\lambda_1 = -b,\ \lambda_2 = 0,\ \lambda_3 = -(\sigma + 1)$, és a dir, un dels valors propis és 0. Considerant aquests valors propis, obtenim els vectors propis $v_1 = (0, 0, 1),\ v_2 = (1, 1, 0)$ *i* $v_3 = (\sigma, -1, 0)$ respectivament. Com que tenim un valor propi 0, $\lambda_2 = 0$, el sistema de Lorenz té una varietat central, veure [10]. Per estudiar la dinàmica en la direcció $v_2 = (1, 1, 0)$, prop de $r = 1$, considerem

$$\begin{cases} \dot{x} = \sigma(y - x), \\ \dot{y} = rx - y - xz, \\ \dot{z} = -bz + xy, \\ \dot{r} = 0, \end{cases} \tag{2.19}$$

que té una varietat central W^c 2-dimensional. Per tal d'estudiar la dinàmica al voltant de l'origen introduïm un nou paràmetre $\eta = r - 1 \approx 0$. Com que $\dot{\eta} = \dot{r} = 0$, el sistema (2.19) esdevé

$$\begin{cases} \dot{x} = \sigma(y - x), \\ \dot{y} = (\eta + 1)x - y - xz, \\ \dot{z} = -bz + xy, \\ \dot{\eta} = 0. \end{cases} \tag{2.20}$$

Pel Teorema de la varietat central, podem representar localment W^c en forma de graf

$$\begin{cases} y = g_1(x, \eta) = a_{10}x + a_{01}\eta + a_{20}x^2 + a_{11}\eta + a_{02}\eta^2 + \mathcal{O}(3), \\ z = g_2(x, \eta) = b_{10}x + b_{01}\eta + b_{20}x^2 + b_{11}\eta + b_{02}\eta^2 + \mathcal{O}(3). \end{cases} \tag{2.21}$$

Fent que aquest graf (2.21) sigui invariant, obtenim les equacions

$$\begin{cases} \dot{y} = \eta x + x - g_1(x, \eta) - xg_2(x, \eta) = \sigma\left(g_1(x, \eta) - x\right)\dfrac{\partial g_1}{\partial x}(x, \eta), \\ \dot{z} = -bg_2(x, \eta) + xg_1(x, \eta) = \sigma\left(g_1(x, \eta) - x\right)\dfrac{\partial g_2}{\partial x}(x, \eta). \end{cases} \tag{2.22}$$

Igualant termes en (2.22) trobem els coeficients $a_{ij},\ b_{ij}$ i obtenim

$$\begin{cases} y = x + \dfrac{1}{\sigma+1}x\eta - \dfrac{1}{b(\sigma+1)}x^3 - \dfrac{\sigma}{(\sigma+1)^3}x\eta^2 + \mathcal{O}(4), \\ z = \dfrac{1}{b}x^2 + \dfrac{2\sigma}{(\sigma+1)b}x^2\eta + \mathcal{O}(4). \end{cases} \tag{2.23}$$

Per tant, la dinàmica sobre W^c és

$$\begin{cases} \dot{x} = \sigma(y-x) = \sigma\left(\dfrac{1}{\sigma+1}x\eta - \dfrac{1}{b(\sigma+1)}x^3 - \dfrac{\sigma}{(\sigma+1)^3}x\eta^2\right) + \mathcal{O}(4), \\ \dot{\eta} = 0. \end{cases} \tag{2.24}$$

Fixant η en (2.24), tenim

$$\dot{x} = \left(\frac{\sigma}{\sigma+1}\eta - \frac{\sigma^2}{(\sigma+1)^3}\eta^2\right)x - \frac{1}{b(\sigma+1)}x^3 + \mathcal{O}(4). \tag{2.25}$$

Si introduïm $\dot{\tilde{x}} = b(\sigma+1)x$, l'equació (2.25) ens queda

$$\dot{\tilde{x}} = \left(b\sigma\eta - \frac{\sigma^2 b\eta^2}{(\sigma+1)^2}\right)x - x^3 = \mu x - x^3.$$

En particular, per valors del paràmetre η suficientment petits tenim $\mu > 0$ i això dona una bifurcació de Pitchfork com hem vist en l'exemple vist en 2.8.

Els càlculs anteriors són anàlegs als fets a [10], però tenint en compte que en [10] els autors adapten les coordenades als vectors propis abans de representar les varietats com a grafs.

2.10 Caos transitori

Per $r > 1$, l'origen es torna inestable. En altres paraules, la majoria de les trajectòries que comencen a prop de l'origen s'allunyen d'ell. Tenim una varietat estable 2-dimensional de l'origen que divideix $\mathbb{R}^3$ en dues parts. Per valors de r pròxims a 1, les trajectòries que comencen a una banda tendeixen a P_2, mentre les que comencen a l'altra banda ho fan a P_3. Les trajectòries que comencen a la varietat estable tendeixen a l'origen. La Figura 4 mostra aquest comportament. Les Figures han estat calculades amb el mètode d'integració *Runge-Kutta* d'ordre 4 amb pas fix $h = 0.01$, veure A.

Però en créixer r, les trajectòries comencen a descriure espirals al voltant de P_2 i P_3 en cicles cada cop més oberts fins a arribar a un valor crític denotat per r_{hom}. Aquest fet es coneix normalment com *explosió homoclínica* i la seva existència fou analíticament provada per C. Sparrow, veure [11] per una anàlisi més detallada.

Per als nostres paràmetres clàssics $\sigma = 10$ i $b = \frac{8}{3}$ tenim que $r_{hom} \approx 13.9265$. Quan $r = r_{hom}$ la varietat inestable de l'origen es retorça al voltant dels punts P_2 i P_3 i torna per la varietat estable d'aquest. Sorgeixen d'aquesta manera dues òrbites homoclíniques que connecten l'origen amb ell mateix. Aquestes òrbites són periòdiques, però com l'origen quan $r > 1$ és un punt de sella, la trajectòria cada cop va més lenta segons s'aproxima a l'origen realitzant un recorregut infinitament llarg, així doncs, el seu període és infinit.

Quan r creix per sobre de r_{hom}, de cada òrbita homoclínica neix una òrbita periòdica inestable al voltant de P_2 i P_3. Aquest fet provoca que una trajectòria procedent de P_2 sigui rebutjada per

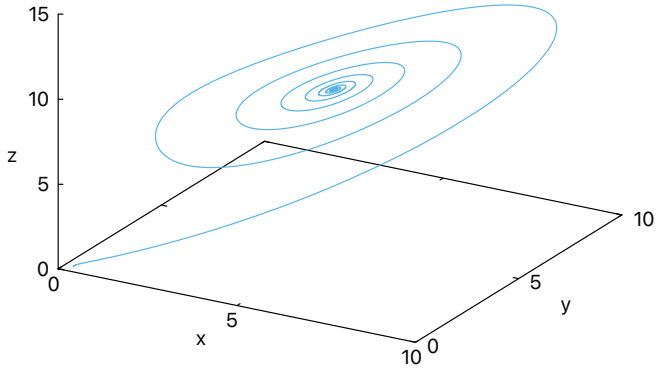

Figura 4: Solució del P.V.I per $x_0 = (0.3,\ 0.2,\ 0.1)$ i pels valors clàssics $\sigma = 10,\ b = \frac{8}{3}$ *i* $r = 10$.

l'òrbita periòdica de P_2 i es dirigeixi a P_3 on torni a ser rebutjada per l'òrbita periòdica i torni cap a P_2, aquest fet es repeteix fins a arribar a un dels dos punts, P_2 o P_3, ja que com hem vist en la secció 2.7 són punts asimptòticament estables. Aquesta situació sembla difícil de distingir del caos i sovint s'anomena *caos transitori*. La Figura 5 mostra aquest règim transitori.

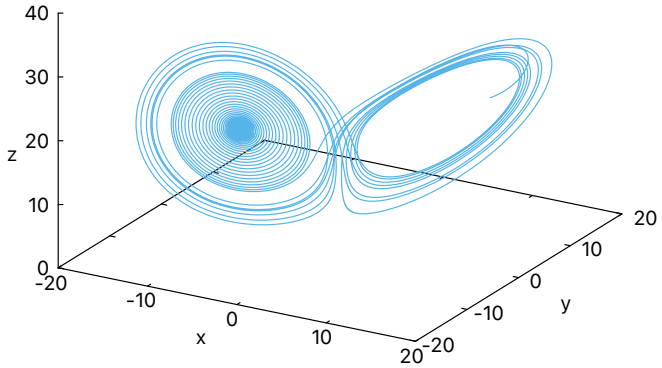

Figura 5: Solució del P.V.I per $x_0 = (7,\ 17,\ 16)$ i pels valors clàssics $\sigma = 10,\ b = \frac{8}{3}$ *i* $r = 20$.

Quan r creix fins a arribar a un altre valor crític $r_{het} \approx 24.0579$ es produeix una altra bifurcació, veure [12]. En aquest cas, tenim una bifurcació heteroclínica que crea l'atractor caòtic. Pels valors de r tals que $r_{het} < r < r_H$ l'atractor caòtic coexisteix amb els dos punts d'equilibri P_2 i P_3 fins que aquests desapareixen en la bifurcació de Hopf quan $r = r_H$. La Figura 6 mostra aquest comportament.

Les òrbites periòdiques inestables que neixen en l'explosió homoclínica, tenen la propietat que la seva amplitud va decreixent a mesura que r augmenta, fins que col·lapsen a P_2 i P_3 en la bifurcació

de Hopf quan $r = r_H$. Així doncs, quan $r > r_H$ l'atractor caòtic és l'únic atractor.

Quan r supera el valor crític r_H els dos punts P_2 i P_3 deixen de ser estables i es converteixen en punts inestables, per tant, el flux de trajectòries que giren entorn d'ells deixa de ser atret pels dos punts i segueix donant voltes eternament. Aquest fenomen rep el nom de *règim caòtic* i la figura geomètrica que sorgeix s'anomena *atractor estrany de Lorenz*. La Figura 6 mostra aquest atractor estrany similar a les ales d'una papallona.

L'existència d'aquest atractor estrany fou provada en una demostració assistida per ordinador per W. Tucker [7].

La Figura 7 mostra un resum de l'espai de paràmetres.

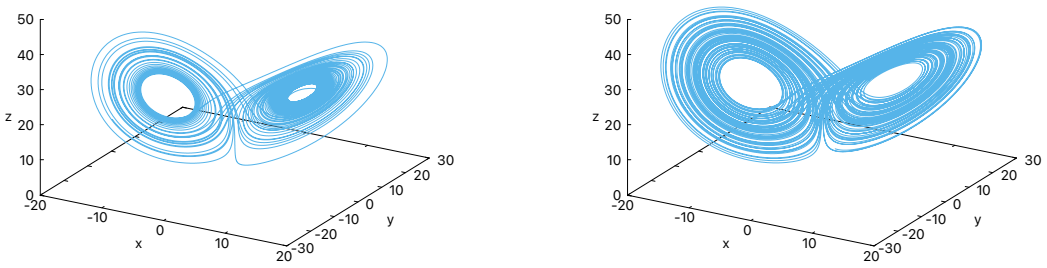

Figura 6: A l'esquerra, solució del P.V.I per $x_0 = (12,\ 8,\ 15)$ i pels valors clàssics $\sigma = 10,\ b = \frac{8}{3}$ *i* $r = 24.5$. A la dreta, solució del P.V.I per $x_0 = (1,\ 3,\ 7)$ i pels valors clàssics $\sigma = 10,\ b = \frac{8}{3}$ *i* $r = 28$.

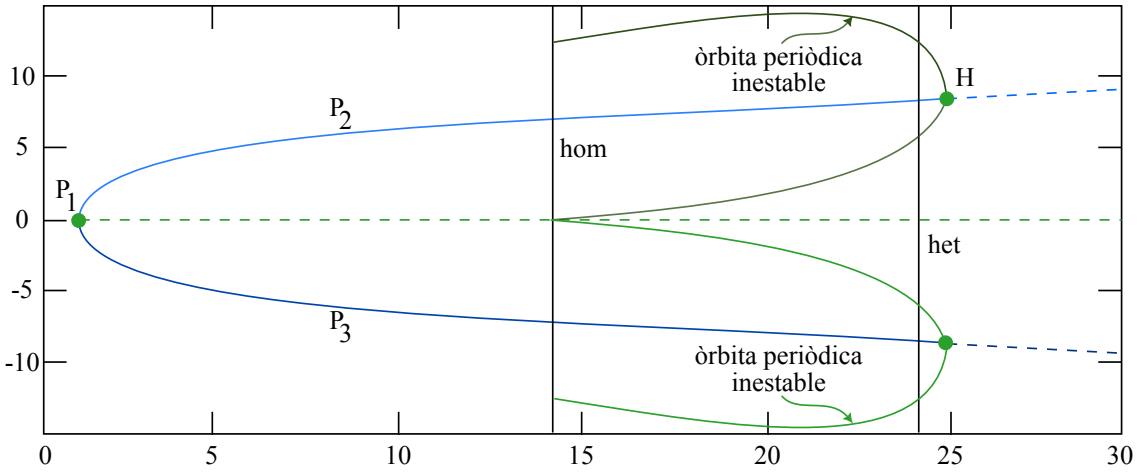

Figura 7: El diagrama de bifurcació 7 mostra els punts d'equilibri P_1, $P_{2,3}$ les òrbites periòdiques que neixen de la bifurcació *hom*, la bifurcació de Pitchfork per $r = 1$, la bifurcació homoclínica per $r \approx 13.9265$, la bifurcació heteroclínica $r \approx 24.0579$ i la bifurcació de Hopf de $P_{2,3}$ per $r \approx 24.7468$.

