

# INSTITUTO POTOSINO DE INVESTIGACIÓN CIENTÍFICA Y TECNOLÓGICA, A.C.

## POSGRADO EN CONTROL Y SISTEMAS DINÁMICOS


# GENERACIÓN DE SECUENCIAS SEUDO-ALEATORIAS CON BASE EN SISTEMAS DINÁMICOS DISCRETOS

Tesis que presenta


**Carlo Aurelio Beltrán González**


Para obtener el grado de

## Maestro en Control y Sistemas Dinámicos


**Director de la Tesis:**

Dr. Eric Campos Cantón



San Luis Potosí, S.L.P., Diciembre de 2017

IPICYT

# Constancia de aprobación de la tesis

La tesis ***"Generación de secuencias seudo-aleatorias con base en sistemas dinámicos discretos"*** presentada para obtener el Grado de Maestro en Ciencias en Biología Molecular fue elaborada por **Carlo Aurelio Beltrán González** y aprobada el ocho de diciembre del dos mil diecisiete por los suscritos, designados por el Colegio de Profesores de la División de Matemáticas Aplicadas del Instituto Potosino de Investigación Científica y Tecnológica, A.C.

**Dr. Eric Campos Cantón**
Director de la tesis

**Dr. Hugo Cabrera Ibarra**
Jurando en el Examen

**Dr. Javier Salvador González Salas**
Jurando en el Examen

**Dr. Juan Gonzalo Barajas Ramírez**
Jurando en el Examen


# Créditos institucionales

Esta tesis fue elaborada en la División de Matemáticas Aplicadas del Instituto Potosino de Investigación Científica y Tecnológica, A. C., bajo la dirección del Dr. Eric Campos Cantón.

Durante la realización del trabajo el autor recibió una beca académica del Consejo Nacional de Ciencia y Tecnología No. 337124 y del Instituto Potosino de Investigación Científica y Tecnológica, A. C.

IPICYT

# Instituto Potosino de Investigación Científica y Tecnológica, A.C.

## Acta de Examen de Grado

El Secretario Académico del Instituto Potosino de Investigación Científica y Tecnológica, A.C., certifica que en el Acta 025 del Libro Primero de Actas de Exámenes de Grado del Programa de Maestría en Control y Sistemas Dinámicos está asentado lo siguiente:

En la ciudad de San Luis Potosí a los 8 días del mes de diciembre del año 2017, se reunió a las 12:00 horas en las instalaciones del Instituto Potosino de Investigación Científica y Tecnológica, A.C., el Jurado integrado por:

| | | |
|---|---|---|
| **Dr. Javier Salvador González Salas** | **Presidente** | **UPSLP** |
| **Dr. Hugo Cabrera Ibarra** | **Secretario** | **IPICYT** |
| **Dr. Eric Campos Cantón** | **Sinodal** | **IPICYT** |
| **Dr. Juan Gonzalo Barajas Ramírez** | **Sinodal** | **IPICYT** |

a fin de efectuar el examen, que para obtener el Grado de:

MAESTRO EN CONTROL Y SISTEMAS DINÁMICOS

sustentó el C.

**Carlo Aurelio Beltrán González**

sobre la Tesis intitulada:

***Generación de secuencias seudo-aleatorias con base en sistemas dinámicos discretos***

que se desarrolló bajo la dirección de

**Dr. Eric Campos Cantón**

El Jurado, después de deliberar, determinó

APROBARLO

Dándose por terminado el acto a las 13:20 horas, procediendo a la firma del Acta los integrantes del Jurado. Dando fe el Secretario Académico del Instituto.

A petición del interesado y para los fines que al mismo convengan, se extiende el presente documento en la ciudad de San Luis Potosí, S.L.P., México, a los 8 días del mes de diciembre de 2017.

**Dr. Horacio Flores Zúñiga**
Secretario Académico

**Mtra. Ivonne Lizette Cuevas Vélez**
Jefa del Departamento del Posgrado

INSTITUTO POTOSINO DE INVESTIGACIÓN CIENTÍFICA Y TECNOLÓGICA, A.C.
IPICYT
SECRETARIA ACADEMICA

*A todo aquel que considero un placer llamar familia y*
*a mi compañera de vida...*

# Índice general

# Índice de tablas

# Índice de figuras

**Resumen**

El “efecto mariposa” es un término que se acuñó para describir como una pequeña perturbación puede tener grandes repercusiones. Este concepto está relacionado con la sensibilidad a las condiciones iniciales que presenta el comportamiento caótico. Indica que la evolución a largo plazo de una órbita caótica que se genera al aplicar ecuaciones deterministas a una condición inicial con cualquier tipo de incertidumbre “no se puede predecir”; es decir, parece el resultado de un proceso aleatorio aunque es completamente determinista. En este documento se aprovecha las características del comportamiento caótico para construir generadores de bits seudo-aleatorios. Se propone una familia multimodal con base en un tipo de mapeo logístico; entre las ventajas que presenta es que al variar un parámetro de control se obtiene distintas dinámicas, caóticas incluidas. Se desarrolla un generador de bits con base en dicha familia. Por último se evalúa el generador de bits por medio del banco de pruebas estadísticas del Instituto Nacional de Estándares y Tecnología (NIST por sus siglas en Inglés) para verificar si éste produce secuencias indistinguibles de una aleatoria.

*Palabras clave: Caos, generador de bits seudo-aleatorios, NIST, sistemas dinámicos discretos.*

**Abstract**

The "butterfly effect" is a term born to describe how a little perturbation could have a lot of repercutions. This term is close to a property present in chaotic behavior, sensitivity to initial conditions. It indicates that the long-term evolution of a chaotic orbit generated from applying deterministic equations to an initial condition with any type of uncertainty "cannot be predicted". In other words, while it may seem like a random process it is completely deterministic. This document takes advantage of chaotic behavior to build pseudo-random bit generators. A multimodal family is proposed based on a type of logistic map. Among the advantages it presents, one is that when varying a control parameter it obtains distinct dynamics, including chaotic ones. A bit generator based on the multimodal family is developed. Lastly the bit generator is evaluated using the National Institute of Standards and Technology (NIST) statistical tests suit in order to verify if it produces sequences indistinguishable from random ones.

*Key words: Chaos, discrete dynamical systems, NIST, pseudo-random bit generator.*

# Capítulo 1

# Introducción

La interrogante planteada por Edward Lorenz en su artículo de 1972 [1] sobre: *Predictibilidad ¿El movimiento de las alas de una mariposa en Brasil podría comenzar un tornado en Texas?*[1], ha servido para aclarar conceptos en el área de los sistemas dinámicos no lineales. Frecuentemente el análisis de sistemas físicos se restringe a modelos matemáticos lineales debido a que son más sencillos de resolver que su contraparte no lineal; no obstante, la mayoría de los fenómenos naturales presentan características no lineales [2].

Uno de los pioneros en el análisis en los fenómenos naturales es Henri Poincaré, en 1890 estudia la posibilidad de que cada planeta continúe de manera indefinida en sus órbitas o que alguno se aproxime al sol o hacia la oscuridad del infinito [1]; aunque no encuentra una respuesta definitiva a esta pregunta, se convierte en un gran contribuyente de una de las mayores áreas de estudio en matemáticas, la *topología* [2] y; además, propone una idea de lo que implica el comportamiento caótico.

Tiempo más tarde, a causa del avance tecnológico que se obtuvo en la década de 1950 se pudo realizar nuevos experimentos; de manera puntual la *simulación por computadora de sistemas de ecuaciones diferenciales*. Lorenz en 1963 estudia un modelo reducido del clima representado por tres ecuaciones diferenciales mediante simulaciones por computadora y observa que no sólo su sistema parece exhibir comportamiento no periódico; sino también obtiene resultados distintos al cambiar las condiciones iniciales por otras aproximadamente iguales, una idea de lo que es el *caos determinista*.

[1] El título original corresponde a "Predictability: Does the Flap of a Butterfly's wings in Brazil Set Off a Tornado in Texas?"

Una característica necesaria y central en los sistemas dinámicos para exhibir caos determinista es la *sensibilidad a las condiciones iniciales* [3]; esto indica que la evolución de condiciones iniciales aproximadamente iguales es completamente distinta. Observe en la Figura 1.1 la evolución de los puntos iniciales $x_0 = 0.2$ y $x_0 = 0.2001$ al ser iterados bajo el *mapeo logístico*:

$$x_{n+1} = 4(1 - x_n)x_n, \tag{1.1}$$

note que para el instante $n = 8$ se observa una pequeña diferencia y para el $n = 13$ la evolución de ambos puntos iniciales es completamente distinta. Es por esto que se puede obtener un largo número de órbitas no correlacionadas que parecen aleatorias; sin embargo, son deterministas y se pueden reproducir al conocer el punto inicial [4]. Cabe mencionar que usualmente un sistema dinámico con comportamiento caótico tiene un *parámetro de control* para el cual el sistema bifurca.

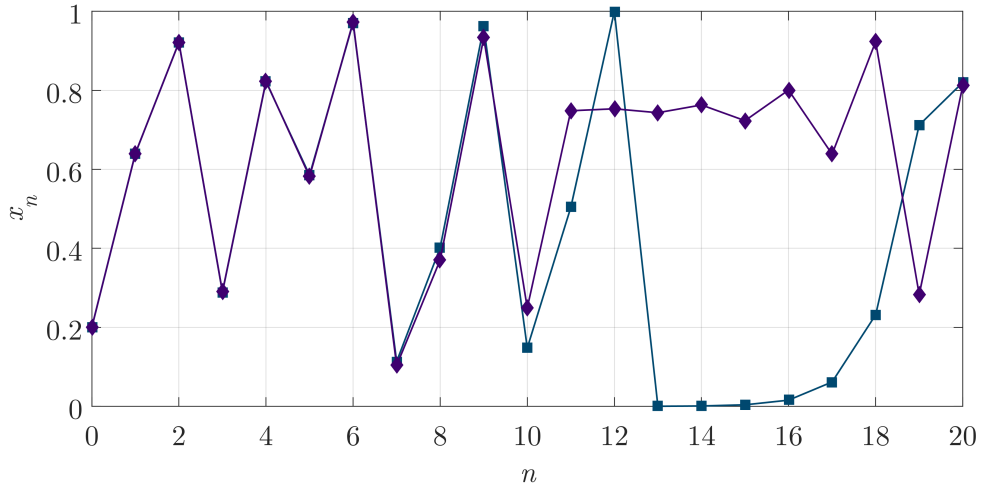



Figura 1.1: Exhibición de la sensibilidad a las condiciones iniciales que presenta un sistema dinámico con comportamiento caótico. La evolución de $x_0 = 0.2$ se representa por cuadros y la de $x_0 = 0.2001$ mediante rombos.

Los sistemas dinámicos con comportamiento caótico han servido para desarrollar sistemas criptográficos, Robert A. J. Matthews en 1989 se convierte en uno de los pioneros en esta área ya que desarrolla un cifrador con base en caos [5], su publicación al respecto ostenta el título: "*Sobre la derivación de un algoritmo de cifrado caótico*[2]" en el cual se sugiere la realización de un cifrador de flujo con base en el mapeo logístico

[2]El título original es *On the derivation of a "chaotic" encryption algorithm.*

generalizado que se presenta enseguida [6]:

$$x_{n+1} = g(\lambda, \alpha, \beta, x) = \lambda x_n(\alpha - x_n)^{\beta}, \tag{1.2}$$

donde $x$ es la variable de estado, $\lambda$, $\alpha$ y $\beta$ son parámetros del sistema.

## 1.1. Estado del arte

Debido al comportamiento *ergódico*, *sensibilidad a las condiciones iniciales*, *transitividad* y *evolución impredecible* los sistemas dinámicos con comportamiento caótico son idóneos para desarrollar generadores de números seudo-aleatorios [7]; algunas aplicaciones de estos generadores incluyen simulaciones numéricas, la industria de los videojuegos, comunicaciones [8] y sistemas criptográficos [9].

Los sistemas dinámicos discretos que se conforman por más de una moda se han estudiado por Smania en [10]; en dicho documento se analiza la dinámica del operador de renormalización para mapeos multimodales. Particularmente desarrolló una teoría combinatoria para cierto tipo de mapeos multimodales. Por otro lado, Campos *et al.* [11] muestran una construcción de mapeos multimodales con base en el mapeo logístico y muestran como dicho mapeo puede exhibir comportamiento caótico. García *et al.* desarrollan una aplicación de dichos mapeos multimodales. La aplicación consiste en un generador seudo-aleatorio de números que funge como el núcleo de un cifrador de flujo, ver [12].

Li y Sajeeth *et al.* recomiendan en [5, 13, 14] que para aumentar la seguridad y en algunos casos la eficiencia de los generadores de bits seudo-aleatorios se debe mezclar la salida de más de un mapeo caótico; de esto surge el interés por generar nuevos sistemas dinámicos tanto en tiempo discreto, como continuo. Pellicer-Lostao en 2008 publica un artículo de un generador que mezcla dos mapeos tipo logísticos de dos dimensiones; además, Patidar publica en 2009 dos artículos sobre este tipo de generadores con base en mapeos caóticos y realiza un análisis estadístico; en el primero usa dos *mapeos estándar* que se describen por:

$$\begin{aligned} x_{n+1} &= x_n + k \sin y_n \mod 2\pi, \\ y_{n+1} &= y_n + x_{n+1} \mod 2\pi, \end{aligned} \tag{1.3}$$

y en el segundo un par de *logísticos*; generan la secuencia al mezclar la salida de ambos mapeos en lo que se podría llamar una *función umbral variable* y realizan un análisis con base en dos bancos de pruebas estadísticas [15, 16, 17].

## 1.2. Objetivo general

Desarrollar un generador de bits seudo-aleatorios con base en sistemas dinámicos discretos con comportamiento caótico que se describan mediante funciones continuas por partes.

### 1.2.1. Objetivos específicos

- Construir una familia monoparamétrica con base en un sistema dinámico discreto que se forma con múltiples mapeos unimodales.
- Desarrollar un generador de bits mediante las series de tiempo caóticas generadas por medio de una familia multimodal.
- Caracterizar los generadores de bits que se obtienen mediante un banco de pruebas estadísticas.

## 1.3. Contenido

En este capítulo se introduce algunos de los fundamentos que permiten incorporar los sistemas dinámicos con comportamiento caótico al área de generadores de secuencias seudo-aleatorias; el estado del arte y los objetivos que llevan a la realización de este documento. En el capítulo dos se encuentran los conceptos y definiciones que se emplean en los capítulos posteriores; además, se establecen algunas convenciones y notaciones. En el capítulo tres se propone una familia multimodal con base en un tipo de mapeo logístico y el desarrollo de un generador de bits con base en ésta. En el capítulo cuatro se desarrolla un generador de bits con el método propuesto y éste se analiza mediante el banco de pruebas estadísticas del Instituto Nacional de Estándares y Tecnología. Para terminar, en el capítulo cinco se presentan las conclusiones que se obtuvo en el desarrollo de este trabajo y el trabajo a futuro que permitiría extender los resultados.

# Capítulo 2

# Preliminares

En este capítulo se presentan los conceptos básicos de las áreas de análisis matemático y sistemas dinámicos que serán usados en capítulos posteriores. Para mayor detalle se recomienda consultar [1, 18, 19].

## 2.1. Análisis matemático

Un conjunto es una colección de elementos y será denotado por $S = \{x : P(x)\}$, esto significa que $S$ es el conjunto de los elementos $x$ que satisfacen la condición $P(x)$. Un conjunto que tiene un único elemento se conoce como *unitario* y uno que carece de elementos se llama *vacío* y se denota por $\varnothing$.

Una regla $f$ que asigna a cada elemento de un conjunto no vacío $X$ un único elemento de un conjunto $Y$ se llama *función o mapeo de* $X$ a $Y$ y se denota por:

$$f : X \to Y, \tag{2.1}$$

a $X$ se le conoce como el *dominio* de $f$ y al conjunto $\{f(x) : x \in X\}$ como el *rango* o *imagen* de $f$; conviene subrayar que el rango de $f$ se puede distinguir del espacio objetivo de $f$ que es $Y$. Si la imagen de $f$ es todo $Y$, $f$ se llama *sobreyectiva*; en caso de que $f(x) = f(y)$ siempre que $x = y$, la función $f$ se conoce como *inyectiva*; una función que es sobreyectiva e inyectiva se llama *biyectiva* [20].

En caso de que exista un mapeo biyectivo $\varphi$ de $\{1, 2, \ldots, n\}$ a $S$ para algún $n \in \mathbb{N}$, el conjunto $S$ se dice ser *finito*; el valor de $n$ es único y se llama *cardinalidad* de $S$

denotado por *card* $S$ o $\#S$, al conjunto vacío se le asigna cardinalidad 0 [20]. Algunas características adicionales se describen a continuación:

**Definición 2.1.** *Sea $S$ un conjunto no vacío. Una partición $\Pi$ de $S$ es una colección de subconjuntos no vacíos de $S$ (bloques) tales que cada elemento de $S$ es un elemento de exactamente uno de estos subconjuntos [21].*

Sea $f^{(k)}$ la $k$-ésima derivada del mapeo $f$ donde $k$ es un entero no negativo. Siempre que $f^{(k)}$ exista y sea continua en un conjunto $S \subset \mathbb{R}^m$ se denota como:

$$f \in C^k(S, \mathbb{R}^m), \tag{2.2}$$

por conveniencia, en caso de que $k = 0$ se denota como $f \in C(S, \mathbb{R}^m)$; además, si $S$ es invariante bajo $f$, i.e. $f(S) \subset S$ se denota como $f \in C(S)$ [22].

### 2.1.1. Línea real

En este trabajo se estudian los mapeos únicamente definidos en espacios euclidianos uni-dimensionales, donde la *métrica euclidiana* es dada como sigue:

$$d(x, y) = |x - y|, \tag{2.3}$$

donde $x, y \in \mathbb{R}$. A continuación se presentan conceptos que son usados a lo largo del documento:

**Definición 2.2.** *Si $s_0$ es un número real y $\varepsilon > 0$; entonces el intervalo abierto:*

$$(s_0 - \varepsilon, s_0 + \varepsilon), \tag{2.4}$$

*es una $\varepsilon$-vecindad de $s_0$. Si un conjunto $S$ contiene una $\varepsilon$-vecindad de $s_0$; entonces $S$ es una vecindad de $s_0$ y este es un punto interior de $S$. El conjunto de puntos interiores de $S$ es el interior de $S$ y se denota por $S^\circ$ [19].*

Se agrega que en dimensiones mayores a uno, usualmente la vecindad de un punto se define como una *bola abierta de radio epsilon y centro* $s_0$ que se denota como $B_\varepsilon(s_0)$.

**Definición 2.3.** *Sea $S$ un subconjunto de $\mathbb{R}$, siempre que cualquier vecindad de $s_o$ contenga al menos un punto en $S$ y uno en el complemento de $S$ se dice que $s_0$ es un* punto frontera *de $S$; al conjunto de puntos frontera de $S$ se le conoce como frontera de $S$ y se denota por $\partial S$. La cerradura de $S$ se denota por $\overline{S}$ y es $\overline{S} = S \cup \partial S$ [19].*

Un conjunto $X \subset \mathbb{R}$ se dice ser *acotado por arriba* siempre que existe un $b \in \mathbb{R}$ tal que para todo $x \in X$ se satisface la desigualdad:

$$x \leq b, \tag{2.5}$$

al número real $b$ se le conoce como *cota superior de* $X$. A condición de que $b$ sea una cota superior de $X$ y no exista un número menor que cumpla esta condición, $b$ se llama *supremo* de $X$ y se denota a lo largo del documento como:

$$\beta = \sup X, \tag{2.6}$$

de forma análoga, un conjunto $X \subset \mathbb{R}$ se conoce como *acotado por abajo* siempre y cuando exista un $a \in \mathbb{R}$ tal que para todo $x \in X$ se satisface que:

$$a \leq x, \tag{2.7}$$

al número $a$ se le llama *cota inferior de* $X$; además, con tal que $a$ sea una cota inferior de $X$ y ningún real mayor a este lo sea, este valor se llama *ínfimo* de $X$ y se denota en este documento mediante:

$$\alpha = \text{ínf}\, X, \tag{2.8}$$

un conjunto $X \subset \mathbb{R}$ es acotado a condición de que existan números reales $a$ y $b$ tales que para todo $x \in X$ se satisface que $a \leq x \leq b$; se debe agregar que un conjunto no vacío acotado tiene un único supremo e ínfimo donde se satisface que:

$$\text{ínf}\, X \leq \sup X, \tag{2.9}$$

un conjunto no vacío $X \subset \mathbb{R}$ es *no acotado por arriba* si carece de cota superior y de forma similar se define uno *no acotado por abajo* [19].

