



## **División de Ciencias Básicas e Ingeniería**

**Mapeos caóticos unidimensionales aplicados a la  
generación de ruido**

**que presenta**

**Rubén Vázquez Medina**

**PARA OBTENER EL GRADO DE  
DOCTOR EN CIENCIAS**

**Asesor:**

**Dr. José Luis Del Río Correa**

**Octubre 16, 2008**

**Sinodales:**

<b>Presidente:</b>	<b>Dr. Arturo Sarmiento Reyes</b>
<b>Secretario:</b>	<b>Dr. José Luis Del Río Correa</b>
<b>Vocales:</b>	<b>Dr. Joaquín Delgado Fernández</b>
	<b>Dr. José Guadalupe Reyes Victoria</b>
	<b>Dr. Alejandro Díaz Sánchez</b>

THE UNIVERSITY OF CHICAGO  
DEPARTMENT OF CHEMISTRY  
5800 S. UNIVERSITY AVENUE  
CHICAGO, ILLINOIS 60637

RECEIVED  
JAN 15 1964

1964

## CONTENIDO

	PÁGINA
<b>Agradecimientos</b> .....	5
<b>Dedicatoria</b> .....	6
<b>Resumen de la Tesis</b> .....	7
<b>Organización de la Tesis</b> .....	9
<b>CAPÍTULO 1: Contexto de la Investigación</b> .....	11
<b>Resumen</b> .....	11
<b>1.1 Delimitación de Tema</b> .....	11
<b>1.2 Planteamiento del Problema</b> .....	15
<b>1.3 Objetivos</b> .....	18
Objetivo General: .....	18
Objetivos Particulares: .....	18
<b>1.4 Justificación</b> .....	19
<b>CAPÍTULO 2: Estudio del Mapeo Logístico</b> .....	27
<b>Resumen</b> .....	27
<b>2.1 Antecedentes</b> .....	27
Universalidad y Escalamiento .....	28
Definición de Mapeo Logístico .....	31
Diagrama de Bifurcación .....	32
Teorema de Sharkowskii .....	39
<b>2.2 Distribución Invariante y Teorema Ergódico</b> .....	40
Uso del Teorema Ergódico de Birkhoff .....	41
Medida Estadística y Distribución Invariante .....	42
Convergencia de Medidas Estadísticas .....	46
Divergencia de Kullback Leibler .....	51
Diagrama de Bifurcación y Distribución Invariante .....	55
<b>2.3 Del orden al caos y del caos al orden</b> .....	61
Doblamiento del periodo en órbitas .....	63
Doblamiento del periodo en distribuciones .....	70
<b>2.4 Análisis de Estabilidad</b> .....	78
Exponente de Lyapunov .....	78
Cálculo Numérico del Exponente de Lyapunov .....	82
<b>2.5 Sensitividad ante condiciones iniciales</b> .....	84
<b>2.6 Mezclado y Dispersión</b> .....	85
Propiedad de Mezclado .....	85
Propiedad de Dispersión .....	95
<b>CAPÍTULO 3: Generación de ruido analógico caótico</b> .....	97
<b>Resumen</b> .....	97
<b>3.1 Antecedentes</b> .....	97
<b>3.2. Mapeo Logístico Generalizado</b> .....	100
Modelos Generalizados .....	100

Main body of the document containing several paragraphs of text. The text is extremely faint and largely illegible due to low contrast and blurring. It appears to be a formal document or report.

---

Modelo de R. Mathews .....	101
<b>3.3. Circuito MOS QT de Wiegerink.....</b>	<b>103</b>
Consideraciones .....	103
Funcionamiento del Circuito de Wiegerink .....	103
Función de Transferencia .....	105
<b>3.4. Generador analógico de ruido.....</b>	<b>106</b>
El Modelo Generalizado y la Función de Transferencia .....	106
Circuito de Retroalimentación .....	108
<b>3.5. Procedimiento de Diseño .....</b>	<b>109</b>
Consideraciones del procedimiento .....	109
Distribución Estadística de la Señal de Salida .....	110
Descripción del Procedimiento .....	112
Ejemplo de aplicación del procedimiento .....	116
<b>3.6. Consideraciones para su implementación.....</b>	<b>119</b>
Variaciones del Proceso de Fabricación.....	119
Análisis de Monte Carlo. ....	120
<b>CAPÍTULO 4: Comentarios y Conclusiones .....</b>	<b>125</b>
<b>Resumen .....</b>	<b>125</b>
<b>4.1 Hechos y Consideraciones .....</b>	<b>125</b>
<b>4.2 Conclusiones finales .....</b>	<b>127</b>
<b>4.3 Trabajo a Futuro.....</b>	<b>130</b>
<b>Bibliografía .....</b>	<b>133</b>
<b>Índice de Tablas.....</b>	<b>151</b>
<b>ANEXO A. Diagramas de Bifurcación de dos mapeos unimodales.....</b>	<b>153</b>
<b>ANEXO B. Mapeos Caóticos Unidimensionales .....</b>	<b>155</b>
<b>ANEXO C. Sentido del Teorema Ergódico.....</b>	<b>159</b>
<b>ANEXO D. Generador de Ruido en HSPICE™ .....</b>	<b>163</b>
<b>D.1. Circuito Generador de Ruido.....</b>	<b>163</b>
<b>D.2. Circuito de Polarización .....</b>	<b>169</b>
<b>D.3. Circuito Multiplicador .....</b>	<b>170</b>
<b>D.4. Circuito Muestreo y Retención .....</b>	<b>170</b>
<b>ANEXO E. Publicaciones en revistas .....</b>	<b>171</b>
<b>ANEXO F. Publicaciones en congresos.....</b>	<b>173</b>

The first part of the report deals with the general conditions of the country, and the second part with the details of the various districts. The first part is divided into two sections, the first of which deals with the general conditions of the country, and the second with the details of the various districts. The second part is divided into three sections, the first of which deals with the details of the various districts, the second with the details of the various districts, and the third with the details of the various districts.

## Presentación

Esta tesis pone de manifiesto que es posible utilizar *mapeos* caóticos unidimensionales en el diseño de sistemas, subsistemas o dispositivos orientados a la protección de información, estableciendo criterios objetivos que garanticen un comportamiento adecuado, en términos de lo que demanda una aplicación específica. En particular, se presenta el procedimiento que se debe seguir para el diseño de un generador de ruido caótico usando el *mapeo* logístico, considerando como criterios de diseño el Teorema Ergódico de Birkhoff, el diagrama de bifurcación y el exponente de Lyapunov.

Esta tesis es un fragmento de un trabajo más amplio que se ha podido realizar bajo la atinada dirección del Dr. José Luis del Río Correa, quien con tiempo de calidad y mucha paciencia atendió las innumerables sesiones de trabajo.

Esta tesis constituye un logro importante en mi desarrollo profesional y me pone en condiciones de generar nuevos proyectos que, usando elementos de la teoría del caos, contribuyan a desarrollar sistemas para la protección de información.

**Rubén Vázquez Medina**

### 2000-2001

1. The first part of the document discusses the importance of maintaining accurate records of all transactions. It emphasizes that proper record-keeping is essential for the integrity of the financial system and for the ability to detect and prevent fraud. The text outlines the various methods used to collect and analyze data, including the use of computerized databases and statistical software. It also discusses the challenges of data collection and the need for standardized procedures to ensure consistency across different studies and institutions.

2. The second part of the document focuses on the analysis of the data. It describes the various statistical techniques used to test hypotheses and to estimate the parameters of the models. The text discusses the importance of choosing the appropriate statistical test and the need to check the assumptions of the tests. It also discusses the interpretation of the results and the need to be cautious about over-interpreting the findings. The text concludes by discussing the implications of the results for policy-making and for the future of the field.



## Agradecimientos

A Dios por manifestarse en mi vida cada día

A Annabel por compartir su vida conmigo

A Rubén por su ternura y grandes sueños

A Ana Isabel por sus atenciones y cariño

Al Dr. José Luis del Río por creer en este proyecto

A la UAM Iztapalapa por ser una Casa Abierta al Tiempo

A mi familia por los valores con que llenaron mi vida

A los Doctores que fungieron como sinodales en la revisión de este trabajo

Al Instituto Politécnico Nacional por más 11 años de trabajo en su planta docente

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

## **Dedicatoria**

A mi Mamá, por mostrarme que en la vida se debe dar todo

A mi país, México

1. The first part of the document discusses the importance of maintaining accurate records of all transactions and activities. It emphasizes the need for transparency and accountability in financial reporting.

2. The second part of the document outlines the various methods and techniques used to collect and analyze data. It includes a detailed description of the experimental procedures and the statistical tools employed.

3. The third part of the document presents the results of the study, including a comparison of the different methods and a discussion of the implications of the findings. It also includes a section on the limitations of the study and suggestions for future research.

4. The fourth part of the document provides a conclusion and a summary of the key findings. It also includes a list of references and a list of figures and tables.

5. The fifth part of the document is a list of references, which includes a comprehensive list of the sources used in the study. It also includes a list of figures and tables.

6. The sixth part of the document is a list of figures and tables, which includes a detailed description of each figure and table. It also includes a list of references and a list of figures and tables.

7. The seventh part of the document is a list of references, which includes a comprehensive list of the sources used in the study. It also includes a list of figures and tables.

8. The eighth part of the document is a list of figures and tables, which includes a detailed description of each figure and table. It also includes a list of references and a list of figures and tables.

9. The ninth part of the document is a list of references, which includes a comprehensive list of the sources used in the study. It also includes a list of figures and tables.

10. The tenth part of the document is a list of figures and tables, which includes a detailed description of each figure and table. It also includes a list of references and a list of figures and tables.

## Resumen de la Tesis

El tema principal de esta tesis es el análisis de *mapeos*<sup>1</sup> caóticos unidimensionales con técnicas de mecánica estadística para su aplicación en generadores de ruido. Se analiza el *mapeo* logístico usando, en función del parámetro que gobierna el *mapeo*, el diagrama de bifurcación, el diagrama de trayectorias, el Exponente de Lyapunov y su distribución estadística. También, analizando el comportamiento de las órbitas del *mapeo*, y usando el Teorema de Ergódico, se determina una expresión para calcular la distribución invariante.

En particular, usando el diagrama de bifurcación se describe el fenómeno del doblamiento del periodo desde dos puntos de vista. El primero, que es la forma tradicional, analiza la ruta del orden al caos. Se describe el doblamiento del periodo de las órbitas que produce el *mapeo* haciendo variar el parámetro de  $\mu = 0$  hasta  $\mu = \mu_{\infty}$ , que de acuerdo al criterio de estabilidad,  $\mu_{\infty}$  es el punto para el cual el *mapeo* entra al caos. De esta manera, se enfatiza la posibilidad de generar señales periódicas siempre que el valor del parámetro del *mapeo* sea tal que  $\mu \in (0, \mu_{\infty})$  y aperiódicas si el valor del parámetro es tal que  $\mu \in (\mu_{\infty}, 4)$ . El segundo punto de vista, corresponde a un enfoque muy poco abordado, y considera la ruta del caos al orden. Se describe el doblamiento del periodo, pero ahora ya no es un fenómeno sobre las órbitas del *mapeo*, sino sobre las distribuciones invariantes de dicho *mapeo*. Esto se demuestra, haciendo variar, en forma decreciente, el parámetro en el intervalo  $\mu \in (\mu_{\infty}, 4)$  y calculando numéricamente la distribución invariante del *mapeo* para aquellos valores del parámetro en los que se hace la bifurcación de distribuciones.

---

<sup>1</sup> En esta tesis se emplea el término *mapeo* para referirse a transformaciones como se conoce formalmente en matemáticas.

## MEMORANDUM

TO : [Name]

FROM : [Name]

SUBJECT : [Subject]

[Text]

[Text]

[Text]

[Text]

[Text]

[Text]

[Text]

[Text]

[Text]

[Text]

[Text]

[Text]

Se muestra que, para ambos puntos de vista, es posible calcular la constante de Feigenbaum, usando las distancias que existen entre los valores del parámetro para los cuales ocurre la bifurcación (de órbitas o de distribuciones). Se muestra que en ambos casos se sigue un patrón similar de comportamiento cuando ocurre una bifurcación.

Por otro lado, también usando el Teorema Ergódico y usando la distribución invariante, se determina una expresión que permite calcular el valor que tiene el Exponente de Lyapunov en función del parámetro del *mapeo*; además, apoyados en el diagrama de bifurcación se determinan las islas de estabilidad que posee el *mapeo* logístico dentro de la región de comportamiento caótico.

A partir del análisis hecho para el *mapeo* logístico, se presenta un procedimiento que permite diseñar un generador de ruido analógico usando un circuito Translineal Cuadrático (QT: Quadratic Translinear) con transistores MOS (Metal-Oxide Semiconductor), comúnmente llamado circuito MOS QT, cuya función de transferencia tiene un comportamiento consistente con el *mapeo* logístico. El proceso de iteración de la función logística para la función de transferencia de este circuito se logra considerando la existencia de un amplificador de ganancia  $\mu$  retroalimentando la salida hacia la entrada. Se muestra el diseño de un circuito MOS QT de Wiegerink, para el que se simula su comportamiento en tiempo y en frecuencia usando MatLab<sup>TM</sup> y HSPICE<sup>TM</sup>. Para tal efecto, se usa una generalización del *mapeo* logístico que permite considerar niveles de corriente adecuados para la implementación real de los circuitos MOS. Finalmente, se muestran los resultados obtenidos del análisis de Monte Carlo hecho para el circuito diseñado considerando variaciones en el voltaje de umbral  $V_{th}$  y en las dimensiones de los transistores que constituyen el circuito.

...the ... of ...

...the ... of ...

...the ... of ...

...the ... of ...

...the ... of ...

...the ... of ...

...the ... of ...

...the ... of ...



## Organización de la Tesis

Esta tesis está organizada en cuatro capítulos y seis anexos. El **capítulo 1** denominado “**Contexto de la Investigación**” ofrece al lector el escenario completo bajo el cual está planteado este trabajo doctoral. En este primer capítulo, se hace una reseña que incluye la evolución que tuvo el trabajo al paso del tiempo y la motivación para su realización. Además, incluye la delimitación del tema, se plantean los problemas que se identificaron, se ofrece la justificación y se hacen explícitos los objetivos que se tuvieron en este trabajo. El **capítulo 2** denominado “**Mapeo Logístico**” comienza con la descripción del *Mapeo Logístico* y la presentación de los conceptos de *Universalidad* y *Escalamiento*, el Diagrama de Bifurcación y el Teorema de Sharkowskii. Posteriormente, se muestra la manera en que se determina la distribución invariante de un *mapeo* caótico unidimensional usando el Teorema Ergódico. Luego, haciendo uso del diagrama de bifurcación se analiza la ruta del orden al caos y la ruta del caos al orden. Enseguida, se presenta el análisis de estabilidad de los *mapeos* caóticos unidimensionales apoyándose en el Exponente de Lyapunov. Este exponente puede calcularse numéricamente a través de la distribución invariante previamente calculada y haciendo uso del Teorema Ergódico. Finalmente, se presenta el análisis de sensibilidad del *mapeo* ante condiciones iniciales, así como la importancia de las propiedades de mezclado y dispersión de este tipo de *mapeos*. El **capítulo 3** denominado “**Generador de ruido analógico caótico**” presenta el procedimiento que permite diseñar un generador de ruido analógico usando un circuito MOS QT, cuya función de transferencia tiene un comportamiento consistente con el *mapeo* logístico. En este procedimiento, se tiene como criterio principal la distribución invariante del *mapeo*, se hace uso del diagrama de bifurcación y de una generalización del *mapeo* logístico. Se discuten también aspectos relacionados con las implicaciones de la variación del valor del parámetro derivada de procesos de fabricación y realización física de un circuito, en



particular, se consideran las variaciones del voltaje de umbral ( $V_{th}$ ) y las dimensiones de los transistores. Al final de este capítulo se presentan los resultados para el análisis de Monte Carlo, usando los parámetros de la fábrica *Austria Micro Systems*. El **capítulo 4** denominado **“Conclusiones”**, presenta de inicio los hechos y consideraciones que se tuvieron en cuenta a lo largo de este trabajo de tesis, para luego presentar las conclusiones más relevantes de este trabajo. Se destaca la importancia del uso de la distribución invariante y el Teorema Ergódico en el diseño de generadores de señales de ruido. Finalmente, se incluye un apartado denominado **“Trabajo a futuro”** en el que se describe un conjunto de ideas que permiten mostrar que este tema sigue vigente y que el enfoque que se presenta en esta tesis permite la aplicación de esta teoría en otras áreas relacionadas con la protección de la información.

Al final de esta tesis se incluyen seis anexos. El anexo A “Diagramas de Bifurcación de dos *Mapeo* Unimodales” muestra como el *mapeo* logístico y el *mapeo* senoidal tienen un diagrama de bifurcación muy parecido, por lo que su entrada al caos, en ambos casos, se hace a través del fenómeno de doblamiento del periodo. El anexo B “*Mapeos* Caóticos Unidimensionales” incluye definiciones de los *mapeos* caóticos y el análisis general de puntos fijos. El Anexo C “Sentido del Teorema Ergódico” ofrece el enfoque detallado bajo el cual se ha considerado el Teorema Ergódico en esta tesis. El Anexo D “Generador de Ruido en HSPICE<sup>TM</sup>” incluye el código fuente usado para las simulaciones que se hicieron en HSPICE<sup>TM</sup>, se incluye el código del generador de ruido. El Anexo E “Publicaciones en Revistas” incluye la evidencia de los trabajos que se generaron y que fueron publicados en revistas internacionales. Finalmente, el Anexo F “Publicaciones en Congresos” incluye la evidencia de los trabajos que se generaron y que fueron presentados en congresos nacionales e internacionales.

1950

...

...

...

...

...

...

...

# CAPÍTULO 1: Contexto de la Investigación

## Resumen

Este capítulo ofrece al lector el escenario completo bajo el cual está planteado este trabajo doctoral. En este primer capítulo, se hace una reseña que incluye la evolución que tuvo el trabajo al paso del tiempo y la motivación para su realización. Además, incluye la delimitación del tema, se plantean los problemas que se identificaron, se ofrece la justificación y se hacen explícitos los objetivos que se tuvieron en este trabajo.

## 1.1 Delimitación de Tema

Durante el desarrollo del trabajo doctoral, se investigaron diferentes herramientas y modelos matemáticos, relacionados con la Teoría del Caos, que permitieran analizar, diseñar y describir un sistema que contribuyera a la protección de la información. Inicialmente, se abordaron temas relacionados con la generación de secuencias autosimilares basadas en la estructura fractal (autosimilar) de los cuasicristales<sup>2</sup> [1] [2] [3] y de los números de plata<sup>3</sup>, en particular el número de oro<sup>4</sup>. Estas investigaciones permitieron la publicación en el año 2001 de dos artículos de investigación en revista internacional (ver Anexo E), y la presentación de varios trabajos en congresos, tanto nacionales como internacionales (ver Anexo F). Los comentarios que se recibieron, derivados del proceso de evaluación y arbitraje de estos trabajos, nos motivaron a abordar un tema de investigación concreto relacionado también con la Teoría del Caos,

---

<sup>2</sup> Un cuasicristal es la extensión natural de la noción de un cristal para estructuras que existen en la naturaleza con orden traslacional cuasi periódico, las cuales pueden describirse a través de los números de plata.

<sup>3</sup> Se refiere a los números irracionales que pueden describirse a través de una fracción continua periódica de la forma  $\mathbb{Q}_n = [0; n, n, \dots]$ .

<sup>4</sup> Se refiere al número de plata más grande, esto es  $\mathbb{Q}_n = [0; 1, 1, 1, \dots] = 2/(1 + \sqrt{5})$  definida por muchas culturas como la perfecta proporción o perfecta armonía entre dos partes desiguales.

pero con mayores posibilidades de éxito, en su aplicación a la protección de información. Este tema fue el uso de los *mapeos* caóticos unidimensionales.

Así, en esta tesis se considera como tema principal el análisis de *mapeos* caóticos unidimensionales con técnicas de mecánica estadística, de manera que puedan utilizarse para la generación de señales de ruido útiles en procesos de protección de la información. La decisión de estudiar *mapeos* caóticos unidimensionales se debe a que permiten, de manera sencilla y bajo condiciones específicas, generar señales o secuencias con distribuciones cercanas a la distribución uniforme, dependiendo del *mapeo* que se utilice, y del valor del parámetro que gobierne su comportamiento.

Durante cada etapa de esta investigación doctoral se consultaron diferentes artículos de investigación publicados en revistas y congresos internacionales que permitieron enfocar el trabajo. Dichos artículos de investigación pudieron conseguirse con el apoyo y dirección del Dr. José Luis del Río Correa, asesor de este trabajo.