2.11 Caos

La teoria del caos és una branca dels sistemes dinàmics no lineals, que s'encarrega de l'estudi dels sistemes caòtics. Un dels precursors de la teoria del caos fou el matemàtic francès Henri Poincaré (1854-1912), que descobrí que quan existeix sensibilitat a les condicions inicials és impossible

realitzar una predicció evolutiva d'un sistema a llarg termini. El Teorema de Poincaré-Bendixson demostra que un sistema dinàmic autònom continu en una o dues dimensions no presenta un comportament caòtic. Tanmateix, en tan sols 3 dimensions ja podem trobar sistemes caòtics com hem vist amb el sistema de Lorenz.

En les últimes dècades s'han dut a terme moltes investigacions sobre el caos de tal manera que s'han trobat comportaments caòtics en molts tipus de sistemes com ara: làsers, reaccions químiques, circuits elèctrics, etc. Avui en dia la teoria dels sistemes dinàmics caòtics és de gran interès en nombrosos àmbits que estudiïn sistemes dinàmics, en particular, com veurem en el capítol 3.4, és d'especial interès en l'àmbit de la criptografia.

En aquest apartat introduïm el significat de caos aplicat a un sistema dinàmic determinista i expliquem la noció d'atractor estrany. En general, el caos determinista posa de manifest trajectòries que reflecteixen l'evolució temporal de manera molt irregular donant la sensació de ser completament atzaroses, però en realitat són totalment deterministes. Malgrat que existeixin diverses definicions sobre els sistemes dinàmics caòtics la majoria verifiquen les següents característiques:

1. **Determinista.** Un sistema determinista és un sistema on un estat inicial determina completament els estats futurs del sistema. Per tant, no hi ha aleatorietat en la producció dels estats futurs. Si a un sistema determinista se li assignen condicions inicials, el model produirà els mateixos estats cada vegada.

2. **No periodicitat.** Les trajectòries no s'ajusten a un punt fix o òrbita periòdica per a valors de t prou grans. Els sistemes caòtics són sistemes dinàmics pels quals les variables d'estat es mouen en un espai acotat, no periòdicament i aparentment "aleatòria".

3. **Dependència sensible respecte les condicions inicials.** Trajectòries que comencen molt properes poden tenir comportaments qualitativament molt diferents.

4. **Transitivitat topològica.** Òrbites allunyades poden arribar a aproximar-se. Això es deu al plegament de l'espai de fases sobre si mateix, donant lloc a orbites que estan dins d'una regió de l´espai de fases, però que no es tallen.

5. **Densitat d'òrbites periòdiques.** Perquè un sistema caòtic tingui òrbites periòdiques denses significa que cada punt de l'espai s'apropa arbitràriament de prop per òrbites periòdiques.

A continuació, mostrem el significat del caos aplicat a la noció d'atractor estrany. Considerem un sistema dinàmic autònom no lineal $\dot{x} = f(x),\ x \in \mathbb{R}^n,\ f \in C^r\ (r \geq 1)$.

Denotem per $\phi(t, x)$ el flux generat pel sistema anterior. A més, suposem que Λ és un subconjunt compacte de $\mathbb{R}^n$ invariant sota el flux $\phi(t, x)$.

Definició 2.29. *Es diu que el flux $\phi(t, x)$ té dependència sensible respecte les condicions inicials en Λ si existeix $\epsilon > 0$ de manera que, per a tot punt $x \in \Lambda$ i tot entorn del punt U_x, existeixen $y \in U_x$ i $t > 0$ tals que $|\phi(t, x) - \phi(t, y)| > \epsilon$.*

Com hem comentat abans, existeixen diverses definicions de sistemes dinàmics caòtics, segons la definició formulada per W. Hirsh, S. Smale i L. Devaney [6] tenim el següent.

Definició 2.30. *Es diu que Λ és caòtic si compleix les següents propietats:*

1. *$\phi(t, x)$ té dependència sensible respecte les condicions inicials en Λ.*

2. *Les òrbites periòdiques de $\phi(t, x)$ són denses en Λ.*

3. *$\phi(t, x)$ és topològicament transitiu en Λ.*

A l'apartat 2.6 hem donat la definició de conjunt atractor (2.20) i hem vist que el sistema de Lorenz té un conjunt atractor global. En particular, hem anomenat l'existència d'un *atractor estrany* en el sistema de Lorenz.

Definició 2.31. *Suposem que $\mathscr{A} \subset \mathbb{R}^n$ és un atractor. Direm que $\mathscr{A}$ és un atractor estrany si és caòtic.*

Quan Lorenz representà en tres dimensions les trajectòries del sistema de Lorenz observà que s'instal·laven en un conjunt semblant a un parell d'ales de papallona. Aquest conjunt és l'atractor estrany. Lorenz intentà donar una explicació a l'estructura geomètrica de l'atractor estrany, veure [1]. Es referí a aquest atractor com: "Un complex infinit de superfícies, cadascuna extremadament propera a una o l'altra de les dues superfícies que es fusionen."

Avui en dia, aquest "complex infinit de superfícies" s'anomena *fractal*. En particular, els experiments numèrics mostren que les òrbites s'aproximen a un atractor estrany amb dimensió fractal $D \approx 2.06$, veure [13]. A continuació, estudiarem el caos amb més detall.

Divergència exponencial de trajectòries properes

El moviment de l'atractor de Lorenz mostra dependència respecte de les condicions inicials. Això significa que dues trajectòries amb condicions inicials properes divergiran ràpidament l'una de l'altra. Els exponents de Lyapunov donen una mesura mitjana a la velocitat exponencial amb què les òrbites properes d'una aplicació $f : X \to X$ se separen. Això, requeriria un valor positiu de la taxa exponencial mitjana amb el qual les òrbites properes divergeixen, per tant, un valor positiu de l'exponent de Lyapunov és una indicació per tenir comportament caòtic.

Considerem l'aplicació 1-dimensional $x_{n+1} = f(x_n)$ amb dues condicions inicials properes x_0 i $x_0 + \delta_0$, on δ_0 és una quantitat petita. L'enèsim pas d'iteració pren la forma $x_0 \to f^N(x_0)$ i $x_0 + \delta_0 \to f^N(x_0 + \delta_0)$. En el límit $N \to +\infty$ es defineix el nombre λ depenent de la condició inicial x_0 com

$$\lim_{N\to+\infty} e^{\lambda N} = \lim_{N\to+\infty} \frac{\left|f^N(x_0 + \delta_0) - f^N(x_0)\right|}{\delta_0},\ \delta_0 \to 0 \textit{ quan } N \to +\infty. \tag{2.26}$$

El nombre λ s'anomena exponent de Lyapunov. Prenent el logaritme de (2.26) en el límit obtenim

$$\begin{aligned}\lambda &= \lim_{\substack{N\to+\infty \\ \delta_0\to 0}} \frac{1}{N} \log \frac{\left|f^N(x_0 + \delta_0) - f^N(x_0)\right|}{\delta_0} = \lim_{N\to+\infty} \frac{1}{N} \log \left|\frac{df^N}{dx}(x_0)\right| \\ &= \lim_{N\to+\infty} \frac{1}{N} \log \left|\left(f^N\right)'(x_0)\right|.\end{aligned}$$

Utilitzant la regla de la cadena tenim que

$$\begin{aligned}\left(f^N\right)'(x_0) &= \left(f\left(f^{N-1}\right)\right)'(x_0) \\ &= \left(f'\left(f^{N-1}\right)\right)(x_0)\left(f^{N-1}\right)'(x_0) \\ &= f'\left(f^{N-1}(x_0)\right)\left(f'\left(f^{N-2}\right)\right)(x_0)\left(f^{N-2}\right)'(x_0) \\ &= f'\left(f^{N-1}(x_0)\right)\cdots f'\left(f(x_0)\right)f'(x_0).\end{aligned} \tag{2.27}$$

Com que $f^k(x_0) = x_k \ \forall k \in \mathbb{Z}$, és a dir, $x_1 = f(x_0),\ x_2 = f^2(x_0),\ x_3 = f^3(x_0), ...$, podem reescriure (2.27) de la següent forma

$$\left(f^N\right)'(x_0) = f'\left(x_{N-1}\right) \cdots f'(x_1)f'(x_0) = \prod_{i=0}^{N-1} f'(x_i).$$

Definició 2.32. *Sigui $f : X \to X$ una funció de classe C^1 i x_0 una condició inicial. Definim l'exponent de Lyapunov com*

$$\lambda(x_0) = \lim_{N\to+\infty} \frac{1}{N} \log \left| \prod_{i=0}^{N-1} f'(x_i) \right| = \lim_{N\to+\infty} \frac{1}{N} \sum_{i=0}^{N-1} \log \left| f'(x_i) \right|,$$

si el límit existeix.

En el cas continu el concepte és el mateix. Sigui $\dot{x} = f(x)$, $x(0) = x_0$ un sistema de n equacions diferencials, on f és de classe C^1. Sigui $\phi_t(x)$ el seu flux associat, l'aplicació $\phi_t(x)$ ens diu l'estat del sistema després de t unitats de temps. Si considerem dos punts propers x_0, $x_0 + \delta_0$, on δ_0 és una petita pertorbació del punt inicial x_0, obtenim que a temps t, les imatges sota el flux seran $\phi_t(x_0)$ i $\phi_t(x_0 + \delta_0)$ respectivament. I la pertorbació $\delta(t)$ esdevindrà

$$\delta(t) = \phi_t(x_0 + \delta_0) - \phi_t(x_0) = D_{x_0}\phi_t(x_0)\delta_0,$$

on l'últim terme s'obté linealitzant. Fixant t, $D_{x_0}\phi_t(x_0)$ és una aplicació lineal en $\mathbb{R}^n$, que pren forma de matriu $n \times n$. Intuïtivament, el vector $D_{x_0}\phi_t(x_0)\delta_0$ és una petita variació de la solució del sistema autònom anterior $\dot{x} = f(x),\ x(0) = x_0$ a temps t causada per un petit canvi en el valor inicial $t = 0$ de x_0 a $x_0 + \delta_0$.

Encara que no hi ha una fórmula explícita per $D_{x_0}\phi_t(x_0)$ podem trobar una equació diferencial que pot ser resolta en paral·lel amb el sistema autònom. Com que $\{\phi_t(x_0) |\ t \in \mathbb{R}\}$ és la solució del sistema autònom amb valor inicial x_0, tenim per definició que

$$\frac{d}{dt}\phi_t(x_0) = f\left(\phi_t(x_0)\right).$$

Aquesta equació té 2 variables t i x_0. Diferenciant respecte x_0 i usant la regla de la cadena obtenim

$$\frac{d}{dt} D_{x_0}\phi_t(x_0) = Df\left(\phi_t(x_0)\right) D_{x_0}\phi_t(x_0), \tag{2.28}$$

anomenada equació variacional de l'equació diferencial. Si poguéssim solucionar l'equació (2.28) per $D_{x_0}\phi_t(x_0)$, coneixeríem la matriu de derivació de $\phi_t(x_0)$, obtenint així com $\phi_t(x_0)$ actua sota petites variacions del valor inicial x_0.