Por último, se hace énfasis en que los *bloques* que se trabaja en este documento son únicamente intervalos acotados abiertos, cerrados o semi-cerrados por la izquierda o derecha. Como ejemplo de estos intervalos se tiene a $X = \{x : 0 < x \leq 1\}$ que tiene como ínfimo y supremo los valores $\alpha = 0$, $\beta = 1$ donde $\alpha < \beta$.

## 2.2. Sistemas dinámicos

Un sistema dinámico es la descripción matemática del comportamiento de un sistema físico, mecánico, eléctrico, biológico, ecológico, etc. desde la perspectiva de un proceso

*determinista* que se expresa por un número finito de *variables de estado* [23]; éstas se usan para determinar el estado instantáneo del sistema y las ecuaciones de evolución entre un *instante inicial* y el siguiente. Si las reglas de evolución se describen mediante *ecuaciones diferenciales* se obtienen *sistemas dinámicos de tiempo continuo*; por otro lado, si sus reglas de evolución son las *iteraciones de un mapeo* en un tiempo discreto se origina un *sistema dinámico de tiempo discreto* o *sistema dinámico discreto* [24].

### 2.2.1. Sistemas dinámicos discretos uni-dimensionales

Acorde con lo que se menciona anteriormente, las reglas de evolución de un sistema dinámico discreto o *mapeo* consisten en iteraciones y se denotan mediante:

$$x_{n+1} = f(x_n), \tag{2.10}$$

en la cual $n \in \mathbb{Z}$ o $n \in \mathbb{Z}^+$ y $f : X \to X$ mapea del *espacio de estados* (espacio fase) en sí mismo, dicha relación describe una *ecuación en diferencias* o *relación recursiva* de *primer orden*; al valor $x_0$ se le conoce como *semilla* o *punto inicial* y con este se genera una trayectoria o solución $\{f^n(x_0)\}$ de forma recursiva donde $n \in \mathbb{Z}^+$. Se conoce a $f(x_0)$ como la primera iteración de $x_0$ bajo $f$, a $f^2(x_0) = f(f(x_0))$ como la segunda iteración de $x_0$ bajo $f$ y de forma general, $f^n(x_0) = f(f^{n-1}(x_0))$ es la $n$-ésima iteración de $x_0$ bajo $f$. Al conjunto de las iteraciones positivas de $x_0$ se le conoce como la órbita positiva [18] y se denota mediante:

$$\mathcal{O}^+(x_0) = \{f^n(x_0) : n \in \mathbb{Z}^+\} = \{x_0, x_1, \ldots, x_n, x_{n+1}, \ldots\} = \{x_n\}_{n=0}^{\infty}, \tag{2.11}$$

siempre que el mapeo $f$ sea invertible, a la secuencia de iteraciones $\{f^{-n}(x_0)\}$ se le conoce como la órbita negativa de $x_0$ para la que $f^{-n} \doteq (f^{-1})^n$.

En caso de que el mapeo (2.10) se describa por $f(x_n) = a_n \cdot x_n$ donde $a_n \in \mathbb{R}$ se dice ser una *ecuación en diferencias lineal*; en caso contrario se dice ser *no lineal*, generalmente se excluye el caso de los mapeos lineales afin $f(x_n) = a \cdot x_n + b$ [22].

Un punto *fijo* o *periódico* de un sistema dinámico discreto es un punto $x \in \mathbb{R}$ o un conjunto finito de puntos $\{x, f(x), \ldots, f^{h-1}(x) : x \in \mathbb{R}, h \in \mathbb{Z}^+\}$ con cardinalidad $h$ tales que al ser iterados bajo $f$, se repiten; para el caso de que sea un punto se dice ser un *punto fijo* de $f$ y se denota por $\overline{x}$. Si es un conjunto finito de puntos se conoce como un *h-ciclo* o ciclo de $f$ de longitud $h$ para la que el valor de $h$ es el mínimo $n \in \mathbb{Z}^+$ para el que se satisface la relación $f^n(x) = x$.

Un punto fijo $\overline{x}$ del mapeo (2.10) se conoce como hiperbólico siempre que se cumple la restricción:

$$|f'(\overline{x})| \neq 1, \tag{2.12}$$

donde $f'$ es la derivada del mapeo (2.10) con respecto a $x_n$ [18]. Una forma analítica para entender el comportamiento de los h-ciclos y puntos fijos de un sistema dinámico discreto se presentan a continuación:

**Teorema 2.1** (**Hartman-Grobman**). *Sea $\overline{x}$ un punto fijo del mapeo (2.10) y se asume que $f \in C^1(B_\varepsilon(\overline{x}), \mathbb{R}^m)$ para $\varepsilon > 0$. Si $\overline{x}$ es un punto fijo hiperbólico y $f'(\overline{x})$ es invertible; entonces $f$ es conjugado al mapeo lineal $f'(\overline{x})$ [22].*

**Corolario 1** (**La línea real**). *Sea $F \in C^1(S, \mathbb{R})$ donde $S$ es un intervalo no trivial.*

- *Se supone que $\bar{x}$ es un punto fijo del mapeo (2.10) en $S^\circ$. Si $|f'(\overline{x})| < 1$ ($|f'(\overline{x})| > 1$) entonces $\overline{x}$ es asintóticamente estable (inestable).*

- *Un ciclo $\{x_1, x_2, \ldots, x_h\} \subset S^\circ$ de $f$ es asintóticamente estable (inestable) siempre que $\prod_{i=1}^{h} |f'(x_i)| < 1$ $\left(\prod_{i=1}^{h} |f'(x_i)| > 1\right)$ [22].*

Para observar gráficamente el comportamiento de una órbita se puede emplear una herramienta que se conoce como el método de *iteración gráfica* [3] o *diagrama de escalón* (cobweb en inglés); esto es un procedimiento que superpone la *ecuación de la recta* $g(x_n) = x_n$ a la "curva" $x_{n+1} = f(x_n)$ para *trazar la órbita* que describe un *punto inicial*; paso por paso, el método inicia al trazar una línea recta entre los puntos $(x_0, 0)$ y $(x_0, x_1)$, luego se dibuja una línea horizontal entre los puntos $(x_0, x_1)$ y $(x_1, x_1)$; después se dibuja una línea vertical entre $(x_1, x_1)$ y $(x_1, x_2)$, se traza una recta entre $(x_1, x_2)$ y $(x_2, x_2)$; a continuación se sigue el mismo proceso de manera iterativa hasta graficar la órbita $\{x_n\}_{n=0}^{m}$ para algún $m \in \mathbb{N}$ [18]; sirva de ejemplo la órbita que describe el mapeo logístico que se muestra en la figura 2.1, este representa un modelo idealizado de población; un rasgo que aparece son los puntos fijos de $f$ que se encuentran donde los valores de $f$ y $g$ coinciden, i.e. $f(x_n) = g(x_n)$. Observe que la órbita de $x_0$ bajo $f$ converge al punto fijo que aparece en la parte superior derecha.

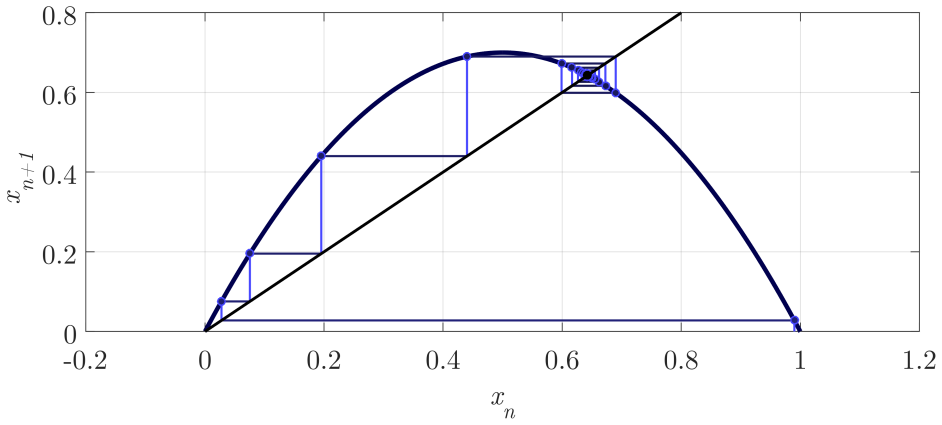



Figura 2.1: Diagrama de escalón de la órbita del punto inicial $x_0 = 0.99$ bajo el mapeo logístico $f(x_n) = 2.8(1 - x_n)x_n$.

Una forma adicional de observar el comportamiento de la órbita de un punto inicial se presenta enseguida, esta representación se conoce como *series de tiempo* y es una gráfica que tiene como *dominio el instante de tiempo* $n \in \mathbb{Z}^+$ y rango el *componente escalar* $f^n(x_0)$, así que se grafica el conjunto de puntos $(n, f^n(x_0))$ [22]; baste, como muestra la figura 2.2 que exhibe los primeros elementos de la órbita positiva que se presenta en la figura 2.1; de forma análoga a la anterior, se percibe que la órbita se aproxima al punto fijo.

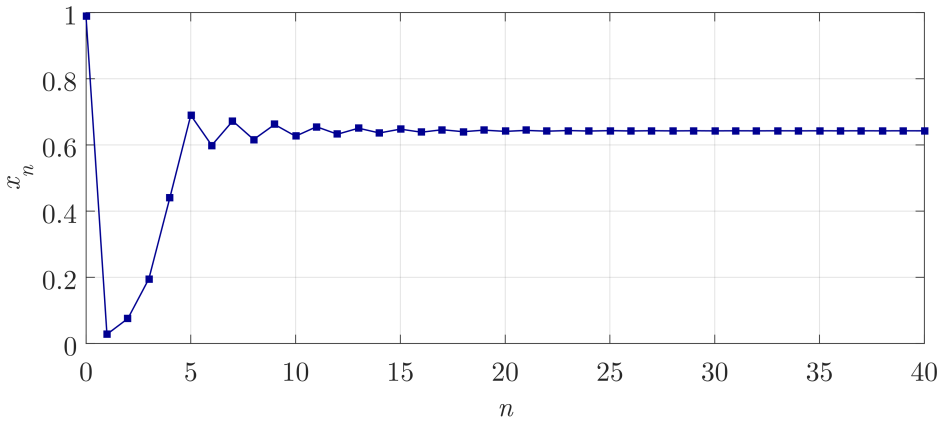


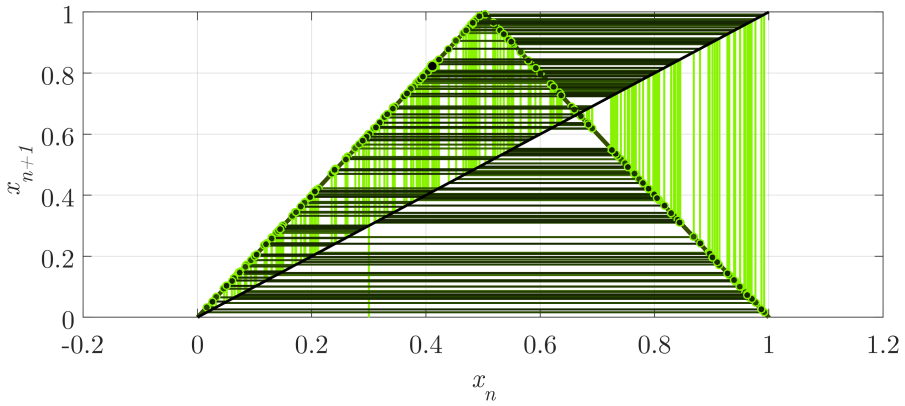

Figura 2.2: Serie de tiempo del punto inicial $x_0 = 0.99$ bajo el mapeo $f(x_n) = 2.8(1 - x_n)x_n$.

### 2.2.2. Sistemas dinámicos discretos caóticos

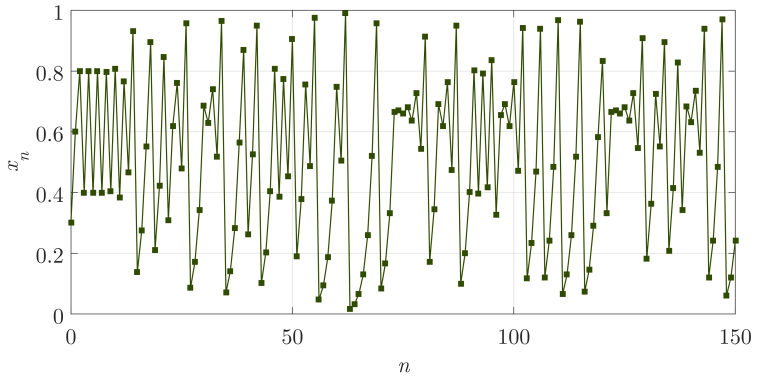
Con la intención de abordar el siguiente concepto se introduce el mapeo casa de campaña, este mapeo se representa mediante una ecuación en diferencias lineal por partes que se describe mediante la relación:

$$x_{n+1} = t(x_n) = \begin{cases} 2x_n, & 0 \leq x_n \leq \frac{1}{2}; \\ 2(1 - x_n), & \frac{1}{2} < x_n \leq 1; \end{cases} \tag{2.13}$$

este es un ejemplo de sistema dinámico capaz de exhibir comportamiento complejo; así, por ejemplo, se muestra en las Figuras 2.3a y 2.3b la órbita de un punto inicial $x_0 \in (0, 1)$ bajo el mapeo (2.13). Observe que la órbita aparenta exhibir un comportamiento *no periódico* que parece *aleatorio*; además, ya que es un sistema dinámico determinista se reproduce la misma órbita para el mismo punto inicial. Este comportamiento se conoce como *caos determinista* [2] y se ha demostrado que (2.13) lo presenta [25].




(a) Diagrama de escalón




(b) Series de tiempo

Figura 2.3: Representación gráfica de la órbita del punto inicial $x_0 = 0.30001$ bajo el mapeo casa de campaña (2.13).

Algunas de las características que se atribuye al comportamiento caótico son la sensibilidad a las condiciones iniciales y un aparente comportamiento similar al aleatorio que en realidad es determinista [26]. Debido a que no existe una única definición para explicar este comportamiento, se presentan dos definiciones de las más utilizadas que existen; en primer lugar, se presenta la descripción de este comportamiento que se conoce como *Caos en el sentido de Devaney*:

Se dice que un mapeo $f : X \to X$ es caótico siempre que [3]:

- Los puntos periódicos de $f$ son densos en $X$.
- $f$ es transitivo en $X$; esto es, dado cualquier par de abiertos $U_1$ y $U_2$ de $X$, existe un punto $x_0 \in U_1$ y un $n > 0$ para el que $f^n(x_0) \in U_2$.
- $f$ tiene dependencia sensible en $X$; esto es, existe una constante $\gamma$ tal que, para cualquier $x_0 \in X$ y cualquier intervalo abierto $U$ sobre $x_0$, existe algún punto inicial $y_0 \in U$ y $n > 0$ tal que:

$$|f^n(x_0) - f^n(y_0)| > \gamma. \tag{2.14}$$

La segunda descripción toma como base el *espectro de los exponentes de Lyapunov*, cada exponente representa la tasa exponencial promedio en que divergen o convergen las órbitas en el espacio de estados. En el caso de un sistema dinámico discreto unidimensional se tiene un único exponente de Lyapunov [27]. Siempre que se presente una divergencia exponencial al iterar un par de condiciones iniciales aproximadamente iguales, las órbitas que se obtiene experimentan un comportamiento distinto; mas aún, si la órbita está contenida en un conjunto cerrado y acotado; entonces el sistema experimenta repetidamente una expansión y contracción en una dirección que resulta en descorrelacionar estados cercanos. Así que el comportamiento a largo plazo de una condición inicial con cualquier tipo de incertidumbre no se puede predecir, es lo que se llama *caos* [28].

Los sistemas dinámicos discretos exhiben comportamiento complejo y caótico desde una dimensión [26]; en contraste con lo anterior, un sistema dinámico de tiempo continuo exhibe comportamiento caótico para dimensiones mayores o iguales a tres [28]. En pocas palabras, el comportamiento de un mapeo se caracteriza por el exponente de Lyapunov del siguiente modo: Si el valor es positivo y la órbita se contiene en un conjunto cerrado y acotado; entonces indica comportamiento caótico; en caso de que sea negativo, indica la

existencia de un h-ciclo asintóticamente estable y siempre que sea nulo señala una órbita marginalmente estable [28]. El método que se emplea para calcular una *aproximación del exponente de Lyapunov* se discute a continuación:

**Definición 2.4.** *El exponente de Lyapunov $\lambda$ que se computa usando el método de la derivada se define como:*

$$\lambda = \frac{1}{n}\left(\sum_{i=1}^{n} ln\left|F'(x_i,\mu)\right|\right), \tag{2.15}$$

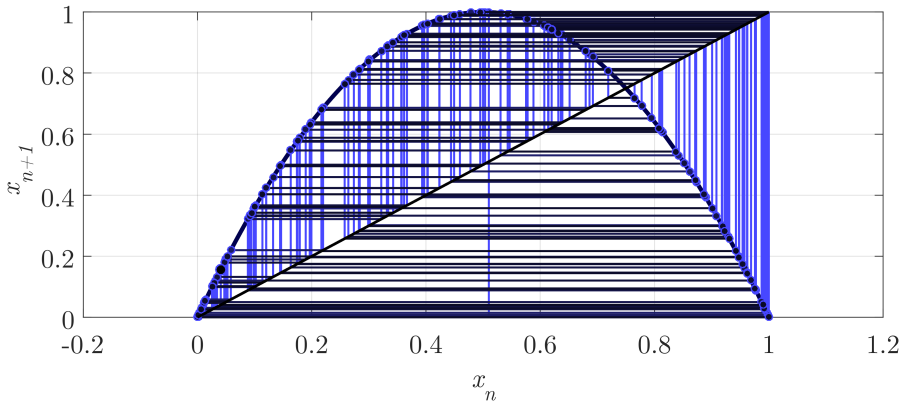
*para la que $F'$ representa la derivada con respecto a $x$ y los valores $x_0, x_1, x_2, \cdots, x_n$ son iteraciones sucesivas. El exponente de Lyapunov se puede computar para una muestra de puntos cerca del atractor para obtener un exponente promedio de Lyapunov [27].*

Donde el valor de $n$ en este documento es del orden de millones. A continuación se presentan dos sistemas dinámicos discretos adicionales al casa de campaña que son capaces de exhibir comportamiento complejo e inclusive caótico; en primer lugar se presenta en las Figuras 2.4a y 2.4b la iteración de un punto inicial $x_0 \in (0,1)$ bajo el mapeo logístico:

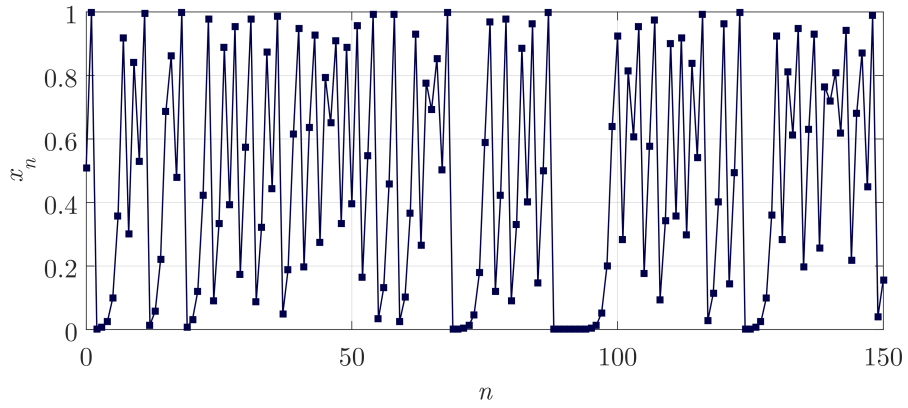
$$x_{n+1} = f(x_n) = 4(1-x_n)x_n, \tag{2.16}$$

en segundo lugar se muestra en las Figuras 2.5a y 2.5b la iteración de un punto inicial $x_0 \in (-1,1)$ bajo el mapeo iterativo de Gauss:

$$x_{n+1} = g(x_n) = e^{6.20\cdot x_n^2} - 0.58. \tag{2.17}$$

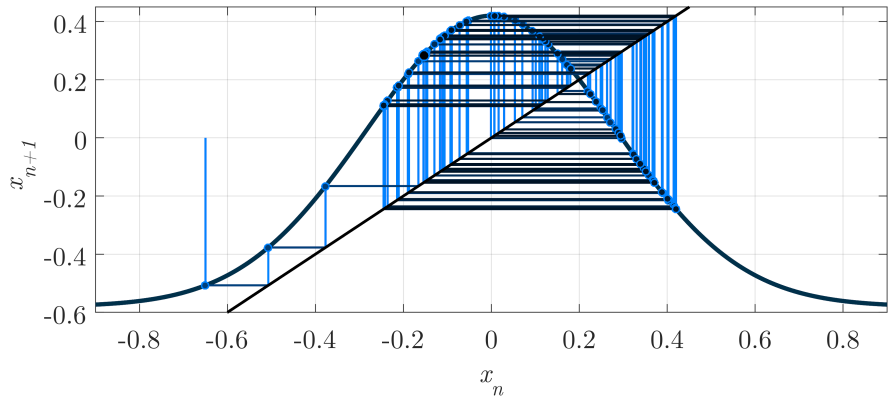



(a) Iteración gráfica

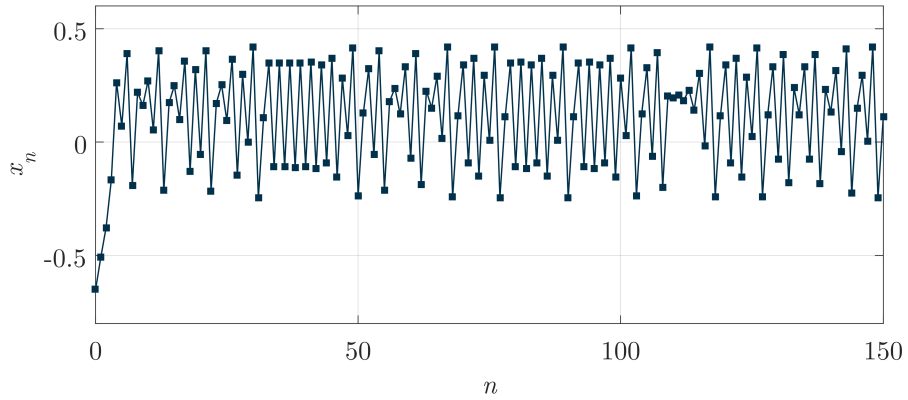



(b) Series de tiempo

Figura 2.4: Representación gráfica de la órbita de $x_0 = 0.51$ bajo el mapeo logístico (2.16).




(a) Diagrama de escalón




(b) Series de tiempo

Figura 2.5: Representación gráfica de la órbita de $x_0 = -0.65$ bajo el mapeo de Gauss (2.17).

## 2.3. Generadores aleatorios y seudo-aleatorios de bits

Una *secuencia de bits aleatoria* $(s_i)_{i=0}^{\infty} = (s_0, s_1, s_2, \ldots)$ donde cada valor $s_i \in \{0, 1\}$, se interpreta como el resultado de *lanzar una moneda no cargada*. En cada lanzamiento se tiene como probabilidad exactamente 0.5 de producir un *cero* o un *uno*; mas aún, cada lanzamiento es independiente de los demás por lo que a pesar de conocer algunos términos de la secuencia $s_n, s_{n+1}, \ldots, s_{n-1+m}$ no se puede predecir el valor del término siguiente $s_{n+m}$ con una probabilidad mayor a 0.5. Se hace énfasis que éste es el punto de referencia al analizar si una secuencia tiene comportamiento aleatorio [29].

Los generadores de bits aleatorios usan una fuente no determinista como por ejemplo el ruido de semiconductores, clics de un ratón de computadora, etc. anexa a una función de procesado para computar cada bit de la secuencia [29]; en vista de que esto requiere de mucho tiempo y puede ser costoso, en la práctica es común el uso de *generadores de bits seudo-aleatorios* [30]. El objetivo del generador de bits seudo-aleatorios es *expandir* una *pequeña secuencia de bits aleatoria* en una secuencia de bits de *longitud mucho mayor* que presenta características similares a una aleatoria. La pequeña secuencia de bits aleatoria se conoce como *semilla* y frecuentemente el generador computa una secuencia de forma recursiva como se muestra a continuación [9]:

$$s_{i+1} = f(s_i), \tag{2.18}$$

donde $s_0$ es la semilla, $i \in \mathbb{Z}^+$. El bit $s_{n+1}$ de la secuencia donde $n \in \mathbb{N}$ se calcula acorde con $s_{n+1} = f^n(s_0)$; de forma análoga al estado $x_n$ de un sistema dinámico discreto.

### 2.3.1. Banco de pruebas estadísticas

De manera frecuente se emplean tres bancos de pruebas para analizar aleatoriedad en una secuencia; el primero son las pruebas estadísticas Diehard de Marsaglia [31], el segundo son las pruebas estadísticas TestU01 [32] y el último son el banco de pruebas del Instituto Nacional de Estándares y Tecnología (NIST) [29]. El banco de pruebas estadísticas que se emplea en este documento para caracterizar un generador de bits es el del Instituto Nacional de Estándares y Tecnología.

El banco de pruebas estadísticas del Instituto Nacional de Estándares y Tecnología cuenta con 15 pruebas estadísticas. De acuerdo a la información de [29] al aplicar

cada prueba estadística se plantea como hipótesis nula ($H_0$) que la secuencia que se analiza es aleatoria y como hipótesis alternativa ($H_a$) que ésta no es aleatoria, así que al aplicar cualquier prueba se obtiene un *valor-p* que representa la probabilidad de que un generador aleatorio de números perfecto hubiera producido una secuencia menos aleatoria que la examinada y a condición de que:

$$\textit{valor-p} \geq \delta, \tag{2.19}$$

donde $\delta$ es el nivel de significancia, no se refuta $H_0$ con una confianza de $100(1-\delta)\,\%$; en caso contrario, se acepta $H_a$ con igual confianza.

Para interpretar los resultados empíricos de cada prueba se emplea los dos enfoques que recomienda [29], examinar el porcentaje de secuencias que pasan la prueba (no se refuta $H_0$) y su distribución en búsqueda de uniformidad. Así se puede concluir que los resultados empíricos del análisis indican claramente *una desviación de aleatoriedad*, *no indican una desviación de aleatoriedad* o son *inconclusos*.

Conviene subrayar que en este documento se realiza cada prueba para los valores predeterminados de $SP800-22$ por lo que acorde con [29] el primer enfoque requiere analizar por lo menos 1 000 de secuencias para que su resultado sea confiable. El segundo enfoque un mínimo de 80 secuencias para que su resultado sea confiable. Por último la menor longitud que debe tener la secuencia para poder aplicarle todas las pruebas es de 1 000 000. Es por esto que en este documento se *emplea* muestras de 2 000 secuencias en la que cada una tiene longitud de 1 000 000.

# Capítulo 3

# Sistemas dinámicos discretos

En este capítulo se describe la construcción de una familia de sistemas dinámicos discretos que son útiles para desarrollar generadores de bits con comportamiento similar al aleatorio. El interés es generar una familia monoparamétrica que presente comportamiento caótico para diferentes valores de un parámetro de control. Así en la primer parte de este capítulo, se desarrolla una familia monoparamétrica mediante sistemas dinámicos discretos que son funciones por partes con base en un mapeo similar al logístico. En la segunda parte, se presenta a detalle las etapas que permiten la obtención de una secuencia de bits a partir de sistemas dinámicos discretos con comportamiento caótico.

## 3.1. Familia monoparamétrica

Sea $(I, d)$ un espacio métrico donde $I = [0, 1] \subset \mathbb{R}$ es el intervalo unitario y $d$ es la métrica euclidiana. A lo largo del documento siempre que se refiere al intervalo $I$ se considera únicamente al intervalo unitario. Hecha esta salvedad, se prosigue a proponer una definición de mapeo unimodal [33].

**Definición 3.1.** *Sean $S \subset I$ un intervalo y $f \in C(S, I)$. Si se satisface que:*

- *Existe un $x_c \in S^\circ = (\alpha, \beta)$ para el que $f|_{(\alpha, x_c)}$ es estrictamente creciente y $f|_{(x_c, \beta)}$ es estrictamente decreciente.*

*El mapeo $f$ se llama unimodal en $S$.*

Si $S = I$ entonces se puede tener un mapeo unimodal en $I$; por ejemplo, los mapeos *logístico* y *casa de campaña* son mapeos unimodales en $I$. En caso de que un mapeo:

$$f(x) = \begin{cases} f_1, & x \in S_1; \\ f_2, & x \in S_2, \end{cases} \tag{3.1}$$

satisface que $f_1$ es unimodal en $S_1$, $f_2$ es unimodal en $S_2$, $I = S_1 \cup S_2$ y; además $S_1 \cap S_2 = \varnothing$ entonces se tiene dos mapeos unimodales en $I$ o un *mapeo bimodal* en $I$. De manera análoga se puede generalizar la idea a un número arbitrario de mapeos unimodales para obtener un *mapeo m-modal*. El interés de este trabajo es construir mapeos m-modales con base en el tipo de mapeo logístico que se presenta a continuación:

$$f_\gamma(\beta, \alpha, x) = \gamma(\beta - x)(x - \alpha), \tag{3.2}$$

donde $x$ es la *variable de estado*; $\gamma$ es un *parámetro de control* y $\alpha$, $\beta$ son *parámetros arbitrarios pero fijos*. Es importante mencionar que se restringe los valores de los elementos $\alpha, \beta \in \mathbb{R}$ acorde con las desigualdades:

$$0 \leq \alpha < \beta \leq 1. \tag{3.3}$$

Al expandir la ecuación (3.2) se obtiene que:

$$f_\gamma(\beta, \alpha, x) = -\gamma x^2 + (\alpha + \beta)x - \alpha\beta, \tag{3.4}$$

entonces la primer y segunda derivada de $f_\gamma$ son $f_\gamma^{'} = \gamma(-2x + \alpha + \beta)$ y $f_\gamma^{''} = -2\gamma$, respectivamente. La primer derivada de $f_\gamma$ existe para todo $x \in \mathbb{R}$ por lo que $f_\gamma$ es continua en todo $\mathbb{R}$. Dado que $f_\gamma^{'} = 0$ y $f_\gamma^{''} < 0$ en $x_c = (\alpha + \beta)/2$, si $\gamma > 0$ entonces $f_\gamma$ presenta un máximo local en $x_c$ para el que $f|_{(\alpha, x_c)}$ es estrictamente creciente y $f|_{(x_c, \beta)}$ es estrictamente decreciente. Es por esto que el parámetro de control $\gamma \in \mathbb{R}$ debe ser positivo con el objetivo de conseguir un mapeo unimodal en $(\alpha, \beta)$ con base en la ecuación (3.2).

Al dividir $I$ en múltiples subintervalos para poder tener en cada uno un mapeo unimodal se distingue dos posibilidades. La primera es que se divida $I$ en intervalos de *igual longitud* y la segunda es que exista *por lo menos uno con longitud distinta*. De manera formal ambas posibilidades se definen a continuación:

**Definición 3.2.** *Sea* $(\zeta_i)_{i=0}^m$ *una secuencia finita tal que* $\zeta_0 = 0 < \zeta_1 < \cdots < \zeta_m = 1$ *donde* $m \in \mathbb{N} \setminus \{1\}$ *que determina la partición de* $I$*:*

$$\Pi = \{S_1 = [\zeta_0, \zeta_1], S_2 = (\zeta_1, \zeta_2], \ldots, S_m = (\zeta_{m-1}, \zeta_m]\}, \tag{3.5}$$

*el diámetro de cada bloque $S_i$ se da por $\sigma_i = d(\zeta_{i-1}, \zeta_i)$, $i, j \in \{1, 2, \ldots, m\}$. Si existe al menos un par de bloques $S_i$ y $S_j$ para los que $\sigma_i \neq \sigma_j$, entonces la partición de $I$ se llama no uniforme. En caso contrario, la partición de $I$ se llama uniforme.*

Para ilustrar la definición anterior se presenta tres ejemplos de secuencias finitas con 4 términos; es decir, secuencias finitas que determinan particiones de $I$ con tres bloques. Como primer ejemplo se usa la *secuencia finita* $(\zeta_i)_{i=0}^3 = \left(0, \frac{1}{3}, \frac{2}{3}, 1\right)$, dado que $\zeta_0 = 0 < \zeta_1 = \frac{1}{3} < \zeta_2 = \frac{2}{3} < \zeta_3 = 1$ determina la partición de $I$:

$$\Pi_1 = \left\{ \left[0, \frac{1}{3}\right], \left(\frac{1}{3}, \frac{2}{3}\right], \left(\frac{2}{3}, 1\right] \right\}, \tag{3.6}$$

como el diámetro de cada bloque es $d(0, \frac{1}{3}) = d(\frac{1}{3}, \frac{2}{3}) = d\left(\frac{2}{3}, 1\right) = \frac{1}{3}$; no existe un par de bloques $S_i$ tales que $\sigma_i \neq \sigma_j$, por lo tanto la partición (3.6) de $I$ es *uniforme*. El segundo ejemplo de *secuencia finita* es $(\zeta_i)_{i=0}^3 = \left(0, \frac{1}{2}, \frac{2}{3}, 1\right)$, ya que $\zeta_0 = 0 < \zeta_1 = \frac{1}{2} < \zeta_2 = \frac{2}{3} < \zeta_3 = 1$ determina la partición de $I$:

$$\Pi_2 = \left\{ \left[0, \frac{1}{2}\right], \left(\frac{1}{2}, \frac{2}{3}\right], \left(\frac{2}{3}, 1\right] \right\}, \tag{3.7}$$

de forma análoga a la anterior, como los diámetros de los bloques $S_1$ y $S_2$ son $\sigma_1 = \frac{1}{2}$, $\sigma_2 = \frac{1}{6}$, respectivamente; existe un par de bloques $S_1$ y $S_2$ tales que $\sigma_1 \neq \sigma_2$ por lo que la partición (3.7) de $I$ es *no uniforme*. Por último se presenta la *secuencia finita* $(\zeta_i)_{i=0}^3 = \left(0, \frac{1}{2}, 1, 1\right)$; en vista de que $\zeta_0 = 0 < \zeta_1 = \frac{1}{2} < \zeta_2 = 1 \not< \zeta_3 = 1$ no se satisface que $\zeta_2 < \zeta_3$ por lo que no se satisface la definición 3.2.

Una vez que se define el mapeo unimodal además de las particiones uniformes y no uniformes de $I$, se procede a dar una definición de mapeo m-modal.

**Definición 3.3.** *Sean $g \in C(I, \mathbb{R})$ y $\Pi = \{S_1, \ldots, S_m\}$ una partición de $I$ con $m \in \mathbb{N} \setminus \{1\}$ bloques. Si para todo $S_i \in \Pi$, el mapeo $g$ es unimodal en $S_i$; al mapeo $g$ se le llama m-modal.*

Conviene subrayar que para denotar un mapeo m-modal se emplea prefijos numerales latinos de manera análoga al unimodal; así, por ejemplo, se indica el que tiene dos mapeos unimodales por *bimodal*, tres por *trimodal*, cuatro por *termodal* (quadrimodal), cinco por *quinquemodal*, etc.

A continuación se construye un mapeo m-modal con base en el mapeo unimodal (3.2), para esto se toma una secuencia finita $(\zeta_i)_{i=0}^m = (\zeta_0, \zeta_1, \zeta_2, \cdots \zeta_m)$ que describe una

partición uniforme o no uniforme de $I$ para determinar los dominios de una función por partes. Después, cada parte de la función se describe por el mapeo unimodal $\gamma\left(\zeta_i - x\right)\left(x - \zeta_{i-1}\right)$. Así se obtiene la función por partes continua en $I$:

$$h(\gamma, \zeta_0, \zeta_1, \ldots, \zeta_m, x) = \begin{cases} \gamma\left(\zeta_1 - x\right)\left(x - \zeta_0\right), & \zeta_0 \leq x \leq \zeta_1; \\ \gamma(\zeta_2 - x)(x - \zeta_1), & \zeta_1 < x \leq \zeta_2; \\ \vdots & \vdots \\ \gamma(\zeta_m - x)(x - \zeta_{m-1}), & \zeta_{m-1} < x_n \leq \zeta_m. \end{cases} \tag{3.8}$$

En caso de que la secuencia finita $(\zeta_i)_{i=0}^m$ determine una partición *uniforme* de $I$, i.e. todo $\sigma_i = \frac{1}{m}$, con $i, j \in \{1, 2, \ldots, m\}$; el máximo local de cada parte de la función (3.8) es $h\left(x_c^{(i)}\right) = \frac{\gamma}{4m^2}$ donde $x_c^{(i)} = \frac{\zeta_{i-1}+\zeta_i}{2}$. En contraste con lo anterior, si la secuencia finita determina una partición *no uniforme* de $I$; el máximo local del mapeo (3.8) en cada bloque de (3.5) es $h\left(x_c^{(i)}\right) = \frac{\gamma}{4}\sigma_i^2$ y por lo menos existe un par de bloques $S_i$ y $S_j$ tales que $\sigma_i \neq \sigma_j$; por consiguiente, para el *mismo parámetro de control* $\gamma$ se consiguen múltiples máximos locales, i.e. $h\left(x_c^{(i)}\right) \neq h\left(x_c^{(j)}\right)$.

Es importante mencionar que para un parámetro de control fijo la secuencia finita $(\zeta_i)_{i=0}^m$ determina los máximos locales del mapeo (3.8). Con el objetivo de *seleccionar* los máximos locales de manera independiente a la secuencia finita, se *agrega el parámetro* $\frac{\rho_i}{\sigma_i^2}$ donde $\rho_i > 0$ a cada parte del mapeo (3.8). Como resultado se obtiene $f_i(x) = \gamma\frac{\rho_i}{\sigma_i{}^2}\left(\zeta_i - x\right)\left(x - \zeta_{i-1}\right)$ y cada máximo local es $f_i\left(x_c^{(i)}\right) = \rho_i\frac{\gamma}{4}$. Así se obtiene el mapeo m-modal:

$$g_\gamma(\zeta_0, \ldots \zeta_m, \rho_1, \ldots, \rho_m, x) = \begin{cases} \gamma\frac{\rho_1}{\sigma_1{}^2}\left(\zeta_1 - x\right)\left(x - \zeta_0\right), & \zeta_0 \leq x \leq \zeta_1; \\ \gamma\frac{\rho_2}{\sigma_2{}^2}(\zeta_2 - x)(x - \zeta_1), & \zeta_1 < x \leq \zeta_2; \\ \vdots & \vdots \\ \gamma\frac{\rho_m}{\sigma_m{}^2}(\zeta_m - x)(x - \zeta_{m-1}), & \zeta_{m-1} < x_n \leq \zeta_m, \end{cases} \tag{3.9}$$

donde los parámetros $\zeta_0, \zeta_1, \ldots, \zeta_m, \rho_1, \rho_2, \ldots, \rho_m$ son *arbitrarios pero fijos*, $x$ es la *variable de estado* y $\gamma$ es un parámetro que se *manipula*; es decir, el *parámetro de control*.