Así, el primer paso en la investigación fue el estudio de los *mapeos* caóticos unidimensionales, concretamente el *Mapeo* Logístico y el *Mapeo* de Bernoulli. Posteriormente, considerando sus características específicas, se investigó sobre la posibilidad de aplicarlos a la protección de la información.

Los *mapeos* caóticos unidimensionales aplicados a la protección de la información no es un tema nuevo, ya ha sido explorado por diferentes investigadores en el mundo, tal como se muestra en el apartado “1.4 Justificación” de este documento. Sin embargo, en esta tesis se buscó investigarlos y estudiarlos a partir de nuevas circunstancias teóricas y considerando diferentes aplicaciones prácticas que aseguraran un trabajo original. Para el desarrollo de esta tesis se estudiaron ampliamente dos temas: los sistemas de protección de información y los *mapeos* caóticos unidimensionales.

En general, los sistemas de protección de información se encargan de fortalecer ú otorgar uno o más de los tres servicios existentes: la disponibilidad, la integridad o la confidencialidad de la información. La *disponibilidad* de la información es un servicio que tiene que ver con el fortalecimiento de la seguridad de los sistemas informáticos que la contienen o de los sistemas de comunicaciones que la transmiten. También, tiene que ver con los mecanismos y procedimientos que permiten detectar cuando un destinatario válido ha sido víctima de una denegación de servicio, lo cual se relaciona con los protocolos de seguridad que permiten identificar cuando a un destinatario válido se le impide disponer de su información en tiempo y forma. La *disponibilidad* de la información es, entonces, un servicio que no se podría fortalecer ú otorgar directamente con la aplicación de los *mapeos* caóticos, al menos NO de manera evidente. Por otro lado, la *integridad* de la información es un servicio que considera la posibilidad de evitar o detectar la modificación que la información hubiere sufrido, derivado de la intervención de un agente (persona) no autorizado para hacerlo. Así, la *integridad* implica tradicionalmente la aplicación de procedimientos que involucren funciones unidireccionales<sup>5</sup> [4] [5] que cumplan con criterios de NO colisión [6]: fuertemente libre de colisiones<sup>6</sup> o débilmente libre de colisiones<sup>7</sup>. Debido a que los *mapeos* caóticos unidimensionales son funciones unidireccionales, entonces, pueden ser aplicados en sistemas que otorguen el servicio de *integridad* y por ello, se hace necesario investigar sobre la viabilidad de esta posibilidad. Finalmente, la *confidencialidad* de la información considera la aplicación de procesos de transformación que permitan obtener una versión incomprensible de la información, de

---

<sup>5</sup> También se llaman funciones Hash, y se refiere a aquellas funciones que transforman un mensaje de longitud variable a uno de longitud fija denominado resumen. Se utilizan para resolver problemas de integridad y autenticidad de origen de los mensajes.

<sup>6</sup> Se refiere a la propiedad de una función Hash que asegura que será computacionalmente difícil encontrar un par cualquiera de mensajes (M, M') de forma que  $H(M)=H(M')$ .

<sup>7</sup> Propiedad de una función Hash que asegura que dada una entrada conocida M, será computacionalmente imposible encontrar otra entrada M' tal que  $H(M)=H(M')$ .

manera que aquellos agentes (personas) ajenos a dicha información no puedan acceder a su versión sin transformar.

De acuerdo a lo anterior, es posible considerar el análisis y diseño de sistemas que fortalezcan u otorguen *integridad* o *confidencialidad* a la información usando *mapeos* caóticos unidimensionales. Con estos antecedentes nuestra decisión quedó orientada a la aplicación de los *mapeos* caóticos unidimensionales a sistemas que otorguen confidencialidad o integridad, o bien, a la aplicación en alguno de los componentes de estos sistemas. Un componente común en estos sistemas son los generadores de secuencias pseudo aleatorias o señales de pseudo ruido, ya que pueden usarse en cifradores de flujo (*confidencialidad*) o sistemas de marcas de agua (*integridad*). Por ello en esta tesis, se muestra la aplicación de los *mapeos* caóticos unidimensionales en la generación de señales de ruido. En particular, se considera y analiza el *Mapeo* Logístico, el cual puede utilizarse para diseñar un generador de ruido analógico con transistores MOS a partir de un circuito cuya función de transferencia siga un modelo de comportamiento logístico.

Ahora bien, los *mapeos* caóticos unidimensionales pueden caracterizarse utilizando herramientas de Mecánica Estadística y se describen con base en su diagrama de bifurcación, su diagrama de trayectorias y su función de distribución; considerando para ello, los diferentes valores que puede tomar el parámetro que gobierna su comportamiento. Con estas herramientas es posible discutir tres aspectos fundamentales de los *mapeos* caóticos unidimensionales: las condiciones que permiten alcanzar la distribución invariante, la dependencia sensitiva ante condiciones iniciales y el proceso de dispersión y mezclado que genera sobre una distribución inicial definida en un intervalo menor al intervalo de definición del *mapeo* [7].



## 1.2 Planteamiento del Problema

Cuando un ingeniero de diseño electrónico pretende diseñar, construir o analizar un generador de ruido empleando *mapeos* caóticos unidimensionales comúnmente procede de la siguiente manera:

1. Busca un circuito cuya función de transferencia sea consistente con un *mapeo* caótico unidimensional. Por ejemplo, un circuito con una función de transferencia cuadrática, si se desea emplear el *mapeo* logístico.
2. Determina las condiciones de operación bajo las cuales el circuito tiene esa función de transferencia. Esto es, precisa los valores de voltaje o corriente de polarización y los voltajes de unión de los transistores, así como las dimensiones y simetría de los transistores.
3. Itera la función de transferencia seleccionada, colocando en el lazo de retroalimentación un amplificador de ganancia  $\mu$ , la cual sea el parámetro que gobierna el comportamiento del *mapeo* que se utiliza, comúnmente considerándose un valor fijo que está en el límite superior de la región caótica.
4. Analiza el comportamiento estadístico de la señal generada por el circuito y lo compara con el comportamiento estadístico esperado.
5. Realiza los ajustes necesarios para que el circuito se comporte de acuerdo con las necesidades de la aplicación.

En este proceder se deben establecer como requisitos de diseño (punto de partida) el rango dinámico y la distribución estadística de la señal de salida del circuito diseñado. El rango dinámico está relacionado con los niveles de corriente o voltaje de la señal que se genera. La distribución estadística de la señal generada debe ser tal que la señal generada sea no periódica y su aspecto debe ser aleatorio. Sin embargo, para obtener la

distribución estadística se debe determinar el comportamiento a largo plazo de la señal generada.

Hasta aquí el ingeniero de diseño se enfrenta al problema de que no se puede determinar el comportamiento a largo plazo de la señal generada, ya que se tendría que analizar una señal infinita, que en la práctica no es posible. Para enfrentar esta situación, el ingeniero de diseño tiene como alternativa aproximar la distribución de la señal de salida usando dos posibilidades: el diseño ciego y el diseño con predicción del comportamiento.

El diseño ciego, también llamado diseño heurístico, consiste en usar herramientas de diseño asistido por computadora (CAD: Computer Aided Design) para simular el circuito; luego en esta simulación, el circuito se hace funcionar un tiempo muy grande; después se analiza la señal generada y se calcula la distribución estadística aproximada. Si la distribución estadística resultante es la deseada entonces el diseño puede considerarse satisfactorio. En caso contrario, es necesario hacer ajustes y repetir el proceso tantas veces como sea necesario hasta obtener la distribución estadística deseada. El inconveniente de este proceder es que el tiempo de prueba y error puede ser muy grande; y en consecuencia, se requiere de un tiempo grande para estimar la distribución estadística. Por otro lado, no se tiene un criterio que permita definir que componentes del circuito deben variarse.

El diseño con predicción del comportamiento consiste en usar el modelo que rige el comportamiento del sistema que se analiza. Con este modelo se elabora un programa de computadora con el cual se predicen los valores que pueda tomar la señal que se espera generar, se analizan estos valores y con ellos se calcula numéricamente la distribución estadística de la señal que pudiera generar el circuito. Los inconvenientes del diseño con predicción del comportamiento son que los sistemas dinámicos presentan sensibilidad ante condiciones iniciales y en la práctica la señal real generada por el

circuito que se construya, a partir de una condición inicial específica, puede no tener nada que ver con la señal predicha, ya que en cada estimación numérica de la señal de interés se lleva a cabo un redondeo, el cual introduce un error. Este error se puede hacer cada vez más grande, con lo que en esta estimación numérica la distribución estadística resultante corresponde a una señal distinta a la señal obtenida en el circuito real.

Ambas alternativas de diseño descritas, demandan un tiempo grande de trabajo y no permiten estimar adecuadamente la distribución estadística de la señal que se genere, ya que el parámetro resultante en el circuito puede ser distinto al considerado. Por lo tanto, el comportamiento estadístico del circuito analizado o diseñado puede ser “no esperado” o “no deseado”. Esta situación obedece a que estas dos formas de proceder no incluyen un criterio que defina con precisión el comportamiento estadístico del sistema. Además, no consideran la potencial influencia del proceso de fabricación en los valores del parámetro que gobierna el comportamiento del circuito o en los valores de los componentes que lo constituyen.

Así, de acuerdo a la delimitación de tema, en esta tesis se aborda el problema de usar el Teorema Ergódico, la distribución invariante, la dependencia sensitiva a condiciones iniciales, el diagrama de trayectorias, el diagrama de bifurcación, el criterio de estabilidad y el Exponente de Lyapunov como herramientas para caracterizar a los *mapeos* caóticos unidimensionales (*mapeo* logístico) y, de esta manera, establecer un procedimiento y los criterios de diseño de un generador de ruido caótico.

El Teorema Ergódico y la distribución invariante son herramientas poderosas con las cuales se puede analizar el comportamiento de los *mapeos* caóticos unidimensionales. Así, cuando el sistema es caótico no se puede determinar de manera práctica el comportamiento de la órbita a largo plazo, ya que se requiere de un análisis estadístico de la órbita que permita averiguar que tan frecuentemente ésta visita diferentes regiones, dando lugar a un histograma asociado a esta órbita. El problema de este punto

de vista radica en que se tendría que analizar una órbita infinita. Para obtener el histograma asociado a la órbita se hace uso del Teorema Ergódico, que dice que se debe estudiar la evolución de una distribución inicial. Luego, a todos y cada uno de los puntos que conforman esta distribución se les aplique el *mapeo*, y cuando se obtenga una distribución que sea invariante ante la aplicación del *mapeo*, tal distribución corresponde a la que se encontraría en el análisis estadístico de la órbita infinita. Así, aunque no se pueda predecir el valor que tome una órbita generada por un *mapeo* caótico unidimensional, si se puede saber el comportamiento estadístico del sistema, el cual es el punto de partida en el diseño de un generador de ruido caótico.

### 1.3 Objetivos

#### **Objetivo General:**

Investigar la manera en que pueden usarse, para diseñar y analizar el comportamiento de generadores de ruido, herramientas como el Teorema Ergódico, la distribución invariante, la dependencia sensitiva ante condiciones iniciales, el diagrama de trayectorias, el diagrama de bifurcación, el criterio de estabilidad y el Exponente de Lyapunov en *mapeos* caóticos unidimensionales. En particular, se consideran diseños basados en el *Mapeo* Logístico.

#### **Objetivos Particulares:**

- a. Investigar y comprender la manera en que se deben aplicar los conceptos como el Teorema Ergódico, la distribución invariante, la dependencia a condiciones iniciales, el diagrama de trayectorias, el diagrama de bifurcación, el criterio de estabilidad y el Exponente de Lyapunov en el análisis y descripción del comportamiento de los *mapeos* caóticos unidimensionales.

- b. Establecer los criterios de diseño de un generador de ruido con base en el Teorema Ergódico, el cual permite calcular numéricamente la distribución invariante de un *mapeo* caótico.
- c. Diseñar y analizar el comportamiento de un generador de ruido analógico que tenga un modelo de comportamiento consistente con el *mapeo* logístico, el cual es uno de los más estudiados.
- d. Dado que el *mapeo* logístico está definido en un intervalo específico que no necesariamente corresponde con las necesidades de operación del circuito a diseñar, se propone un modelo reescalado del *mapeo*.

## 1.4 Justificación

La aplicación de la Teoría del Caos a la protección de la información y las comunicaciones, en general, y a la generación de ruido, en particular, no es un tema nuevo. Desde mediados de los años 90, se han presentado diferentes trabajos en esta dirección y para diferentes aplicaciones. Por ejemplo, en 1998 L. Cong y S. Songgeng presentaron en [8] un esquema de comunicaciones de espectro disperso por salto de frecuencia usando sistemas caóticos. También, en 2001 se publicó el trabajo de A. Tefas et al. de la India, el cual plantea un análisis estadístico de las secuencias caóticas de Markov para aplicaciones en marcas de agua [9]. También en 2002, N. Matsuda y K. Aihara en [10] propusieron un criptosistema con *mapeos* caóticos discretizados superando los problemas de robustez que tenían los criptosistemas caóticos propuestos con anterioridad. Otro ejemplo, es el trabajo realizado por S. Tsekeridou, et al. en 2003, en el cual se aborda el problema de analizar el comportamiento estadístico de las marcas de agua generados por *mapeos* de Bernoulli de n-dimensiones [11]. También en 2003, Zhengguo Li et al. [12], proponen un sistema digital caótico de comunicaciones,

basado en un esquema *one-time-pad*, donde la secuencia aleatoria se sustituye con una secuencia caótica generada por el circuito de Chua. Otros ejemplos mas recientes son: el trabajo realizado en 2004 por N. Sajeeth Philip y K. Babu Joshep de la India, en el cual se aborda el problema de mezclar sistemas caóticos en comunicaciones seguras con cifradores de flujo [13]; el trabajo realizado en 2005 por J. Szczpanski et al. [14], en el cual exploran la posibilidad de usar *mapeos* mezclados al diseño de cajas de sustitución (S-boxes), siguiendo las sugerencias de Shannon en cuanto a los requerimientos de difusión en un cifrador de bloque; y también en 2005, A. Tsuneda, después de la presentación de varios trabajos en esta dirección, propone en [15] el diseño de secuencias binarias basadas en *mapeos* caóticos unidimensionales.

Como puede verse, está vigente el uso de la Teoría del Caos para proponer soluciones tecnológicas que ofrezcan comunicaciones seguras. En esta tesis, se aplica el Teorema Ergódico y las herramientas de Mecánica Estadística con las que se analizan los sistemas dinámicos caóticos (SDC), para caracterizar a los *mapeos* caóticos unidimensionales para su uso en el diseño y el análisis del comportamiento de un generador analógico de ruido que tenga un comportamiento consistente con el *mapeo* logístico.

Es importante mencionar que existen trabajos similares que procuran la generación de señales de ruido empleando sistemas caóticos con implementaciones basadas en transistores MOS, pero en ninguno de ellos se hace mención del uso de las herramientas de mecánica estadística (el Teorema Ergódico, el Diagrama de Bifurcación, la Distribución Estadística y el Exponente de Lyapunov) para establecer los criterios de diseño en el comportamiento estadístico del circuito, tal y como se hace en este trabajo. Por ejemplo, A. G. Radwan et al. [16] sugieren el diagrama de bloques de un oscilador caótico cuyo comportamiento sigue un sistema caótico de Lorenz modificado. El circuito propuesto por Radwan se basa en integradores gm-C, usando transistores MOS

operando en bajo voltaje. Otro artículo en esta dirección está referido en [17] y fue desarrollado por H. Tanaka et al., en este artículo ellos mostraron dos diseños de un generador de ruido compacto para circuitos de gran escala de integración usando tecnología CMOS.

Existen otros trabajos reportados relacionados con el diseño de generadores discretos de ruido que pueden revisarse en [18], [19] y [20], y otros relacionados con generadores analógicos de ruido que pueden revisarse en [21], [22] y [23]. En ambos casos, las señales de salida pueden usarse para aplicaciones criptográficas y para comunicaciones seguras. De la misma manera, que las señales discretas de ruido (secuencias de pseudo ruido), las señales analógicas de ruido deben tener condiciones de aleatoriedad y deben ser impredecibles. La aleatoriedad es una condición que está relacionada con la distribución estadística de la señal de salida que produce el generador de ruido; mientras que la impredecibilidad es una condición relacionada con la seguridad y la producción de la semilla que se usa como condición inicial en el generador de ruido. Para asegurar la impredecibilidad, debería no ser factible determinar la semilla de cualquier valor generado. Esto es, no debe existir ninguna correlación entre una semilla y cualquier valor producido por el generador de ruido; cada muestra de la señal de salida debería tener la apariencia de ser un evento aleatorio independiente.

Típicamente para el diseño de generadores analógicos de ruido se emplean herramientas de diseño asistido por computadora (CAD: Computer Aided Design), se supone una etapa de prueba y error para ajustar el comportamiento del sistema al comportamiento esperado. En este proceder se establece y utiliza un modelo matemático rígido que opera en la región caótica, el cual supone que el parámetro que gobierna el comportamiento del *mapeo* tiene un valor fijo siempre. Sin embargo, no siempre las cuestiones prácticas hacen posible el uso estricto de estos modelos, ya que el valor del parámetro que gobierna un *mapeo* caótico unidimensional puede variar

debido a las condiciones de la implementación. Por ejemplo, el comportamiento de un sistema caótico puede ser distinto al esperado debido a las variaciones del proceso de fabricación de un circuito integrado, o bien, debido a las variaciones en los valores de los componentes del circuito, o por el manejo de la precisión en la representación de un número en un equipo de cómputo. El impacto de esta condición es que la distribución estadística de la señal generada sea distinta a la distribución estadística esperada (deseada), ya que la distribución estadística de la señal generada depende también del parámetro del *mapeo* en cuestión. Por ello, se hace necesario un modelo flexible del *mapeo* que considere las posibles variaciones del parámetro del *mapeo* y que describa con mayor precisión el comportamiento del sistema caótico que se analiza. Por ejemplo, un *mapeo* muy utilizado es el *mapeo* logístico y, típicamente, se considera un valor fijo  $\mu = 4$  para el parámetro que gobierna su comportamiento, y para el cual se produce una distribución estadística conocida. Sin embargo, en esta tesis se muestra que existen otros valores del parámetro con los cuales es posible conocer la distribución estadística invariante de la señal de salida a través de la aplicación del Teorema Ergódico. Con estos valores se puede producir señales con otras distribuciones estadísticas útiles. Adicionalmente, en esta tesis, aprovechando el Teorema Ergódico, se calcula la distribución invariante del *mapeo* caótico, la cual servirá como uno de los criterios principales en el diseño y análisis del generador de ruido caótico. Este criterio puede aplicarse en sistemas de protección de información para otorgar confidencialidad, por ejemplo en cifradores de flujo<sup>8</sup> o sistemas de espectro disperso<sup>9</sup>, o para otorgar integridad, por ejemplo en sistemas de marcas de agua<sup>10</sup>.

---

<sup>8</sup> Sistemas que emplean una función de combinación y una secuencia de pseudo ruido con distribución uniforme para afectar la sintáctica, la semántica y la estadística de un mensaje en texto claro para transformarlo en un mensaje incomprensible.

<sup>9</sup> Sistemas de comunicaciones que transforman el espectro de una señal de interés, de manera que la hacen en apariencia una señal con condiciones similares a una señal de ruido



De la Figura 1 a la Figura 4 se muestra el diagrama a bloques de cada uno de los sistemas en los que se emplean generadores de ruido.

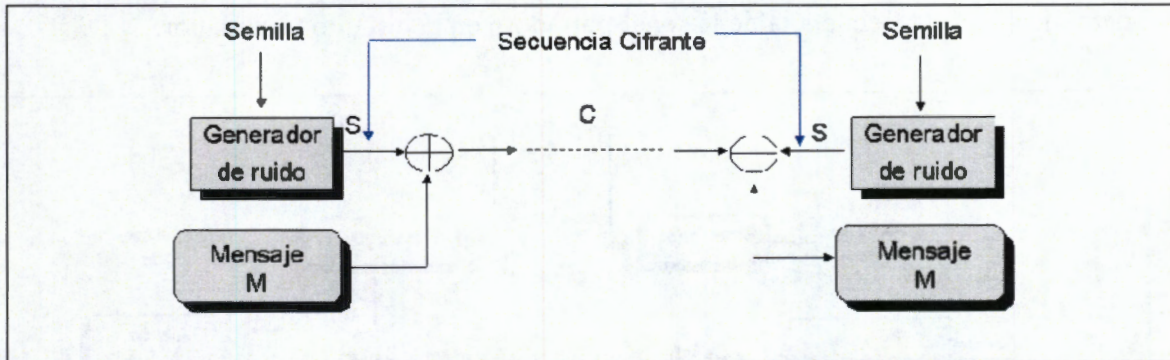


Figura 1. Diagrama a bloques de un cifrador de flujo.