Simplificant (2.28), definim

$$Y_t = D_{x_0}\phi_t(x_0) \ i \ J(t) = Df\left(\phi_t(x_0)\right),$$

aleshores podem reescriure (2.28) com

$$\begin{aligned} &\dot{Y}_t = J(t)Y_t, \\ &Y_0 = I, \textit{on } I \textit{ és la matriu identitat, ja que } \phi_0(x_0) = x_0. \end{aligned} \tag{2.29}$$

Suposem que $\det(Y(t)) > 0\ \forall t$, la qual cosa implica que les trajectòries inicialment separades romanen separades durant tot el temps. Geomètricament, la solució fonamental $Y(t)$ es pot visualitzar com una aplicació lineal que envia una m-esfera inicial de l'espai de fases a un el·lipsoide en evolució. Els vectors de Lyapunov es defineixen com els eixos principals de l'el·lipsoide. L'i-èsim *vector de Lyapunov* ve donat per

$$p_i(t) = Y(t)\,\xi_i(t),$$

on $\xi_i(t)$ és un vector propi unitari de la matriu $\sqrt{Y_t^T Y_t}$, on Y_t^T denota la transposada de Y_t. Podem definir l'i-èsim exponent de Lyapunov com

$$\lambda_i = \lim_{t\to+\infty} \frac{1}{t} \log \|p_i(t)\|.$$

L'exponent caracteritza la taxa mitjana de creixement exponencial a llarg temps de l'i-èsim eix principal de l'el·lipsoide. En [14] i [15] es fa un estudi detallat dels exponents de Lyapunov i es donen mètodes per calcular-los.

En particular, estudis numèrics de l'atractor de Lorenz, mostren que $\|\delta_0\| \sim \|\delta_0\| e^{\lambda t}$ on $\lambda \approx 0.9056$, veure [16]. La Figura 8 mostra la divergència en la component $z(t)$ entre dues trajectòries amb condicions inicials molt properes amb els paràmetres clàssics $\sigma = 10,\ b = \frac{8}{3}\ i\ r = 28$.

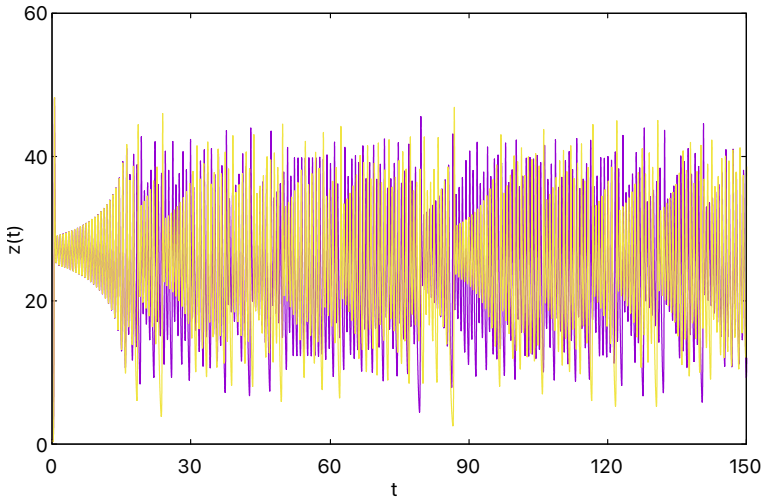

Figura 8: Divergència en la component z. Dues solucions de la component z amb un lleuger canvi en les condicions inicials $(0.1,\ 0.2,\ 0.5)$ i $(0,11,\ 0.21,\ 0.51)$ per la solució lila i groga respectivament.

Pas pel màxim

Com sabem que l'atractor de Lorenz no és només un cicle límit estable? Les trajectòries no semblen mai repetir, però podríem pensar que potser és perquè mai s'ha integrat per un temps prou gran i les trajectòries eventualment tindran al final un comportament periòdic.

Lorenz intentà donar una resposta [1] a aquest argument mostrant que no hi ha cicles límits estables, almenys per als paràmetres $\sigma = 10,\ b = \frac{8}{3}\ i\ r = 28$ que estudià.

Per fer-ho, va examinar el comportament dels màxims successius de les trajectòries en la direcció z. És una manera de reduir la complexa dinàmica, contínua i tridimensional del sistema de Lorenz a la

d'una aplicació unidimensional. Per dur a terme aquest estudi, Lorenz dibuixà els punts (z_n, z_{n+1}) per diferents valors de n, on z_n és l'enèsim màxim local de $z(t)$. Per veure aquesta relació hem integrat l'equació de Lorenz mitjançant el mètode *Runge-Kutta 4*, veure A, i hem anat calculant el màxim local z_n a cada pas. El resultat obtingut és el que veu es veu a la primera gràfica de la Figura 9.

A la funció $z_{n+1} = f\left(z_n\right)$ que representa aquesta gràfica se la coneix com a pas pel màxim. Observem que la funció f té moltes similituds amb l'aplicació tenda de la Figura 9 en particular verifiquen $|f'(z)| > 1$, $\forall z$. Definim l'aplicació tenda $T_2 : I \to I$ en $I = [0,1]$ com $T_2(z) = 1 - |1 - 2z|$.

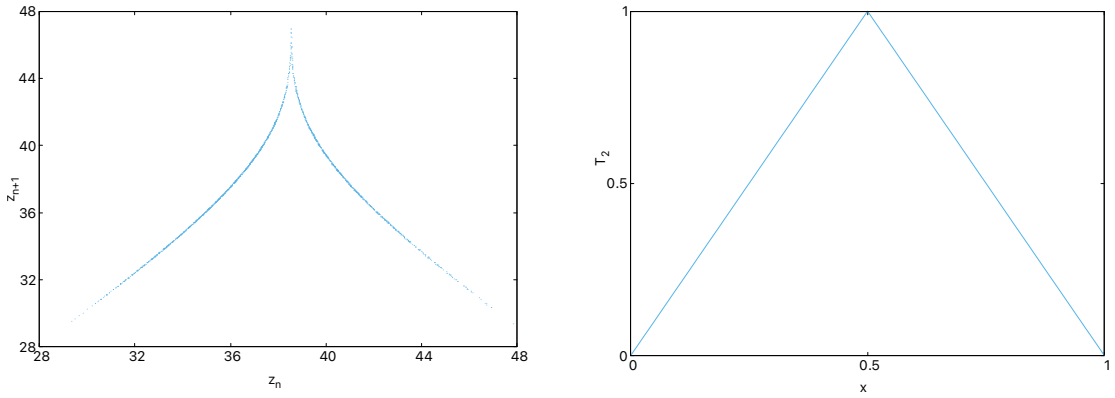

Figura 9: A l'esquerra, gràfica de z_{n+1} *vs* z_n per als valors clàssics $\sigma = 10$, $b = \frac{8}{3}$ *i* $r = 28$. A la dreta, l'aplicació tenda.

Proposició 2.33. *Si el sistema de Lorenz posseeix una òrbita periòdica, aleshores aquesta òrbita és inestable.*

Demostració. Considerem la seqüència $\{z_n\}$ corresponent a l'òrbita periòdica. Aquesta seqüència, eventualment es repetirà, és a dir, $z_{n+p} = z_n$, per algun enter $p \geq 1$. Alhora, considerem una pertorbació de l'òrbita periòdica que passa a través del punt $z_n + \eta_n$, on η_n denota la distància de la trajectòria a l'òrbita periòdica.

L'objectiu serà considerar η_n, i veure què passarà després de p iteracions. Veurem que $|\eta_{n+p}| > |\eta_n|$, fet que implica que la desviació ha crescut i l'òrbita tancada és inestable.

Per estimar η_{n+p}, fem un pas d'iteració, linealitzant al voltant de z_n,

$$z_{n+1} + \eta_{n+1} = f\left(z_n + \eta_n\right) \approx f\left(z_n\right) + f'\left(z_n\right)\eta_n = z_{n+1} + f'\left(z_n\right)\eta_n,$$

i concloem que $\eta_{n+1} \approx f'\left(z_n\right)\eta_n$.

Anàlogament, $\eta_{n+2} \approx f'\left(z_n\right)\eta_{n+1} = f'\left(z_{n+1}\right)f'\left(z_n\right)\eta_n$. Procedint d'aquesta manera, després de p iteracions

$$\eta_{n+p} \approx \left[\prod_{i=0}^{p-1} f'\left(z_n + i\right)\right]\eta_n. \tag{2.30}$$

Com que $|f'(z)| > 1$ cada factor de (2.30) té valor absolut més gran que 1, per tant $|\eta_{n+p}| > |\eta_n|$. Per tant, concloem que una trajectòria que comença a prop d'una òrbita periòdica s'allunya d'ella mateixa amb el temps. Això prova que l'òrbita periòdica és inestable. □

És natural preguntar-se què passa per valors de r molt superiors al valor crític r_H. És conegut, però menys clar, ja que no disposem d'eines d'anàlisis d'estabilitat, que per a valors majors de r apareix un cicle límit estable. Augmentant encara més r, el cicle límit perd la seva estabilitat i torna a aparèixer l'atractor estrany. D'aquesta manera apareixen intervals per diferents valors de r pels quals el w-límit del sistema és un atractor estrany i intervals on existeixen cicles límits estables. Per exemple dos dels intervals més grans en els quals apareix un cicle límit estable són: $99,524 < r < 100,795$ i $145 < r < 166$. Aquest fet és estudiat en [11].

A continuació la següent Figura 10 mostra com l'atractor de Lorenz ha desaparegut i totes les trajectòries calculades numèricament semblen "veure's atretes" cap a una o altra de dues òrbites periòdiques molt simples.

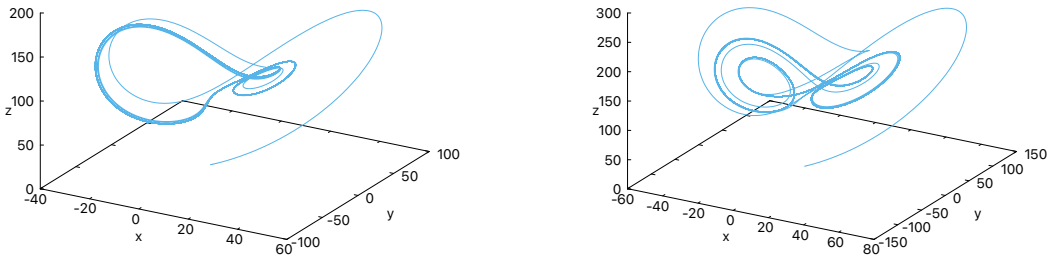

Figura 10: A l'esquerra, solució del P.V.I per $x_0 = (0.1,\ 0.2,\ 0.3)$, $r = 100$. A la dreta, solució del P.V.I per $x_0 = (0.1,\ 0.2,\ 0.3)$, $r = 150$.

3 Aplicació del sistema de Lorenz en criptografia

3.1 Criptografia

La criptografia es defineix, tradicionalment, com l'estudi i la pràctica de formes de convertir informació, des de la seva forma original cap a un codi inintel·ligible, de manera que sigui incomprensible a receptors no autoritzats.

La majoria dels fonaments de la teoria criptogràfica actuals foren presentats en els treballs desenvolupats per C. Shannon [17][18] i en el treball fet per W. Diffie i M. Hellman [19], que introduïren el concepte de Criptografia de Clau Pública.

En general, en un sistema de xifratge, la informació es transmet entre dos usuaris A i B, típicament A, «Alice», pel transmissor i B, «Bob», pel receptor. El transmissor A converteix el «missatge» o «text pla», en el «text xifrat» o «criptograma» sota el control de la «clau de xifratge». A continuació, envia el text xifrat al receptor B usant un canal públic insegur. Finalment, l'usuari B desxifra el criptograma mitjançant la clau de xifratge, obtenint el missatge original.

Formalment, es pot definir aquest procés de la següent manera.

Definició 3.1. *Un **criptosistema** és una tupla* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *on:*

- $\mathcal{P}$ *és el conjunt finit de tots els textos plans possibles.*
- $\mathcal{C}$ *és el conjunt de tots els textos xifrats possibles.*
- $\mathcal{K}$ *és el conjunt de totes les claus possibles.*
- $\mathcal{E} = \{E_e : k \in \mathcal{K}\}$ *és el conjunt de funcions* $E_e : \mathcal{P} \to \mathcal{C}$ *que representa totes les regles de xifratge possibles.*
- $\mathcal{D} = \{D_d : d \in \mathcal{K}\}$ *és el conjunt de funcions* $D_d : \mathcal{C} \to \mathcal{P}$ *que representa totes les regles de desxifratge possibles.*

Amb la propietat que per a cada $(p, e) \in \mathcal{P} \times \mathcal{K}$*, existeix una única regla de desxifratge* $D_d \in \mathcal{D}$*, tal que* $D_d\left(E_e(p)\right) = p$*. Si* $e = d$ *parlarem de criptosistemes simètrics i si* $e \neq d$ *parlarem de criptosistemes asimètrics.*

Per tal de dissenyar correctament un criptosistema és necessari que les funcions de xifratge i desxifratge verifiquin les regles de la teoria del secret perfecte introduïda per C. Shannon [17]. Anomenem «secret perfecte» a l'existència d'un procediment que creï un text encriptat que no contingui cap mena d'informació addicional sobre el text original i, per tant, sigui impossible de desencriptar amb anàlisis estadístiques. El que busca tot criptograma és ser estadísticament independent de la clau i del text pla. És a dir, un bon criptosistema ha de tenir les propietats de *confusió* i *difusió*.