A continuación se define una familia de mapeos con base en uno m-modal para la que existen $m \in \mathbb{N}$ parámetros de control $\gamma_1, \gamma_2, \ldots, \gamma_m$ que debe satisfacer dos propiedades. La primera es que el intervalo unitario siempre sea invariante bajo cada mapeo con dicho parámetro de control; así que se puede obtener una serie de tiempo de longitud arbitraria al iterar cualquier punto inicial $x_0 \in I$. La segunda es que para cada mapeo con parámetro de control $\gamma_i$, que se va a denotar como $g_{\gamma_i}$ donde $i \in \{1, 2, \ldots, m\}$ el

intervalo $[0, \zeta_i]$ sea invariante bajo $g_{\gamma_i}$. Es importante mencionar que únicamente se cambia el parámetro de control, los parámetros $\zeta_i$ y $\rho_i$ son arbitrarios pero fijos. De manera formal:

**Definición 3.4.** *Sea $g_\gamma$ un mapeo m-modal donde $m \in \mathbb{N} \setminus \{1\}$, si existen $m$ distintos parámetros de control $\gamma_1, \gamma_2, \ldots, \gamma_m$ tales que satisfacen:*

- $g_{\gamma_i} : [0, \zeta_i] \to [0, \zeta_i]$ *es sobreyectivo.*
- $I$ *es invariante bajo* $g_{\gamma_i}$.

*La familia monoparamétrica $\{g_{\gamma_i}\}_{i=1}^m$ se llama multimodal.*

Para ejemplificar la definición anterior se toma la secuencia finita $(\zeta_i)_{i=0}^2 = \left(0, \frac{3}{5}, 1\right)$ que determina una partición no uniforme de $I$ para fijar los dominios de la función por partes (3.9); además, se selecciona los valores que determinan cada máximo local de (3.9) mediante la secuencia $(\rho_i)_{i=1}^2 = \left(\frac{1}{2}, 1\right)$. Como resultado se obtiene el mapeo bimodal:

$$g_\gamma\left(0, 0.6, 1, 0.5, 1, x\right) = \begin{cases} \gamma \cdot 1.39(0.6 - x)(x - 0), & 0 \leq x \leq 0.6; \\ \gamma \cdot 6.25(1 - x)(x - 0.6), & 0.6 < x \leq 1, \end{cases} \tag{3.10}$$

es importante mencionar que los parámetros $\zeta_0, \zeta_1, \zeta_2, \rho_1, \rho_2$ son *arbitrarios pero fijos*. El máximo local del mapeo bimodal (3.10) cuando $x \in [0, 0.6]$ es $g_\gamma\left(0.3\right) = 0.5\frac{\gamma}{4}$ y $g_\gamma\left(0.8\right) = \frac{\gamma}{4}$ para $x \in (0.6, 1]$. Como $g_\gamma$ es continua en $I$ y $g_\gamma(0) = g_\gamma(0.6) = 0$, para que $g_\gamma$ sea sobreyectiva en $S_1 = [0, 0.6]$ se requiere un parámetro de control $\gamma_1$ tal que $g_\gamma\left(0.3\right) = 0.6$; así se consigue el parámetro de control $\gamma_1 = 0.6\frac{4}{0.5} = 4.8$. Para dicho parámetro de control los máximos locales del mapeo bimodal (3.10) son $g_{4.8}(0.3) = 0.6$ y $g_{4.8}(0.8) = 1.2$; ya que $g_{4.8}(0.8) \notin I$, $I$ no es invariante bajo $g_{4.8}$ por lo que no existen parámetros de control $\gamma_1$ y $\gamma_2$ tales que satisfacen la definición 3.4.

Se hace énfasis en que la selección de los parámetros de las secuencias finitas $(\zeta_i)_{i=0}^m$ y $(\rho_i)_{i=1}^m$ es lo que determina la existencia de los parámetros de control con los que se consigue la familia multimodal. Para encontrar las condiciones que se deben satisfacer se desarrolla el siguiente Teorema. En este se presenta las condiciones necesarias y suficientes para formar una familia multimodal mediante un mapeo m-modal que es *sobreyectivo en $I$ para el parámetro de control $\gamma = 4$.*

**Teorema 3.1 (Configuraciones).** *Sea $g_\gamma(\zeta_0, \zeta_1, \ldots, \zeta_m, \rho_1, \rho_2, \ldots, \rho_m, x)$ un mapeo m-modal descrito por (3.9) sobreyectivo en $I$ para $\gamma = 4$. Existen parámetros de control*

$\gamma_1, \gamma_2, \ldots, \gamma_m$ *tales que la familia* $\{g_{\gamma_1}, g_{\gamma_2}, \ldots, g_{\gamma_m}\}$ *es multimodal si y sólo si:*

$$\frac{\zeta_1}{\rho_1} \neq \frac{\zeta_2}{\underset{i\leq 2}{\max}\,\rho_i} \neq \cdots \neq \frac{\zeta_{m-1}}{\underset{i\leq m-1}{\max}\,\rho_i}, \tag{3.11}$$

*y para todo* $j \in \{1, 2, \ldots, m-1\}$*:*

$$\frac{\zeta_j}{\underset{i\leq j}{\max}\,\rho_i} < 1. \tag{3.12}$$

*Demostración.* $\Longrightarrow$ Sea $g_4$ un mapeo m-modal sobreyectivo en $I$ y se supone que se satisfacen las condiciones (3.11) y (3.12); se debe probar que existen $m$ distintos parámetros de control $\gamma_1, \gamma_2, \ldots, \gamma_m$ para los que $g_{\gamma_i} : [0, \zeta_i] \to [0, \zeta_i]$ es sobreyectivo y que $I$ es invariante bajo cada mapeo $g_{\gamma_i}$ donde $i \in \{1, 2, \ldots, m\}$, i.e. $g_{\gamma_i}(I) \subset I$.

Como $g_4$ es un mapeo m-modal descrito por (3.9), para cada bloque de la partición $\Pi = \{S_1, S_2, \ldots, S_m\}$ de $I$ se satisface que $g_4(\partial S_i) = 0$, $g_4\left(x_c^{(i)}\right) = \rho_i$ y todo $\rho_i > 0$ porque son máximos locales. Además, ya que $g_4$ es continua y sobreyectiva en $I$ existe al menos un máximo local $\rho_i = 1$ y también se satisface que todo $\rho_i \leq 1$.

Para un parámetro de control $\gamma_i > 0$ se satisface que el máximo local de $g_{\gamma_i}$ en cada bloque de $\Pi$ es:

$$g_{\gamma_i}\left(x_c^{(i)}\right) = \rho_i \frac{\gamma_i}{4}, \tag{3.13}$$

por consiguiente al restringir el dominio de $g_{\gamma_i}$ al intervalo $J_i = [0, \zeta_i]$ donde $i \in \{1, 2, \ldots, m-1\}$, $\zeta_i \in (\zeta_h)_{h=0}^m$; se tiene $i$ máximos locales $\rho_1 \frac{\gamma_i}{4}, \rho_2 \frac{\gamma_i}{4}, \ldots, \rho_i \frac{\gamma_i}{4}$. Como el parámetro $\frac{\gamma_i}{4}$ es constante para cada máximo local, el máximo valor de $g_{\gamma_i}$ en dicho intervalo es:

$$\underset{x\in J_i}{\max}\, g_{\gamma_i}(x) = \frac{\gamma_i}{4} \underset{j\leq i}{\max}\, \rho_j, \tag{3.14}$$

por lo tanto al calcular cada parámetro de control $\gamma_i$ acorde con:

$$\gamma_i = 4 \frac{\zeta_i}{\underset{j\leq i}{\max}\,\rho_j}, \tag{3.15}$$

resulta que el máximo local de $g_{\gamma_i}$ en $J_i = [0, \zeta_i]$ es:

$$\underset{x\in J_i}{\max}\, g_{\gamma_i}(x) = \frac{4}{\underset{j\leq i}{\max}\,\rho_j} \frac{\underset{j\leq i}{\max}\,\rho_j}{4} \zeta_i = \zeta_i, \tag{3.16}$$

y como $g_{\gamma_i}$ es continuo en $J_i$ se satisface que $g_{\gamma_i}$ es sobreyectiva en $J_i = [0, \zeta_i]$; además, ya que $i$ es arbitrario existen $m$ parámetros de control $\gamma_1, \gamma_2, \ldots, \gamma_{m-1}, \gamma_m$ tales que $g_{\gamma_i} : [0, \zeta_i] \to [0, \zeta_i]$ es sobreyectiva.

Como el máximo local de $g_{\gamma_i}$ en cada bloque de $\Pi$ es (3.13) y el máximo valor de los parámetros $\rho_i$ es uno, se satisface que:

$$\max_{x \in I} g_{\gamma_i}(x) = \frac{\gamma_i}{4}, \tag{3.17}$$

al sustituir en (3.17) cada uno de los parámetros de control $\gamma_i$ que se calculan mediante (3.15) y considerar que se satisface (3.11):

$$\max_{x \in I} g_{\gamma_1} = \frac{\zeta_1}{\rho_1} \neq \max_{x \in I} g_{\gamma_2} = \frac{\zeta_2}{\max\limits_{j \leq 2} \rho_j} \neq \cdots \neq \max_{x \in I} g_{\gamma_{m-1}} = \frac{\zeta_{m-1}}{\max\limits_{j \leq m-1} \rho_j}, \tag{3.18}$$

resulta que para parámetros de control arbitrarios $\gamma_i$ y $\gamma_j$ donde $i \neq j$ se satisface que si $\frac{1}{4}\gamma_i \neq \frac{1}{4}\gamma_j$ entonces $\gamma_i \neq \gamma_j$; además, como $\max\limits_{x \in I} g_4(x) = 1$ y se satisface (3.12). Para cualquier parámetro $\gamma_i \neq \gamma_m = 4$ el máximo valor de $g$ en $I$ es menor a uno por lo que $\gamma_1 \neq \gamma_2 \neq \cdots \neq \gamma_{m-1} \neq \gamma_m$ e $I$ es invariante bajo cada $g_{\gamma_i}$ donde $i \in \{1, 2, \ldots, m\}$; por todo esto la familia $\{g_{\gamma_i}\}_{i=1}^{m}$ es multimodal.

$\Longleftarrow$ Sea $g_4$ un mapeo m-modal descrito por (3.9) sobreyectivo en $I$ y se supone que existen parámetros de control que forman una familia multimodal; se debe probar que la existencia de dichos parámetros de control implican que se satisfacen las condiciones (3.11) y (3.12).

Al tener en cuenta que para un parámetro de control $\gamma_i$ en $J_i = [0, \zeta_i]$ donde $i \in \{1, 2, \ldots, m\}$ se tiene $i$ máximos locales que son $g_{\gamma_i}\left(x_c^{(1)}\right) = \rho_1 \frac{\gamma_i}{4}$ , $g_{\gamma_i}\left(x_c^{(2)}\right) = \rho_2 \frac{\gamma_i}{4}, \ldots, g_{\gamma_i}\left(x_c^{(i)}\right) = \rho_i \frac{\gamma_i}{4}$ y se satisface que:

$$\max_{x \in J_i} g_{\gamma_i}(x) = \zeta_i, \tag{3.19}$$

porque $g_{\gamma_i}$ es sobreyectivo en $J_i$. Resulta que $\rho_j \frac{\gamma_i}{4} < \zeta_i$ o $\rho_j \frac{\gamma_i}{4} = \zeta_i$ donde $j \in \{1, 2, \ldots, i\}$. Por lo tanto para el máximo valor $\rho_j$ se satisface que:

$$\max_{j \leq i} \rho_j \frac{\gamma_i}{4} = \zeta_i, \tag{3.20}$$

así que el parámetro de control $\gamma_i$ se describe por:

$$\gamma_i = 4 \frac{\zeta_i}{\max\limits_{j \leq i} \rho_j}, \tag{3.21}$$

como $\gamma_i$ es arbitrario para $i, j \in \{1, 2, \ldots, m\}$; para parámetros de control $\gamma_i$ y $\gamma_j$ donde $i \neq j$ se satisface que:

$$4\frac{\zeta_i}{\max\limits_{k\leq i} \rho_k} \neq 4\frac{\zeta_j}{\max\limits_{k\leq j} \rho_k}, \tag{3.22}$$

entonces $\frac{\zeta_i}{\max\limits_{k\leq i} \rho_k} \neq \frac{\zeta_j}{\max\limits_{k\leq j} \rho_k}$ y como ambos son arbitrarios se satisface la condición (3.11); además, considerando que para el parámetro $\gamma_m = 4$ el mapeo $g_4 : I \to I$ es sobreyectivo, todos los parámetros de control son distintos y para todo $\gamma_i$, $I$ es invariante bajo el mapeo $g_{\gamma_i}$. Si $x \in I$ para cualquier $\gamma_i \in \{\gamma_1, \gamma_2, \ldots, \gamma_{m-1}\}$ se satisface que:

$$\max_{x\in I} g_{\gamma_i}(x) = \frac{\zeta_i}{\max\limits_{j\leq i} \rho_j} < 1, \tag{3.23}$$

por lo que se satisface la condición (3.12). En consecuencia, si existen los parámetros que forman la familia multimodal se satisfacen las condiciones (3.11) y (3.12). □

Como segundo ejemplo se toma la secuencia finita $(\zeta_i)_{i=0}^3 = \left(0, \frac{1}{5}, \frac{3}{5}, 1\right)$ que determina una partición no uniforme de $I$ y también la secuencia $(\rho_i)_{i=1}^3 = (1, 0.7, 0.6)$ para fijar los dominios y máximos locales de cada parte del mapeo (3.9), respectivamente. Así se obtiene el mapeo trimodal:

$$g_\gamma(0, 0.2, 0.6, 1, 1, 0.7, 0.6, x) = \begin{cases} \gamma \cdot 25(0.2 - x)(x - 0), & 0 \leq x \leq 0.2; \\ \gamma \cdot 4.375(0.6 - x)(x - 0.2), & 0.2 < x \leq 0.6; \\ \gamma \cdot 3.75(1 - x)(x - 0.6), & 0.6 < x \leq 1, \end{cases} \tag{3.24}$$

como $\max\limits_{j\leq 3} \rho_j = 1$ el mapeo $g_4$ es sobreyectivo en $I$; además, como se satisface que $\max\limits_{j\leq 3} = \rho_1$ al verificar si se satisfacen las condiciones (3.11) y (3.12) se obtiene que:

$$\frac{0.2}{1} = 0.2 < \frac{0.6}{1} = 0.6 < 1, \tag{3.25}$$

y ya que los valores de la secuencia finita $(\zeta_i)_{i=0}^3$ satisfacen que $\zeta_0 = 0 < \zeta_1 < \cdots < \zeta_{m-1} < \zeta_m = 1$, *por construcción se satisfacen ambas condiciones* y por lo tanto existen parámetros $\gamma_1, \gamma_2, \gamma_3$ tales que se satisface la definición 3.4.

Los parámetros de control se calculan mediante (3.15) y son $\gamma_1 = 4(0.2) = 0.8$, $\gamma_2 = 4(0.6) = 2.4$ y $\gamma_3 = 4$. Así que la familia $\{g_{0.8}, g_{2.4}, g_4\}$ es multimodal donde $g_\gamma$ es el mapeo trimodal (3.24). Observe en la tabla 3.1 los máximos locales del mapeo (3.24) para cada parámetro de control. En la primer columna se presenta los parámetros de control; en las siguientes se presenta el máximo local de $g_{\gamma_i}$ para $x_c^{(1)} = 0.1$, $x_c^{(2)} = 0.4$ y $x_c^{(3)} = 0.8$, respectivamente.

Tabla 3.1: Máximos locales de la familia multimodal $\{g_{0.8}, g_{2.4}, g_4\}$.

| $i$ | $g_{\gamma_i}\left(x_c^{(1)}\right)$ | $g_{\gamma_i}\left(x_c^{(2)}\right)$ | $g_{\gamma_i}\left(x_c^{(3)}\right)$ |
|---|---|---|---|
| 1 | 0.2 | 0.14 | 0.12 |
| 2 | 0.6 | 0.42 | 0.36 |
| 3 | 1 | 0.7 | 0.6 |

### 3.1.1. Análisis de la dinámica del mapeo m-modal

Una vez que se tiene las condiciones necesarias y suficientes para seleccionar mapeos m-modales que forman una familia multimodal se prosigue a analizar la dinámica de cada uno de sus mapeos. Como cada uno de los mapeos se va a utilizar para desarrollar un generador de bits seudo-aleatorios, deben presentar comportamiento *caótico* ya que éste parece *impredecible* aunque es completamente *determinista*; es decir, su comportamiento es *seudo-aleatorio*. Es importante mencionar que hay dinámicas que no se desean; por ejemplo, los puntos fijos asintóticamente estables. Si la órbita de algún mapeo converge a un punto fijo en un estado $n \in \mathbb{N}$, entonces los términos posteriores a éste son los mismos por lo que se obtiene un *comportamiento completamente predecible*, que es contrario al que se busca.

Para evitar la existencia de mapeos en una familia multimodal que presenten puntos fijos asintóticamente estables se realiza un análisis de estabilidad local. La familia multimodal se compone de $m$ mapeos $\{g_{\gamma_i}\}_{i=1}^{m}$; para encontrar los puntos fijos de cada uno se resuelve la ecuación:

$$x_{n+1} = g_{\gamma_i}(\zeta_0, \dots \zeta_m, \rho_1, \dots, \rho_m, x_n) = x_n, \tag{3.26}$$

donde $g_{\gamma_i}$ es un mapeo m-modal que se describe por (3.9). Para calcular los puntos fijos del mapeo m-modal, se analiza cada una de sus partes por separado; así que los puntos fijos de cada una de éstas se calculan acorde con:

$$f_{\gamma_i}^{(j)}(x_n) = \gamma_i \frac{\rho_j}{\sigma_j^2}(\zeta_j - x_n)(x_n - \zeta_{j-1}) = x_n, \tag{3.27}$$

donde $i, j \in \{1, 2, \dots, m\}$. Entonces cada parte de la función puede tener hasta dos puntos fijos; por lo tanto, un mapeo m-modal puede tener hasta $2m$ puntos fijos y una

familia multimodal hasta $2m^2$. Los puntos fijos del mapeo (3.27) que se obtienen son:

$$\overline{x}_{+,-}^{(i,j)} = \frac{{\sigma_j}^2 - \gamma_i\rho_j\left(\zeta_j + \zeta_{j-1}\right) \pm \sigma_j\sqrt{\gamma_i{}^2{\rho_j}^2 - 2\gamma_i\rho_j\left(\zeta_{j-1} + \zeta_j\right) + {\sigma_j}^2}}{-2\gamma_i\rho_j}, \tag{3.28}$$

y existen siempre que:

$$\gamma_i > \frac{\zeta_{j-1} + \zeta_j + \sqrt{\zeta_{j-1}\zeta_j - \sigma_j^2}}{\rho_j}, \tag{3.29}$$

ya que cada uno de los parámetros de control de la familia multimodal satisface que $\gamma_i > 0$.