La Figura 1 muestra el diagrama a bloques de un cifrador de flujo, en el cual se emplea un generador de ruido. Este generador contiene un algoritmo determinístico que se hace operar con una semilla, que en el caso de *mapeos* caóticos es la condición inicial. La Figura 2 muestra el diagrama a bloques de un sistema de comunicaciones de espectro disperso, el cual opera bajo la técnica de secuencia directa, y en el que se usa un multiplicador para combinar una señal de ruido con la señal de interés. En este tipo de sistemas un aspecto importante es la sincronía que debe existir entre el transmisor y el receptor, de modo que se pueda lograr una comunicación eficiente.

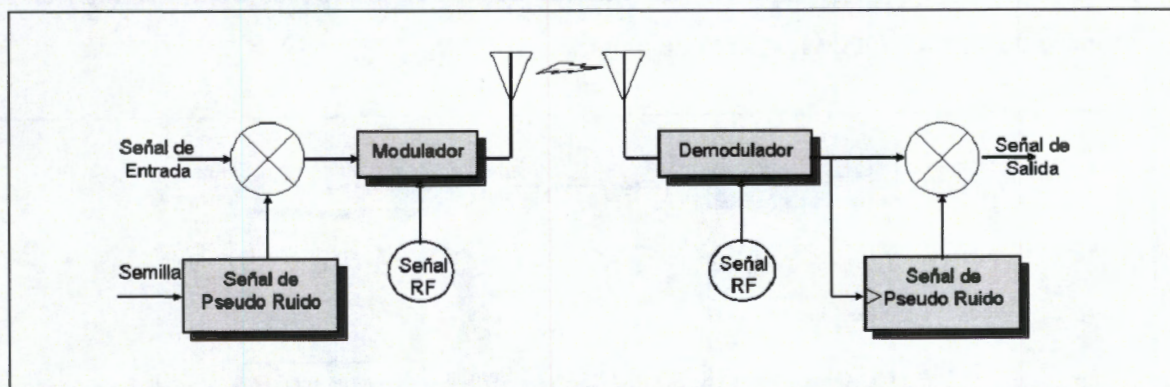


Figura 2. Diagrama a bloques de sistemas de comunicaciones de Espectro Disperso Secuencia Directa.

<sup>10</sup> Sistemas que buscan proteger los derechos de propiedad de un medio digital a través de la inclusión de un atributo resistente a los procesos de transformación que pueda sufrir dicho medio digital.

La Figura 3 muestra el diagrama a bloques de un sistema de comunicaciones de espectro disperso por salto de frecuencias, en el que se emplea un generador de ruido para modificar la frecuencia de la señal portadora en el circuito modulador.

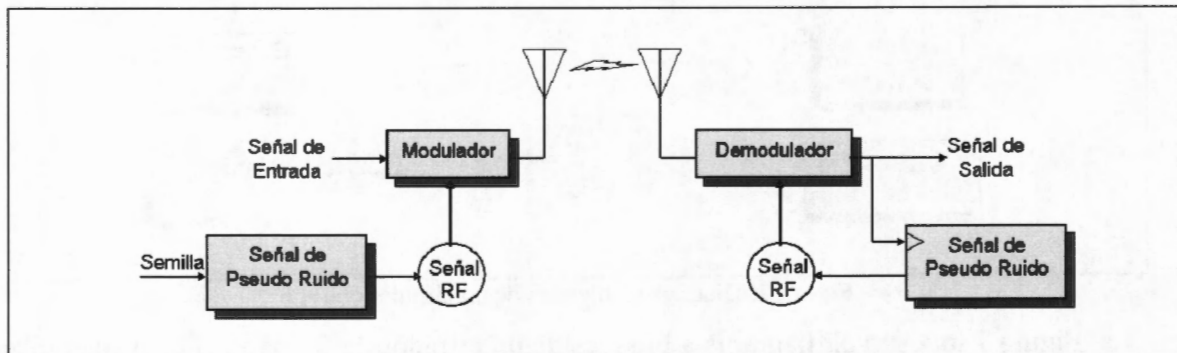


Figura 3. Diagrama a bloques de sistemas de comunicaciones de Espectro Disperso por Salto de Frecuencias.

La Figura 4 muestra el diagrama a bloques de un sistema de marcas de agua en el que se utiliza un circuito generador de pseudo ruido que se hace operar con una semilla y que sirve para dispersar la marca de agua en una imagen que se pretende autenticar con propósitos de proteger los derechos de autor de dicha imagen. De la misma manera que en los sistemas de comunicaciones de espectro disperso, es importante la sincronía, ya que se requiere sincronizar los generadores usados en el proceso de inserción y en el proceso de extracción de la marca de agua.

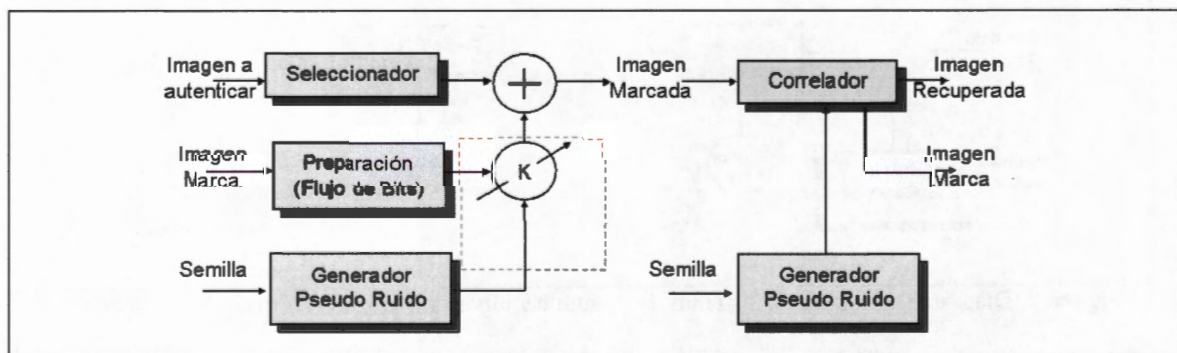


Figura 4. Diagrama a bloques de un sistema de marcas de agua.

Hasta aquí se ha planteado el problema que en esta tesis se aborda, los objetivos que se han definido y que se pretenden alcanzar y la justificación de esta tesis, así como una breve reseña de algunos trabajos en los que se pone de manifiesto el uso de la teoría del caos en distintas áreas de las telecomunicaciones y la protección de la información.

En el siguiente capítulo se aborda y se estudia con detalle el *mapeo* logístico de modo que se pueda entender como puede utilizarse en la generación de señales de ruido. De igual forma, se describen las herramientas de mecánica estadística con las que se describen y analizan sistemas dinámicos, las cuales pueden usarse para diseñar generadores de señales de ruido con *mapeos* caóticos unidimensionales.



---

## CAPÍTULO 2: Estudio del Mapeo Logístico

### Resumen

Este capítulo comienza con la descripción del *Mapeo* Logístico y la presentación de los conceptos de *Universalidad* y *Escalamiento*, el Diagrama de Bifurcación y el Teorema de Sharkowskii. Posteriormente, se muestra la manera en que se determina la distribución invariante de un *mapeo* caótico unidimensional usando el Teorema Ergódico. Luego, haciendo uso del diagrama de bifurcación, se analiza la ruta del orden al caos y la ruta del caos al orden. Enseguida, se presenta el análisis de estabilidad de los *mapeos* caóticos unidimensionales apoyándose en el Exponente de Lyapunov. Este exponente puede calcularse numéricamente a través de la distribución invariante previamente calculada y haciendo uso del Teorema Ergódico. Finalmente, se presenta el análisis de sensibilidad del mapeo ante condiciones iniciales, así como la importancia de las propiedades de mezclado y dispersión de este tipo de *mapeos*.

### 2.1 Antecedentes.

El *Mapeo* Logístico es un *mapeo* caótico unidimensional<sup>11</sup> que fue popularizado en 1976 por el Biólogo Robert May [24] [25] como un modelo demográfico discreto similar al modelo demográfico logístico originalmente publicado en 1838 por Pierre Francois Verhulst [26]. En 1920 el modelo de Verhulst fue redescubierto por Raymond Pearl y Lowell Reed [27] al emplearlo para un estudio demográfico de la población de los Estados Unidos considerando registros desde el año 1790.

También, al final de los años 1940s, John von Neumann sugirió el uso del *mapeo* definido por  $x_{n+1} = 4x_n(1 - x_n)$  como un generador de números aleatorios basados en computadora [28]. Actualmente este *mapeo* se conoce como *Mapeo* de Ulam-von Neumann [29], y es un caso particular del *Mapeo* Logístico cuando  $\mu = 4$ .

---

<sup>11</sup> Ver anexo B para la definición de mapeo caótico unidimensional

Posteriormente, surgieron otros trabajos importantes relacionados con el uso y estudio del *Mapeo* Logístico, pero los que marcaron la diferencia en el estudio analítico detallado del *Mapeo* Logístico son los realizados en los años 1950s. Uno de ellos fue el estudio de la curva de reproducción de peces realizado por William Ricker (1954) [30] y el otro fue el estudio extenso en computadora realizado por Paul R. Stein y Stanislaw Ulam [31] para varios *mapeos* iterados de transformaciones no lineales. Con estos estudios se mostraron las propiedades tan complicadas que tiene el *Mapeo* Logístico. Ciertas propiedades de universalidad del *mapeo* fueron descubiertas en 1973 por M. L. Metropolis, M. L. Stein y P. R. Stein [32]. Mientras que el escalamiento en el punto crítico del doblamiento del periodo fue descubierto independientemente y casi simultáneamente; por un lado, en Alemania por Grossmann y Thomae, pero no llegaron a la universalidad [33]; y por el otro lado, Feigenbaum.

### Universalidad y Escalamiento

La *universalidad* de Feigenbaum se refiere a que existen ciertas propiedades implícitas comunes (tales como el orden en que aparecen los atractores periódicos para diferentes *mapeos*) en todos los sistemas que gobiernan la transición de su comportamiento regular a su comportamiento caótico; en otras palabras, la *universalidad* implica que existen sistemas diferentes que se hacen caóticos de la misma forma<sup>12</sup>. Por otro lado, el *escalamiento* es una propiedad que tienen los sistemas caóticos, a través de la cual presentan un comportamiento autosimilar bajo alguna transformación. El *escalamiento* es un comportamiento de ley de potencia logarítmica presente en todos los fractales<sup>13</sup>.

---

<sup>12</sup> Un ejemplo que muestra el concepto de *universalidad* ver en el Anexo A los diagramas de bifurcación del mapeo senoidal ( $x_{n+1}=r\text{sen}(\pi x_n)$ ) y el mapeo logístico ( $x_{n+1}=rx_n(1-x_n)$ ). Notará que ambas curvas son suaves, cóncavas hacia abajo y tienen un solo máximo.

<sup>13</sup> En el apartado denominado "Doblamiento del Periodo en Órbitas" de la sección 2.3 del capítulo 2 de esta tesis se puede ver como el diagrama de bifurcación del mapeo logístico tiene autosimilaridad si se hace un acercamiento a algunas de sus regiones. Con esto se pone de manifiesto el concepto de *escalamiento*.

La *universalidad* y el *escalamiento* fueron descubiertos en 1978 por Feigenbaum, quien estudió la secuencia de bifurcación del *mapeo* logístico con una calculadora de mano [34] [35]. Feigenbaum primero desarrolló una complicada (ahora olvidada) “Teoría de la función generadora” para predecir  $\mu_n$ , esto es, los valores del parámetro que gobierna el *mapeo*, para los cuales aparece por primera vez un ciclo de orden  $2^n$ . Ambos conceptos, la *universalidad* y el *escalamiento*, se presentan en el apartado que describe el diagrama de bifurcación de este mismo capítulo.

Para finales de los años 1970, la Teoría del Caos se comenzó a conformar como una ciencia y, fue en 1977 cuando surgió la primera Conferencia sobre Teoría del Caos, la cual tuvo lugar en Como, Italia [36]. En esta conferencia hubo trabajos relacionados con el estudio del orden y el caos.

Aunque *orden* en el *caos* parece paradójico, no lo es. *Caos* en lugar de “Confusión, desorden” se refiere a una sensibilidad extraordinaria a las condiciones iniciales y un comportamiento aperiódico a largo plazo que caracteriza a sistemas deterministas no lineales; por determinista se entiende que el sistema no tiene entradas ni parámetros aleatorios. El comportamiento irregular es debido a la no linealidad del sistema. Esta sensibilidad se ha detectado tanto en sistemas matemáticos [37], como en sistemas reales tales como grifos que gotean [38], convección térmica en líquidos, circuitos electrónicos, reacciones químicas y latidos del corazón. Esta sensibilidad que origina *caos* se manifiesta claramente al investigar las trayectorias (en el espacio fase<sup>14</sup>) que describen la variación temporal del estado dinámico de los sistemas disipativos<sup>15</sup>. En

---

<sup>14</sup> Espacio fase es el conjunto de todos los posibles estados de un sistema.

<sup>15</sup> Hay dos tipos de sistemas dinámicos: conservativos y disipativos. Un sistema conservativo puro es tan improbable como un sistema estático. Los sistemas disipativos están expuestos a la progresiva variación de la energía útil y, debido a ello, su evolución queda ligada a una estructura denominada atractor. Un sistema disipativo demuestra que es posible crear orden en el desorden, ya que en estos sistemas surgen estructuras llamadas disipativas, las cuales solo existen lejos del equilibrio y para que existan exigen una cierta disipación de energía. En estos sistemas el no equilibrio es fuente de estructura. Un sistema se llama disipativo o cibernético porque la conservación del orden (información) en su seno, y más su ampliación requieren de la disipación permanente de energía.

presencia de caos, las trayectorias típicas tiende hacia variedades matemáticas con carácter *fractal*, esto es, dimensión fraccionaria. A estas variedades se les conoce como *atractores extraños*<sup>16</sup>. Por el contrario, los sistemas no caóticos muestran *atractores ordinarios* con estructuras sencillas y de dimensión entera.

Así, *Caos y universalidad* lejos de estar en conflicto son conceptos complementarios [39]. La teoría del caos dice que no puede conocerse exactamente como se comportará un sistema dinámico debido a la pérdida de información espacial que sufre su comportamiento con el paso del tiempo (impredecibilidad). Por otro lado, la universalidad asegura que, a pesar de todo, es posible conocer el comportamiento aproximado de dicho sistema dinámico. En este sentido, han surgido trabajos relacionados con la existencia de orden en la región caótica, como el presentado por el E. Piña en 1983 [40]. En dicho trabajo se propone un algoritmo que predice, para la familia de *mapeos* logísticos, el número de órbitas periódicas de periodo arbitrario que ocurren para valores del parámetro menores a otros que corresponden a una órbita periódica estable dada. Dicho algoritmo produce el número de puntos periódicos inestables coexistiendo con la órbita periódica estable.

Además de trabajos de investigación, se han escrito también documentos y libros de divulgación que ofrecen conceptos importantes en términos fácilmente entendibles. Tal es el caso del libro "Order within Chaos: Toward a deterministic approach to Turbulence" publicado en 1986 por Pierre Berge et al [41]. En este libro se aborda una introducción clásica a los sistemas dinámicos desde el punto de vista de la física y la química. Por otro lado, R. L. Devaney en 1989 publicó su libro titulado "An

---

<sup>16</sup> A los atractores caóticos inicialmente se les llamó atractores extraños. En la actualidad tienen poco de extraño, pero se dice así coloquialmente debido a que muchas personas desconocen aún la teoría del caos. Los atractores no son una novedad debida al caos. También existen atractores no caóticos bien conocidos, como el atractor de punto fijo a través del cual el sistema tiende a estabilizarse (Ejemplo: el péndulo simple), el atractor de ciclo límite (Ejemplo: el péndulo alimentado para compensar la fricción), o el atractor periódico (Ejemplo: la trayectoria que describe un planeta alrededor del sol, si se desprecia la influencia de otros astros).



introduction to chaotic dynamical Systems” [42]. En este libro se estableció la definición de lo que significa un sistema dinámico caótico y aproximadamente la mitad del libro está dedicado al estudio de la dinámica de los *mapeos* unidimensionales.

### Definición de Mapeo Logístico

El *Mapeo* Logístico es un *mapeo* unidimensional (1-D) que puede obtenerse de ecuaciones no lineales simples [43] [44] y se define por la familia de curvas parabólicas mostradas en la Figura 5. Esta familia de curvas se pueden obtener usando la ecuación (1) con  $x \in (0, 1)$  y  $\mu \in (0, 4)$ .

$$\tau_{\mu}(x) = \mu x(1-x) \quad (1)$$

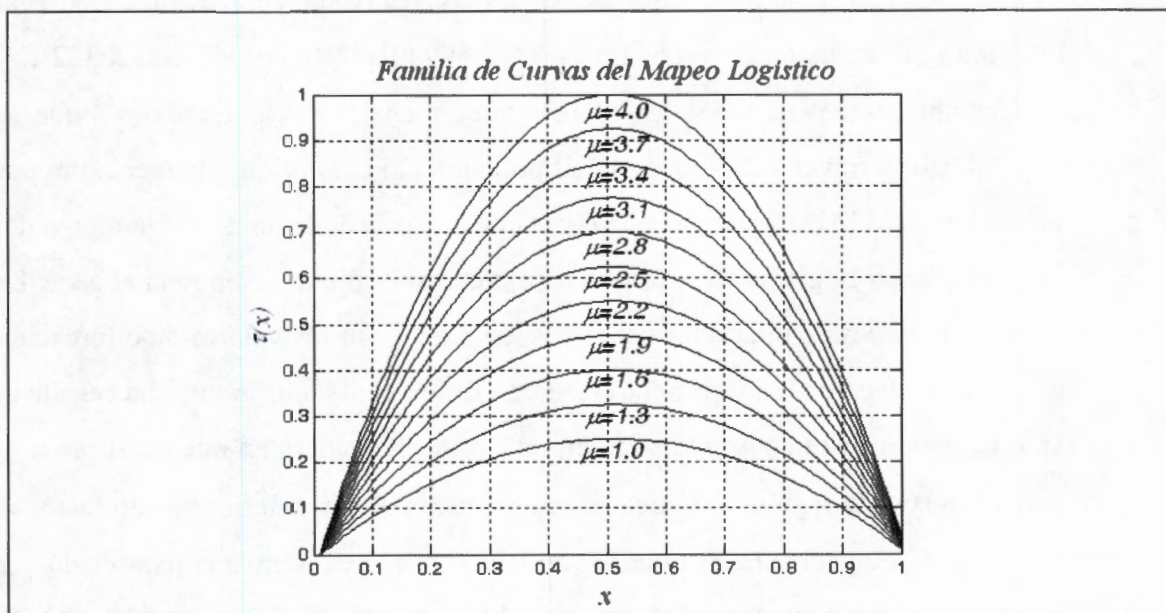


Figura 5. Familia de curvas para el *Mapeo* Logístico para parámetros desde  $\mu = 1$  hasta  $\mu = 4$ .

Esta familia de curvas tiene su máximo en  $x = 1/2$  y su valor es  $\mu/4$  y también puede representarse en forma equivalente, usando la ecuación de iteración (2).

$$x_{n+1} = \mu x_n(1-x_n) \quad (2)$$

### Diagrama de Bifurcación.

En el estudio de los sistemas dinámicos un diagrama de bifurcación<sup>17</sup> es una herramienta útil que muestra las posibles órbitas a las que tiende un sistema (*mapeo*), como una función del parámetro que lo gobierna, y permite determinar donde existe un comportamiento periódico y donde existe un comportamiento caótico. Típicamente, el parámetro de control del *mapeo* se muestra en el eje horizontal y las posibles órbitas del *mapeo* en el eje vertical de la gráfica. Así, el diagrama de bifurcación permite observar en un plano las bifurcaciones de periodo de las órbitas estables (atractoras) del *mapeo*, las cuales ocurren para valores específicos del parámetro que lo gobierna.