La propietat de *confusió* pretén que la relació entre la clau i el text xifrat sigui tan complexa com sigui possible.

D'altra banda, la propietat de *difusió* implica que petits canvis en el text pla produeixin grans canvis en el text xifrat.

Resumint, un criptosistema ha de complir els següents requisits:

1. Ser sensible a les claus, de manera que la modificació de tan sols un bit de la clau es produeixin texts xifrats completament diferents utilitzant el mateix text pla.

2. Ser sensible al text pla, de manera que la modificació d'un sol bit del text pla produeixi texts xifrats completament diferents.

3. No ha d'existir cap patró en el text xifrat que el relacioni amb el text pla.

4. La cardinalitat del conjunt d'espai de claus $\mathcal{K}$, ha de ser prou gran, ja que d'altra manera es podria recuperar el text pla aplicant la funció de desxifrat amb cada valor possible de la clau.

D'acord amb la manera en què es distribueix la clau, existeixen dos tipus fonamentals de criptosistemes:

- Criptosistemes **simètrics** o de **clau privada**. Aquests criptosistemes usen la mateixa clau $k \in \mathcal{K}$, tant per xifrar com per desxifrar. A més, necessiten un canal de comunicació segur per tal de poder intercanviar amb seguretat la clau k. El sistema de clau privada més conegut actualment s'anomena «Advanced Encryption Standard» i fou proposat l'any 1998 [20].

- Criptosistemes **asimètrics** o de **clau pública**. Aquests usen dues claus (k_p, k_q), privada i pública respectivament. La clau pública pot ser distribuïda lliurement, mentre que la clau privada ha de romandre en secret, el coneixement de la clau pública k_q no ha de permetre accedir a la clau privada k_p de cap manera. En els criptosistemes asimètrics, la clau pública k_q s'utilitza per xifrar i la clau privada k_p per desxifrar. D'aquesta manera s'estableix una comunicació segura per canals insegurs. Aquest mètode fou proposat per W. Diffie i M. Hellman l'any 1976 [19], fet que canviaria els mètodes de xifratge per complet, ja que fins aleshores només es coneixia el sistema de clau privada. Els mètodes de clau pública més coneguts actualment són: *RSA* [21] i *ElGamal* [22] proposats als anys 1979 i 1984 respectivament.

3.2 Sincronització del caos

Un sistema caòtic és un sistema no-lineal determinista que exhibeix un comportament erràtic i irregular. En particular, els sistemes caòtics tenen alta sensibilitat a les condicions inicials, és a dir, dues condicions inicials arbitràriament properes seguiran trajectòries que divergiran ràpidament.

Aquestes característiques semblen desafiar la sincronització, tanmateix, Pecora i Carroll [23][24], provaren que és possible sincronitzar dos sistemes caòtics de tal manera que les trajectòries es mantinguin properes, encara que les condicions inicials siguin diferents.

L'objectiu d'aquest apartat és presentar i provar de forma rigorosa la sincronització entre dos sistemes caòtics, en particular, provarem la sincronització en el cas del sistema de Lorenz. Al llarg de l'apartat, considerarem el mètode de sincronització basat en la descomposició en subsistemes que fou provat primerament per Pecora i Carroll [23].

Per un sistema que condueix un altre entenem que els dos sistemes estan acoblats de manera que el comportament del segon depèn del primer, però el primer no es veu influenciat pel segon. El primer sistema l'anomenarem transmissor o conductor i el segon receptor o resposta. De manera similar, podem generalitzar aquestes idees per incloure qualsevol sistema que es pugui dividir en dos subsistemes. Aquest tipus de sistemes es diu que tenen la propietat d'autosincronització.

Per tal de facilitar l'anàlisi podem dividir el sistema transmissor en aquelles variables que condueixen el subsistema de resposta i aquelles que no ho fan. Això, proporcionarà una subdivisió del sistema original en dos subsistemes.

Formalment, considerem un sistema dinàmic autònom n-dimensional:

$$\dot{x} = f(x),\ x(0) = x_0, \tag{3.1}$$

on $f : U \subset \mathbb{R}^n \to \mathbb{R}^n$, U és un subconjunt obert de $\mathbb{R}^n$ i $f \in C^r(U)$, $r \geq 1$. Tenim el flux associat al sistema (3.1) $\phi : I(x_0) \times U \to \mathbb{R}^n$ definit per $\phi\left(t; x_0\right) = \phi\left(t; 0, x_0\right)$ de classe C^r, $r \geq 1$, respecte el temps.

Aleshores, considerant la descomposició en subsistemes, dividim el sistema original (3.1) en dos subsistemes $x = (u, v)^T$. Així doncs, expressem $U = U_1 \times U_2 \subset \mathbb{R}^m \times \mathbb{R}^{n-m}$, on $(u, v) \in U_1 \times U_2$. Obtenim d'aquesta manera els dos subsistemes autònoms següents:

$$\dot{u} = g(u, v),\ u(0) = u_0 \in U_1, \tag{3.2}$$
$$\dot{v} = h(u, v),\ v(0) = v_0 \in U_2, \tag{3.3}$$

on $u = \left(x_1, \ldots, x_m\right)$, $g = \left(f_1(x), \ldots, f_m(x)\right)$, $v = \left(x_{m+1}, \ldots, x_n\right)$ *i* $h = \left(f_{m+1}(x), \ldots, f_n(x)\right)$. Així doncs, també tindrem el flux $\phi(t; x_0) = \left(\phi_1(t; u_0, v_0), \phi_2(t; u_0, v_0)\right)$.

Ara, considerem el subsistema autònom $(n - m)$-dimensional següent

$$\dot{w} = h\left(\phi_1(t; u_0), w\right),\ w(0) = w_0 \in U_2, \tag{3.4}$$

amb el seu respectiu flux associat $\phi_2^r(t; w_0)$ definit a $\mathbb{R}^{n-m}$.

El sistema n-dimensional definit per l'equació (3.2) i (3.3) és l'anomenat sistema transmissor i el sistema definit per l'equació $(n - m)$-dimensional (3.3) s'anomena sistema resposta. Segons la descomposició en subsistemes presentada anteriorment l'equació (3.2) té el flux associat que condueix el subsistema de resposta (3.4). La Figura 11 mostra l'esquema de la descomposició en subsistemes d'un sistema dinàmic autònom.

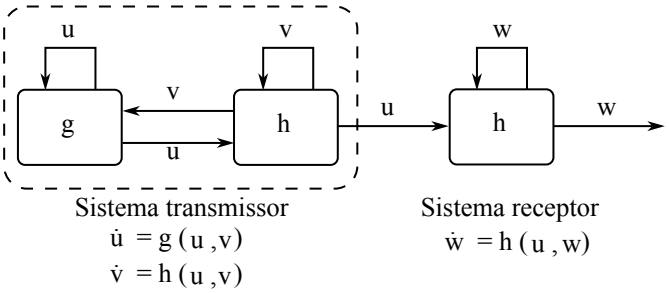

Figura 11: Esquema sistema transmissor-receptor. La variable u del sistema receptor prové de l'evolució del sistema transmissor.

Definició 3.2. *La sincronització completa té lloc quan les trajectòries dels sistemes transmissor i receptor verifiquen:* $\lim_{t\to+\infty} \|\phi_2(t; u_0, v_0) - \phi_2^r(t; w_0)\| = 0$, $\forall v_0 \in U_1$ *i* $\forall w_0 \in U_2$.

La pregunta central esdevé ara: Quan el subsistema de resposta és "estable"? Això és, quan $\phi_2^r(t; w_0)$ és immune a pertorbacions? Això garantiria que per un conjunt de condicions inicials del sistema transmissor sabríem que per qualsevol w_0, $\phi_2^r(t; w_0)$ sincronitzarà.

Tenim doncs $\phi_2^r(t; w_0)$ i volem determinar la seva estabilitat. Considerem una altra trajectòria amb la condició inicial propera $w'(0) = w_0'$ en $t = 0$. El senyal conductor és el mateix pels dos subsistemes, és a dir, tenim:

$$\dot{w} = h\left(\phi_1(t;u_0), w_0\right), w(0) = w_0, \quad \dot{w}' = h\left(\phi_1(t;u_0), w_0'\right), w'(0) = w_0', \tag{3.5}$$

on $\phi_2'^r(t;w_0')$ és el flux associat al segon subsistema de (3.5). Sota quines condicions tindrem $e(t) = |\phi_2'^r(t;w_0') - \phi_2^r(t;w_0)| \to 0$ quan $t \to +\infty$? Per alleugerir la notació escriurem $\phi_1 = \phi_1(t;u_0)$, $\phi_2'^r = \phi_2'^r(t;w_0')$ i $\phi_2^r = \phi_2^r(t;w_0)$ en el que segueixi.

En termes del subsistema (3.5) linealitzant l'error al voltant de $e(t) = 0$ tenim

$$\begin{aligned}\dot{e}(t) &= \frac{d}{dt}\phi_2'^r - \frac{d}{dt}\phi_2^r = h\left(\phi_1, \phi_2'^r\right) - h\left(\phi_1, \phi_2^r\right) \\ &= h\left(\phi_1, \phi_2^r\right) - h\left(\phi_1, \phi_2^r\right) + D_w h\left(\phi_1, \phi_2^r\right)\left(\phi_2'^r - \phi_2^r\right) + \mathcal{O}\left(|\phi_2'^r - \phi_2^r|^2\right) \\ &= D_w h\left(\phi_1, \phi_2^r\right) e\,(t) + \mathcal{O}\left(|\phi_1, \phi_2^r|^2\right),\end{aligned} \tag{3.6}$$

on $D_w h\,(u, w)$ és la diferencial del subsistema (3.4) lineal respecte la variable resposta w. Negligint termes d'ordre superior obtenim l'equació

$$\dot{e} = D_w\left(\phi_1(t;u_0), \phi_2^r(t;w_0)\right) e. \tag{3.7}$$

L'equació (3.7) és una equació bàsica per a bona part de la discussió sobre la sincronització de sistemes caòtics. Es pot donar una definició rigorosa en termes dels exponents de Lyapunov descrits en la seccio 2.11. Els exponents de (3.7) s'anomenen exponents de Lyapunov condicionals, perquè depenen de la variable del sistema transmissor $u(t)$. La sincronització només es pot produir quan els exponents condicionals de Lyapunov del subsistema de resposta (3.4) són negatius.

Com a exemple per il·lustrar aquesta idea, considerem el sistema de Lorenz com a sistema transmissor i considerem el subsistema de resposta (y_r, z_r)

$$\begin{aligned}\dot{y}_r &= -xz_r + rx - y_r, \\ \dot{z}_r &= xy_r - bz_r,\end{aligned}$$

conduït per $x(t)$, on $y_r = y + e_y$ i $z_r = z + e_z$. Aleshores, restant els subsistemes (y, z) i (y_r, z_r) i linealitzant l'error com en (3.6) obtenim

$$\begin{pmatrix}\dot{e}_y \\ \dot{e}_z\end{pmatrix} = \begin{pmatrix}-1 & -x \\ x & -b\end{pmatrix}\begin{pmatrix}e_y \\ e_z\end{pmatrix}. \tag{3.8}$$

Efectivament, els exponents de Lyapunov de (3.8) depenen de la variable transmissora $x(t)$, i per això s'anomenen condicionals. De manera anàloga a com procedim per trobar els exponents habituals de Lyapunov, evolucionem l'equació (3.8) al llarg del temps juntament amb la variable conductora $x(t)$ i calculem els exponents de Lyapunov. La determinació analítica dels exponents condicionals de Lyapunov sovint no és possible, és per això que una aproximació numèrica, com per exemple mitjançant el mètode de descomposició QR exposada per Eckmann i Ruelle [25] és necessària, veure A.2.

Observació 3.3. Aquest fet ens dona una condició necessària, però no suficient per determinar la sincronització entre el sistema transmissor i receptor.

3.3 Sincronització en el sistema de Lorenz

Seguint l'esquema presentat en la Figura 11 considerem el sistema de Lorenz (3.9) com a sistema transmissor

$$\begin{aligned} \dot{x} &= \sigma(y - x), \\ \dot{y} &= -xz + rx - y, \\ \dot{z} &= xy - bz, \end{aligned} \tag{3.9}$$

on els valors b, σ i r són tals que el sistema de Lorenz es troba en règim caòtic. Per exemple, podríem considerar els valors clàssics $\sigma = 10$, $b = \frac{8}{3}$ i $r = 60$.

En el cas del sistema de Lorenz (3.9), aquest es pot descompondre en 2 subsistemes estables en el sentit de la sincronització, ja que com mostra la Taula 1 tenen exponents condicionals de Lyapunov negatius.