Al restringir el dominio de cada mapeo m-modal $g_{\gamma_i}$ al bloque $S_1 = [\zeta_0 = 0, \zeta_1]$ siempre existe el punto fijo $\overline{x}_-^{(i,1)} = 0$ que es asintóticamente estable a condición de que $\left|{f'_{\gamma_i}}^{(1)}\left(\overline{x}_-^{(i,1)}\right)\right| < 1$. A continuación se busca los parámetros de control $\gamma_i$ tales que satisfacen dicha desigualdad. Para esto primero se evalúa ${f'_{\gamma_i}}^{(1)}$ en el punto fijo $\overline{x}_-^{(i,1)} = 0$:

$${f'_{\gamma_i}}^{(1)}(0) = -2\gamma_i\frac{\rho_1}{\sigma_1^2}(0) + \gamma_i\frac{\rho_1}{\sigma_1^2}(\zeta_0 + \zeta_1) = \gamma_i\frac{\rho_1}{\zeta_1}, \tag{3.30}$$

después se busca los parámetros $\gamma_i$ tales que satisfacen:

$$\left|\gamma_i\frac{\rho_1}{\zeta_1}\right| < 1, \tag{3.31}$$

al resolver la desigualdad y como todo $\gamma_i > 0$ se obtiene que si:

$$\gamma_i \in \left(0, \frac{\zeta_1}{\rho_1}\right), \tag{3.32}$$

el punto fijo $\overline{x}_-^{(i,1)} = 0$ es asintóticamente estable. En caso de que $\gamma_i > \frac{\zeta_1}{\rho_1}$ se tiene un segundo punto fijo que es:

$$\overline{x}_+^{(i,1)} = \frac{\gamma_i\zeta_1\rho_1 - {\zeta_1}^2}{\gamma_i\rho_1}, \tag{3.33}$$

de forma análoga, se busca los parámetros $\gamma_i > 0$ tales que satisfacen la desigualdad $\left|{f'_{\gamma_i}}^{(1)}\left(\overline{x}_+^{(i,1)}\right)\right| < 1$. Al resolverla se obtiene que el punto fijo $\overline{x}_+^{(i,1)}$ es asintóticamente estable si el parámetro de control pertenece a la región:

$$\gamma_i \in \left(\frac{\zeta_1}{\rho_1}, 3\frac{\zeta_1}{\rho_1}\right). \tag{3.34}$$

Se prosigue el análisis con los puntos fijos que pertenecen a los demás intervalos de la partición uniforme o no uniforme de $I$. Por consiguiente, siempre y cuando existen ambos puntos fijos, $\overline{x}_-^{(i,j)}$ es asintóticamente estable a condición de que $\left|{f'_{\gamma_i}}^{(j)}\left(\overline{x}_-^{(i,j)}\right)\right| < 1$; como

no existe un $\gamma_i$ tal que satisface dicha condición este punto fijo es *inestable*. En cuanto el punto fijo $\overline{x}_+^{(i,j)}$, es asintóticamente estable a condición de que $\left|f'^{\,(j)}_{\gamma_i}\left(\overline{x}_+^{(i,j)}\right)\right| < 1$, al resolver la desigualdad se obtiene que si:

$$\gamma_i \in \left(\frac{\zeta_{j-1}+\zeta_j+2\sqrt{\zeta_{j-1}\zeta_j}}{\rho_j}, \frac{\zeta_{j-1}+\zeta_j+2\sqrt{\sigma_j^2+\zeta_{j-1}\zeta_j}}{\rho_j}\right), \tag{3.35}$$

el punto fijo $\overline{x}_+^{(i,j)}$ es asintóticamente estable. De esta forma se puede verificar si algún parámetro de control $\gamma_i$ de la familia multimodal $\{g_{\gamma_1}, g_{\gamma_2}, \ldots, g_{\gamma_m}\}$ se encuentra en la región donde los puntos fijos son asintóticamente estables; en cuyo caso dicha familia multimodal *no es de interés* para desarrollar generadores de números seudo-aleatorios.

Para ejemplificar el resultado del análisis de estabilidad local se emplea la familia multimodal $\{g_{0.8}, g_{2.4}, g_4\}$ para la que el mapeo trimodal $g_\gamma$ se describe por (3.24). El primer mapeo de la familia multimodal es:

$$x_{n+1} = g_{0.8}(x_n) = \begin{cases} 20(0.2-x_n)(x_n-0), & 0 \le x_n \le 0.2; \\ 3.5(0.6-x_n)(x_n-0.2), & 0.2 < x_n \le 0.6; \\ 3(1-x_n)(x_n-0.6), & 0.6 < x_n \le 1, \end{cases} \tag{3.36}$$

el mapeo $g_{0.8}$ tiene dos puntos fijos que son $\overline{x}_-^{(1,1)} = 0$ y $\overline{x}_+^{(1,1)} = 0.15$. El segundo mapeo de la familia multimodal es:

$$x_{n+1} = g_{2.4}(x_n) = \begin{cases} 60(0.2-x_n)(x_n-0), & 0 \le x_n \le 0.2; \\ 10.5(0.6-x_n)(x_n-0.2), & 0.2 < x_n \le 0.6; \\ 9(1-x_n)(x_n-0.6), & 0.6 < x_n \le 1, \end{cases} \tag{3.37}$$

el segundo mapeo $g_{2.4}$ tiene cuatro puntos fijos que son $\overline{x}_-^{(2,1)} = 0$, $\overline{x}_+^{(2,1)} = 0.183$, $\overline{x}_-^{(2,2)} = 0.288$ y $\overline{x}_+^{(2,2)} = 0.417$. El último mapeo de la familia multimodal es el mapeo:

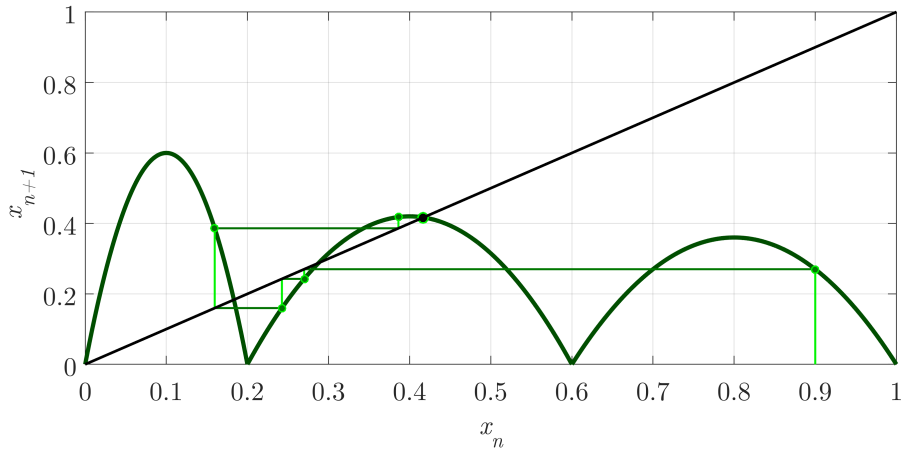
$$x_{n+1} = g_4(x_n) = \begin{cases} 100(0.2-x_n)(x_n-0), & 0 \le x_n \le 0.2; \\ 17.5(0.6-x_n)(x_n-0.2), & 0.2 < x_n \le 0.6; \\ 15(1-x_n)(x_n-0.6), & 0.6 < x_n \le 1, \end{cases} \tag{3.38}$$

el último mapeo $g_4$ tiene cuatro puntos fijos que son $\overline{x}_-^{(3,1)} = 0$, $\overline{x}_+^{(3,1)} = 0.19$, $\overline{x}_-^{(3,2)} = 0.237$ y $\overline{x}_+^{(3,2)} = 0.505$. Esta familia multimodal tiene un total de diez puntos fijos; el siguiente paso es verificar si algún parámetro de control se encuentra en las regiones donde los puntos fijos son asintóticamente estables. Así que al calcular las regiones de estabilidad para cada punto fijo:

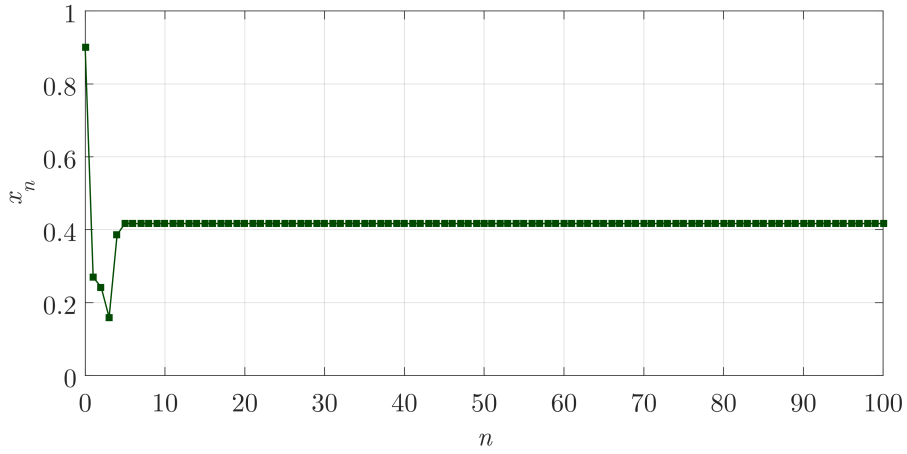
$$\gamma_i \in (0, 0.2) \cup (0.2, 0.6) \cup (2.133, 2.655), \tag{3.39}$$

se encuentra que $\gamma_2 \in (2.133, 2.655)$ por lo que el punto fijo $\overline{x}_+^{(2,2)} = 0.417$ es asintóticamente estable.

Observe en la Figura 3.1 como la órbita de un punto inicial $x_0 \in (0,1)$ bajo $g_{2.4}$ converge al punto fijo $\overline{x}_+^{(2,2)} = 0.417$. Una vez que la órbita converge al punto fijo sus términos posteriores son iguales; por lo tanto su evolución a largo plazo es *completamente predecible* aunque se desconozca el punto inicial que produce dicha órbita, contrario al comportamiento seudo-aleatorio que se busca.




(a) Diagrama de escalón



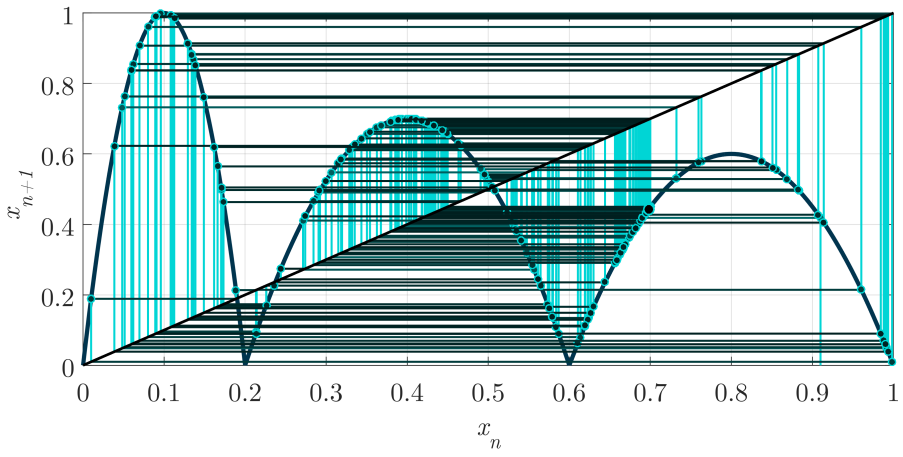

(b) Serie de tiempo

Figura 3.1: Representación gráfica de la órbita de $x_0 = 0.9$ bajo el mapeo trimodal $g_{0.8}$ en la que se muestra como la evolución a largo plazo converge al punto fijo $\overline{x}_+^{(2,2)} = 0.417$.

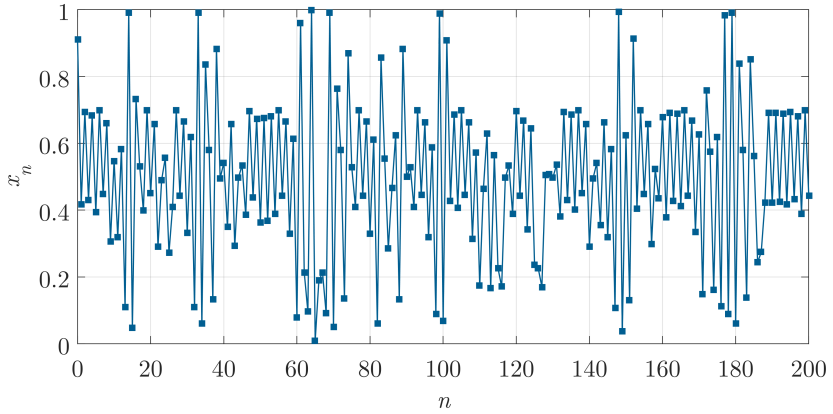
En cuanto a los demás mapeos de la familia multimodal; aunque se sabe que no presentan puntos fijos asintóticamente estables, se desconoce si presentan algún $h-ciclo$

asintóticamente estable donde $h \in \mathbb{N}$. Es por esto que se emplea el *exponente de Lyapunov*; así, por ejemplo, se calcula el exponente de Lyapunov para la órbita de un punto inicial $x_0 \in (0,1)$ bajo el mapeo $g_4$. Se itera $x_0 = 0.91$ bajo $g_4$ un total 400 000 000 veces y se calcula el exponente de Lyapunov; así se obtiene que $\lambda_3 = 0.6932$. Como $\lambda_3 > 0$, $g_4$ es un sistema dinámico determinista e $I$ es invariante bajo $g_4$; cada elemento de la órbita está acotado por 0 y 1; indica *comportamiento caótico*.

Observe en la Figura 3.2 la órbita que se usa para calcular el exponente de Lyapunov. Como $g_4$ presenta comportamiento caótico, la evolución a largo plazo de una condición inicial que se desconoce es impredecible; no obstante, ya que $g_{2.4}$ presenta comportamiento predecible, esta familia multimodal se descarta para la realización de un generador de bits seudo-aleatorios..




(a) Diagrama de escalón




(b) Series de tiempo

Figura 3.2: Representación gráfica de la órbita de $x_0 = 0.91$ bajo el mapeo trimodal $g_4$ que presenta comportamiento caótico.

#### 3.1.1.1. Propiedad de transitividad

Una de las propiedades que presenta el comportamiento caótico acorde con la definición de Devaney es la *transitividad*, dicha propiedad describe que dado cualquier par de abiertos $U_1$ y $U_2$ de $X$, existe un punto $x_0 \in U_1$ y un $n > 0$ para el que $f^n(x_0) \in U_2$. Es importante mencionar que el Teorema 3.1 *únicamente permite conocer* si los parámetros del mapeo m-modal sirven para obtener una familia multimodal. Puesto que se busca condiciones necesarias para que la propiedad de transitividad se pueda satisfacer para cada mapeo de la familia multimodal $g_{\gamma_i}$ en el intervalo $[0, \zeta_i] \subset I$ donde $i \in \{1, 2, \ldots, m\}$ se realiza el siguiente análisis:

Para comenzar se analiza un mapeo m-modal con parámetros que satisfacen las desigualdades $\rho_1 < \rho_2 < \cdots < \rho_m$. Así, por ejemplo, se toma la secuencia finita $(\zeta_i)_{i=0}^3 = \left(0, \frac{1}{4}, \frac{1}{2}, 1\right)$ que determina una partición no uniforme de $I$ y también la secuencia $(\rho_i)_{i=1}^3 = (0.26, 0.51, 1)$ para fijar los dominios y máximos locales de cada parte del mapeo trimodal:

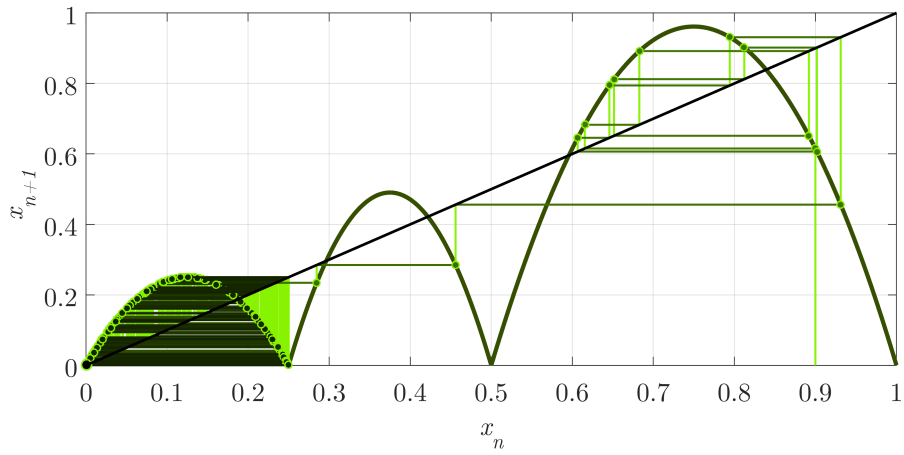
$$x_{n+1} = g_\gamma(x_n) = \begin{cases} \gamma \cdot 4.16(0.25 - x_n)(x_n - 0), & 0 \leq x_n \leq 0.25; \\ \gamma \cdot 8.16(0.5 - x_n)(x_n - 0.2), & 0.25 < x_n \leq 0.5; \\ \gamma \cdot 4(1 - x_n)(x_n - 0.5), & 0.5 < x_n \leq 1, \end{cases} \tag{3.40}$$

como $\underset{j\leq 3}{\max} \rho_j = 1$ y $\frac{\zeta_1}{\rho_1} = 0.962 < \frac{\zeta_2}{\underset{i\leq 2}{\max} \rho_i} = 0.980 < 1$, se satisfacen las condiciones del Teorema 3.1 por lo que existen parámetros $\gamma_i$ que forman una familia multimodal. Los parámetros son $\gamma_1 = 4\frac{0.25}{0.26} = 3.846$, $\gamma_2 = 4\frac{0.5}{0.51} = 3.922$ y $\gamma_3 = 4$. En la tabla 3.2 se presentan los parámetros de interés de la familia multimodal; en la primer columna los parámetros de control; en las siguientes tres los máximos locales en cada bloque de la partición de $I$ y por último los puntos fijos del mapeo (3.40) para los parámetros de control $\gamma_1$, $\gamma_2$ y $\gamma_3$.

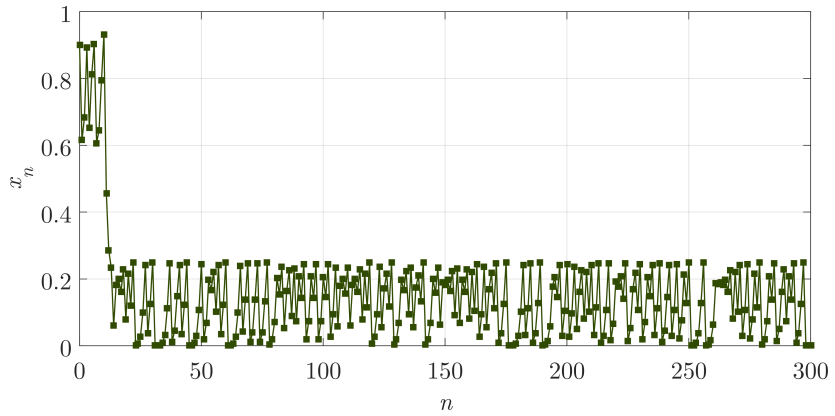
Tabla 3.2: Características de la familia multimodal $\{g_{3.846}, g_{3.922}, g_4\}$.

| $i$ | $g_{\gamma_i}\left(x_c^{(1)}\right)$ | $g_{\gamma_i}\left(x_c^{(2)}\right)$ | $g_{\gamma_i}\left(x_c^{(3)}\right)$ | $\overline{x}_{-,+}^{(i,1)}$ | $\overline{x}_{-,+}^{(i,2)}$ | $\overline{x}_{-,+}^{(i,3)}$ |
|---|---|---|---|---|---|---|
| 1 | 0.25 | 0.49 | 0.962 | 0, 0.188 | 0.296, 0.422 | 0.596, 0.839 |
| 2 | 0.255 | 0.5 | 0.98 | 0, 0.189 | 0.295, 0.424 | 0.593, 0.843 |
| 3 | 0.26 | 0.51 | 1 | 0, 0.19 | 0.294, 0.426 | 0.59, 0.848 |

Como el mapeo $g_{3.846}$ es sobreyectivo en $J_1 = [0, \zeta_1 = 0.25]$ por construcción; cada valor de $J_1$ es alcanzable por $g_{3.846}(x_n)$ cuando $x_n \in J_1$. Observe en la Figura 3.3 como la evolución a largo plazo de un punto inicial $x_0 \in I$ bajo el mapeo $g_{3.846}$ se esparce por el intervalo $J_1$.