En un diagrama de bifurcación existen dos constantes matemáticas y el nombre que tienen es en honor al matemático que las descubrió, Mitchell Feigenbaum [34] [45] [46]. La primera constante de Feigenbaum es  $\delta = 4.66920160910299067185320382\dots$  y se considera universal para todos los *mapeos* unidimensionales unimodales<sup>18</sup> que se aproximan al caos a través del fenómeno del doblamiento del periodo. Feigenbaum por primera vez, en 1975 [47], relacionó esta constante con el fenómeno de doblamiento del periodo en el *Mapeo* Logístico y se utiliza para predecir el punto de entrada al caos. La razón de las longitudes de intervalos sucesivos generados por los valores de bifurcación del parámetro, convergen a la primera constante de Feigenbaum, la cual ha resultado ser la más conocida. Esta constante se interpreta como la manera en que un sistema se aproxima al caos, cada región periódica es más pequeña que la anterior por un factor  $\delta$ . Esta constante de Feigenbaum es importante debido a que es la misma para cualquier función o sistema que sigue la ruta al caos por el fenómeno de doblamiento del periodo

---

<sup>17</sup> Una bifurcación se puede definir como un punto crítico de un sistema, y usualmente se describe como una ramificación (fork) en el comportamiento del sistema, a través de la cual el sistema puede tomar dos posibles ramas que lo conduzcan al caos.

<sup>18</sup> Una función  $f(x)$  se dice que es unimodal en un intervalo específico, si para algún valor de  $\mu$  (el modo de la función), dígame  $\mu_c$ , es monótonamente creciente para  $x \leq \mu_c$  y monótonamente decreciente  $x \geq \mu_c$ . En tal caso, el valor máximo de  $f(x)$  es  $f(\mu_c)$  y no hay otro máximo local en el intervalo en cuestión.

(*universalidad*), para otros *mapeos* se tienen diferentes constantes. La primera constante de Feigenbaum puede usarse para calcular directamente la posición del centro de gravedad del conjunto de Mandelbrot [48]. La segunda constante de Feigenbaum no es tan conocida y tiene un valor de  $\alpha = 2.502907875095892822283902873218\dots$  Esta constante es el factor de escala entre el ancho de una rama de la bifurcación y la rama siguiente. Feigenbaum dice “Asintóticamente, la separación de elementos adyacentes de atractores de periodo doblado es reducido por un valor constante  $\alpha$  de un doblamiento al siguiente” [49]. Si  $d_n$  es la distancia algebraica entre dos elementos cercanos del ciclo atractor de periodo  $2^n$ , entonces  $d_n/d_{n+1}$  converge a  $\alpha$ .

Existen sistemas físicos en los cuales  $\alpha$  y  $\delta$  son relevantes [50]. Por ejemplo, en los años 1980's se realizó una amplia variedad de experimentos de hidrodinámica (en agua, helio y mercurio líquido), óptica (láser retroalimentado), acústica (helio), electrónica (diodo/transistor de Joshepson) [51], biología (músculos del corazón), química, entre otros, en los que aparecen las constantes de Feigenbaum [52]. En estos experimentos fue difícil medir con alta precisión estas constantes universales, debido a los problemas en el manejo de la precisión de las mediciones de las distancias entre bifurcaciones y el ruido inherente en el sistema, así como los problemas teóricos, ya que en muchos de estos experimentos no se tenía una suficiente comprensión acerca de la dinámica de comportamiento del sistema analizado y como la teoría unidimensional podría ayudar a describirlos. En este sentido, ha habido esfuerzos muy importantes para determinar con mayor precisión el valor de ambas constantes de Feigenbaum. Al respecto, se puede consultar el trabajo de Keith Briggs, quien calculó dichas constantes para 576 dígitos decimales [53] [54] y el trabajo de David Broadhurst, quien ha precisado estas constantes para 1018 dígitos decimales [55]. El interés de calcular la mayor precisión posible estas constantes, es para conocer sus propiedades matemáticas, determinar las relaciones algebraicas que satisfacen y evaluar las conjeturas concernientes a estos

números. Estas constantes alcanzan una importancia similar a la de otras constantes con  $\pi$ .

Ahora bien, para construir el diagrama de bifurcación se emplea una serie de experimentos que permiten explorar el comportamiento a largo plazo de la órbita al iterar el *mapeo* logístico para valores de parámetro  $\mu \in (0, 4)$ . Como experimento inicial, considérese que para la ecuación (2) se emplea un valor de parámetro  $\mu = 2$  y se escoge aleatoriamente una condición inicial  $x_0 \in (0, 1)$ . La Figura 6 muestra el comportamiento de la órbita usando esos valores. Nótese que existe un intervalo en el que la órbita no toma al valor estable final directamente, más bien oscila alrededor de dicho valor hasta que después de cierto número de iteraciones la órbita cae en el punto fijo estable (estado final). Si este experimento se repite para diferentes condiciones iniciales siempre que  $x_0 \in (0, 1)$ , invariablemente la órbita alcanzará el mismo estado final (punto fijo estable), cuyo valor es 0.5. Este experimento se puede realizar para diferentes valores del parámetro  $\mu$ , usando una condición inicial aleatoria y para generar una gráfica que muestre el estado final en función de  $\mu$ . Es importante notar que existirán estados finales de más de un punto fijo, conformando órbitas estables. Con estas ideas es posible construir el diagrama de bifurcación de acuerdo con el siguiente procedimiento que evita la fase transitoria de la órbita:

- a) Se selecciona una condición inicial aleatoriamente  $x_0 \in (0, 1)$  y se itera el *mapeo*  $N > 500$  veces, calculando  $x_1, x_2, x_3, \dots, x_N$ .
- b) Se desprecian las primeras 100 iteraciones ( $x_1, x_2, x_3, \dots, x_{100}$ ) para garantizar que se ha superado la etapa transitoria.
- c) Se grafican las iteraciones restantes,  $x_{101}, x_{102}, x_{103}, \dots, x_{200}$ .

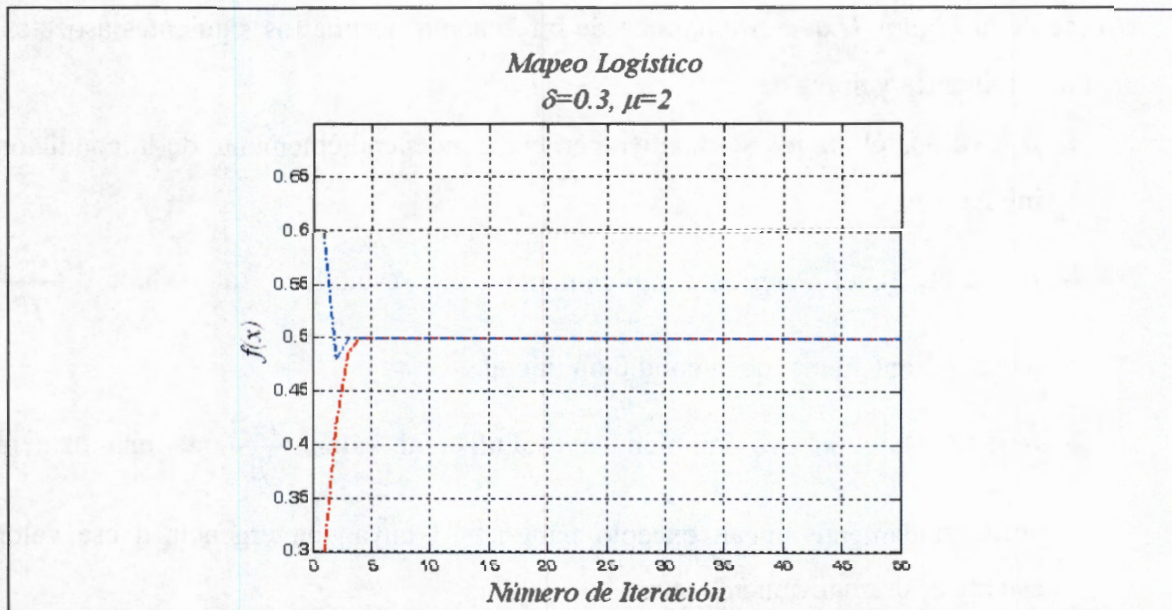


Figura 6. Comportamiento de la órbita con dos condiciones iniciales con  $\delta=0.3$  para el Mapeo Logístico

La Figura 7 muestra la gráfica resultante de este procedimiento para valores del parámetro  $\mu \in (0.0, 4.0)$ .

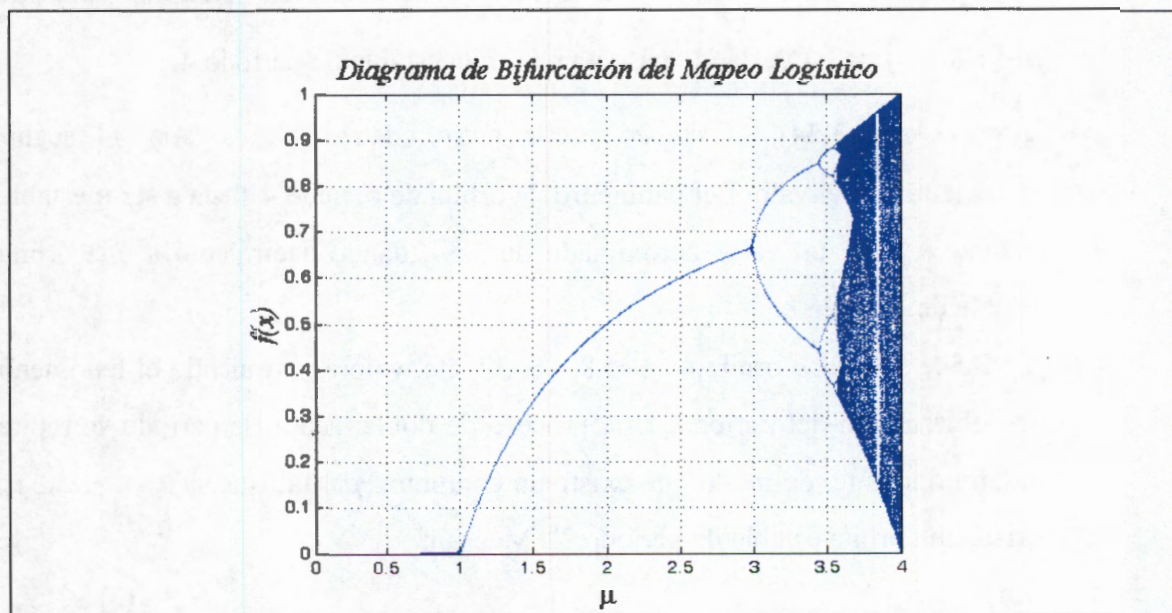


Figura 7. Diagrama de Bifurcación del Mapeo Logístico

Nótese de la Figura 7, que el diagrama de bifurcación resume los siguientes aspectos, para los siguientes valores de  $\mu$ :

- ✚  $\mu \in (0, 1)$ , el *mapeo* se mantiene en cero, independientemente de la condición inicial.
- ✚  $\mu \in (1, 2)$ , el *mapeo* rápidamente se estabiliza al valor  $\frac{\mu-1}{\mu}$  independientemente de la condición inicial.
- ✚  $\mu \in (2, 3)$ , el *mapeo* también se estabiliza al valor  $\frac{\mu-1}{\mu}$  de una manera aproximadamente lineal, excepto para  $\mu = 3$  cuya convergencia a ese valor estable es dramáticamente lenta.
- ✚  $\mu \in (3, 1+\sqrt{6})$ , el *mapeo* oscila entre dos valores, los cuales son dependientes del valor de  $\mu$ . Nótese que conforme el valor del parámetro del *mapeo* se incrementa el periodo de orden 2 llega a ser inestable para un valor de  $\mu = 1+\sqrt{6}$  ( $\mu \cong 3.45$ ), dando paso a una órbita estable de periodo 4.
- ✚  $\mu \in (1+\sqrt{6}, 3.54)$ , el *mapeo* oscila entre cuatro valores. Así, al seguir incrementando el valor del parámetro, la órbita de periodo 4 llega a ser inestable cuando  $\mu$  tiene un valor aproximado de 3.54, dando nacimiento a una órbita estable de periodo 8.
- ✚  $\mu > 3.54$ , el *mapeo* oscilará entre 8, 16, 32, etc. valores, siguiendo el fenómeno de doblamiento del periodo. Este proceso de doblamiento de periodo se repite indefinidamente, de modo que existe un conjunto  $\{\mu_n\}$  tal que si  $\mu_{n+1} > \mu \geq \mu_n$  existe una órbita estable de periodo  $2^n$ . Más aún,

$$\lim_{n \rightarrow \infty} \mu_n \equiv \mu_{\infty} \tag{3}$$

A este valor del parámetro se le llama punto crítico de Feigenbaum.

La órbita que se genera para  $\mu = \mu_\infty$  es obviamente no periódica, y además no contiene ninguna de las órbitas inestables que mueren en el proceso del doblamiento del periodo; de hecho, entre dos puntos de la órbita para  $\mu_\infty$ , se encuentra un punto inestable. De esta forma, el conjunto  $X = \{x_n\}$  que conforma la órbita para  $\mu_\infty$ , es no conexo, ya que en una vecindad alrededor de uno de ellos siempre se encuentra un punto que no pertenece a él. Así, el conjunto  $X$  tiene un número infinito de agujeros, conformando un conjunto de Cantor<sup>19</sup>, que junto con su complemento por todas las órbitas inestables  $\tilde{X}$ , conforman un conjunto continuo  $X \cup \tilde{X} = (x_{\min}, x_{\max})$  cuando  $\mu = \mu_\infty$ . Así, tanto  $X$  como  $\tilde{X}$  son conjuntos de Cantor [56], los cuales poseen una distribución estadística sobre objetos fractales<sup>20</sup>. La Tabla 1 muestra los valores de  $\mu$  para los cuales ocurre el doblamiento del periodo en el *Mapeo* logístico, siendo  $\mu_\infty = 3.569946$ .

---

<sup>19</sup> El Conjunto de Cantor fue introducido por el matemático alemán Georg Cantor en 1883 y se refiere a un conjunto infinito de puntos que existen en el intervalo (0, 1) cuyas propiedades son extraordinarias. El conjunto de Cantor más común es el Ternario y se construye removiendo iterativamente el segmento intermedio de intervalos resultantes de haber removido el segmento central de un intervalo unitario que se ha dividido en tres partes iguales.

<sup>20</sup> Un fractal es un objeto semi geométrico cuya estructura básica, fragmentada o irregular, se repite a diferentes escalas. El término fue propuesto por el matemático Benoît Mandelbrot en 1975 y deriva del Latín fractus, que significa quebrado o fracturado.

$\mu_1 = 3.0$	$\mu_2 = 3.449490\dots$
$\mu_3 = 3.544090\dots$	$\mu_4 = 3.564407\dots$
$\mu_5 = 3.568759\dots$	$\mu_6 = 3.569692\dots$
$\mu_7 = 3.569891\dots$	$\mu_8 = 3.569934\dots$

Tabla 1. Valores de  $\mu$  para los que ocurre el doblamiento del periodo.

- ✚  $\mu \cong 3.569946$ , ( $\mu_\infty$ ) es la entrada del *mapeo* al caos. En ese punto se reconoce el final del fenómeno de doblamiento del periodo.
- ✚  $\mu > \mu_\infty$ , el *mapeo* exhibe un comportamiento caótico, existiendo ciertos valores del parámetro para los cuales existen un comportamiento no caótico. A estas regiones se les llama comúnmente islas de estabilidad.

El diagrama de bifurcación tiene un comportamiento fractal, también llamado autosimilar, y se conoce también como diagrama de Feigenbaum debido a que está muy relacionado con el trabajo de Mitchell Feigenbaum [34]. Se dice que el diagrama de bifurcación es un fractal debido a que si se hace un acercamiento (*zoom*) a alguna de las regiones del diagrama original, se encontrará un diagrama con un comportamiento semejante al que tiene el diagrama original.

El diagrama de bifurcación es una herramienta representativa de la Teoría del Caos, que muestra la estructura que indica los cambios en el comportamiento dinámico del *mapeo*, manifestándose el fenómeno del doblamiento del periodo o fenómeno de bifurcación, al cual René Thom en 1969 vio como un ejemplo de lo que él llamó “*catástrofe generalizada*” [57][59][60].



### Teorema de Sharkowskii

Cuando se analiza el diagrama de bifurcación no se puede dejar de paso la mención del Teorema de Sharkowskii<sup>21</sup>, el cual describe la manera en que se hacen presentes las islas de estabilidad dentro del diagrama de bifurcación de *mapeos* como el *Mapeo* Logístico. Bajo este contexto, las órbitas de periodo 3 son de particular importancia, debido a que cuando aparece la órbita de periodo 3 ya han ocurrido un número incontable de órbitas de periodo infinito de acuerdo con lo que indica el Teorema de Sharkowskii [57]. Para observar esto considere el siguiente orden de números naturales en donde la expresión  $p \succ q$  indica que  $p$  está listado antes que  $q$ :

$$3 \succ 5 \succ 7 \succ \dots \succ 2 \cdot 3 \succ 2 \cdot 5 \succ \dots \succ 2^2 \cdot 3 \succ 2^2 \cdot 5 \succ \dots \succ 2^n \cdot 3 \succ 2^n \cdot 5 \succ \dots \succ 2^n \succ \dots \succ 2^3 \succ 2^2 \succ 2 \succ 1$$

Nótese que primero se tienen todos los números impares mayores que uno; después los números impares multiplicados por dos, luego los números impares multiplicados por dos al cuadrado, luego los números impares multiplicados por dos al cubo, etc. Los números restantes son las potencias de dos, los cuales se escriben en orden descendiente hasta llegar a  $2^0=1$ .

Con estos antecedentes el Teorema de Sharkowskii se puede escribir de la siguiente manera:

*Sea  $F: I \rightarrow I$  con  $I \subseteq \mathbb{R}$  un mapeo continuo. Si  $f$  tiene una órbita periódica de periodo  $k$ , y  $k \succ d$  de acuerdo con el orden de la lista anterior, entonces  $F$  tiene una órbita periódica de periodo  $d$ .*

El Teorema de Sharkowskii es muy general y aplica a todos los *mapeos* continuos de  $\mathbb{R}$ . Por otro lado, es un resultado estrictamente unidimensional y no se conserva para *mapeos* de dimensión de orden mayor. Dentro de estos límites este teorema es una

<sup>21</sup> En algunas referencias bibliográficas se encuentra escrito como Teorema de Charkovsky

herramienta muy poderosa de investigación. Dos implicaciones de este teorema son de particular interés en este trabajo. Primero, si  $f$  tiene una órbita periódica cuyo periodo no es una potencia de dos, entonces  $f$  debe tener un número infinito de órbitas periódicas. Contrariamente, si existe un número finito muy grande de órbitas periódicas, ellas deben ser necesariamente de periodo  $2^k$  ( $k \geq 1$ ). Adicionalmente este teorema implica que si  $f$  tiene una órbita de periodo 3, entonces debe tener un número incontable de órbitas de periodo infinito, esto es, órbitas aperiódicas.

Li and Yorke en 1975 probaron independientemente los principales resultados del Teorema de Sharkowskii y argumentaron que periodo 3 implica caos en el sentido que si  $f$  tiene una órbita de periodo 3, entonces existe un conjunto  $S$  incontable de órbitas aperiódicas (algunas veces llamado conjunto mezclado “scrambled”).

## 2.2 Distribución Invariante y Teorema Ergódico

Un sistema que es caótico, como es el *Mapeo* Logístico, cuenta con dos atributos importantes, su sensibilidad ante condiciones iniciales y la pérdida de la información espacial con el tiempo [61]. Debido a ello, para un sistema caótico no se puede determinar el comportamiento de su órbita a largo plazo. Entonces, se requiere un análisis estadístico de la órbita, el cual consiste en averiguar que tan frecuentemente la órbita visita diferentes regiones, dando lugar a un histograma asociado a esta órbita. El problema de este punto de vista radica en que se tendría que analizar una órbita infinita, lo cual no es posible numéricamente; sin embargo, se puede determinar aproximadamente la distribución invariante (estacionaria),  $\rho_{est}$ , al considerar órbitas del *mapeo* muy grandes.

### Uso del Teorema Ergódico de Birkhoff

Para obtener la distribución invariante asociada al *mapeo* se hace uso del Teorema Ergódico de Birkhoff<sup>22</sup>, que implica que es equivalente estudiar la evolución de una distribución inicial, y a todos y cada uno de los puntos que la conforman se les aplique el *mapeo*, y cuando se obtenga una distribución que sea invariante ante la aplicación del *mapeo*, tal distribución corresponde a la que se encontraría en el análisis estadístico de la órbita infinita. Así, aunque no se pueda predecir el valor que tome una órbita generada por un sistema dinámico caótico<sup>23</sup>, si se puede saber el comportamiento estadístico del sistema. El Teorema Ergódico de Birkhoff es uno de los mayores resultados en la Teoría Ergódica, fue probado por primera vez en 1931 por G.D. Birkhoff [62], y desde entonces ha habido varios autores que lo han probado [63], la prueba más reciente fue realizada por Rudolph en 1990 [64].