El primer subsistema de resposta estable (x_1, z_1) ve donat per

$$\begin{aligned} \dot{x}_1 &= \sigma(y - x_1), \\ \dot{z}_1 &= x_1 y - b z_1. \end{aligned} \tag{3.10}$$

El segon subsistema de resposta estable (y_2, z_2) ve donat per

$$\begin{aligned} \dot{y}_2 &= -x z_2 + rx - y_2, \\ \dot{z}_2 &= x y_2 - b z_2. \end{aligned} \tag{3.11}$$

Observem que seguint l'esquema de la Figura 11, el sistema (3.9) pot interpretar-se com el sistema transmissor, ja que el seu comportament dinàmic és independent dels sistemes de resposta (3.10) i (3.11). Les equacions (3.10) i (3.11) representen els sistemes de resposta «conduïts» pels senyals del transmissor $y(t)$ i $x(t)$ respectivament.

D'altra banda, podríem considerar el subsistema de resposta (x_3, y_3) donat per

$$\begin{aligned} \dot{x}_3 &= \sigma(y_3 - x_3), \\ \dot{y}_3 &= -x_3 z + r x_3 - y_3. \end{aligned} \tag{3.12}$$

Tot i això, aquest subsistema és inestable ja que té un exponent condicional de Lyapunov positiu, veure la Taula 1. A continuació, la Taula 1 mostra els exponents condicionals de Lyapunov per als valors clàssics $\sigma = 10$, $b = \frac{8}{3}$ i $r = 60$ calculats en el treball [26].

Taula 1: Exponents condicionals de Lyapunov per als subsistemes de resposta (y_2, z_2), (x_1, z_1) *i* (x_3, y_3) considerant els paràmetres clàssics $\sigma = 10$, $b = \frac{8}{3}$ *i* $r = 60$.

V. Sincronització	S. Resposta	E. Lyapunov
$x(t)$	(y_2, z_2) (3.11)	(-1.81, -1.86)
$y(t)$	(x_1, z_1) (3.10)	(-2.67, -10)
$z(t)$	(x_3, y_3) (3.12)	(+0.01, -11.01)

La Figura 12 mostra la sincronització dels sistemes (3.9) i (3.11). D'altra banda, la Figura 13 mostra com el sistema (3.12) és inestable. S'observa com en el cas de la Figura 12 el subsistema de resposta (3.11), tot i tenir condicions inicials poc properes, el sistema sincronitza en $t = 20$.

En canvi, la Figura 13 mostra com el subsistema de resposta (3.12), tot i tenir les condicions molt properes al sistema transmissor, no sincronitza. Per sincronitzar els sistemes hem utilitzat el mètode d'integració numèrica d'Euler amb pas fix $h = 0.01$, considerant els paràmetres clàssics $\sigma = 10,\ b = \frac{8}{3}\ i\ r = 28$.

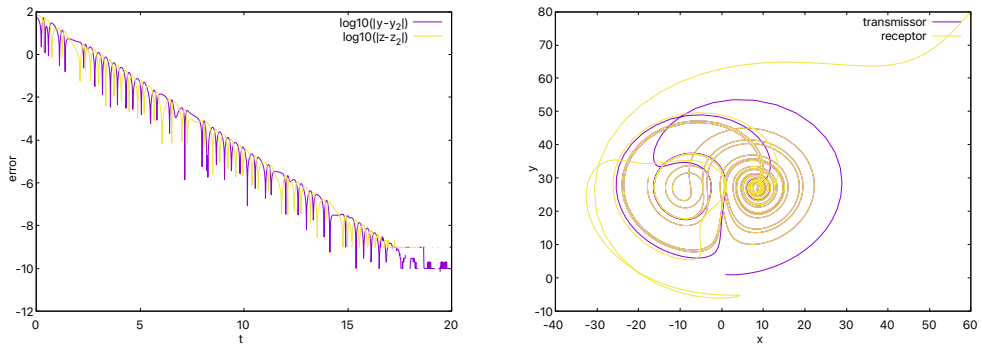

Figura 12: A l'esquerra, error entre les components y i z del sistema transmissor (3.9) i receptor (3.11). A la dreta, solució del P.V.I amb $x_0 = (1,\ 1,\ 1)$ pel sistema transmissor i solució del P.V.I amb condicions inicials $(60, 80)$ pel receptor. Ambdós considerant els paràmetres clàssics i $r = 28$.

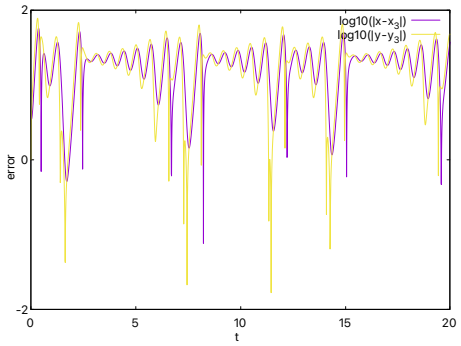

Figura 13: Error entre les components x i y del sistema transmissor (3.9) i receptor (3.12). El sistema transmissor té condicions inicials $(1, 1, 1)$ i el sistema receptor $(5, 2, 7)$. Considerant els paràmetres clàssics i $r = 28$.

Cal destacar que diverses aplicacions, en particular en l'àmbit de la comunicació privada com veurem en la pròxima secció 3.4, són possibles gràcies a la capacitat del sistema de resposta de recuperar la dinàmica $(x(t), y(t), z(t))$ del sistema transmissor. És per això, que considerem el següent sistema de resposta

$$\begin{aligned} \dot{x}_r &= \sigma(y_r - x_r), \\ \dot{y}_r &= rx - y_r - xz_r, \\ \dot{z}_r &= xy_r - bz_r, \end{aligned} \tag{3.13}$$

en aquest cas el sistema de resposta (3.13) és "idèntic" a (3.9) excepte que substituïm $x(t)$ per $x_r(t)$ en les equacions (y_r, z_r). El sistema de resposta (3.13) és conduït pel senyal $x(t)$ enviat pel transmissor (3.9).

Un altre sistema de resposta possible seria el següent

$$\begin{aligned} \dot{x}_r &= \sigma(y - x_r), \\ \dot{y}_r &= rx_r - y_r - x_r z_r, \\ \dot{z}_r &= x_r y - bz_r, \end{aligned} \tag{3.14}$$

en aquest cas el sistema de resposta (3.14) és conduït pel senyal $y(t)$ enviat pel transmissor (3.9).

Seguidament, provem la sincronització dels sistemes (3.9) i (3.13). Definim els errors de sincronització de la següent manera

$$e_x(t) = x(t) - x_r(t),\ e_y(t) = y(t) - y_r(t),\ e_z(t) = z(t) - z_r(t). \tag{3.15}$$

Observació 3.4. La sincronització del sistema (3.9) amb el subsistema estable (3.11) la podem trobar en [23]. La sincronització asimptòtica del sistema transmissor (3.9) i el sistema receptor (3.13) la podem trobar en [27]. A continuació 3.5, provarem que la sincronització entre el sistema transmissor (3.9) i el sistema receptor (3.13) és exponencial. La sincronització exponencial entre el sistema transmissor (3.9) i el sistema receptor (3.14) es demostra de forma anàloga.

Lema 3.5. *Per qualsevol $e_x(0)$, $e_y(0)$, $e_z(0)$, els errors definits per* (3.15) *associats als sistemes* (3.9) *i* (3.13) *disminueixen exponencialment a zero respecte el temps.*

Demostració. En primer lloc, tenim que

$$\dot{e}_y = \dot{y} - \dot{y}_r = -e_y - xe_z, \quad \dot{e}_z = \dot{z} - \dot{z}_r = xe_y - be_z. \tag{3.16}$$

En segon lloc, definim la funció de Lyapunov $V = \frac{1}{2}e_y^2 + 2e_z^2$ i busquem si $\dot{V} \leq -kV$ per alguna constant $k > 0$. Considerant la derivada orbital de V al llarg d'una solució de (3.16) obtenim que

$$\dot{V} = e_y\dot{e}_y + 4e_z\dot{e}_z = -e_y^2 - 4be_z^2. \tag{3.17}$$

Llavors $\dot{V} \leq -kV \iff -e_y^2 - 4be_z^2 \leq -\frac{k}{2}e_y^2 - 2ke_z^2$ i això és cert per a $k \leq 2min\{1, b\}$. Per simplificar, considerem $b \geq 1$ i, per tant, podem agafar $k = 2$. Aleshores, tenim que es verifica $\dot{V} + 2V = 0$ i integrant aquesta equació obtenim $0 \leq V(t) = V(0)e^{-2t}$. En conseqüència, e_y i e_z disminueixen exponencialment a 0 i sincronitzen amb el subsistema resposta (3.11). Seguidament, veurem que l'error e_x també disminueix exponencialment aconseguint d'aquesta manera la sincronització entre el sistema transmissor (3.9) i el sistema resposta (3.13).

Notem que l'error e_y està acotat superiorment. Efectivament, tenim que $\frac{1}{2}e_y^2 \leq V(t) \leq V(0)e^{-2t}$, per tant, $|e_y| \leq Ce^{-\gamma t}$, per alguna $\gamma > 0$. Per provar que e_x disminueix exponencialment a 0 considerem l'equació de l'error $\dot{e}_x$ i la multipliquem per un factor integrant $e^{\sigma t}$. Com que e_y està acotat superiorment, podem utilitzar aquest fet en la següent equació

$$\begin{aligned} &\dot{e}_x = \sigma\left(e_y - e_x\right) \iff \frac{d}{dt}\left(e_x e^{\sigma t}\right) = \sigma e_y e^{\sigma t} \Rightarrow \\ &-\sigma C e^{-\gamma t}e^{\sigma t} \leq \frac{d}{dt}\left(e_x e^{\sigma t}\right) = \sigma e_y e^{\sigma t} \leq \sigma C e^{-\gamma t}e^{\sigma t} \iff \\ &-\sigma C e^{(\sigma-\gamma)t} \leq \frac{d}{dt}\left(e_x e^{\sigma t}\right) \leq \sigma C e^{(\sigma-\gamma)t}. \end{aligned} \tag{3.18}$$

Canviant la variable a s i integrant de $s = 0$ a $s = t$ l'equació (3.18) obtenim

$$
\begin{aligned}
&-\int_0^t \sigma C e^{(\sigma-\gamma)s} ds \leq \int_0^t \frac{d}{ds}(e_x e^{\sigma s}) ds \leq \int_0^t \sigma C e^{(\sigma-\gamma)s} ds \iff \\
&-\frac{\sigma C}{\sigma-\gamma}\left(e^{(\sigma-\gamma)t}-1\right) \leq e_x(t)e^{\sigma t} - e_x(0) \leq \frac{\sigma C}{\sigma-\gamma}\left(e^{(\sigma-\gamma)t}-1\right) \iff \\
&\left(e_x(0) - \frac{\sigma C}{\sigma-\gamma}\left(e^{(\sigma-\gamma)t}-1\right)\right) e^{-\sigma t} \leq e_x(t) \leq \left(e_x(0) + \frac{\sigma C}{\sigma-\gamma}\left(e^{(\sigma-\gamma)t}-1\right)\right) e^{-\sigma t}.
\end{aligned} \tag{3.19}
$$

Com que $e_x(0)$ i $\frac{\sigma C}{\sigma-\gamma}$ són constants, $\sigma > 0$, $e^{(\sigma-\gamma)t}e^{-\sigma t} = e^{-\gamma t}$ i $\gamma > 0$, ambdós termes a banda i banda de la desigualtat (3.19) decreixen exponencialment a 0 quan $t \to +\infty$, el que significa que $e_x(t)$ decreix exponencialment a 0. En conclusió, hem provat que els errors de l'equació (3.15) associats als sistemes transmissor i receptor decreixen exponencialment a 0. □

El fet que la sincronització entre sistema transmissor i receptor sigui exponencial respecte el temps ens permet pensar en una possible aplicació en l'àmbit de la comunicació privada 3.4. Aquest fet ens permet sincronitzar dos sistemes ràpidament i d'aquesta manera xifrar i desxifrar senyals en un temps raonable com veurem en 3.6.

3.4 Criptografia caòtica

L'evolució constant de les tecnologies de telecomunicacions, especialment d'Internet i el comerç electrònic, juntament amb la digitalització de la societat, han augmentat cada cop més la necessitat que les dades multimèdia - imatges, àudio, vídeos i text - es transmetin a través de les xarxes obertes de forma segura.

Els mètodes de xifratge de clau pública més populars actualment, com *RSA* i el *Gamal*, no ofereixen velocitats de xifratge adequades per al xifratge d'imatges i arxius grans, és per això que són xifrats mitjançant els mètodes simètrics. La seguretat dels mètodes de xifratge de clau pública es veu compromesa pels avenços en tècniques d'algoritmes i teoria de nombres, necessitant cada vegada claus més llargues per poder garantir la seguretat. A més, amb la irrupció de la computació quàntica, els ordinadors quàntics podrien ser capaços de desxifrar aquests mètodes.