(a) Iteración gráfica




(b) Series de tiempo

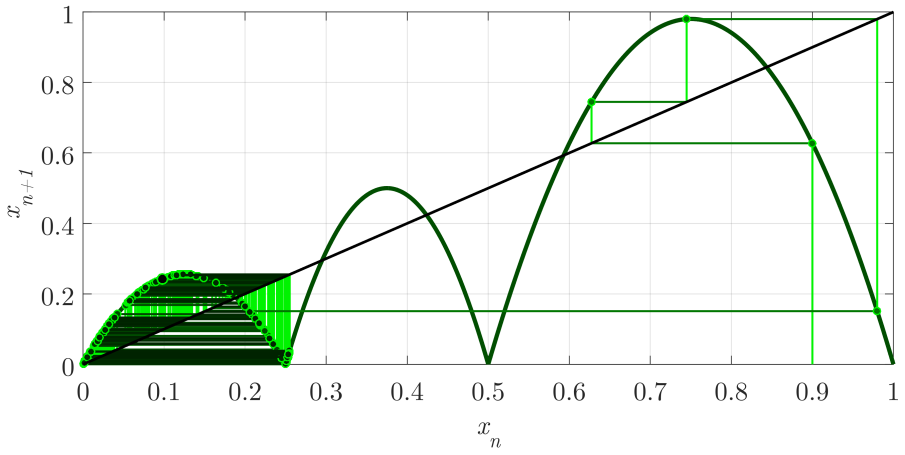
Figura 3.3: Representación gráfica de la órbita de $x_0 = 0.9$ bajo $g_{3.846}$ donde se observa que se esparce por todo $J_1 = [0, 0.25]$.

Se prosigue el análisis con el mapeo $g_{3.922}$, observe que si $x_n \in \left[0, \overline{x}_-^{(2,2)} = 0.295\right]$; entonces el máximo valor de $g_{3.922}$ en $[0, 0.295]$ puede ser el máximo local $g_{3.922}\left(x_c^{(1)}\right) = 0.255$ o el punto fijo $\overline{x}_-^{(2,2)} = 0.295$. Como $g_{3.922}\left(x_c^{(1)}\right) < \overline{x}_-^{(2,2)}$ el intervalo $[0, 0.295]$ es invariante bajo $g_{3.922}$; por esto si $x_n \in [0, 0.295]$ entonces no existe un $n > 0$ tal que $g_{3.922} > 0.295$ y por lo tanto una *condición necesaria* para que $g_{\gamma_2}$ sea transitivo en

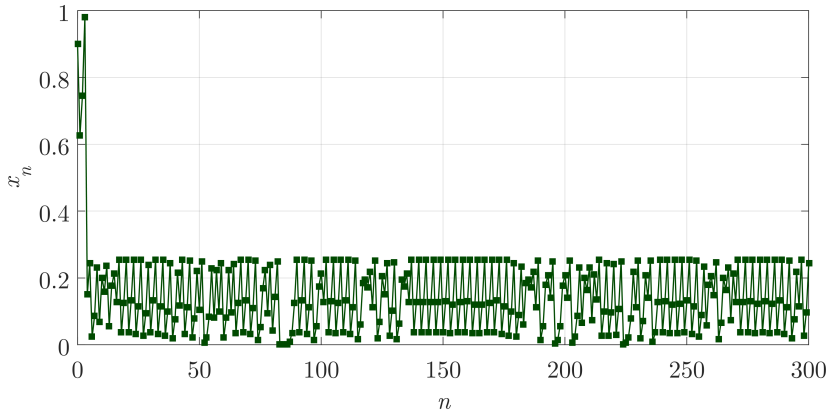
$J_2 = [0, \zeta_2]$ es que se cumpla la desigualdad:

$$\rho_1 > \frac{4}{\gamma_2}\overline{x}_{-}^{(2,2)}, \tag{3.41}$$

para ilustrar dicha condición se presenta en la Figura 3.4 la evolución a largo plazo de un punto inicial $x_0 \in I$ bajo el mapeo $g_{3.922}$. Observe que cuando se obtiene un estado $x_n \in [0, 0.295]$ en la órbita, los valores posteriores se mantienen acotados por el punto fijo $\overline{x}_{-}^{(2,2)} = 0.295$ y cero.




(a) Iteración gráfica




(b) Series de tiempo

Figura 3.4: Representación gráfica de la órbita de $x_0 = 0.9$ bajo el mapeo $g_{3.922}$ donde se observa que la evolución a largo plazo no se esparce por todo $J_2 = [0, 0.5]$.

El último mapeo de la familia multimodal es $g_4$ y se busca que sea transitivo en $I$. En este caso aparecen dos intervalos de interés que son $\left[0, \overline{x}_{-}^{(3,2)} = 0.294\right]$ y $\left[0, \overline{x}_{-}^{(3,3)} = 0.59\right]$. De forma análoga a la anterior, si $x_n \in [0, 0.294]$ el máximo valor de $g_4$ es el máximo local

$g_4\left(x_c^{(1)}\right) = \rho_1$ o el punto fijo $\overline{x}_-^{(3,2)}$ por lo que si $\rho_1 < \overline{x}_-^{(3,2)}$ dicho intervalo es invariante bajo $g_4$. Puesto que se quiere que $g_4$ sea transitivo en $I$ una *condición necesaria* es que:

$$\rho_1 > \frac{4}{\gamma_3}\overline{x}_-^{(3,2)} = \overline{x}_-^{(3,2)}, \tag{3.42}$$

por lo que se refiere al segundo intervalo; en caso de que $x_n \in [0, 0.59]$ el máximo valor del mapeo $g_4$ es el máximo local $g_4\left(x_c^{(2)}\right) = \rho_2$ debido a que $g_4\left(x_c^{(1)}\right) = \rho_1 < g_4\left(x_c^{(2)}\right) = \rho_2$ o el punto fijo $\overline{x}_-^{(3,3)}$. Por lo cual si $\rho_2 < \overline{x}_-^{(3,3)}$ el intervalo $[0, 0.59]$ es invariante bajo $g_4$. Así que para que dicho intervalo no sea invariante bajo $g_4$ se debe satisfacer que:

$$\rho_2 > \frac{4}{\gamma_3}\overline{x}_-^{(3,3)} = \overline{x}_-^{(3,3)}, \tag{3.43}$$

otra *condición necesaria* para que $g_4$ sea transitivo en $I$.

Es importante mencionar que para satisfacer dichas condiciones se puede cambiar los máximos locales o los términos que determinan la partición de $I$ en el mapeo (3.40). Para este ejemplo se modifica los máximos locales debido a que el término queda de manera explícita. Como $\rho_2 = 0.51 < \overline{x}_-^{(3,3)} = 0.59$ se modifica este parámetro por $\rho_2 = 0.7$ de modo que se satisface (3.43). Así se obtiene un nuevo punto fijo $\overline{x}_-^{(2,2)} = 0.284$; también se cambia el parámetro $\rho_1 = 0.21$ por $\rho_1 = 0.4$ debido a que $\rho_1 > \frac{4}{\gamma_2}\overline{x}_-^{(2,2)} = 0.354$ y $\rho_1 > \frac{4}{\gamma_3}\overline{x}_-^{(3,2)} = 0.284$ por lo que se satisfacen ambas condiciones (3.41) y (3.42). Así se obtiene un nuevo mapeo trimodal:

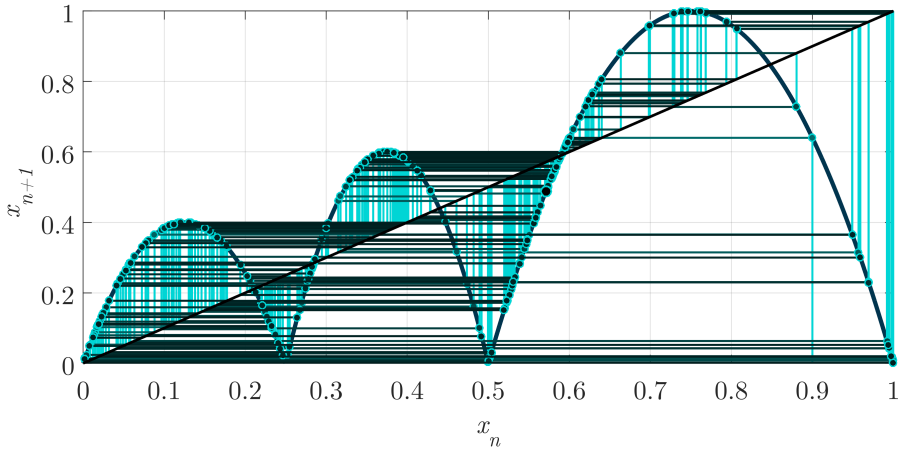
$$x_{n+1} = g_\gamma(x_n) = \begin{cases} \gamma \cdot 6.4(0.25 - x_n)(x_n - 0), & 0 \leq x_n \leq 0.25; \\ \gamma \cdot 9.6(0.5 - x_n)(x_n - 0.2), & 0.25 < x_n \leq 0.5; \\ \gamma \cdot 4(1 - x_n)(x_n - 0.5), & 0.5 < x_n \leq 1, \end{cases} \tag{3.44}$$

como $\underset{j\leq 3}{\max}\rho_j = 1$ y se satisfacen las desigualdades $\frac{\zeta_1}{\rho_1} = 0.625 < \frac{\zeta_2}{\underset{i\leq 2}{\max}\rho_i} = 0.833 < 1$. Existen parámetros $\gamma_i$ que forman una familia multimodal. Los parámetros son $\gamma_1 = 2.5$, $\gamma_2 = 3.333$ y $\gamma_3 = 4$. De forma análoga a la anterior, se presenta los parámetros de interés de la familia multimodal en la tabla 3.3 donde se observa que se cumplen las condiciones anteriores.

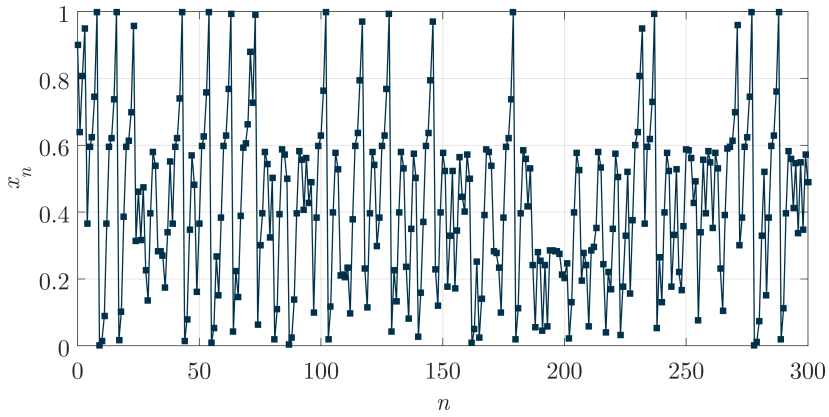
Tabla 3.3: Características de la familia multimodal $\{g_{2.5}, g_{3.333}, g_4\}$.

| $i$ | $g_{\gamma_i}\left(x_c^{(1)}\right)$ | $g_{\gamma_i}\left(x_c^{(2)}\right)$ | $g_{\gamma_i}\left(x_c^{(3)}\right)$ | $\overline{x}_{-,+}^{(i,1)}$ | $\overline{x}_{-,+}^{(i,2)}$ | $\overline{x}_{-,+}^{(i,3)}$ |
|---|---|---|---|---|---|---|
| 1 | 0.25 | 0.375 | 0.625 | 0, 0.188 | 0.333, 0.375 | - |
| 2 | 0.333 | 0.5 | 0.833 | 0, 0.203 | 0.295, 0.424 | 0.625, 0.8 |
| 3 | 0.4 | 0.6 | 1 | 0, 0.211 | 0.284, 0.44 | 0.59, 0.848 |

Como muestra del análisis anterior se presenta en la Figura 3.5 la evolución a largo plazo de un punto inicial $x_0 \in I$ bajo $g_4$. Note que los intervalos que se forman $\left[0, \overline{x}_{-}^{(3,2)} = 0.284\right]$ y $\left[0, \overline{x}_{-}^{(3,3)} = 0.59\right]$ no son invariantes bajo $g_4$.




(a) Iteración gráfica




(b) Series de tiempo

Figura 3.5: Representación gráfica de la órbita de $x_0 = 0.9$ bajo el mapeo $g_4$ en la cual se observa que la evolución a largo plazo se esparce por el intervalo unitario $I$.

Es importante mencionar que en caso de que el parámetro $\rho_1$ tenga valor unitario; es decir, sea el máximo valor de $\rho_i$ donde $i \in \{1, 2, \ldots, m\}$. Entonces las condiciones necesarias que se encuentran se satisfacen automáticamente lo que facilita la selección de parámetros. Esto se observa al reescribir las condiciones (3.42) y (3.43) como:

$$\max_{i \leq 2} \rho_i > \frac{4}{\gamma_3} \overline{x}_{-}^{(3,3)} = \overline{x}_{-}^{(3,3)}, \tag{3.45}$$

ya que el máximo valor del mapeo en $I$ es $g_{\gamma_3}\left(x_c^1\right) = 1$ y los puntos fijos por construcción

son menores a uno, ambos intervalos $[0, \overline{x}_{-}^{(3,2)}]$ y $[0, \overline{x}_{-}^{(3,3)}]$ no van a ser invariantes bajo $g_{\gamma_3}$. Además, de forma análoga a la anterior; por construcción el máximo valor del mapeo en $[0, \zeta_2]$ es $g_{\gamma_2}(x_c^i) = \zeta_2$ y lo tanto los puntos fijos que aparecen en dicho intervalo tienen valores menores por lo que se satisface la condición (3.41).

Observe en la tabla 3.4 los parámetros de interés de la familia multimodal que se obtiene a partir del mapeo:

$$g_\gamma(x_n) = \begin{cases} \gamma \cdot 25(0.2 - x_n)(x_n - 0), & 0 \leq x_n \leq 0.2; \\ \gamma \cdot 4.375(0.6 - x_n)(x_n - 0.2), & 0.2 < x_n \leq 0.6; \\ \gamma \cdot 3.75(1 - x_n)(x_n - 0.6), & 0.6 < x_n \leq 1, \end{cases} \tag{3.46}$$

que se obtuvo anteriormente. Note que los intervalos que aparecen anteriormente se evitan completamente al fijar el parámetro $\rho_1$ a tener valor unitario. Para un número mayor o menor de $m$ se realiza un análisis similar al que se presenta en este documento.

Tabla 3.4: Características de la familia multimodal $\{g_{0.8}, g_{2.4}, g_4\}$.

| $i$ | $g_{\gamma_i}\left(x_c^{(1)}\right)$ | $g_{\gamma_i}\left(x_c^{(2)}\right)$ | $g_{\gamma_i}\left(x_c^{(3)}\right)$ | $\overline{x}_{-,+}^{(i,1)}$ | $\overline{x}_{-,+}^{(i,2)}$ | $\overline{x}_{-,+}^{(i,3)}$ |
|---|---|---|---|---|---|---|
| 1 | 0.2 | 0.14 | 0.12 | 0, 0.15 | - | - |
| 2 | 0.6 | 0.42 | 0.36 | 0, 0.183 | 0.28, 0.417 | - |
| 3 | 1 | 0.7 | 0.6 | 0, 0.19 | 0.227, 0.505 | - |

## 3.2. Desarrollo del generador de bits

Para desarrollar un generador de bits con base en el mapeo m-modal se comienza *eligiendo el número* $m \in \mathbb{N}\backslash\{1\}$; esto es, el número de mapeos unimodales que van a existir en $I$. Después se *selecciona parámetros que permitan obtener una familia multimodal*; para esto se elige los valores de la secuencia finita $(\zeta_i)_{i=0}^m$ que van a determinar una partición uniforme o no uniforme de $I$; es importante hacer énfasis en que los parámetros de la secuencia finita deben satisfacer que:

$$\zeta_0 = 0 < \zeta_1 < \cdots < \zeta_{m-1} < \zeta_m = 1, \tag{3.47}$$

al mismo tiempo se elige los máximos locales $\rho_1, \rho_2, \ldots, \rho_{m-1}, \rho_m$ de tal forma que se satisfacen las condiciones del Teorema 3.1; no aparecen los invariantes que se mencionan

en la parte de transitividad y cada parámetro de control $\gamma_1, \gamma_2, \ldots, \gamma_m$ se debe encontrar fuera de las regiones en las que hay puntos fijos asintóticamente estables.

Para la siguiente etapa se toma puntos iniciales $x_0 \in I$ de 16 cifras significativas de un generador de números seudo-aleatorios que toma como entrada ruido atmosférico [34]. Con estos puntos iniciales se calcula el exponente de Lyapunov de cada mapeo de la familia multimodal para órbitas de 1 000 000 de elementos. Si todas las órbitas de cada mapeo $g_{\gamma_i}$ presenta comportamiento caótico en $J_i \subset [0, \zeta_i]$ se prosigue el método; en caso contrario se aborta el proceso.

El siguiente paso es binarizar la serie de tiempo que se obtiene de cada mapeo. Se asume que cada mapeo de la familia multimodal presenta comportamiento ergódico por lo que la *evolución a largo plazo* es independiente de la condición inicial [35]. El proceso que se emplea para binarizar es el que presentan en [12, 17, 36], buscar un umbral $\xi \in I$ que permite dividir $I$ en dos intervalos $A_1 = [0, \xi]$ y $A_2(\xi, 1]$. Así que la evolución a largo plazo de un punto inicial $x_0 \in I$ tiene el mismo número de elementos en $A_1$ y $A_2$. Después utilizar una *función umbral* que se define como:

$$\Xi_i(x_n) = \begin{cases} 0, & 0 \leq x_n < \xi_i; \\ 1, & \xi_i \leq x_n \leq 1. \end{cases} \tag{3.48}$$

Con el objetivo de aplicar la función (3.48) se busca un umbral $\xi_i$ por cada mapeo $g_{\gamma_i}$ tal que permita dividir $[0, 1]$ en dos regiones $[0, \xi_i)$ y $[\xi_i, 1]$. Se satisface que $\xi_i < \zeta_i$ debido a que la evolución a largo plazo de la órbita se contiene en $[0, \zeta_i]$ para $g_{\gamma_i}$. Se realiza un método iterativo para obtener los umbrales. Se va a iterar cada mapeo para el mismo punto inicial hasta obtener una órbita con 1 000 001 elementos. Se emplea los elementos de la serie de tiempo $(x_i)_{i=1}^{1000001}$ de cada mapeo y se realiza el proceso que se muestra en la Figura 3.6. El primer paso es suponer que el umbral es $xi = 0.5$, después se realiza el método iterativo. La aproximación realiza la ecuación:

$$xi = xi\frac{50}{P_m}, \tag{3.49}$$

donde $P_m$ es el porcentaje medido, esto se realiza un total de quince veces o un número menor si se encuentra el porcentaje deseado que es $50 \pm 0.1$ %; después, simplemente se incrementa el valor del umbral o decrementa si el porcentaje medido es menor o mayor al deseado, respectivamente. Se continua el método hasta encontrar una aproximación al umbral para el que se consigue el porcentaje deseado.

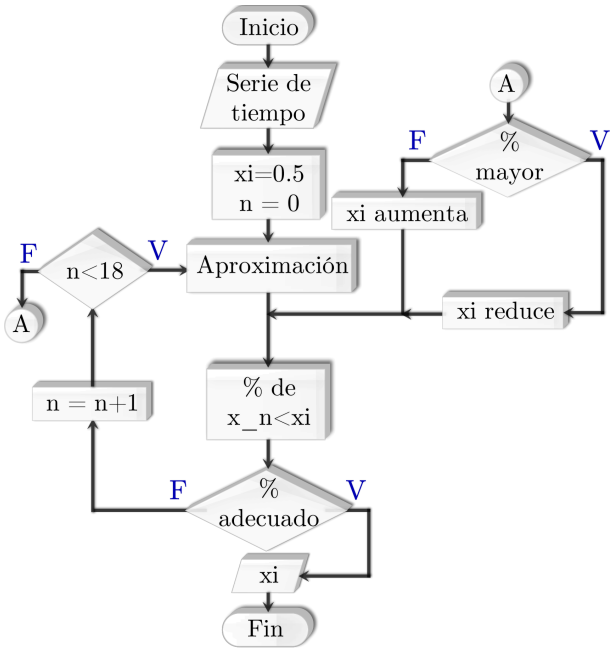



Figura 3.6: Diagrama de flujo del algoritmo iterativo que se usa para calcular el valor de cada uno de los umbrales.