Para entender esto, considérese que cuando se itera el *mapeo*  $f(x)$  sobre algún valor  $x_0$  se genera la órbita,

$$O(x_0) = \{x_0, f(x_0), \dots, f^n(x_0), \dots\} \quad (4)$$

De modo que, el promedio de una función  $b(x)$  sobre la órbita  $O(x_0)$  está definida por

$$\overline{b(x_0)} = \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{j=0}^{n-1} b(f^j(x_0)) \quad \text{con } f^0(x_0) = x_0 \quad (5)$$

Ahora bien, el primer Teorema de Birkhoff [65] asegura la existencia de este límite para casi todas las condiciones iniciales  $x_0$ , y además, es constante casi en cualquier punto del espacio. En tanto que el segundo Teorema de Birkhoff establece que, cuando el *mapeo* es ergódico, este promedio es igual al promedio sobre el espacio fase definido por:

<sup>22</sup> El Teorema Ergódico es frecuentemente interpretado de la siguiente forma: "Para una transformación ergódica, el promedio estadístico es seguramente igual al promedio aritmético". En general el promedio estadístico y el promedio aritmético son diferentes, pero si la transformación es ergódica y la medida invariante, son iguales casi siempre. Véase el Anexo C para ver el sentido del Teorema Ergódico.

$$\overline{b(x_0)} = \langle b(x) \rangle = \int b(x) \rho_{est}(x) dx \quad (6)$$

Esto es conocido como el Teorema Ergódico de Birkhoff, su importancia yace en el hecho de que los sistemas dinámicos caóticos presentan sensibilidad ante condiciones iniciales, lo que implica que en la práctica no sea posible calcular la órbita de un punto  $x_0$ , ya que en cada evaluación  $f^j(x_0)$  se lleva a cabo un redondeo que introduce un error en la iteración, y este error se hace cada vez mayor, de forma que la órbita calculada puede no tener nada que ver con la órbita real. Sin embargo, de (6), se establece que el promedio sobre la órbita es igual al promedio sobre el espacio fase, de manera que si se puede determinar la distribución invariante,  $\rho_{est}$ , entonces, es posible evaluar  $\langle b(x) \rangle$  que es idéntico al promedio sobre la órbita.

### Medida Estadística y Distribución Invariante

Con estos resultados es posible determinar la medida de un conjunto  $A$ ,  $\mu_{est}(A)$ , la cual está definida por

$$\mu_{est}(A) = \int_A \rho_{est}(x) dx \quad (7)$$

Para ello, considérese que  $b(x) = I_A(x)$ , donde  $I_A(x)$  está definida por,

$$I_A(x) = \begin{cases} 1, & \text{si } x \in A \\ 0, & \text{si } x \notin A \end{cases} \quad (8)$$

Así,

$$\overline{b(x_0)} = \lim_{n \rightarrow \infty} \frac{n_i}{n} \quad (9)$$

siendo  $n_i$  es el número de veces que la órbita visita al intervalo  $A_i$  y  $n$  es el número de elementos que conforman la órbita. Así,

<sup>23</sup> Ver anexo B donde se incluye la definición dada por R.L. Devaney para Sistemas Caóticos

$$\begin{aligned}\int b(x)\rho_{est}(x)dx &= \int I_A(x)\rho_{est}(x)dx \\ &= \int \rho_{est}(x)dx \\ &= \mu_{est}(A)\end{aligned}\tag{10}$$

Ahora, usando la ecuación (6), se encuentra el valor de  $\mu_{est}(A)$ ,

$$\mu_{est}(A) = \lim_{n \rightarrow \infty} \frac{n_i}{n}\tag{11}$$

Se dice que esta medida es invariante cuando se cumple la propiedad de invarianza<sup>24</sup> [66] [67] [68], la cual dice que para cualquier conjunto  $A$ :

$$\mu_{est}(A) = \mu_{est}(f^{-1}(A))\tag{12}$$

en donde  $f^{-1}(A)$  es el conjunto de puntos que van a  $A$  después de una aplicación del mapeo  $f$ , o sea:

$$f^{-1}(A) = \{x | f(x) \in A\}\tag{13}$$

Lo que significa que la medida estadística para un intervalo es igual a la medida estadística de su preimagen, lo cual se desprende del hecho de que el promedio sobre la órbita es independiente del punto inicial. Cuando se satisface la propiedad de invarianza se dice que la medida es invariante ante el mapeo  $f(x)$ .

Numéricamente existen dos formas de encontrar la medida invariante utilizando el Teorema Ergódico de Birkhoff. La primera forma es la siguiente: dada una condición inicial estudiar el comportamiento estadístico de una órbita larga. Esto se hace dividiendo el dominio del mapeo  $f(x)$  en  $K$  regiones  $A_i$  con  $i = 1, 2, 3, \dots, K$ , asociándole a cada una de ellas una medida estadística que corresponde a la frecuencia

<sup>24</sup> También llamada Principio de Invarianza o Propiedad Invariante y se refiere a la propiedad que tiene un objeto de mantenerse sin cambio a pesar de que se le haya aplicado alguna transformación u operación. A este principio también se le llama simetría o invarianza. En sistemas dinámicos se conoce como el Principio de Krasovskii-Lasalle y se considera un criterio de estabilidad asintótica o estabilidad de Lyapunov de un sistema dinámico (posiblemente no lineal). LaSalle fue el primer autor del Oeste en publicar este principio en 1960. Sin embargo, su primera publicación fue en 1952 por Barbashin y Krasovskii en un caso especial y en 1959 por Krasovskii en el caso general.

de visitas a  $A_i$ , es decir:  $P_i = \frac{n_i}{n}$ , donde  $n_i$  es el número de veces que la órbita visita a  $A_i$  y  $n$  es el número de elementos que conforman la órbita. Es posible demostrar usando el Teorema de Birkhoff que la medida invariante del intervalo está dada por el límite de la frecuencia de visitas cuando la órbita tiende a infinito [69], así,

$$P_i^{inv} = \lim_{n \rightarrow \infty} \frac{n_i}{n} \quad (14)$$

Esta ecuación, puede expresarse en términos del *mapeo* de la siguiente manera:

$$P_i^{inv} = \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{j=1}^{n+1} I_{A_i}(f^j(x_0)) \quad \text{con } i = 1, 2, \dots, K \text{ y } f^0(x_0) = x_0 \quad (15)$$

Donde  $I_{A_i}$  denota la función característica o de pertenencia al intervalo  $A_i$  definida por la ecuación (8). Así, la medida invariante está definida por la densidad de probabilidad,

$$\rho_{inv}(x) = \sum_{i=1}^K \frac{P_i^{inv}}{L(A_i)} I_{A_i}(x) \quad (16)$$

donde  $L(A_i)$  es la longitud del intervalo.

La segunda manera de encontrar la distribución invariante está basada en el hecho de que los sistemas dinámicos tienen la propiedad de mezclado<sup>25</sup> (son mixing), lo que significa que al aplicar iterativamente el *mapeo* a casi cualquier función de distribución inicial, eventualmente, se llegará a la distribución invariante [69]. Para llevar a cabo una simulación numérica utilizando esta propiedad, se estudia la evolución temporal de  $M \gg 1$  condiciones iniciales que se eligen al azar, generadas por una distribución  $\rho_0(x)$ , i.e.:  $\{x_0^1, x_0^2, x_0^3, \dots, x_0^M\}$ , estos números son  $M$  realizaciones de la variable aleatoria  $x_0$  con distribución de probabilidad dada  $\rho_0(x_0)$ .

<sup>25</sup> Se dice que un sistema dinámico es mezclado si el espacio fase del sistema llega a ser fuertemente entrelazado (strongly intertwined). El mezclado es un concepto aplicado en Teoría de Ergodicidad, esto es, el estudio de procesos estocásticos y sistemas dinámicos que conservan su medida (measure-preserving dynamical systems).

Para conocer la evolución de esta distribución se aplica el *mapeo* a cada una de las realizaciones y se obtienen los nuevos valores:  $\{x_1^1, x_1^2, x_1^3, \dots, x_1^M\}$ , donde  $x_1^i = f(x_0^i)$  con  $i=1, 2, 3, \dots, M$  que son realizaciones de una variable aleatoria  $x_1$  con distribución de probabilidad  $\rho_1(x_1)$ . Llevando a cabo este procedimiento iterativamente se obtiene  $\{x_n^1, x_n^2, x_n^3, \dots, x_n^M\}$ , donde  $x_n^i = f(x_{n-1}^i)$  corresponde a realizaciones de la variable aleatoria  $x_n$  con distribución de probabilidad  $\rho_n(x_n)$ .

La densidad de probabilidad  $\rho_n(x)$  se estima, dividiendo el intervalo unitario en  $K$  partes, encontrando la frecuencia relativa de las realizaciones de la variable aleatoria  $x_n$  en cada uno de los  $K$  intervalos, y construyendo la función:

$$\rho_n(x) = \sum_{i=1}^K \varphi_n(i) I_{A_i}(x) \quad (17)$$

en donde  $I_{A_i}$  denota la función de pertenencia al intervalo  $A_i$  y  $\varphi_n(i)$  está definida como sigue,

$$\varphi_n(i) = \frac{P_i^{(n)}}{L(A_i)} \quad (18)$$

siendo  $P_i^{(n)} = \frac{n_i^{(n)}}{M}$ , con  $n_i^{(n)}$  el número de realizaciones de  $x_n$  que se encuentran en el intervalo  $A_i$  y  $L(A_i)$  la longitud del intervalo.

De esta manera, el *mapeo* en cuestión define un proceso estocástico caracterizado por la secuencia de funciones de distribución,

$$\{\rho_0(x_0), \rho_1(x_1), \rho_2(x_2), \dots\} \quad (19)$$

Esta secuencia de funciones tiende a una distribución límite, la cual es independiente de la forma explícita de la distribución inicial, la cual existe. Esta propiedad surge debido a que el *mapeo* es mezclado. Así se tiene que:

$$\rho_{\infty}(x) = \lim_{n \rightarrow \infty} \rho_n(x) \quad (20)$$

Por otro lado, esta función límite en la secuencia de funciones de densidad generadas se puede encontrar por el operador de Perron-Frobenius (PF)<sup>26</sup> [43], considerando que,

$$\rho_n(x) = \hat{U}\rho_{n-1}(x) \quad (21)$$

donde  $\hat{U}$  denota el operador de PF y se expresa de la siguiente manera,

$$\rho_n(x_n) = \int_{X_{n-1}} \delta(f(x_{n-1}) - x_n) \rho_{n-1}(x_{n-1}) dx_{n-1} \quad (22)$$

Es fácil ver que al aplicarle el operador de Perron-Frobenius a  $\rho_{\infty}(x)$  esta distribución permanece invariante.

### Convergencia de Medidas Estadísticas

Teóricamente la medida invariante se encuentra cuando las variables aleatorias  $x_n$  y  $x_{n+1}$  tienen la misma distribución, de forma que  $\rho_n(x_n) = \rho_{n+1}(x_{n+1})$ . Sin embargo, desde el punto de vista numérico se requiere definir una distancia  $\varepsilon_n$  entre distribuciones de dos secuencias resultantes de iteraciones consecutivas. Para ello, es necesario considerar que de acuerdo con A. Lasota y M.C. Mackey [69] es posible calcular la convergencia débil y fuerte de medidas estadísticas.

*Definición de Convergencia Débil:* Sea  $\{\mu_n\}$  con  $\mu_n \in M$  una secuencia de medidas y sea  $\mu \in M$ . Se dice que  $\{\mu_n\}$  es débilmente convergente a  $\mu$  si,

$$\lim_{n \rightarrow \infty} \int_X h(x) \mu_n(dx) = \int_X h(x) \mu(dx) \quad \text{para cada } h \in C_0 \quad (23)$$

<sup>26</sup> Es un operador que describe la evolución en el tiempo de densidades en un espacio fase. Se llama así en honor a los matemáticos alemanes Oskar Perron (1880-1975) y Ferdinand Georg Frobenius (1849-1917).



Observe que en el caso cuando  $\mu_n$  y  $\mu$  son absolutamente continuos, y tienen densidades  $\rho_n$  y  $\rho$  respectivamente, la condición de la definición anterior se reduce a<sup>27</sup>,

$$\langle h, \rho_n \rangle = \int_X h(x) \rho_n(x) dx \rightarrow \int_X h(x) \rho(x) dx = \langle h, \rho \rangle \quad \text{para cada } h \in C_0 \quad (24)$$

Antes de dar la definición de convergencia fuerte es necesario introducir el concepto de distancia entre dos medidas  $\mu_1, \mu_2 \in M_{fin}$ . Sea  $(X_1, X_2, \dots, X_n)$  una partición medible de

$X$ , esto es,  $X = \bigcup_{i=1}^n X_i$ ,  $X_i \cap X_j = \emptyset$ , para  $i \neq j$ . Así se tiene que,

$$\|\mu_1 - \mu_2\| = \sup \sum |\mu_1(X_i) - \mu_2(X_i)|, \quad (25)$$

Donde el supremo se toma sobre todas las particiones medibles de  $X$  con  $n$  arbitrario. El valor  $\|\mu_1 - \mu_2\|$  es la distancia deseada<sup>28</sup>.

*Definición de Convergencia Fuerte:* Se dice que una secuencia  $\{\mu_n\}$ ,  $\mu_n \in M_{fin}$  es fuertemente convergente a una medida  $\mu \in M_{fin}$  si,

$$\lim_{n \rightarrow \infty} \|\mu_n - \mu\| = 0 \quad (26)$$

Donde  $\|\mu_n - \mu\|$  es la norma en el caso cuando las medidas  $\mu_n$  y  $\mu$  son absolutamente continuas con derivadas Radon-Nikodym  $\rho_n$  y  $\rho$  respectivamente. De este modo se tiene que,

<sup>27</sup> Para simplificar la notación se usa la noción de producto escalar para medidas,  $\langle h, \mu \rangle = \int_X h(x) \mu(dx)$ . Con esta notación

la convergencia débil de medidas tiene una forma simple. Esto es,  $\{\mu_n\}$  converge a  $\mu$  débilmente si

$$\lim_{n \rightarrow \infty} \langle h, \mu_n \rangle = \langle h, \mu \rangle \quad \text{para } h \in C_0.$$

<sup>28</sup> En el caso especial de que  $\mu = \mu_1$  es arbitrario y  $\mu_2 = 0$  se tiene que,  $\|\mu\| = \sup \sum_{i=1}^n \mu_1(X_i) = \mu(X)$

$$\begin{aligned}
 \|\mu_n - \mu\| &= \sup \sum_{i=1}^n \left| \int_{X_i} (\rho_n(x) - \rho(x)) dx \right| \\
 &\leq \sup \sum_{i=1}^n \int_{X_i} |\rho_n(x) - \rho(x)| dx \\
 &= \int_{X_i} |\rho_n(x) - \rho(x)| dx
 \end{aligned} \tag{27}$$

De acuerdo con estas definiciones de convergencia de medidas, para esta tesis se ha seleccionado la convergencia fuerte, por lo que  $\varepsilon_n$  puede expresarse por la ecuación siguiente:

$$\varepsilon_n = \int_{\Omega} |\rho_{n+1}(x) - \rho_n(x)| dx \tag{28}$$

A partir de las ecuaciones (17) y (18), la ecuación (28) queda como sigue:

$$\varepsilon_n = \sum_{i=1}^K \frac{|n_i^{(n+1)} - n_i^{(n)}|}{M} \tag{29}$$

de manera que se considerará que se ha obtenido la distribución invariante cuando  $\varepsilon_n \leq \delta$ , con  $\delta$  un número pequeño establecido de antemano.

De esta manera, con la ecuación (22) también es posible determinar la expresión dada en la ecuación (28) para  $\varepsilon_n$ . En la Figura 8, se muestra el comportamiento de  $\varepsilon_n$  y de  $\varepsilon_{2n}$  para el Mapeo Logístico usando el valor del parámetro  $\mu = 3.75$ . La distribución inicial seleccionada es una distribución uniforme en el intervalo (0.7, 0.8), generada con 10000 valores aleatorios en este intervalo.

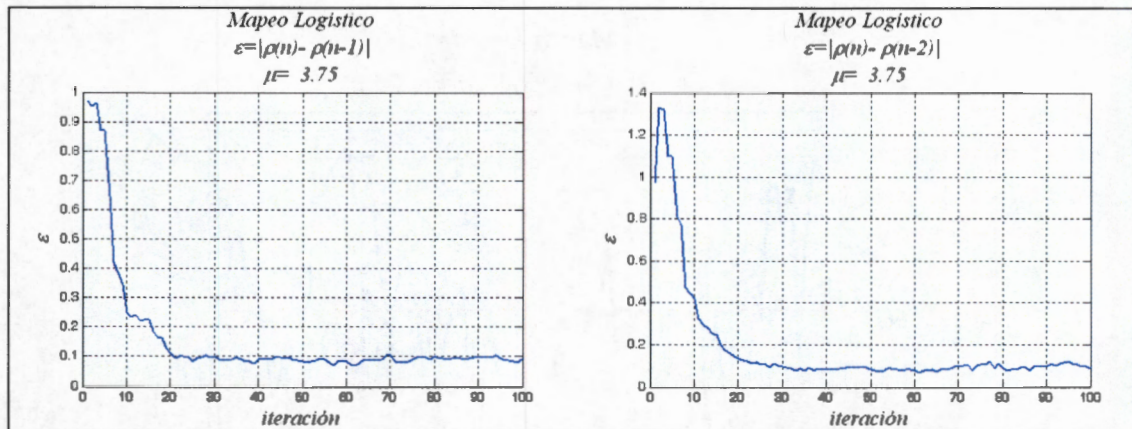


Figura 8. Comportamiento de  $\varepsilon_n$  y  $\varepsilon_{2n}$  para el Mapeo Logístico cuando  $\mu = 3.75$

En ambas gráficas de la Figura 8 se observa que después de 20 iteraciones el valor de  $\varepsilon$  se ha estabilizado, lo que indica que se ha alcanzado la distribución invariante, ya que después de esta iteración,  $\langle \varepsilon_n \rangle$  es 0.0894 con una desviación estándar de 0.0091 dentro del intervalo  $[0.0696, 0.1078]$  para  $\varepsilon_n$ , considerando un rango entre 20 y 100 iteraciones, como se muestra en la Figura 9.

Los resultados para ambas gráficas de la Figura 8 indican que se requieren alrededor de 20 iteraciones para alcanzar la distribución invariante, la cual se muestra en la Figura 10, siendo su dominio de definición el intervalo  $(0.21, 0.95)$  considerando una partición de 100 intervalos dentro del intervalo unitario.