D'altra banda, tot i que més segura, la criptografia de clau privada també podria ser amenaçada pels diferents avenços en tècniques de criptoanàlisi i de computació quàntica.

Aquests fets provoquen que la criptografia s'enfronti a nous reptes contínuament i s'intentin trobar solucions a aquests problemes, explorant diferents àmbits més enllà de la criptografia i la criptoanàlisi. Entre aquestes solucions trobem l'aplicació matemàtica dels sistemes no lineals i la teoria del caos, que juntament amb la criptografia originen la «criptografia caòtica».

Els mètodes de xifratge basats en la teoria del caos poden classificar-se en dos grans grups:

- Criptosistemes basats en caos en temps continu. Utilitzen la sincronització dels sistemes dinàmics caòtics continus i seran els que desenvoluparem en el treball, en particular utilitzant el sistema de Lorenz.
- Criptosistemes basats en caos en temps discret. En aquest tipus de criptosistemes s'utilitzen sistemes dinàmics caòtics discrets, destaquem principalment *l'aplicació logística* definida per $x_{n+1} = rx_n(1 - x_n)$.

Aquests mètodes de xifratge poden ser utilitzats per xifrar: àudios [27], imatges [28], text [29], per generar claus de xifratge [30] i d'altres aplicacions que es puguin trobar en l'àmbit de la criptografia. En aquest treball ens centrarem principalment en el xifratge de senyals seguint el mètode proposat per Cuomo i Oppenheim [27].

La idea fonamental dels criptosistemes de caos continu és utilitzar un sistema dinàmic en règim caòtic per generar un senyal caòtic, i combinar-lo amb el missatge pla per produir un senyal d'aspecte inintel·ligible que és el missatge xifrat que es transmet per un canal insegur. A continuació, mitjançant la sincronització d'aquests sistemes, el receptor combina el senyal rebut i el senyal caòtic mitjançant l'operació inversa recuperant el missatge original.

Els esquemes de xifratge caòtics continus es diferencien entre si pel tipus de sincronització emprada i per la manera com es transmet el missatge. D'entre els mètodes més comuns per xifrar missatges trobem: l'emmascarament caòtic, els sistemes de commutació caòtica, modulació caòtica i d'altres mètodes presentats en [26].

En aquest treball destaquem l'emmascarament caòtic, perquè serà el que utilitzarem posteriorment considerant, en particular, el sistema de Lorenz com a sistema caòtic. Com es mostra en la Figura 14 el missatge $m(t)$ s'afegeix al senyal d'emmascarament caòtic $x(t)$ originant el senyal de transmissió $s(t)$ que és enviat al receptor. El sistema caòtic del receptor produeix una altra còpia del senyal emmascarat $x_r(t)$ que es resta al senyal transmès $s(t)$ per obtenir el missatge recuperat $\hat{m}(t)$.

Si assumim que tenim sincronització perfecta entre els dos sistemes tindrem que $x(t) = x_r(t)$ i, en conseqüència, $m(t) = \hat{m}(t)$.

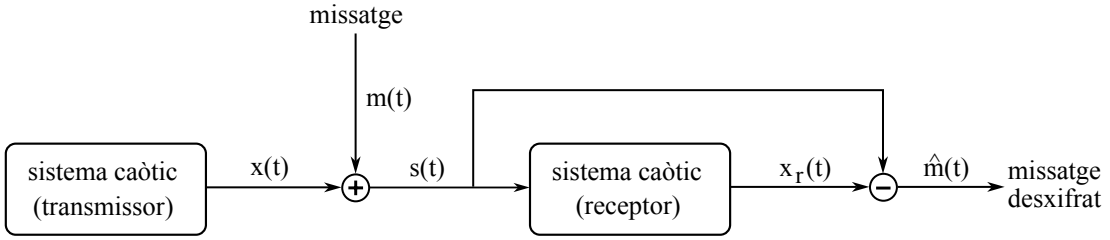

Figura 14: Esquema d'emmascarament caòtic.

Les propietats com alta sensibilitat a les condicions inicials, determinisme i mescla topològica fan atractius els sistemes caòtics des del punt de vista de la criptografia, perquè podríem equiparar aquestes propietats a les característiques de confusió i difusió de la criptografia descrites en (3.1).

Els criptosistemes caòtics basats en la generació d'una seqüència pseudoaleatòria per emmascarar el missatge han de posseir almenys les següents propietats:

1. Sensibilitat respecte dels paràmetres. La lleugera variació d'un dels paràmetres del sistema provoca que les trajectòries obtingudes a partir d'una mateixa condició inicial se separin exponencialment.

2. Sensibilitat respecte de les condicions inicials. Dues trajectòries assolides a partir de dos punts inicials x_0 i x_0' arbitràriament pròxims han de separar-se exponencialment.

3. Mescla topològica. La trajectòria caòtica generada a partir d'una regió aleatòria de l'espai de fases pot cobrir la resta de l'espai de fases a mesura que la trajectòria evoluciona, la qual cosa és una característica atractiva en el caos, ja que és anàloga a la propietat de distribució uniforme en criptografia.

3.5 Emmascarament caòtic mitjançant el sistema de Lorenz

Utilitzant el principi de sincronització caòtica estudiada en 3.2, Cuomo i Oppenheim [27] presentaren un mètode de comunicació privada basat en el mètode d'emmascarament caòtic descrit en la Figura 14, utilitzant el sistema de Lorenz.

És molt important ressaltar que aquest procediment es pot dur a terme gràcies al fet que la capacitat de sincronització del sistema de Lorenz és robusta, és a dir, no és altament sensible a les pertorbacions en el senyal $x(t)$ enviat pel transmissor. Aquest fet, ens permet sincronitzar el senyal emmascarat. Cuomo, Oppenheim i Strogatz [31] estudiaren la robustesa d'aquest esquema. Cal remarcar que aquesta idea no es limita només al sistema de Lorenz, sinó que té un potencial més ampli. Per exemple utilitzant altres sistemes caòtics com el sistema de Rössler [32] i el sistema de Chua [33].

De manera similar a la configuració de la sincronització caòtica 3.2, tenim dos sistemes de Lorenz transmissor i receptor connectats per la variable caòtica contínua $x(t)$. Tanmateix, en aquest cas, la variable enviada pel sistema transmissor és modificada afegint la component del missatge $m(t)$. A continuació, usant la variable enviada pel transmissor $s(t)$ el receptor se sincronitza amb la dinàmica del sistema emissor. Finalment, el receptor resta la dinàmica caòtica $x_r(t)$ al senyal rebut $s(t)$ i obté el missatge $\hat{m}(t)$. La Figura 15 mostra el diagrama d'aquest procediment.

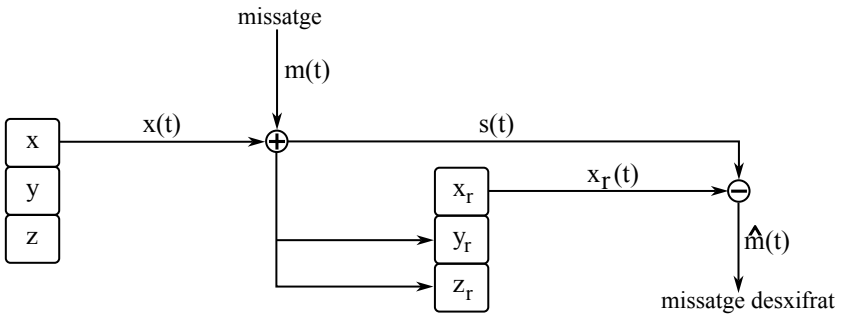

Figura 15: Esquema emmascarament caòtic en el cas del sistema de Lorenz.

En aquesta configuració, el sistema transmissor (3.20) ve definit per les mateixes equacions que en el cas estudiat en la sincronització caòtica del sistema de Lorenz

$$\begin{aligned} \dot{x} &= \sigma(y - x), \\ \dot{y} &= rx - y - xz, \\ \dot{z} &= xy - bz. \end{aligned} \tag{3.20}$$

En canvi, el sistema receptor (3.21) es comporta segons la següent equació:

$$\begin{aligned} \dot{x}_r &= \sigma(y_r - x_r), \\ \dot{y}_r &= rs(t) - y_r - s(t)z_r, \\ \dot{z}_r &= s(t)y_r - bz_r, \end{aligned} \tag{3.21}$$

on $s(t) = x(t) + m(t)$ i $m(t)$ és la component missatge. El missatge recuperat en el sistema receptor és $\hat{m}(t) = s(t) - x_r(t)$.

Hi ha un parell de comentaris a fer sobre aquest enfocament d'emmascarament del senyal. En primer lloc, el procés d'emmascarament i posterior desemmascarament és imperfecte. Tanmateix, de manera anecdòtica, quan $m(t)$ és un senyal d'àudio, el missatge es pot discernir en $\hat{m}(t)$ amb

algun soroll addicional. En segon lloc, la magnitud del senyal, $m(t)$, ha de ser molt inferior a la de la dinàmica del sistema de Lorenz $x(t)$ per a una recuperació eficaç. Tot i que això és analíticament difícil de mostrar, és intuïtivament obvi, ja que $m(t)$ és una pertorbació del senyal de sincronització caòtica. Per tant, una pertorbació més gran provoca un error més gran en la sincronització entre el sistema emissor i receptor, en particular, entre $x(t)$ i $x_r(t)$, i un error posterior més gran en el senyal recuperat.

3.6 Simulació numèrica

Seguint l'esquema de la secció anterior 3.5 considerem els dos sistemes de Lorenz (3.20) i (3.21), transmissor i receptor, amb els paràmetres clàssics $\sigma = 10$, $b = \frac{8}{3}$ *i* $r = 28$. L'experiment original dels autors [27] fou implementat mitjançant dos circuits electrònics, en el nostre cas, però, hem implementat el procés de xifratge i desxifratge mitjançant la integració numèrica dels dos sistemes (3.20) i (3.21) usant el mètode d'Euler i Runge-Kutta d'ordre 4, veure A. Per a realitzar els experiments, hem escollit com a missatge un senyal sinusoïdal $m(t) = A\sin(\omega t)$ i com a clau privada que el transmissor li envia al receptor: els paràmetres σ, b, r, el temps inicial i final d'integració i el pas d'integració. El senyal que condueix el receptor (3.21) és $s(t) = m(t) + x(t)$.

Per a la integració numèrica hem escollit temps inicial $t = 0$ i temps final $t = 50$ amb pas fix $h = 0.01$, així doncs obtenim els temps uniformes $\{t_i = ih |\ i = 0, \dots, 5000\}$. D'aquesta manera, per a cada i, el transmissor (3.20) genera el vector $\big(x(t_i), y(t_i), z(t_i)\big)$ i realitzant l'emmascarament caòtic, presentat en la secció 3.5, envia al receptor (3.21) $s(t_i) = m(t_i) + x(t_i)$. El receptor al seu torn, integra numèricament (3.21) per a cada i, generant el vector $\big(x_r(t_i), y_r(t_i), z_r(t_i)\big)$. Un cop obtingut aquest el vector, el receptor (3.21) obté el missatge recuperat $\hat{m}(t_i) = s(t_i) - x_r(t_i)$, per a cada i.

Com hem comentat en 3.5 la recuperació del missatge $\hat{m}(t)$ és imperfecte quan $m(t) \neq 0$. Observem que quan tenim $m(t) = 0$ la sincronització entre transmissor i receptor ràpidament convergeix, veure Figura 16.

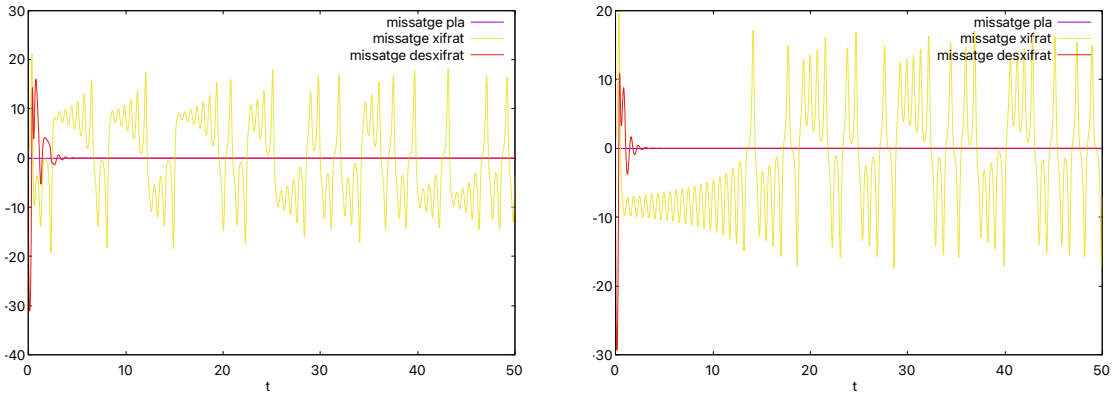

Figura 16: A l'esquerra, missatge pla $m(t) = 0$, xifrat $s(t)$ i desxifrat $\hat{m}(t)$ usant el mètode d'Euler amb $x_0 = (1, 1, 1)$ i $x_0^r = (10, 45, 34)$. A la dreta, mateixes condicions fent servir Runge-Kutta 4.