El último paso es el *cálculo de la secuencia de bits* mediante el uso de las funciones umbral; es decir, una secuencia en la que cada elemento es un *cero* o un *uno*. Se van a usar las $m$ *series de tiempo para generar la secuencia de bits* para aprovechar la dinámica caótica de cada mapeo; además, incrementar el número posible de semillas lo que sería de interés para una posterior aplicación al área de criptografía.

En particular, para obtener el bit $s_{n+1}$ se van a combinar los $m$ valores binarios $\Xi_i\left(g_{\gamma_i}(x_{n_i})\right)$ mediante la operación *OR exclusiva*. En la tabla 3.5 se muestra el resultado de aplicar la operación OR exclusiva a cada combinación de dos entradas binarias.

En conclusión, cada bit de la secuencia que se genera mediante la familia multimodal se calcula conforme a la ecuación:

$$s_{n+1} = \Xi_1\left(g_{\gamma_1}(x_{n_1})\right) \oplus \Xi_2\left(g_{\gamma_2}(x_{n_2})\right) \oplus \cdots \oplus \Xi_m\left(g_{\gamma_m}(x_{n_m})\right). \tag{3.50}$$

donde $n \in \mathbb{N}$ y la semilla es una m-tupla $(x_{0_1}, x_{0_2}, \ldots, x_{0_m})$ donde el punto inicial $x_{0_i}$ se itera bajo el mapeo $g_{\gamma_i}$.

Tabla 3.5: Tabla de verdad de la operación OR exclusiva

| $p$ | $q$ | $p \oplus q$ |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

Es importante mencionar que la prueba más importante del banco de pruebas estadísticas del Instituto Nacional de Estándares y Tecnología es el de frecuencia. Dicha prueba busca que el número de ceros y unos en una secuencia sean aproximadamente iguales. En caso de que no se presente comportamiento ergódico, al iterar distintos puntos iniciales a los que se usa para obtener los umbrales se va a tener una evolución a largo plazo distinta por lo que el número de ceros y unos no van a ser aproximadamente iguales; por consiguiente, la prueba de frecuencia no se va a satisfacer. Como resultado el generador de bits no es seudo-aleatorio.

# Capítulo 4

# Generador de bits seudo-aleatorios

En este capítulo se evalúa un generador de bits por medio de las pruebas estadísticas del Instituto Nacional de Estándares y Tecnología, por sus siglas en inglés NIST. La finalidad de las pruebas es verificar si las secuencias que produce el generador de bits de manera determinista son *indistinguibles* de una secuencia aleatoria. El generador de bits se desarrolla con base en un mapeo m-modal mediante el método que se propone en el capítulo anterior.

## 4.1. Generador de bits con base en un mapeo trimodal

Para comprender mejor cada una de las etapas que conlleva el desarrollo del generador de bits con base en un mapeo m-modal se describen a detalle en este capítulo. El primer paso consiste en elegir el valor de $m \in \mathbb{N} \setminus \{1\}$; a manera de ilustración se elige $m = 3$ por lo que se va a trabajar con un mapeo trimodal. Para diseñar este generador se elige la secuencia finita $(\zeta_i)_{i=0}^{3} = \left(0, \frac{1}{5}, \frac{1}{2}, 1\right)$ que determina una partición no uniforme de $I$ y también la secuencia $(\rho_i)_{i=1}^{3} = (1, 0.9, 0.95)$ para fijar los dominios y máximos locales de cada parte del mapeo trimodal:

$$x_{n+1} = g_\gamma(x_n) = \begin{cases} \gamma \cdot 25(0.2 - x_n)(x_n - 0), & 0 \leq x_n \leq 0.2; \\ \gamma \cdot 10(0.5 - x_n)(x_n - 0.2), & 0.2 < x_n \leq 0.5; \\ \gamma \cdot 3.8(1 - x_n)(x_n - 0.5), & 0.5 < x_n \leq 1, \end{cases} \tag{4.1}$$

como $\underset{j\leq 3}{\text{máx}}\, \rho_j = 1$ y $\rho_1 = 1$ por construcción $\frac{\zeta_1}{1} = 0.2 < \frac{\zeta_2}{\underset{i\leq 2}{\text{máx}}\, \rho_i = 1} = 0.5 < 1$ por lo que se satisfacen las condiciones del Teorema 3.1. Así que existen parámetros de control tales

que se forma una familia multimodal. Los parámetros son $\gamma_1 = 4\zeta_1 = 0.8$, $\gamma_2 = 4\zeta_2 = 2$ y $\gamma_3 = 4$. En la tabla 4.1 se presentan los parámetros de interés de la familia multimodal $\{g_{0.8}, g_2, g_4\}$; en la primer columna los parámetros de control; en las siguientes tres los máximos locales en cada bloque de la partición de $I$ y por último los puntos fijos del mapeo (4.1) para los parámetros de control $\gamma_1$, $\gamma_2$ y $\gamma_3$.

Tabla 4.1: Propiedades de la familia multimodal $\{g_{0.8}, g_2, g_4\}$ que se obtiene mediante el mapeo (4.1).

| $i$ | $g_{\gamma_i}\left(x_c^{(1)}\right)$ | $g_{\gamma_i}\left(x_c^{(2)}\right)$ | $g_{\gamma_i}\left(x_c^{(3)}\right)$ | $\overline{x}_{-,+}^{(i,1)}$ | $\overline{x}_{-,+}^{(i,2)}$ | $\overline{x}_{-,+}^{(i,3)}$ |
|---|---|---|---|---|---|---|
| 1 | 0.2 | 0.18 | 0.19 | 0, 0.15 | - | - |
| 2 | 0.5 | 0.45 | 0.475 | 0, 0.18 | 0.25, 0.4 | - |
| 3 | 1 | 0.9 | 0.95 | 0, 0.19 | 0.212, 0.455 | 0.598, 0.836 |

Observe en la tabla 4.1 que el intervalo que se forma $\left[0, \overline{x}_{-}^{(2,2)} = 0.25\right]$ no es invariante bajo $g_2$ porque $\rho_1 = 1 > \frac{4}{\gamma_2}\overline{x}_{-}^{(2,2)} = 0.5$. De forma similar el intervalo $\left[0, \overline{x}_{-}^{(3,3)} = 0.598\right]$ no es invariante bajo $g_4$ debido a que $\rho_1 = 1 > \overline{x}_{-}^{(3,3)} = 0.598$. Al calcular las regiones en las que los puntos fijos son asintóticamente estables se obtiene las siguiente regiones:

$$\gamma_i \in (0, 0.2) \cup (0.2, 0.6) \cup (1.4805, 1.7465) \cup (3.0676, 3.4022), \tag{4.2}$$

como ningún parámetro de control de la familia multimodal pertenece al intervalo anterior no se tiene puntos fijos asintóticamente estables.

Para la siguiente etapa se emplea múltiples puntos iniciales que se obtienen del generador de números seudo-aleatorios [34]. Los números que se obtienen se distribuyen de manera uniforme en el intervalo $(0, 1)$ y son de 16 cifras significativas. Se itera estos puntos iniciales bajo cada mapeo de la familia multimodal hasta obtener una órbita del orden de millones; después, se calcula su exponente de Lyapunov. Se empleó más de 2 000 puntos iniciales por mapeo y no se encontró algún exponente de Lyapunov no positivo; por ejemplo, para el punto inicial $x_0 = 0.6$ bajo el mapeo $g_{0.8}$ se obtuvo $\lambda_1 = 0.6931$; para el punto inicial $y_0 = 0.7$ bajo el mapeo $g_2$ se obtuvo $\lambda_2 = 0.6932$. Por último para el punto inicial $z_0 = 0.9$ bajo el mapeo $g_4$ se obtuvo el exponente de Lyapunov $\lambda_3 = 1.1004$. Como muestra de las órbitas caóticas se presenta en la Figura 4.1 la órbita que describe un punto inicial $x_0 \in I$ bajo el mapeo $g_4$.

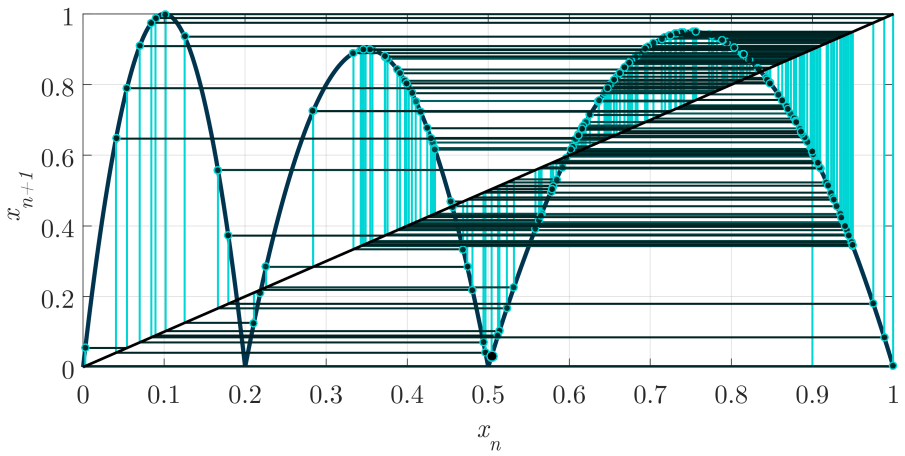



Figura 4.1: Diagrama de escalón de la órbita del punto inicial $x_0 = 0.9$ bajo el mapeo trimodal $g_4$ que se toma como base para desarrollar el generador de bits.

Como se menciona en el capítulo anterior, se transforma los elementos de $I$ al conjunto $\mathbb{Z}_2 = \{0, 1\}$ mediante funciones umbral. Para este caso se va a tener un total de tres funciones umbral, la función umbral $\Xi_i : I \to \mathbb{Z}_2$ se usa para transformar cada iteración que realice el mapeo $g_{\gamma_i}$ donde $i \in \{1, 2, 3\}$ a un valor binario. Así que se va a buscar una aproximación del valor de cada umbral $\xi_1$, $\xi_2$ y $\xi_3$. Para esto se itera cada mapeo bajo el mismo punto inicial $x_0 = 0.127$; se itera $x_0$ bajo cada mapeo $g_{\gamma_i}$ y se usa los elementos de la serie de tiempo $(x_i)_{i=1}^{1000001}$ para encontrar una aproximación del umbral de manera iterativa. El proceso que se realiza es el descrito en el capítulo anterior. Para este ejemplo los umbrales que se encuentran para la órbita que genera cada mapeo de la familia multimodal son $\xi_1 = 0.100059800883484$, $\xi_2 = 0.349840834571766$) y $\xi_3 = 0.7145$ (0.714468009944525). Después, con estos umbrales se puede definir las siguientes tres funciones umbral:

$$\Xi_1(x_n) = \begin{cases} 0, & 0 \leq x_n < 0.1001; \\ 1, & 0.1001 \leq x_n \leq 1, \end{cases} \tag{4.3}$$

$$\Xi_2(y_n) = \begin{cases} 0, & 0 \leq y_n < 0.3498; \\ 1, & 0.3498 \leq y_n \leq 1, \end{cases} \tag{4.4}$$

$$\Xi_3(z_n) = \begin{cases} 0, & 0 \leq z_n < 0.7145; \\ 1, & 0.7145 \leq z_n \leq 1, \end{cases} \tag{4.5}$$

donde $x_n$ es la n-ésima iteración del punto inicial $x_0$ bajo el mapeo $g_{0.8}$; $y_n$ es la n-ésima iteración del punto inicial $y_0$ bajo el mapeo $g_2$ y $z_n$ es la n-ésima iteración del punto inicial $z_0$ bajo el mapeo $g_4$ donde $n \in \mathbb{N}$.

Una vez que se obtiene una familia multimodal en la que cada mapeo exhibe comportamiento caótico y los umbrales se *consigue el generador de bits*. En el caso de que se desarrolle con base en un mapeo trimodal cada bit se calcula acorde con:

$$s_{n+1} = \Xi_1 \left( g_{\gamma_1}(x_n) \right) \oplus \Xi_2 \left( g_{\gamma_2}(y_n) \right) \oplus \Xi_3 \left( g_{\gamma_3}(z_n) \right), \tag{4.6}$$

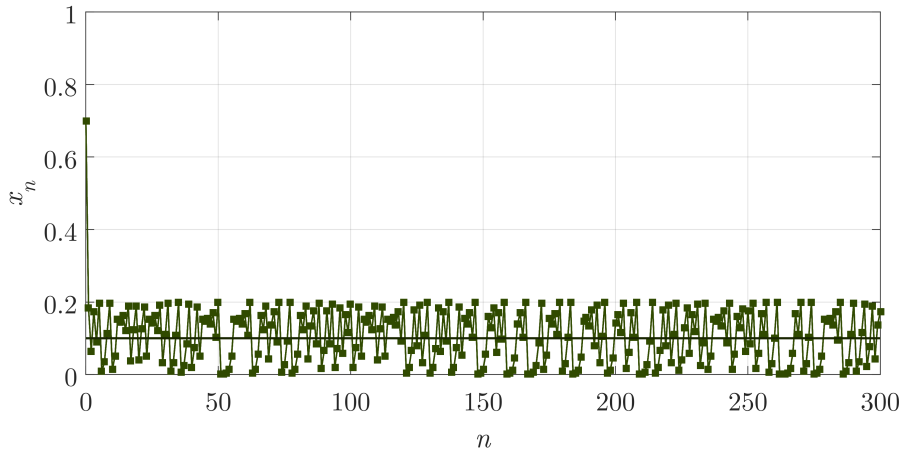
y tiene como semillas las tercias $(x_0, y_0, z_0) \in (0,1)^3$. Como ejemplo ilustrativo se considera la semilla $(0.7, 0.8, 0.9)$; en la tabla 4.2 se muestra como se obtienen los primeros cinco elementos de la secuencia binaria; en la primer columna se muestra el instante de tiempo $n$; las siguientes tres columnas contienen las iteraciones de cada mapeo de la familia multimodal; después se presenta la aplicación de la función umbral a las iteraciones de cada uno de dichos mapeos y por último se presenta el bit $s_{n+1}$ que se obtiene mediante la combinación de las series de tiempo mediante la operación $XOR$.

Tabla 4.2: Secuencia de bits que produce la semilla $(0.7, 0.8, 0.9)$.

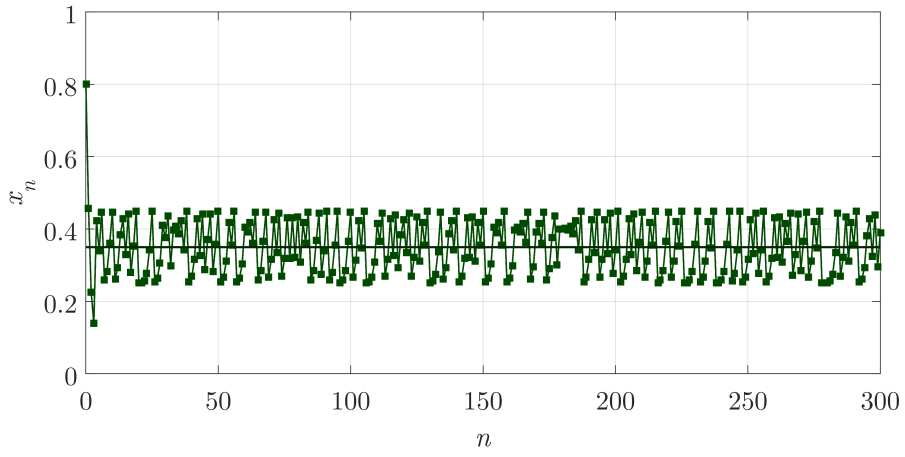
| $n$ | $g_{\gamma_1}(x_n)$ | $g_{\gamma_2}(y_n)$ | $g_{\gamma_3}(z_n)$ | $\Xi_1(g_{\gamma_1}(x_n))$ | $\Xi_2(g_{\gamma_2}(y_n))$ | $\Xi_3(g_{\gamma_3}(z_n))$ | $s_{n+1}$ |
|---|---|---|---|---|---|---|---|
| 0 | 0.1824 | 0.4560 | 0.6080 | 1 | 1 | 0 | 0 |
| 1 | 0.0642 | 0.2253 | 0.6435 | 0 | 0 | 0 | 0 |
| 2 | 0.1744 | 0.1389 | 0.7776 | 1 | 0 | 1 | 0 |
| 3 | 0.0894 | 0.4243 | 0.9384 | 0 | 1 | 1 | 0 |
| 4 | 0.1977 | 0.3395 | 0.4105 | 1 | 0 | 0 | 1 |

Por último se muestra en las Figuras 4.2a, 4.2b y 4.2c elementos de las órbitas de los puntos iniciales 0.7, 0.8, 0.9 bajo el mapeo de la familia multimodal $g_{0.8}$, $g_2$ y $g_4$, respectivamente junto a los umbrales que se obtiene para cada uno. Por último se muestra los primeros elementos de la secuencia binaria que se produce mediante la semilla $(0.7, 0.8, 0.9)$.

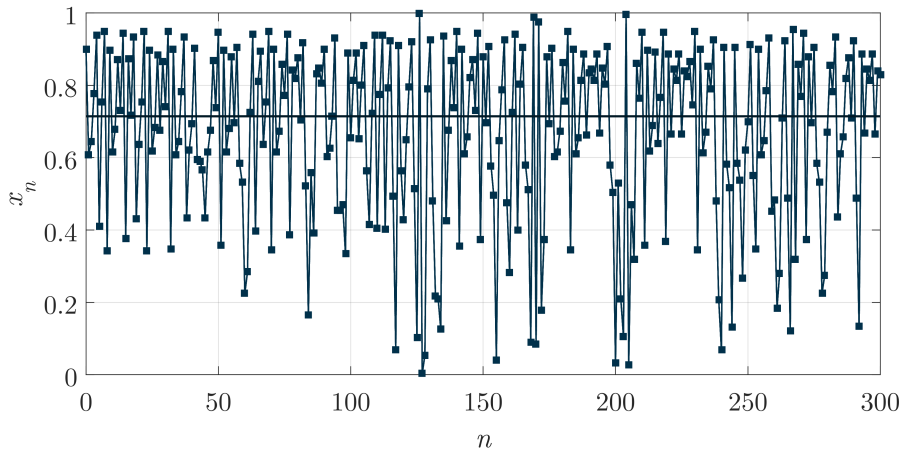
$$\begin{aligned}(s_i)_{i=0}^{1000} = \; & (0,0,0,0,1,0,1,1,1,1,0,0,1,1,1,1,1,1,0,0,0,0,0,0,0,1,0,1,0,1,\\ & 1,0,0,0,0,0,1,1,1,0,1,0,0,0,1,0,0,0,1,1,0,1,0,1,0,0,0,1,1,0,\\ & 0,1,0,1,1,0,0,1,1,1,1,0,0,1,1,0,1,0,1,0,1,1,0,1,1,1,0,1,1,1,\\ & 0,0,1,0,1,1,0,1,1,0,1,1,0,1,1,1,1,0,0,1,1,1,0,0,1,1,0,0,\ldots).\end{aligned} \tag{4.7}$$




(a) Punto inicial $x_0 = 0.7$ bajo $g_{0.8}$.




(b) Punto inicial $x_0 = 0.8$ bajo $g_2$




(c) Punto inicial $x_0 = 0.9$ bajo $g_4$

Figura 4.2: Muestras de las series de tiempo de cada mapeo de la familia multimodal $\{g_{0.8}, g_2, g_4\}$ que se obtienen con base en (4.1).

### 4.1.1. Pruebas estadísticas del generador de bits

Para realizar las pruebas estadísticas se selecciona el nivel de significancia $\delta = 0.01$ por lo que se espera que una de cada cien secuencias que produce el generador (4.6) no sean aleatorias. Se toma una muestra de 2 000 distintas secuencias con una longitud de 1 000 000 de elementos y se aplica el banco de pruebas estadísticas del Instituto Nacional de Estándares y Tecnología. Los resultados se presentan en las tablas 4.3 y 4.4; en la primera columna se muestra el número de cada prueba estadística; en la segunda columna se muestra su nombre; en la tercera columna se presenta el resultado de la búsqueda de uniformidad y en la cuarta la proporción de secuencias que aprueban la prueba estadística.