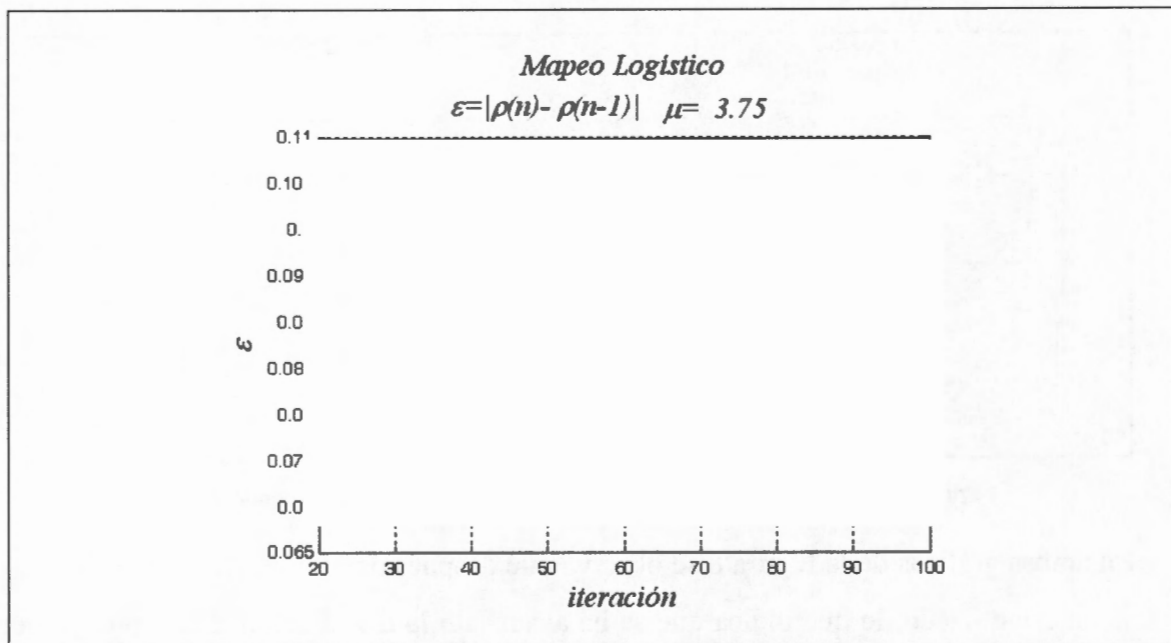


Figura 9. Media y desviación estándar de  $\varepsilon_n$  para el *Mapeo Logístico* cuando  $\mu = 3.75$

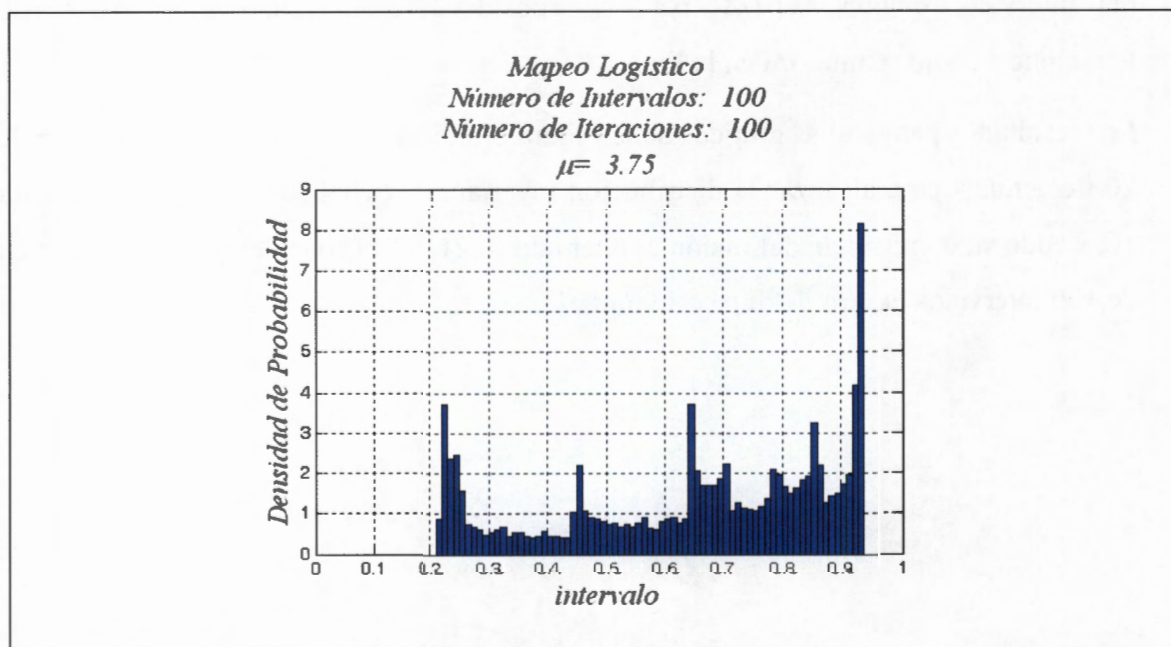


Figura 10. Distribución Invariante para el *Mapeo Logístico* cuando  $\mu = 3.75$

## Divergencia de Kullback Leibler

Otra manera de estimar la diferencia entre dos distribuciones de probabilidad  $\rho_1(x)$  y  $\rho_2(x)$ , es el uso de la divergencia de Kullback-Leibler<sup>29</sup>, la cual es una medida no conmutativa. Típicamente  $\rho_1(x)$  representa la distribución de datos verdadera, observaciones ó una distribución precisa calculada teóricamente. La  $\rho_2(x)$  representa una teoría, un modelo, una descripción, ó una aproximación de  $\rho_1(x)$ . Esta divergencia fue introducida por Solomon Kullback y Richard Leibler en 1951, como la divergencia directa entre dos distribuciones, la cual no es equivalente a la divergencia en cálculo, ya que es NO simétrica, esto es,  $D_{KL}(\rho_1 \parallel \rho_2) \neq D_{KL}(\rho_2 \parallel \rho_1)$ <sup>30</sup>.

Así para distribuciones  $\rho_1(x)$  y  $\rho_2(x)$  de una variable aleatoria discreta, la divergencia de Kullback-Leibler está definida como<sup>31</sup>:

$$D_{KL}(\rho_1 \parallel \rho_2) = \sum_i \rho_1(i) \log \frac{\rho_1(i)}{\rho_2(i)} \quad (30)$$

Para distribuciones de una variable aleatoria continua, las sumas quedan expresadas por integrales, de manera que:

$$D_{KL}(\rho_1 \parallel \rho_2) = \int_{-\infty}^{\infty} p(x) \log \frac{p(x)}{q(x)} dx \quad (31)$$

donde p y q denota las densidades de  $\rho_1(x)$  y  $\rho_2(x)$ .

<sup>29</sup> La divergencia de Kullback-Leibler también se llama divergencia de la información, ganancia de la información ó entropía relativa. La divergencia de Kullback-Leibler es un caso especial de una clase amplia de divergencias llamada "*f-divergencias*". Aunque frecuentemente es reconocida como una distancia métrica, la divergencia de Kullback-Leibler no es una métrica verdadera, ya que es NO simétrica, de ahí que se le considere "divergencia" más que una "distancia".

<sup>30</sup> La divergencia de Kullback-Leibler es bien definida para distribuciones continuas y además es invariante bajo transformaciones de parámetros. Puede verse como una cantidad fundamental en teoría de la información, tal como la información mutua o la entropía de Shannon, las cuales pueden llegar a ser indefinidas ó negativas para probabilidades NO discretas.

<sup>31</sup> La divergencia de Kullback-Leibler puede interpretarse como la longitud esperada extra del mensaje por dato que debe ser comunicada, si se usa un código que es óptimo para una distribución  $\rho_2$  (wrong) dada, comparada con aquella que usa un código basado en una distribución verdadera  $\rho_1$ .

Generalizando los dos casos anteriores, si  $d\rho_1=p d\mu$  y  $d\rho_2=q d\mu$  son medidas de probabilidades sobre el conjunto  $X$ , absolutamente continuos respecto a una medida estadística  $\mu$ , entonces la divergencia de Kullback-Leibler de  $\rho_1$  y  $\rho_2$  se define como:

$$D_{KL}(\rho_1 \parallel \rho_2) = \int_X p \log \frac{p}{q} d\mu \quad (32)$$

considerando que la expresión del lado derecho existe.

Así, si  $\rho_1$  es absolutamente continua con respecto a  $\rho_2$ , lo cual es necesario para que

$D_{KL}(\rho_1 \parallel \rho_2)$  sea finita, entonces,  $\frac{p}{q} = \frac{d\rho_1}{d\rho_2}$ , es la derivada Radon-Nikodym de  $\rho_1$  con

respecto a  $\rho_2$  y la expresión llega a ser:

$$D_{KL}(\rho_1 \parallel \rho_2) = \int_X \log \frac{d\rho_1}{d\rho_2} d\rho_1 = \int_X \frac{d\rho_1}{d\rho_2} \log \frac{d\rho_1}{d\rho_2} d\rho_2 \quad (33)$$

lo cual se reconoce como la entropía de  $\rho_1$  relativa a  $\rho_2$ .

Asimismo, si  $\rho_2$  es absolutamente continua respecto a  $\rho_1$  entonces,

$$D_{KL}(\rho_1 \parallel \rho_2) = - \int_X \log \frac{d\rho_2}{d\rho_1} d\rho_1 \quad (34)$$

En cualquier caso, la divergencia de Kullback-Leibler no depende de la medida estadística  $\mu$ .

De las definiciones dadas anteriormente, se puede ver que para el caso discreto, se tiene que,

$$\begin{aligned} D_{KL}(\rho_1 \parallel \rho_2) &= - \sum_j \rho_1(j) \log \rho_2(j) + \sum_j \rho_1(j) \log \rho_1(j) \\ &= H(\rho_1, \rho_2) - H(\rho_1) \end{aligned} \quad (35)$$

donde  $H(\rho_1, \rho_2)$  es la entropía cruzada de  $\rho_1$  y  $\rho_2$ , y  $H(\rho_1)$  es la entropía de  $\rho_1$ .

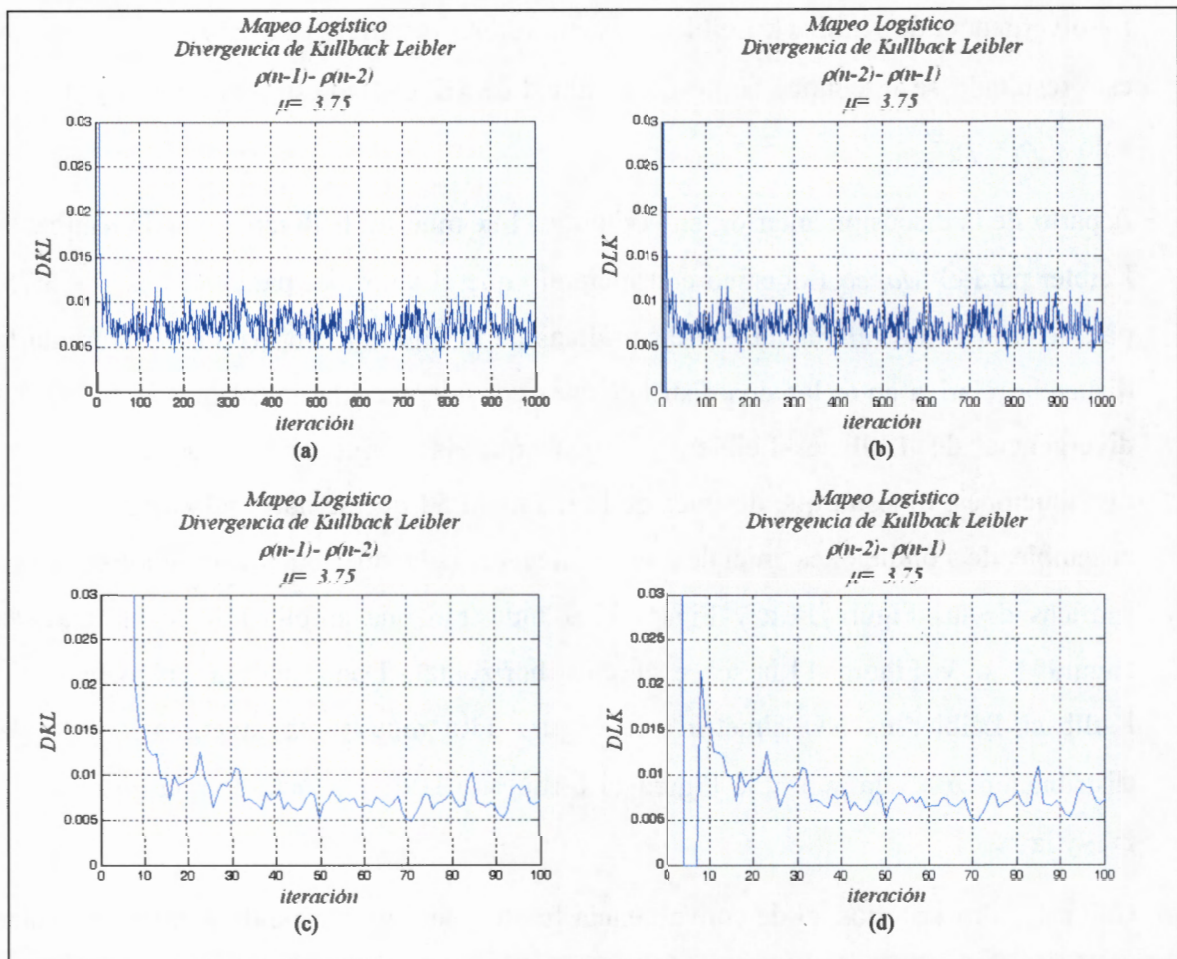
La divergencia de Kullback-Leibler es siempre NO negativa, esto es  $D(\rho_1||\rho_2) \geq 0$ . A este resultado se le conoce como desigualdad de Gibbs. Nótese que  $D(\rho_1||\rho_2)=0$  si y solo si  $\rho_1 = \rho_2$ <sup>32</sup>.

A partir de la discusión anterior, en la Figura 11 se muestra la divergencia de Kullback-Leibler para el *Mapeo* Logístico considerando que el valor del parámetro es  $\mu = 3.75$ , para tenerlo como referencia con las gráficas de la Figura 8, en las que se presenta la distancia relativa entre las dos distribuciones considerando la convergencia fuerte. La divergencia de Kullback-Leibler, al igual que la convergencia fuerte entre las distribuciones, muestra que después de la iteración 50 que se hace del *mapeo* sobre el ensemble de condiciones iniciales se ha llegado a la distribución estacionaria. Las gráficas de las Figura 11.c y Figura 11.d muestran una ampliación de las gráficas Figura 11.a y Figura 11.b sobre el ejes horizontal. Dado que la divergencia de Kullback-Leibler es NO simétrica, la Figura 11.a muestra la divergencia entre la distribución  $\rho_{n-1}$  y la  $\rho_{n-2}$ , y la Figura 11.b muestra la divergencia ente la distribución  $\rho_{n-2}$  y la  $\rho_{n-1}$ .

Con estos dos criterios, el de convergencia fuerte y la divergencia de Kullback-Leibler es posible reconocer que después de unas cuantas decenas de iteraciones aplicadas del *mapeo* sobre la distribución inicial, se llega a la distribución invariante que permite conocer la distribución estadística que tendrá el sistema dinámico que se analiza o se diseña.

---

<sup>32</sup> La entropía  $H(\rho_1)$  entonces establece un valor mínimo de la entropía cruzada  $H(\rho_1, \rho_2)$ , el número esperado de bits requeridos cuando se usa un código basado en  $\rho_2$  más que en  $\rho_1$ , y la divergencia de Kullback-Leibler de este modo representa el número esperado de bits extras que deben ser transmitidos para identificar un valor  $x$  de  $X$ , si se usa un código correspondiente a la distribución de probabilidad  $\rho_2$ , más que la distribución verdadera  $\rho_1$ .



**Figura 11.** Divergencia de Kullback-Leibler para el Mapeo Logístico cuando el valor del parámetro es  $\mu = 3.75$ . (a) Divergencia de Kullback-Leibler entre la distribución de la iteración  $n-1$ ,  $\rho_{n-1}$ , y la distribución de la iteración  $n-2$ ,  $\rho_{n-2}$ . (b) Divergencia de Kullback-Leibler entre la distribución de la iteración  $n-2$ ,  $\rho_{n-2}$ , y la distribución de la iteración  $n-1$ ,  $\rho_{n-1}$ .

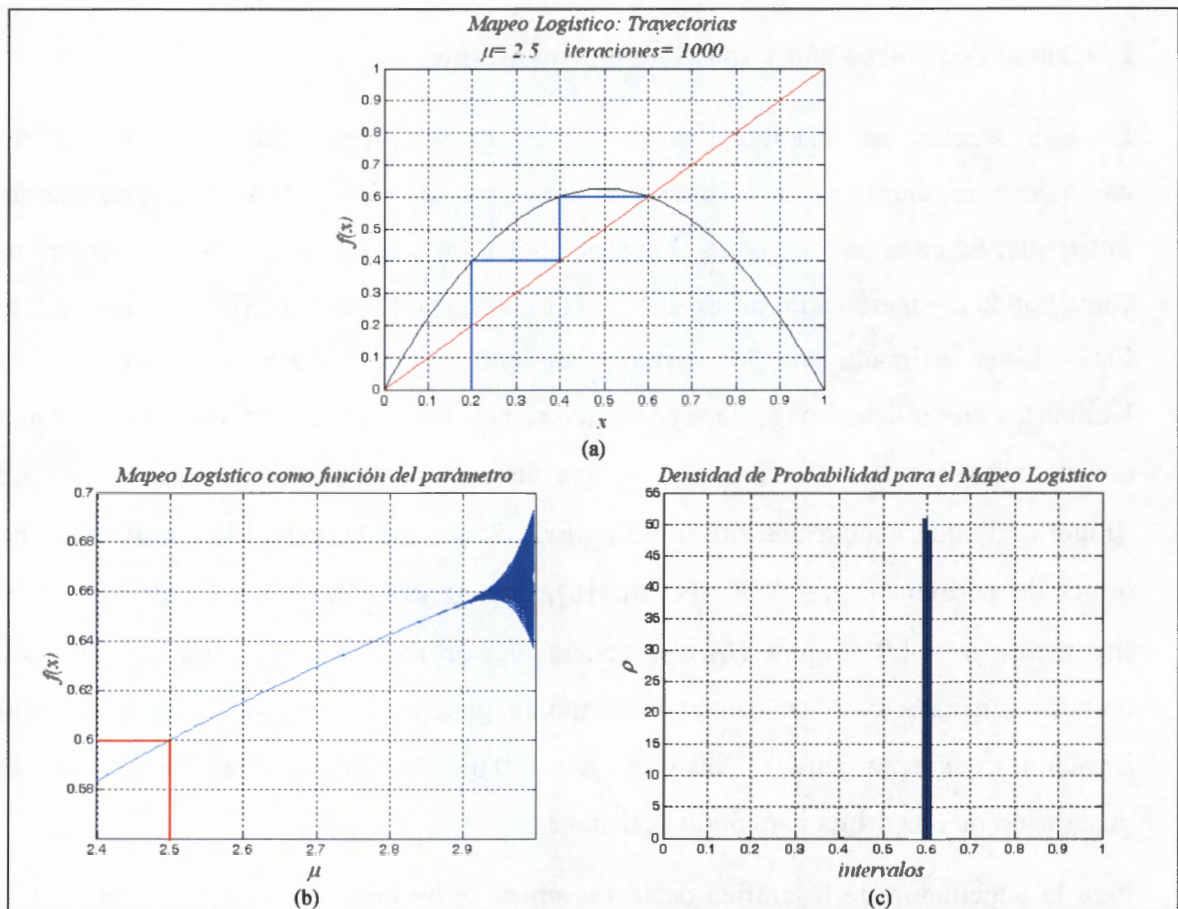


### Diagrama de Bifurcación y Distribución Invariante

En esta sección se relacionan entre sí tres gráficas para diferentes valores del parámetro: el diagrama de órbitas, el diagrama de bifurcación y la distribución invariante. En cada caso la figura a) corresponde a los diagramas de órbitas, la figura b) corresponde al diagrama de bifurcación y la c) corresponde a la distribución invariante. Esta última estimada con los criterios de convergencia fuerte y divergencia de Kullback-Leibler descritos en la sección anterior. Los valores del parámetro que se han considerado son:  $\mu = 2.5$  (Figura 12), que genera una órbita de periodo 1;  $\mu = 3.2$  (Figura 13) que genera una órbita de periodo 2;  $\mu = 3.5$  (Figura 14) que genera una órbita de periodo 4;  $\mu = 3.56$  (Figura 15), que genera una órbita de periodo 8; y finalmente  $\mu = 4.0$  (Figura 16) que genera una órbita que abarca todo el intervalo unitario. En cada caso se han considerado la generación de una órbita para 1000 iteraciones, excepto para el caso de  $\mu = 4.0$  que se ha considerado además, la generación de una órbita para 5000 iteraciones.

Para la generación de la gráfica de histogramas se ha utilizado una partición de 100 intervalos, excepto para el caso en que  $\mu = 4.0$  en que se ha usado una partición de 1000 intervalos para poder apreciar el comportamiento correcto de la distribución.

Para determinar la función de densidad de probabilidad para el *mapeo*, se ha usado un conjunto de condiciones iniciales con una distribución inicial específica y encontrando la frecuencia de visitas de la órbita a una región dada. De esta manera, se obtiene un histograma que corresponde al encontrado al considerar un ensamble de condiciones iniciales con el mismo valor del parámetro.



**Figura 12.** Gráficas del Mapeo Logístico para  $\mu = 2.5$ : (a) Diagrama de Trayectorias, (b) Diagrama de bifurcación y (c) Densidad de Probabilidad.

Así, la Figura 12 se obtiene cuando  $\mu = 2.5$ , y el histograma tiene una función delta de Dirac, la cual está alrededor de 0.6. En la Figura 13, para  $\mu = 3.2$ , el histograma muestra dos deltas de Dirac, una alrededor de 0.52 y la otra alrededor de 0.8. En la Figura 14, para  $\mu = 3.5$  el histograma muestra cuatro deltas de Dirac, colocadas en 0.38, 0.5, 0.83 y 0.88 respectivamente. En la Figura 15 para  $\mu = 3.56$  se presentan 8 deltas de Dirac, lo que habla de un fenómeno conocido como Doblamiento del Periodo.