Tal com hem comentat en la secció anterior 3.5, una pertorbació més gran en el missatge $m(t)$ provoca un error més gran en la sincronització entre sistema emissor i sistema receptor, en particular entre el senyal transmès $x(t)$ i el senyal recuperat $x_r(t)$, ja que $\hat{m}(t) - m(t) = m(t) + x(t) - x_r(t) - m(t) = x(t) - x_r(t)$. Això, ens porta a preguntar-nos com canvia l'error entre el missatge original i el recuperat quan variem el senyal $m(t)$. En particular, estudiarem com canvia l'error $e(t) = |m(t) - \hat{m}(t)|$ quan varia l'amplitud A del nostre senyal $m(t) = A\sin(10t)$.

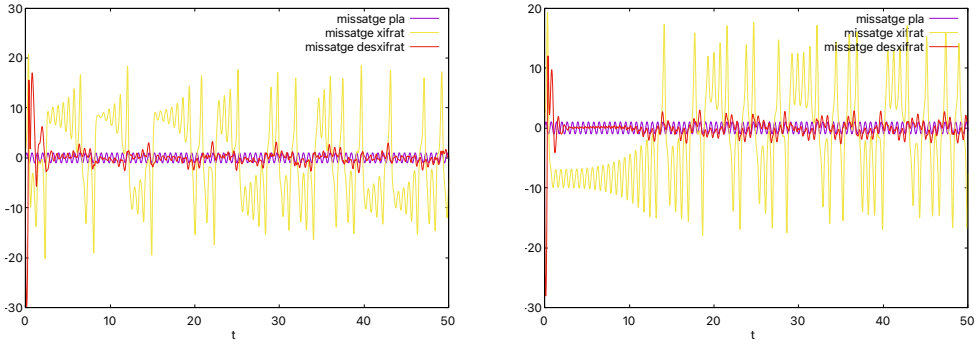

Figura 17: A l'esquerra missatge pla $m(t) = \sin(10t)$, xifrat $s(t)$ i desxifrat $\hat{m}(t)$ usant el mètode d'Euler amb $x_0 = (1, 1, 1)$ i $x_0^r = (10, 45, 34)$. A la dreta, usant el mètode Runge-Kutta 4 amb les mateixes condicions inicials.

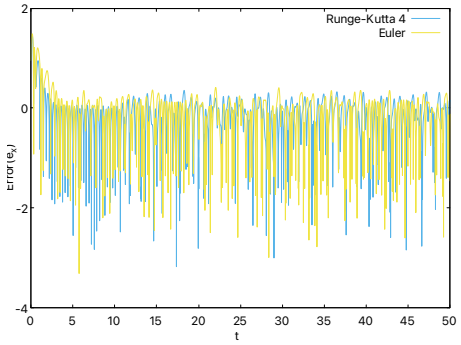

Figura 18: Error $\log_{10}(|m(t) - \hat{m}(t)|) = \log_{10}(|x(t) - x_r(t)|)$ dels missatges $m(t)$ i $\hat{m}(t)$ de la Figura 17

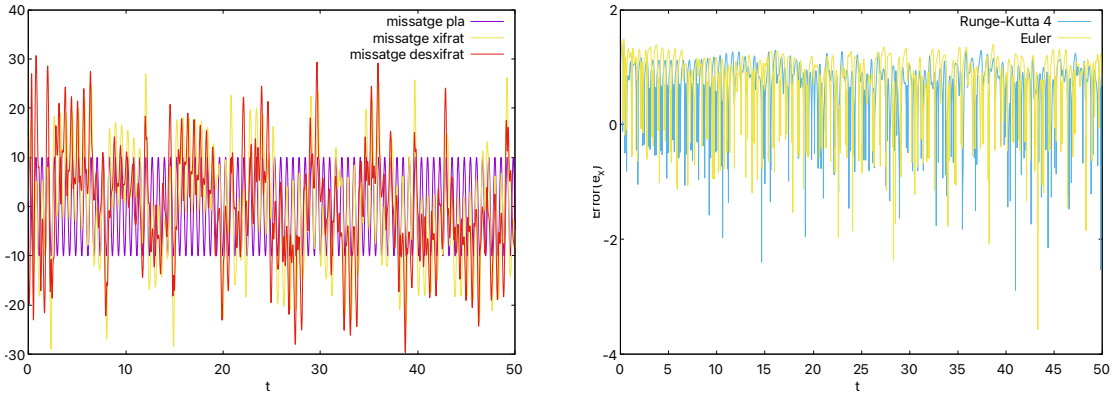

Figura 19: A l'esquerra, missatge pla $m(t) = 10\sin(10t)$, xifrat $s(t)$ i desxifrat $\hat{m}(t)$ usant el mètode d'Euler amb $x_0 = (1, 1, 1)$ i $x_0^r = (10, 45, 34)$. A la dreta, l'error $\log_{10}(|m(t) - \hat{m}(t)|)$ entre el mètode d'Euler i Runge-Kutta 4 del mateix missatge $m(t) = 10\sin(10t)$, del gràfic esquerre, i mateixes condicions inicials.

La Figura 17 mostra el xifratge i desxifratge, mitjançant els dos mètodes d'integració: Euler i Runge-Kutta 4, del senyal $m(t) = \sin(10t)$, és a dir, $A = 1$. D'altra banda, la Figura 19 mostra el xifratge i desxifratge, mitjançant el mètode d'Euler, del senyal $m(t) = 10\sin(10t)$, és a dir, $A = 10$.

Primer de tot, observem, veure Figura 18, que no hi ha una diferència significativa en l'error entre el missatge original $m(t)$ i recuperat $\hat{m}(t)$ usant el mètode d'Euler i el mètode Runge-Kutta 4. Segon, l'error entre $m(t)$ i $\hat{m}(t)$ és superior quan $A = 10$ a quan $A = 1$, veure Figura 18 i 19. En general, veiem com l'error creix quan l'amplitud augmenta, veure 20. A continuació, intentarem veure quina relació existeix entre el missatge original i el recuperat quan variem els valors de l'amplitud A.

Per fer palès aquesta relació entre amplitud i error, hem generat dos gràfics, veure Figura 20. En ells es mostra com varia l'error entre $m(t)$ i $\hat{m}(t)$ a mesura que augmentem l'amplitud A. Per fer-ho, hem xifrat i desxifrat el senyal $m(t) = A\sin(10t)$ mitjançant el mètode d'Euler des de $t = 0$ fins a $t = 50$ amb pas fix $h = 0.01$ variant A des de $A = 0$ fins $A = 20$ amb pas fix 0.001. Per estudiar la dependència entre error i amplitud, hem realitzat una regressió lineal simple, veure Figura 20. En particular, hem obtingut $\log(|m(t) - \hat{m}(t)|) = 0.9594\log(A) + 0.9785$. Així doncs, $|m(t) - \hat{m}(t)| = 2.6605Ae^{0.9594}$, és a dir, $|m(t) - \hat{m}(t| \approx \mathcal{O}(A)$.

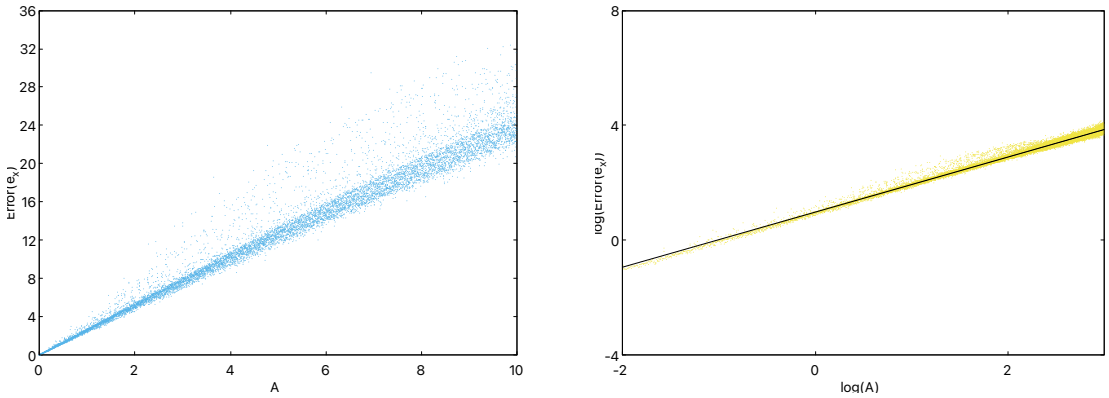

Figura 20: A l'esquerra, recuperació de l'error en la norma L^∞ en funció de l'amplitud del senyal quan xifrem el missatge $m(t) = A\sin(10t)$. A la dreta, gràfica en escala logarítmica en l'eix d'ordenades i abscisses de l'error en norma L^∞ en funció de l'amplitud. Mitjançant regressió simple obtenim la recta $\log(e_x) = 0.9594\log(A) + 0.9785$.

3.7 Criptoanàlisi de l'emmascarament càotic

Per avaluar la seguretat d'un criptosistema cal investigar l'impacte que causarien tots els possibles mètodes criptoanalítics coneguts sobre el criptosistema. Pels sistemes d'emmascarament caòtic existeixen diversos tipus d'atacs. Els més coneguts són: anàlisi de l'aplicació de retorn, anàlisi de la potència espectral i mètodes d'estimació de paràmetres, veure [26].

En particular, el mètode proposat d'emmascarament caòtic mitjançant el sistema de Lorenz 3.5 ja ha estat desxifrat en el treball de [26] mitjançant el mètode d'estimació dels paràmetres del sistema de Lorenz, que representen la clau del criptosistema.

Per utilitzar aquests mètodes només és necessari conèixer el text xifrat i la variable utilitzada per a sincronitzar els sistemes transmissor i receptor. Com que s'usen els valors dels paràmetres com a clau es podria considerar un atac per «força bruta» provant totes les combinacions possibles dels paràmetres, però l'esforç i el temps requerits serien molt considerables. Tanmateix, mitjançant l'explotació d'algunes característiques geomètriques del sistema caòtic estudiades en [26], aquestes

relacionen els punts d'equilibri amb els paràmetres. Aquest fet permet reduir molt l'espai de claus possibles i fa possible un atac per obtenir la clau del sistema.

Per solucionar aquests problemes de seguretat, s'han proposat diverses mesures que augmenten la seguretat, com per exemple emprar sistemes dinàmics més complexos. Entre els sistemes suggerits, trobem el conegut com a sistema de Lorenz hipercaòtic [34]. L'hipercaos ha cridat l'atenció per proporcionar formes d'ona més complexes que els sistemes caòtics simples, millorant així el procés d'emmascarament. Això es deu al fet que l'hipercaos es caracteritza per tenir almenys dos exponents positius de Lyapunov, mentre que els altres sistemes caòtics només en presenten un. A continuació, donem un exemple d'un sistema de Lorenz modificat que mostra comportament hipercaòtic, veure [35].

$$\begin{aligned} \dot{x} &= \sigma(y - x) + u, \\ \dot{y} &= -xz + rx - y, \\ \dot{z} &= xy - bz, \\ \dot{u} &= -xz + du, \end{aligned} \tag{3.22}$$

on $\sigma = 10$, $b = \frac{8}{3}$, $r = 28$ i $d = 1.3$. Els quatre exponents de Lyapunov del sistema (3.22) calculats en [35] són $\lambda_1 = 0.39854$, $\lambda_2 = 0.24805$, $\lambda_3 = 0$ i $\lambda_4 = -12.913$. Observem com (3.22) té 2 exponents de Lyapunov positius i, per tant, és hipercaòtic.

4 Conclusions

En aquest treball hem estudiat diferents aspectes dinàmics del sistema de Lorenz. En particular, hem presentat i demostrat algunes propietats bàsiques, l'existència d'un atractor global i hem descrit els diferents règims de comportament pels paràmetres clàssics en funció del paràmetre r. A continuació, hem utilitzat el sistema de Lorenz, per paràmetres pels quals presenta l'atractor estrany, per il·lustrar la sincronització del caos presentada per Pecora i Carroll [23] i explorar l'enfocament exposat per Cuomo i Oppenheim [27] per a l'emmascarament de senyals mitjançant la sincronització caòtica. Mitjançant experiments numèrics, hem investigat la relació entre la recuperació del senyal i l'amplitud A del senyal, i hem vist que $e_x \approx \mathcal{O}(A)$.