Tabla 4.3: Resultado I de analizar el generador (4.6) mediante *SP800-22*.

| *No.* | *Prueba estadística* | | *valor-$p_T$* | *Muestras que aprueban* |
|---|---|---|---|---|
| 1 | Frecuencia (monobit) | | 0.059734 | 1975/2000 |
| 2 | Frecuencia dentro de un bloque | | 0.407387 | 1984/2000 |
| 3 | Ejecuciones | | 0.311542 | 1984/2000 |
| 4 | Más larga ejecución de unos en un bloque | | 0.920383 | 1976/2000 |
| 5 | Rango de una matriz binaria | | 0.500279 | 1981/2000 |
| 6 | Transformada discreta de Fourier | | 0.281232 | 1979/2000 |
| 8 | Emparejando patrón sobrepuesto | | 0.100709 | 1976/2000 |
| 9 | "Estadística Universal" de Maurer | | 0.247382 | 1985/2000 |
| 10 | Complejidad lineal | | 0.890582 | 1984/2000 |
| 11 | Serial | 1 | 0.475948 | 1984/2000 |
| | | 2 | 0.958917 | 1990/2000 |

Tabla 4.4: Resultado II de analizar el generador (4.6) mediante *SP800-22*.

| *No.* | *Prueba estadística* | | *P-valor*$_T$ | *Muestras que aprueban* |
|---|---|---|---|---|
| 12 | Entropía aproximada | | 0.344048 | 1978/2000 |
| 13 | Sumas acumulativas | Modo 0 | 0.165799 | 1980/2000 |
| | | Modo 1 | 0.489508 | 1977/2000 |
| 14 | Excursiones aleatorias | Estado $-4$ | 0.188457 | 1209/1216 |
| | | Estado $-3$ | 0.431951 | 1207/1216 |
| | | Estado $-2$ | 0.051233 | 1205/1216 |
| | | Estado $-1$ | 0.083712 | 1200/1216 |
| | | Estado $+1$ | 0.656902 | 1197/1216 |
| | | Estado $+2$ | 0.493098 | 1208/1216 |
| | | Estado $+3$ | 0.757969 | 1201/1216 |
| | | Estado $+4$ | 0.797676 | 1203/1216 |
| 15 | Variante de excursiones aleatorias | Estado $-9$ | 0.904765 | 1202/1216 |
| | | Estado $-8$ | 0.818924 | 1203/1216 |
| | | Estado $-7$ | 0.901351 | 1205/1216 |
| | | Estado $-6$ | 0.603601 | 1203/1216 |
| | | Estado $-5$ | 0.343836 | 1200/1216 |
| | | Estado $-4$ | 0.962634 | 1206/1216 |
| | | Estado $-3$ | 0.130798 | 1203/1216 |
| | | Estado $-2$ | 0.375104 | 1200/1216 |
| | | Estado $-1$ | 0.793022 | 1210/1216 |
| | | Estado $+1$ | 0.634538 | 1205/1216 |
| | | Estado $+2$ | 0.643143 | 1208/1216 |
| | | Estado $+3$ | 0.977238 | 1209/1216 |
| | | Estado $+4$ | 0.901351 | 1208/1216 |
| | | Estado $+5$ | 0.459686 | 1209/1216 |
| | | Estado $+6$ | 0.88834 | 1210/1216 |
| | | Estado $+7$ | 0.824844 | 1209/1216 |
| | | Estado $+8$ | 0.869396 | 1211/1216 |
| | | Estado $+9$ | 0.496335 | 1210/1216 |

Se omite en las tablas los resultados de la séptima prueba *emparejando patrón no sobrepuesto* debido a que realiza una gran cantidad de subpruebas (un total de 148). El último paso es interpretar los resultados que se obtiene. Por lo que se refiere a la búsqueda de uniformidad en las muestras; siempre y cuando los resultados de cada prueba satisfacen que:

$$\textit{valor-}p_T \geq 0.0001, \tag{4.8}$$

se puede concluir que no se encuentra una desviación de aleatoriedad; puesto que el menor *valor-*$p_T$ que se obtiene al analizar el generador (4.6) es 0.0201 como se muestra en la Figura 4.3; se concluye que todo *valor-*$p_T$ es mayor o igual que 0.0001 por lo que los valores están uniformemente distribuidos; es decir, no se encuentra una desviación de aleatoriedad.

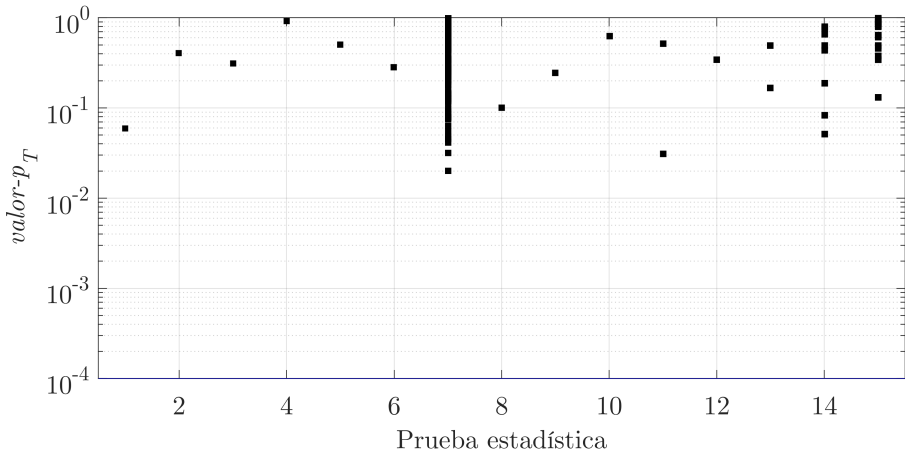



Figura 4.3: Resultados del enfoque de búsqueda de uniformidad que se obtiene al analizar el generador (4.6) mediante $SP800-22$ junto a la "línea crítica".

El segundo enfoque consiste en analizar el porcentaje de muestras que aprueban, se interpreta sus resultados al calcular un intervalo de confianza acorde con:

$$1-\delta \pm 3\sqrt{\frac{\delta(1-\delta)}{p}}, \tag{4.9}$$

donde $p$ es el tamaño de la muestra, así que a condición de que los resultados de cada prueba sean contenidos en 4.9 se puede concluir que no se encuentra una desviación de aleatoriedad; es importante mencionar que se tiene dos tamaños de muestras; de la prueba 1 a la 13 se tiene $p = 2000$ y como $\delta = 0.01$ el intervalo de confianza que se obtiene es:

$$(0.9833, 0.9967), \tag{4.10}$$

para las pruebas 14 y 15 se tiene una muestra de $p = 1216$ por lo que su intervalo de confianza es:

$$(0.9814, 0.9986), \tag{4.11}$$

al considerar que los porcentajes máximo y mínimo que se obtienen de analizar el generador (4.6) son 0.9959 y 0.9844, respectivamente como se presenta en la Figura 4.3; se concluye que todos los porcentajes pertenecen al intervalo de confianza (4.10) por lo que también al intervalo de confianza (4.11); por consiguiente, ya que ambos enfoques se satisfacen se concluye que *no se encuentra una desviación de aleatoriedad en las secuencias que produce el generador* (4.6).

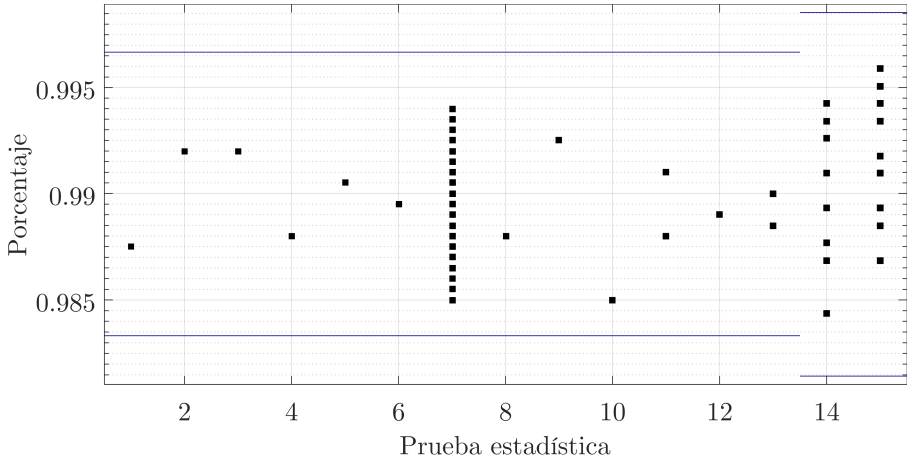



Figura 4.4: Resultados del porcentaje de muestras que aprueban que se obtiene al analizar el generador (4.6) mediante $SP800-22$ dentro del intervalo de confianza (4.10).

En síntesis en este capítulo se exhibe un generador de bits que es capaz de generar secuencias de manera determinista que son indistinguibles de una aleatoria; es decir, es un *generador de bits seudo-aleatorios* mediante el método propuesto. Se hace énfasis en que se asume que cada mapeo presenta comportamiento ergódico y acorde con los resultados que se obtiene, la familia multimodal con la que se trabaja exhibe este tipo de comportamiento. Esto se puede decir debido a que se calcula los umbrales para un punto inicial predeterminado y para las semillas se toma valores de manera seudo-aleatoria; por consiguiente, si no se mantiene el comportamiento a largo plazo se obtendría secuencias binarias que no tienen aproximadamente el mismo número de unos y ceros que es una de las características del comportamiento aleatorio.

# Capítulo 5

# Conclusiones y trabajo a futuro

## 5.1. Conclusiones

En este documento se presentó un estudio sobre una clase de sistemas dinámicos discretos con comportamiento caótico y su aplicación en la construcción de generadores de bits seudo-aleatorios. Se aprovechó la dinámica caótica que presentan esta clase de sistemas para generar una dinámica similar a la aleatoria útil para desarrollar generadores de bits totalmente deterministas.

La primera parte de la tesis corresponde al desarrollo de la familia multimodal. Para realizarla se empleó una función por partes con base en un tipo de mapeo logístico. Dentro de los resultados obtenidos se obtiene condiciones necesarias y suficientes para obtener una familia multimodal; las regiones donde los puntos fijos son asintóticamente estables; condiciones bajo las que aparecen intervalos invariantes bajo el mapeo que son indeseados. Por último, se encuentra familias multimodales para las que cada mapeo presenta comportamiento caótico.

La segunda parte de la tesis corresponde a la construcción de un generador de bits seudo-aleatorios con base en el método propuesto. Para esto se trabajó con un mapeo trimodal. Cabe señalar que con esto se exhibe la existencia de una familia multimodal que permite desarrollar generadores de bits seudo-aleatorios. La semilla del generador que se presenta es una tercia $(x_0, y_0, z_0)$, que son los puntos iniciales de cada mapeo, $x_0$, $y_0$, $z_0$ se itera bajo $g_{\gamma_1}$, $g_{\gamma_2}$, $g_{\gamma_3}$, respectivamente. Ya que cada valor se representa en punto flotante de doble precisión mediante 64 bits, la semilla tiene una longitud de

192 bits y el generador es capaz de expandirla hasta obtener una secuencia de mayor longitud (orden de millones) indistinguible de una aleatoria. Los generadores de bits que se obtienen con base en el método propuesto presentan propiedades interesantes como sensibilidad a las condiciones iniciales y sensibilidad a los parámetros. Estas características dan robustez al generador de secuencias seudo-aleatorias debido a que para reproducir una secuencia se tienen que usar los mismos puntos iniciales y conocer los parámetros del mapeo m-modal. Cualquier variación en condición inicial o parámetros del sistema determinarían distintos mapeos que generarían secuencias seudo-aleatorias distintas.

## 5.2. Trabajo a futuro

Reconocemos que falta mucho trabajo por hacer y por ello visualizamos el siguiente trabajo a futuro donde podemos expandir los resultados que se presentaron en:

- Sistemas Dinámicos:
  - Encontrar condiciones necesarias y/o suficientes tales que al seleccionar los parámetros que forman una familia multimodal, se pueda decir si cada mapeo va a exhibir comportamiento caótico.
  - Demostrar que el mapeo m-modal propuesto presenta comportamiento ergódico; el obtener dicho resultado se podría calcular los umbrales de forma analítica; además, facilitaría el buscar estrategias alternas para la generación de la secuencia de bits.
  - Emplear otro tipo de sistemas dinámicos discretos para desarrollar la familia multimodal propuesta; en particular, explorar la idea de trabajar con el mapeo casa de campaña debido a que es una función lineal por partes y requiere de menos operaciones por iteración a comparación de una función cuadrática.
- Aplicaciones:
  - Desarrollar métodos que permitan incrementar la longitud de las secuencias seudo-aleatorias que produce un generador antes de presentar comportamiento periódico para valores de condiciones iniciales dadas.

- Desarrollar generadores de números aleatorios por medio de su implementación física; esto se realiza para obtener los parámetroos que forman la familia multimodal y/o semillas de forma aleatoria.
- Emplear los generadores de bits que se obtienen con base en la familia multimodal para desarrollar sistemas criptográficos.

# Bibliografía


[1] Peitgen, H., Jürgens, H., & Saupe, D. (2012). *Chaos and fractals: new frontiers of science.* New York, NY, USA: Springer.

[2] Ben-Menahem, A. (2009). *Historical encyclopedia of natural and mathematical sciences.* Berlin: Springer.

[3] Hirsch, M. W., Smale, S., Devaney, R. L. (2004). *Differential equations, dynamical systems, and an introduction to chaos.* Amsterdam. Elsevier.

[4] Guan, Z., Huang, F., & Guan, W. (2005). *A Generalizad Chaos-Based Stream Generator*, Circuits, Systems & Signal Processing, 24(5), 549-555. http://dx.doi.org/10.1007/s00034-005-2406-7.

[5] Li, S. (2005). *Analyses and New Designs of Digital Chaotic Ciphers.* (Tesis de doctorado). Xi'an, China, Xi'an Jiaotong University.

[6] Matthews, R. (1989). *On the Derivation Of A "Chaotic" Encryption Algorithm.* Cryptología, 13(1),29-42. http://dx.doi.org/10.1080/0161-118991863745.

[7] Deng, Y., Hu, H., & Liu, L. (2015). *Feedback control of digital chaotic systems with application to pseudorandom number generator.* Int. J. Mod. Phys. C International Journal of Modern Physics C, 26(02), 1550022. http://dx.doi.org/10.1142/s0129183115500229

[8] François, M., Grosges, T., Barchiesi, D., & Erra, R. (2014). *Pseudo-random number generator based on mixing of three chaotic maps.* Communications in Nonlinear Science and Numerical Simulation, 19(4), 887-895. http://dx.doi.org/10.1016/j.cnsn.2013.08.032

[9] Paar, C., & Pelzl, J. (2010). *Understanding Cryptography: A textbook for students and practitioners*. Heidelberg: Springer.

[10] Smania, D. (2005). *Phase space universality for multimodal maps*. Bull Braz Math Soc, New Series Bulletin of the Brazilian Mathematical Society, New Series, 36(2), 225–274. http://dx.doi.org/10.1007/s00574-005-0038-y

[11] Campos-Cantón, E., Femat, R., & Pisarchik, A. (2011). *A family of multimodal dynamic maps*. Communications in Nonlinear Science and Numerical Simulation, 16(9), 3457−3462. http://dx.doi.org/10.1016/j.cnsns.2010.12.028

[12] García, M. (2015). *Estudio de mapeos caóticos discretos y su aplicación en criptografía* (Tesis de doctorado inédita). Instituto Potosino de Investigación Científica y Tecnológica (IPICyT), San Luis Potosí, México.

[13] Rangan, C. P., & Ding, C. (2001). *Progress in cryptology: INDOCRYPT 2001: Second International Conference on Cryptology in India, Chennai, December 16-20, 2001: proceedings*. Berlin: Springer.

[14] Sajeeth, N., & Babu, K. (2001). *Chaos for stream cipher*. Disponible en línea en http://arxiv.org/abs/cs.CR/0102012

[15] Pellicer-Lostao, C., & López-Ruiz, R. (2008). Pseudo-Random Bit Generation Based on 2D Chaotic Maps of Logistic Type and Its Applications in Chaotic Cryptography. Computational Science and Its Applications – ICCSA 2008 Lecture Notes in Computer Science, 784-796. http://dx.doi.org/10.1007/978-3-540-69848-7_62

[16] Patidar, V., Sud, K.K. (2009). *A Novel Pseudo Random Bit Generator Based on Chaotic Standard Map and its Testing.* Electronic Journal of Theoretical Physics, 6(20), 327-344.

[17] Patidar, V., Sud, K.K. (2009). *A Pseudo Random Bit Generator Based on Chaotic Logistic Map and its Statistical Testing*. Informatica, 33(4), 441-452.

[18] Elaydi, S. (1996). *An Introduction to Difference Equations*. New York: Springer.

[19] Trench, W. (2003). *Introduction to real analysis*. Upper Saddle River, N.J: Prentice Hall/Pearson Education.

[20] Browder, A. (1996). *Mathematical Analysis: an Introduction*. New York, NY: Springer New York.

[21] Kurtz, D. C. (1992). *Foundations of abstract mathematics*. New York: McGraw-Hill.

[22] Sedaghat, H. (2011). *Nonlinear difference equations: Theory with applications to social science models*. Dordrecht: Springer.

[23] Arnol′d, V. I. (1973). *Ordinary differential equations*. Cambridge: MIT Press.

[24] Ginoux, J. (2009). *Differential geometry applied to dynamical systems*. Hackensack, NJ: World Scientific.

[25] Salinelli, E., & Tomarelli, F. (2014). *Discrete dynamical models*. Cham: Springer.

[26] Kocarev, L., & Lian, S. (2011). *Chaos-based cryptography*. Berlin: Springer.

[27] Lynch, S. (2014). *Dynamical systems with applications using MATLAB*. Cham: Birkhauser.

[28] Wolf, A., Swift, J. B., Swinney, H. L., & Vastano, J. A. (1985). *Determining Lyapunov exponents from a time series*. Physica D: Nonlinear Phenomena, 16(3), 285–317. http://dx.doi.org/10.1016/0167-2789(85)90011-9

[29] Bassham, L. E., Rukhin, A. L., Soto, J., Nechvatal, J. R., Smid, M. E., Barker, E. B.,. . . , Vo, S. (2010). *A statistical test suite for random and pseudorandom number generators for cryptographic applications*. http://dx.doi.org/10.6028/nist.sp.800-22r1a

[30] Stinson, D. (2006). *Cryptography: Theory and Practice*. Boca Raton: Chapman & Hall/CRC.

[31] Marsaglia, G. (1997). *DIEHARD: a battery of tests of randomness*, http://stat.fsu.edu/~geo/diehard.html

[32] L'ecuyer, P. Simard, R. (n.d.) *TESTU01: A C library for empirical testing of random number generators.* ACM Trans Math Soft 2007; 33:40 (Articule 22). http://simul.iro.umontreal.ca/testu01/tu01.html

[33] Glendinning, P. (1994). *Stability, instability, and chaos: an introduction to the theory of nonlinear differential equations*. Cambridge England New York: Cambridge University Press.

[34] Haahr, M. (n.d.). *True Random Number Service*. Recuperado Abril 30, 2017, de https://www.random.org/decimal-fractions/28

[35] Arroyo, D. (2009). *Framework for the analysis and design of encryption strategies based on discrete-time chaotic dynamical systems* (Tesis de doctorado). Madrid, España, Universidad Politécnica de Madrid. Recuperada en Abril 2016 de http://digital.csic.es/handle/10261/15668

[36] Kanso, A., & Smaoui, N. (2009). *Logistic chaotic maps for binary numbers generations*. Chaos, Solitons & Fractals, 40(5), 2557–2568. http://dx.doi.org/10.1016/j.chaos.2007.10.049