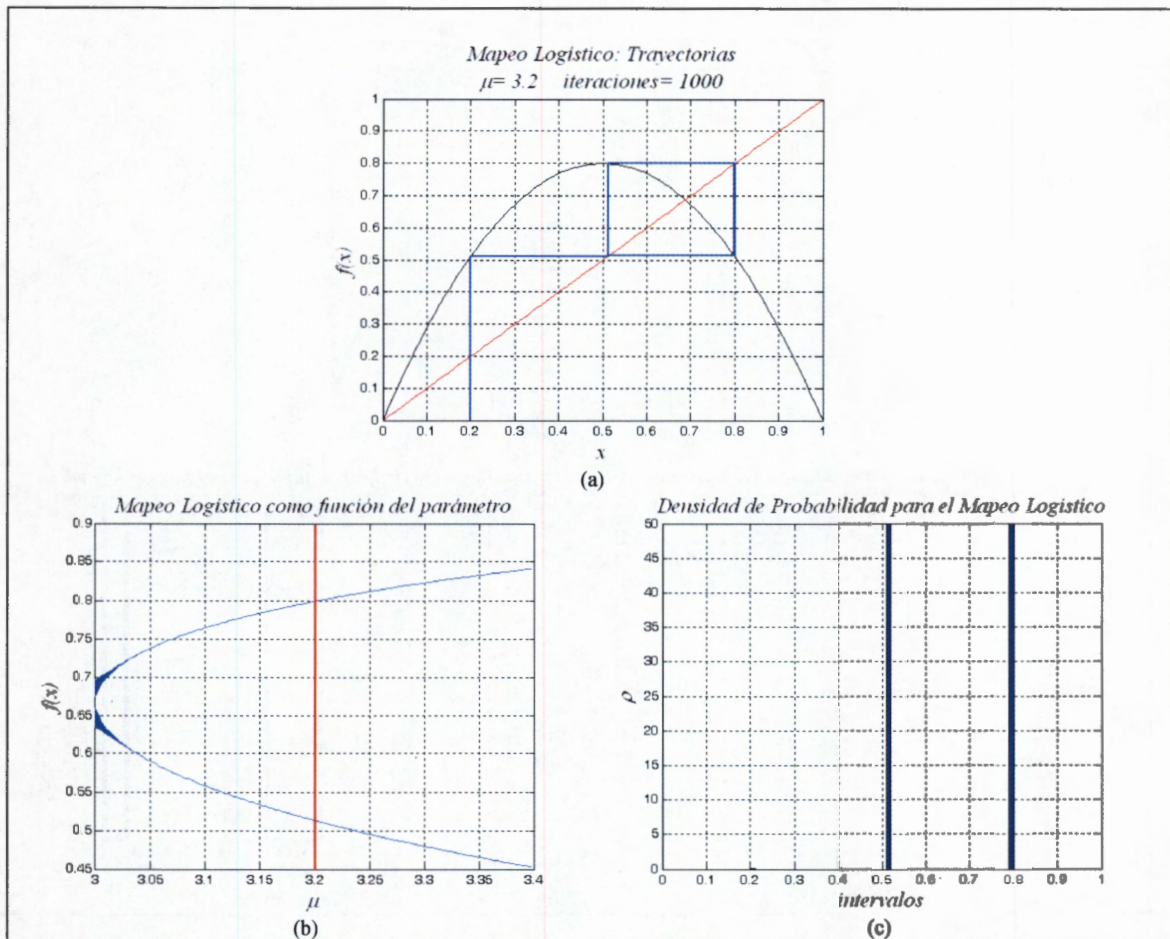
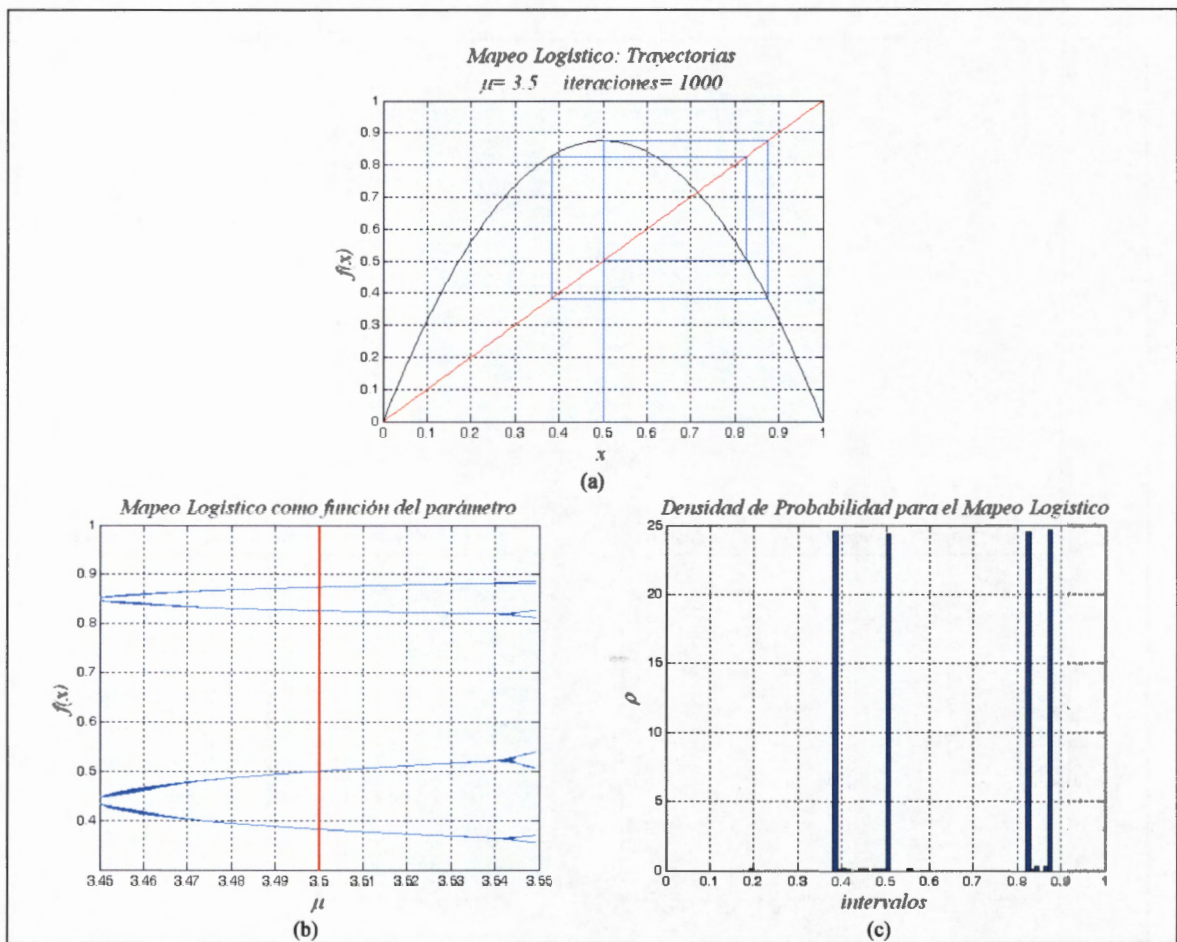
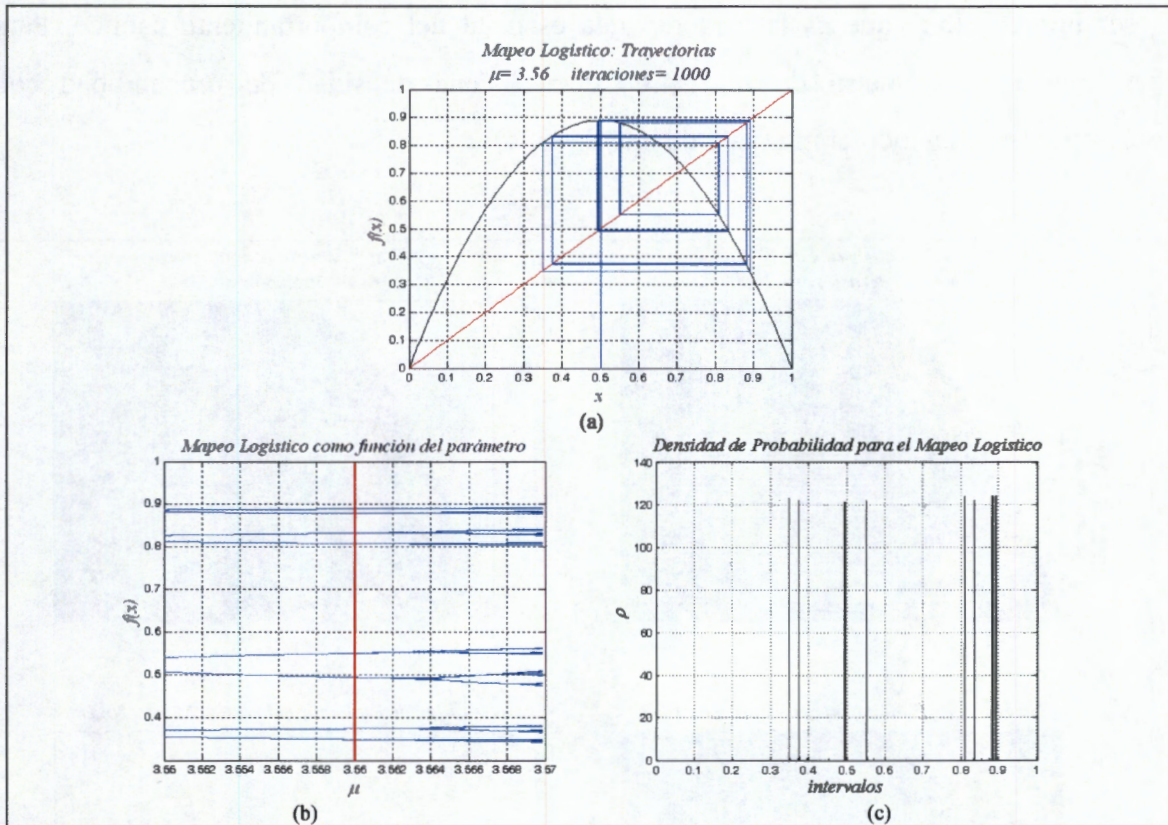


Figura 13. Gráficas del Mapeo Logístico para  $\mu = 3.2$ : (a) Diagrama de Trayectorias, (b) Diagrama de bifurcación y (c) Densidad de Probabilidad.



**Figura 14.** Gráficas del Mapeo Logístico para  $\mu = 3.5$ : (a) Diagrama de Trayectorias, (b) Diagrama de bifurcación y (c) Densidad de Probabilidad.

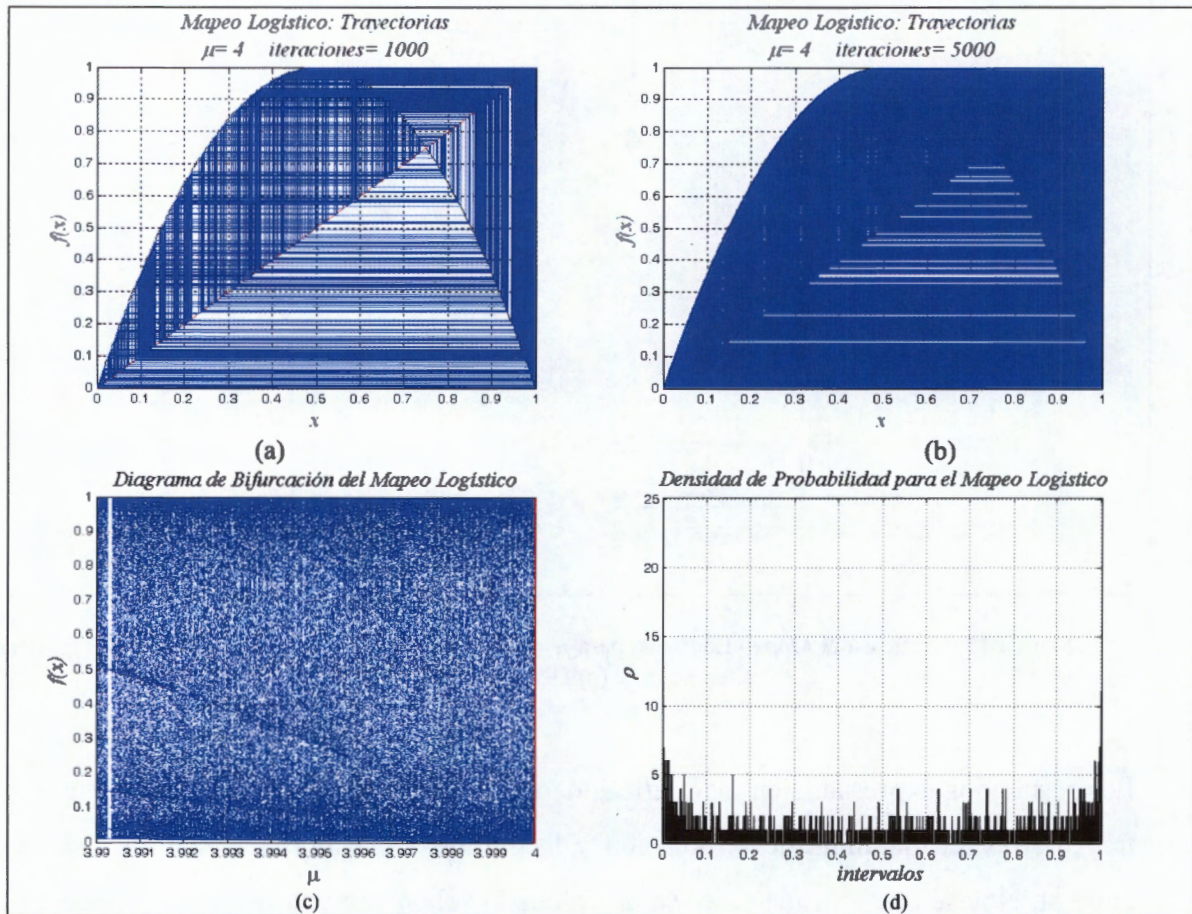


**Figura 15.** Gráficas del *Mapeo Logístico* para  $\mu = 3.56$ : (a) Diagrama de Trayectorias, (b) Diagrama de bifurcación y (c) Densidad de Probabilidad.

Los resultados expresados en las gráficas de las figuras anteriores para el diagrama de trayectorias, el diagrama de bifurcación y la gráfica de histogramas son consistentes entre sí. Nótese que en cada caso, se ha colocado solamente una porción del diagrama de bifurcación y la forma del histograma en cada caso coincide con la densidad de puntos para el valor del parámetro usado.

En la Figura 16 se puede ver que para  $\mu = 4.0$  las regiones de confinamiento se han ensanchado a tal punto que el comportamiento caótico de la órbita abarca todo el intervalo unitario. De esta manera, el comportamiento de la órbita a largo plazo resulta

ser impredecible, que es la característica esencial del comportamiento caótico. Para valores del parámetro de  $\mu = 4.0$  se tiene una densidad de probabilidad con componentes en todo el intervalo de interés (0, 4).



**Figura 16.** Gráficas del *Mapeo* Logístico para  $\mu=4.0$ : (a) Diagrama de Trayectorias para 1000 iteraciones, (b) Diagrama de Trayectorias para 5000 iteraciones, (c) Diagrama de bifurcación y (d) Densidad de Probabilidad.

Los histogramas que describen la función de densidad de probabilidad para este *mapeo* se han calculado aprovechando la propiedad de que el *Mapeo* Logístico es Ergódico, lo que significa que el comportamiento a largo plazo de una sola órbita, que se obtiene al

dar una condición inicial e iterar el *mapeo* un número grande de veces es igual al comportamiento estadístico de un ensemble de condiciones iniciales.

## 2.3 Del orden al caos y del caos al orden

El orden y el caos han sido dos conceptos que se han considerado como antagónicos en diversos campos de las ciencias. De acuerdo con la definición del diccionario Oxford tiene varias páginas relacionadas con la definición de orden y se incluyen términos como “secuencia, arreglo, disposición o condición regular; una división, grado o estrato; arreglo regular, metódico o armonioso; existencia de una regla, ausencia de turbulencia, etc.”<sup>33</sup>. Por otro lado, aunque el término “caos” se ha atribuido a J. Yorke en los años 1960s [70], existen dos trabajos de Norbert Wiener en 1938 [71] y 1943 [72], en los cuales se acuñaron las palabras y frases como “caos homogéneo”, “caos unidimensional”, “caos multidimensional”, “caos puro”, “caos discreto”, “caos polinomial”, etc. y propuso su teoría caos de procesos estocásticos, modelando un nuevo paradigma contrario a de la mecánica determinista de Newton. Sin embargo, el primer descubridor del caos ha sido considerado Jacques Hadamard, quien en 1898 publicó un estudio del movimiento caótico de una partícula libre que se desliza libre de fricción en una superficie de curvatura constante [73] [74]. El término de caos en el diccionario es menos abundante, ya que tiene 3 acepciones. Se refiere como desorden, confusión, primera condición del universo, inherente a la impredecibilidad en el comportamiento de un sistema, etc.<sup>34</sup>. Keller en 1993 define a la teoría del caos como “el estudio cualitativo de un comportamiento inestable en sistemas determinísticos no lineales” [75]. Fue en 1988 cuando Norman Packard definió que existe una línea muy delgada entre orden y caos [76], y de acuerdo con Waldrop en 1992 [77], Chris Langton

---

<sup>33</sup> El diccionario Encarta maneja 24 acepciones para “orden”; [http://encarta.msn.com/dictionary\\_1861697387/order.html](http://encarta.msn.com/dictionary_1861697387/order.html),

<sup>34</sup> El diccionario Encarta, maneja 3 acepciones para “caos”; [http://encarta.msn.com/dictionary\\_1861596245/chaos.html](http://encarta.msn.com/dictionary_1861596245/chaos.html).

de Instituto de Santa Fe<sup>35</sup>, propuso una ecuación interesante que relaciona al caos y al orden a través de la complejidad.

Caos y orden son dos conceptos que pueden relacionarse a través de la Teoría de Universalidad<sup>36</sup> de Feigenbaum [34]<sup>37</sup>, conocida comúnmente como la ruta del orden al caos. Existen tres rutas universales a través de las cuales un sistema llega a ser caótico [78]: Doblamiento el periodo [79], Intermitencia<sup>38</sup> [80] [81] y Cuasiperiodicidad [82]. Sin embargo, la mayoría de las veces la atención de la ruta al caos está en el doblamiento del periodo y es el que también se aprovecha en este trabajo.

Así, cuando se estudia el *Mapeo* Logístico se descubre que ambos estados de apariencia antagónicos pueden estar gobernados por una ley única, el propio *mapeo*, pero usando diferentes valores del parámetro que lo gobierna. En este *mapeo* existe una *ruta* bien definida que deja un estado *-orden-* y pasa a otro estado llamado *-caos-*. Esta ruta es universal y significa que hay un cambio cualitativo abrupto llamado bifurcaciones, que marca la transición gradual del orden al caos, que lleva de la predecibilidad a la impredecibilidad. Se dice que esta ruta es universal debido a que estas bifurcaciones pueden encontrarse cualitativa y cuantitativamente en muchos sistemas naturales.

A continuación se describe el fenómeno de *doblamiento del periodo en órbitas* como la ruta de orden al caos. Sin embargo, cabe mencionar que existe otro fenómeno de doblamiento, pero en distribuciones que permite observar como un sistema puede tener una ruta que va del estado de *-caos-* al estado de *-orden-*. Este fenómeno es muy pocas

---

<sup>35</sup> El Instituto Santa Fe fue fundado en Nuevo México, Estados Unidos en 1984. Es un instituto interdisciplinario que hace uso de economistas, físicos, administradores, biólogos y matemáticos, buscando encontrar orden en sistemas complejos.

<sup>36</sup> En mecánica estadística, la Universalidad se refiere a la existencia de propiedades de un gran número de sistemas, las cuales son independientes de los detalles dinámicos del sistema. El término de Universalidad fue popularizado por Leo Kadanoff al final de los años 1970s, pero el concepto fue conocido desde los años 1950s. Michel Feigenbaum descubrió la Universalidad en Mapeos Iterados en el año de 1976.

<sup>37</sup> En Abril de 1976 Feigenbaum completó un artículo de investigación en este tópico. El lo sometió a arbitraje a un Journal para su evaluación y después de seis meses fue rechazado. Pero después de enviarle una copia a cerca de 1000 científico su trabajo se publicó en 1978.