Una gran part dels sistemes de xifratge basats en caos s'han demostrat gràcies a treballs criptoanalítics que no són segurs, ja que és possible extraure informació sobre els paràmetres. La possibilitat d'atacs per estimar els paràmetres és considerat el problema més gran en la majoria d'aquests sistemes, és per això, que aquest fet mereix més atenció en investigacions futures. La combinació de diversos mètodes de xifratge i sistemes més complexos, com per exemple usant l'hipercaos [34], poden ser una via prometedora per obtenir sistemes criptogràfics més segurs.

La criptografia caòtica és un camp actiu d'investigació, demostrat per la gran quantitat d'articles que es publiquen actualment. La teoria del caos té característiques que s'adapten a l'ús criptogràfic i pot utilitzar-se, per exemple, per millorar els dissenys de sistemes de xifratge tradicionals. Dos dels problemes principals són la velocitat de xifratge i la implementació numèrica. Per tant, futurs estudis es poden centrar a millorar la velocitat de xifratge i reduir l'error en la integració numèrica per tal de poder millorar els criptosistemes caòtics i fer-los viables dins del món criptogràfic.

A Annexos

A.1 Integració numèrica

Mètode d'Euler

Considerem una EDO de problema de valor inicial

$$\dot{x} = f(t, x),\ x(0) = x_0,$$

on $x \in \mathbb{R}^n$. Els mètodes d'un pas estan generats per una funció $\phi(t, x; h; f)$, que escriurem $\phi(t, x; h)$ per tal de simplificar la notació. Començant des del valor inicial (t_0, x_0) i iterant, anem obtenint les aproximacions $\eta_i \approx x(t_i)$ de la solució exacta $x(t)$. Tenim la iteració següent:

$$\begin{aligned} &\eta_0 = x_0, \\ &\eta_{i+1} = \eta_i + h\phi(x_i, \eta_i; h), \\ &t_{i+1} = t_i + h. \end{aligned} \tag{A.1}$$

El mètode d'Euler s'obté observant que per a $h \neq 0$,

$$\frac{x(t+h) - x(t)}{h} \approx f(t, x(t)),\ \textit{i per tant, } x(t+h) \approx x(t) + hf(t, x(t)).$$

Escollint el pas $h \neq 0$ i seguint l'esquema anterior (A.1) obtenim

$$\begin{aligned} &\eta_0 = x_0, \\ &\eta_{i+1} = \eta_i + hf(t_i, \eta_i), \\ &t_{i+1} = t_i + h. \end{aligned}$$

Així doncs, pel mètode d'Euler tenim $\phi(t, x, h) = f(t, x(t))$. El mètode d'Euler és d'ordre 1.

Mètode Runge-Kutta 4

El mètode Runge-Kutta d'ordre 4 també és un mètode d'un pas. La resolució més usada del mètode Runge-Kutta d'ordre 4 és la següent

$$\phi(t, x; h) = \frac{1}{6}(k_1 + 2k_2 + 2k_3 + k_4),$$

on

$$\begin{aligned} k_1 &= f(t, x), \\ k_2 &= f(t + \frac{1}{2}h, x + \frac{1}{2}hk_1), \\ k_3 &= f(t + \frac{1}{2}h, x + \frac{1}{2}hk_2), \\ k_4 &= f(t + h, x + hk_3). \end{aligned}$$

Observació A.1. En situacions on cal una integració numèrica del problema de valor inicial precisa cal ajustar el pas h d'integració per garantir un error local petit. Així, per exemple, s'utilitzen mètodes Runge-Kutta-Fehlberg amb aquesta finalitat, com per exemple el mètode RK45. En aquest treball, l'error de propagació no és important, ja que és pot considerar part del soroll del xifratge del missatge.

A.2 Càlcul dels exponents de Lyapunov de sistemes dinàmics continus

Considerem $\dot{x} = f(x),\ x(0) = x_0$ un sistema de n equacions diferencials, on f és de classe C^1. Sigui $\phi_t(x)$ el seu flux associat. Seguint els passos de la secció 2.11, acabem obtenint l'equació (2.28) que definim com (2.29). Considerem, per tant,

$$\begin{aligned} &\dot{Y}(t) = J(t)Y(t), \\ &Y(0) = I. \end{aligned} \tag{A.2}$$

La descomposició QR és una eina teòrica i numèrica per calcular els exponents de Lyapunov. En comptes d'integrar (A.2) directament, busquem la descomposició $Y(t) = Q(t)R(t)$, on $Q(t)$ és ortogonal i $R(t)$ triangular superior amb elements a la diagonal positius. Substituint $Y(t) = Q(t)R(t)$ en (A.2) obtenim

$$\dot{Q}(t)R(t) + Q(t)\dot{R}(t) = J(t)Q(t)R(t), \tag{A.3}$$

aleshores multiplicant (A.3) a l'esquerra per Q^T i a la dreta per R^{-1} a ambdues bandes de la igualtat obtenim

$$Q^T\dot{Q} + \dot{R}R^{-1} = Q^T J Q. \tag{A.4}$$

Com que $Q^TQ = I$, ja que és ortogonal, $Q^T\dot{Q}$ és antisimètrica. D'altra banda, $\dot{R}R^{-1}$ és triangular superior.

Multiplicant (A.3) a la dreta per R^{-1} a ambdues bandes de la igualtat obtenim

$$\dot{Q} = (I - QQ^T)JQ + QQ^T\dot{Q}, \quad Q(0) = 0.$$

Com que $Q^TQ = I$, $\dot{Q} = QS$, on

$$S_{ij} = \begin{cases} (Q^TJQ)_{ij}, & si\ i > j, \\ 0, & si\ i = j, \\ -(Q^TJQ)_{ij}, & si\ i < j, \end{cases} \tag{A.5}$$

i al ser $Q^T\dot{Q}$ antisimètrica, de (A.4) obtenim

$$\dot{R}_{ii}R_{ii}^{-1} = (Q^TJQ)_{ii},$$

on R_{ii} són els elements de la diagonal de $R(t)$. Llavors, quan $t \to +\infty$ els exponents de Lyapunov estan relacionats amb els elements de la diagonal, veure [36], i obtenim

$$\lambda_i = \lim_{t\to+\infty} \frac{1}{t}\log(R_{ii}),\ 1 \le i \le n.$$

Referències

[1] E. Lorenz, "Deterministic nonperiodic flow," *Journal of Atmospheric Sciences*, vol. 20, no. 2, pp. 130–141, 1963.

[2] B. Saltzman, "Finite amplitude free convection as an initial value problem," *Journal of the Atmospheric Sciences*, vol. 19, no. 329, 1962.

[3] J. Sotomayor, *Liçoes de equações diferenciais ordinárias*. Rio de Janeiro: Instituto de Matemática Pura e Aplicada, 1979.

[4] A. M. LYAPUNOV, "The general problem of the stability of motion," *International Journal of Control*, vol. 55, no. 3, pp. 531–534, 1992. [Online]. Available: https://doi.org/10.1080/00207179208934253

[5] W. R. F. Guckenheimer, John, "Structural stability of lorenz attractors," *Publications Mathématiques de l'IHÉS*, vol. 50, pp. 59–72, 1979. [Online]. Available: http://eudml.org/doc/103965

[6] S. Smale, "Mathematical problems for the next century," *The Mathematical Intelligencer*, vol. 20, 02 2000.

[7] W. Tucker, "A rigorous ode solver and smale's 14th problem," *Foundations of Computational Mathematics*, vol. 2, pp. 53–117, 02 2002.

[8] Z. Nitecki, *Dyfferenciable Dynamics*. M.I.T. Press, 1971.

[9] A. Kelley, "The stable, center-stable, center, center-unstable, unstable manifolds," *Journal of Differential Equations*, vol. 3, no. 4, pp. 546–570, 1967. [Online]. Available: https://www.sciencedirect.com/science/article/pii/0022039667900162

[10] P. H. John Guckenheimer, *Nonlinear Oscillations, Dynamical Systems, and Bifurcations of Vector Fields*. New York: Springer New York, 1983.

[11] C. Sparrow, *The Lorenz Equations: Bifurcations, Chaos, and Strange Attractors*. New York: Springer-Verlag, 1982.

[12] E. J. Doedel, B. Krauskopf, and H. M. Osinga, "Global organization of phase space in the transition to chaos in the lorenz system," *Nonlinearity*, vol. 28, no. 11, p. R113, oct 2015. [Online]. Available: https://dx.doi.org/10.1088/0951-7715/28/11/R113

[13] D. Viswanath, "The fractal property of the lorenz attractor," *Physica D: Nonlinear Phenomena*, vol. 190, pp. 115–128, 03 2004.

[14] A. Wolf, J. Swift, H. Swinney, and J. Vastano, "Determining lyapunov exponents from a time series," *Physica D: Nonlinear Phenomena*, vol. 16, pp. 285–317, 07 1985.

[15] J. P. Eckmann and D. Ruelle, "Ergodic theory of chaos and strange attractors," *Rev. Mod. Phys.*, vol. 57, pp. 617–656, Jul 1985. [Online]. Available: https://link.aps.org/doi/10.1103/RevModPhys.57.617

[16] D. Viswanath, "The fractal property of the lorenz attractor," *Physica D: Nonlinear Phenomena*, vol. 190, pp. 115–128, 03 2004.

[17] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[18] C. Shannon, "A mathematical theory of communication," *The Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, 1948.

[19] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[20] J. Daemen and V. Rijmen, "The block cipher rijndael," *Lecture Notes in Computer Science - LNCS*, vol. 1820, pp. 277–284, 01 1998.

[21] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, p. 120–126, feb 1978. [Online]. Available: https://doi.org/10.1145/359340.359342

[22] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469–472, 1985.

[23] L. Pecora and T. Carroll, "Synchronization in chaotic system," *Physical Review Letters*, vol. 64, p. 821, 03 1990.

[24] L. M. Pecora and T. Carroll, "Driving systems with chaotic signals," *Phys. Rev. A*, vol. 44, pp. 2374–2383, Aug 1991. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.44.2374

[25] J. P. Eckmann, S. O. Kamphorst, D. Ruelle, and S. Ciliberto, "Liapunov exponents from time series," *Phys. Rev. A*, vol. 34, pp. 4971–4979, Dec 1986. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.34.4971

[26] A. Orúe, "Contribución al estudio del criptoánalisis y diseño de los criptosistemas caóticos," Ph.D. dissertation, ETSIT UPM, 2013.

[27] K. Cuomo, A. Oppenheim, and S. Strogatz, "Synchronization of lorenz-based chaotic circuits with applications to communications," *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, vol. 40, no. 10, pp. 626–633, 1993.

[28] O. Al-Hazaimeh, M. Al-Jamal, N. Alhindawi, and A. Omari, "Image encryption algorithm based on lorenz chaotic map with dynamic secret keys," *Neural Computing and Applications*, vol. 31, pp. 1–11, 07 2019.

[29] R. He and P. G. Vaidya, "Implementation of chaotic cryptography with chaotic synchronization," *Phys. Rev. E*, vol. 57, pp. 1532–1535, Feb 1998. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevE.57.1532

[30] A. S. Bader, S. Hameed, and M. A. A. K., "Key generation based on henon map and lorenz system," *Al-Mustansiriyah Journal of Sciences*, vol. 31, pp. 41–46, 2020.

[31] K. M. CUOMO, A. V. OPPENHEIM, and S. H. STROGATZ, "Robustness and signal recovery in a synchronized chaotic system," *International Journal of Bifurcation and Chaos*, vol. 03, no. 06, pp. 1629–1638, 1993. [Online]. Available: https://doi.org/10.1142/S021812749300129X

[32] P. Canyelles-Pericas and K. Busawon, "High gain observer with algorithm transformation to extended jordan observable form for chaos synchronization applications," *2014 UKACC International Conference on Control, CONTROL 2014 - Proceedings*, pp. 262–267, 10 2014.

[33] L. Kocarev, K. S. Halle, K. Eckert, L. O. Chua, and U. Parlitz, "Experimental demonstration of secure communications via chaotic synchronization," *Int. J. Bifurcation Chaos*, vol. 2, pp. 709–713, Sept 1992.

[34] S. Cang, Z. Chen, and Z. Yuan, "Analysis and circuit implementation of a new four-dimensional non-autonomous hyper-chaotic system," *Acta Physica Sinica*, vol. 57, 03 2008.

[35] Q. Jia, "Hyperchaos generated from the lorenz chaotic system and its control," *Physics Letters A*, vol. 366, no. 3, pp. 217–222, 2007. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0375960107002186

[36] L. Dieci, R. Russell, and E. Vleck, "On the compuation of lyapunov exponents for continuous dynamical systems," *Siam Journal on Numerical Analysis - SIAM J NUMER ANAL*, vol. 34, 02 1997.