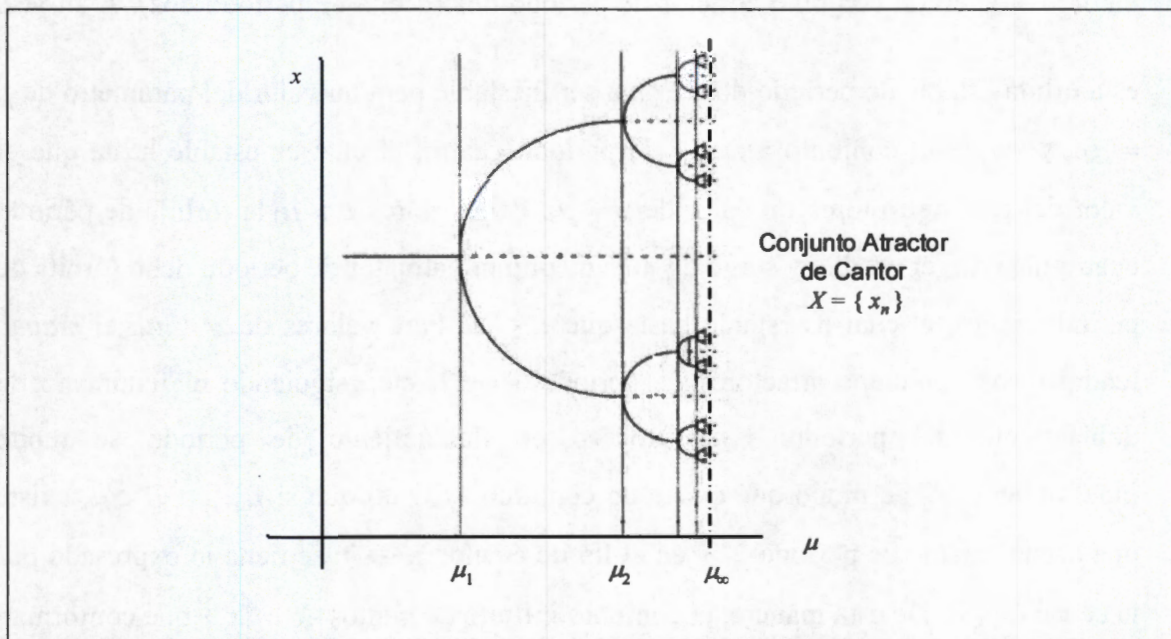
<sup>38</sup> La intermitencia se refiere a la alternancia de una dinámica regular u ordenada a una dinámica caótica.



veces considerado, aquí se ha llamado *doblamiento del periodo en distribuciones*, y se considera la imagen caótica del fenómeno del doblamiento del periodo en órbitas.

### Doblamiento del periodo en órbitas

El *Mapeo* Logístico exhibe el fenómeno de doblamiento de periodo [83], el cual es una condición importante que se debe analizar, ya que para algunas aplicaciones puede ser útil. Este fenómeno puede verse directamente en el diagrama de bifurcación presentado en la Figura 7.



**Figura 17.** Idea intuitiva del proceso de bifurcación y cambio de la condición de los conjuntos atractores estables a conjuntos inestables

Como se vio en la sección 2.1, el diagrama de bifurcación indica que al iterar este *mapeo* es posible generar secuencias de periodo 1, 2, 4, 8, 16, etc. seleccionando el valor apropiado del parámetro que gobierna el *mapeo*. Estas órbitas se generan a través del fenómeno de doblamiento de periodo de las órbitas, de manera que las secuencias periódicas aparecen en el siguiente orden al aumentar el valor del parámetro del *mapeo*:

$1 \rightarrow 2 \rightarrow 4 \rightarrow 8 \rightarrow 16 \rightarrow 32 \rightarrow \dots$ . En cada transición ocurre un cambio en la condición de la secuencia periódica, ya de ser un conjunto atractor estable pasa a ser un conjunto inestable. Esto se ilustra cualitativamente en la Figura 17 usando para ello líneas punteadas para indicar que un conjunto atractor estable de puntos ha cambiado a un conjunto inestable.

Como puede verse en la Figura 18, el fenómeno de doblamiento del periodo inicia con un valor del parámetro  $\mu = 3.0$ , ya que hay una bifurcación de un punto fijo atractor de valor  $\frac{\mu-1}{\mu}$ , en un conjunto atractor de periodo dos (órbita de periodo dos). A su vez, esta órbita estable de periodo dos llega a ser inestable para un valor del parámetro de  $\mu = \mu_2$ , y surge un conjunto atractor de periodo cuatro, el cual es estable hasta que el valor del parámetro toma un valor de  $\mu = \mu_3$ . Para valores  $\mu > \mu_3$  la órbita de periodo cuatro deja de ser estable y surge un nuevo conjunto atractor de periodo ocho (órbita de periodo ocho), el cual es estable hasta que  $\mu = \mu_4$ . Para valores de  $\mu > \mu_4$ , el mapeo tendrá otros conjuntos atractores de periodo 16, 32, etc., siguiendo el fenómeno de doblamiento del periodo. Este proceso de doblamiento de periodo se repite indefinidamente, de modo que existe un conjunto  $\{\mu_n\}$  tal que si  $\mu_{n+1} > \mu \geq \mu_n$  existe una órbita estable de periodo  $2^n$  y en el límite cuando  $n \rightarrow \infty$  se tiene lo expresado por la ecuación (3). De esta manera, el conjunto infinito de puntos  $X = \{x_n\}$  que conforman la órbita estable de periodo  $2^n$  ( $n \rightarrow \infty$ ) conforme  $\mu \rightarrow \mu_\infty$  es de mucho interés, ya que constituye un conjunto atractor de los puntos en el intervalo  $(0, 1)$  y por supuesto no atrae (no contiene) a los puntos periódicos inestables que murieron en el proceso de doblamiento del periodo. De esta manera,  $X$  no es continuo y constituye un conjunto de Cantor [56], el cual posee una distribución estadística sobre objetos fractales. La Tabla 1 muestra los valores de  $\mu$  para los cuales ocurre el doblamiento del periodo en el

Mapeo logístico, siendo  $\mu_\infty = 3.569946$  y se considera la entrada del mapeo al caos. En ese punto se reconoce el final del fenómeno de doblamiento del periodo.

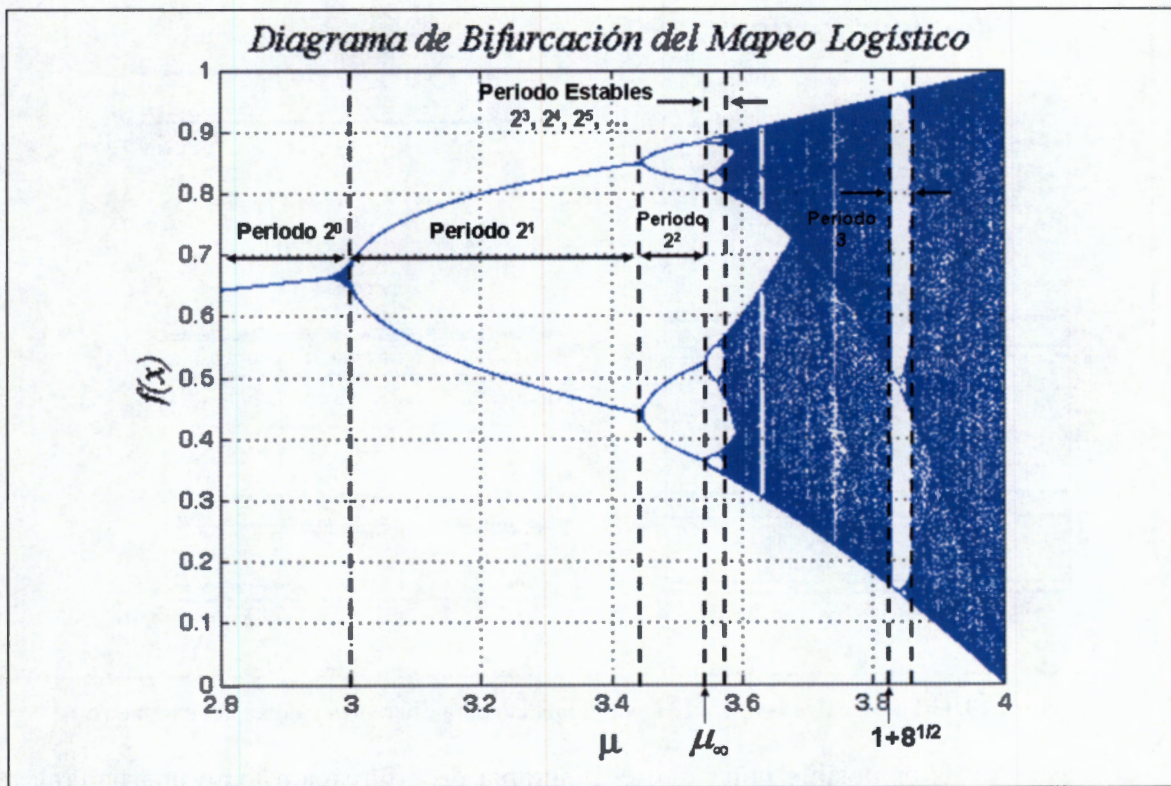


Figura 18. Diagrama de Bifurcación del Mapeo Logístico para  $\mu \in (2.8, 4.0)$

En resumen, y apoyándonos en la definición de puntos y órbitas fijos dados en el Anexo B, en la Figura 18 se pueden identificar regiones específicas en función de los puntos fijos estables que aparecen. Así, cuando  $\mu \in (1, 3)$  existe un punto fijo atractor, cuando  $\mu \in (\mu_1, \mu_2)$  existen una órbita periódica de periodo dos, cuando  $\mu \in (\mu_2, \mu_3)$  existe una órbita periódica de periodo cuatro, cuando  $\mu \in (\mu_3, \mu_4)$  existe una órbita periódica de periodo ocho, cuando  $\mu \in (\mu_4, \mu_5)$  existe una órbita de periodo dieciséis, etc. Este comportamiento se puede cotejar en las gráficas de la Figura 19.

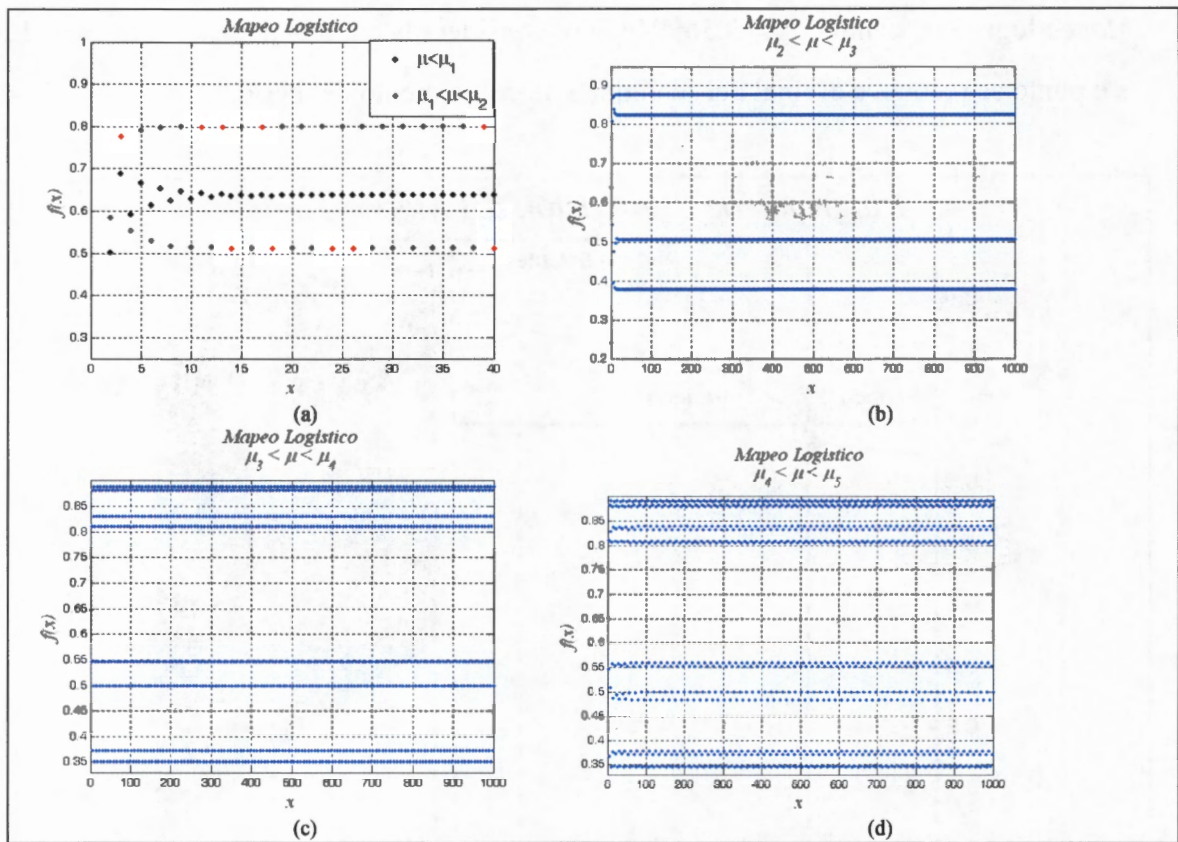
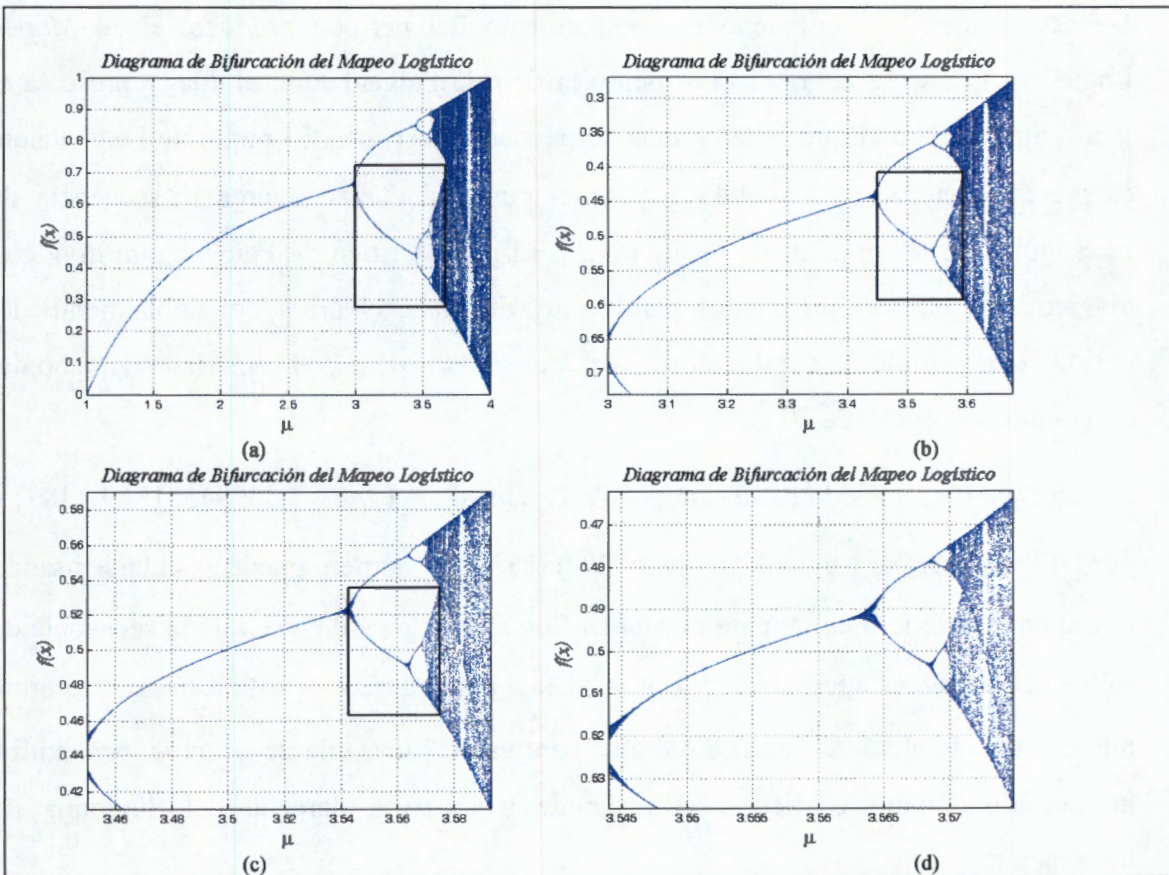


Figura 19. Órbitas generadas por el Mapeo Logístico para diferentes valores del parámetro  $\mu$ .

Con estas ideas es posible notar que el diagrama de bifurcación tiene una naturaleza cualitativa y otra cuantitativa. La condición cualitativa se muestra de las propiedades de autosimilaridad que tiene el mapeo, las cuales indican la ruta del orden al caos. Las figuras siguientes muestran este comportamiento autosimilar. Nótese que se ha realizado una ampliación de la sección que se indica con rectángulo en negro y en las gráficas b y d de la Figura 20 se ha graficado en orden inverso el eje vertical.



**Figura 20.** Acercamientos en el diagrama de bifurcación para apreciar el comportamiento autosimilar

De la misma manera que en el diagrama de bifurcación original (completo), nótese en cada una de las gráficas de la Figura 20 que existe un orden si se recorre la gráfica de izquierda a derecha, conforme se incrementa el valor del parámetro, ya que se van generando ramas de bifurcación a través del fenómeno del doblamiento del periodo en cascada. Esta es la condición cuantitativa del diagrama de bifurcación del *mapeo*. Con la ampliación hecha en la presentación sucesiva de las gráficas de la Figura 20 se puede evidenciar que las longitudes de las ramas de bifurcación van decreciendo después de cada punto de bifurcación. Este comportamiento existe hasta que la longitud de las ramas de bifurcación es prácticamente cero.

De esta manera, el fenómeno del doblamiento del periodo produce, en el *Mapeo* Logístico, lo que se conoce como punto crítico de Feigenbaum, el cual representa el punto umbral para el que estas ramas no pueden crecer más. El punto de Feigenbaum es precisamente  $\mu_{\infty} = 3.5699456\dots$  y es el punto al cual converge la secuencia de rectángulos de las gráficas de la Figura 20. El punto crítico de Feigenbaum divide el diagrama de bifurcación en dos partes muy distintas, el árbol del doblamiento del periodo (lado izquierdo del diagrama) y el área gobernada por el caos (lado derecho del diagrama), véase Figura 20.a.

El valor para  $\mu_{\infty}$  ha sido precisado por A. K. Dewdney ( $\mu_{\infty}^D = 3.56994571869$ ) [87] y por D. R. Hofstadter ( $\mu_{\infty}^H = 3.5699456720$ ) [88]. Este número puede calcularse usando el Exponente de Lyapunov para el *Mapeo* Logístico y puede verse que la secuencia de salida del *mapeo* es aperiódica si  $\mu \geq \mu_{\infty}$ . En el apartado 2.4 de esta tesis se determina numéricamente el valor para  $\mu_{\infty}$ . Así que, para valores más allá de  $\mu_{\infty}$  el *mapeo* exhibe un comportamiento caótico y corresponde a la parte derecha del diagrama de bifurcación.

Existe una regla que cuantifica, a partir de una la primera constante de Feigenbaum, la manera en que el doblamiento del periodo se aproxima al punto crítico de Feigenbaum, considerando que las longitudes de las ramas de bifurcación van decreciendo después de cada punto de bifurcación. Para ello, considérese la razón que existe entre la longitud de dos ramas de bifurcación consecutivas. Esta razón debe ser aproximadamente la primera constante de Feigenbaum  $\delta = 4.6692\dots$  [84-85], sin importar que ramas consecutivas se consideren. La relevancia de  $\delta$  como una constante del caos, es en el mismo sentido de números como  $\pi$ . La constante  $\delta$  aparece en muchos diferentes sistemas (por ejemplo, la oscilación del helio líquido y el comportamiento de las poblaciones nómadas de polilla) y se conoce como *universalidad*, también

mencionada en la sección 2.1 de este capítulo. Sin embargo, una interpretación posible y muy útil de la *universalidad* de  $\delta$  podría ser usarla para predicciones. Por ejemplo, midiendo dos bifurcaciones sucesivas se pueden predecir las bifurcaciones siguientes y también predecir donde estaría el umbral. El trabajo de Feigenbaum, en los años inmediatos posteriores, tuvo gran relevancia, ya que el significado de la *universalidad* no solamente cubría modelos matemáticos elementales, sino que también cubría lo relacionado a fenómenos físicos verdaderos. La Figura 21 muestra la manera en que se determina el valor de  $\delta$  usando el diagrama de bifurcaciones.

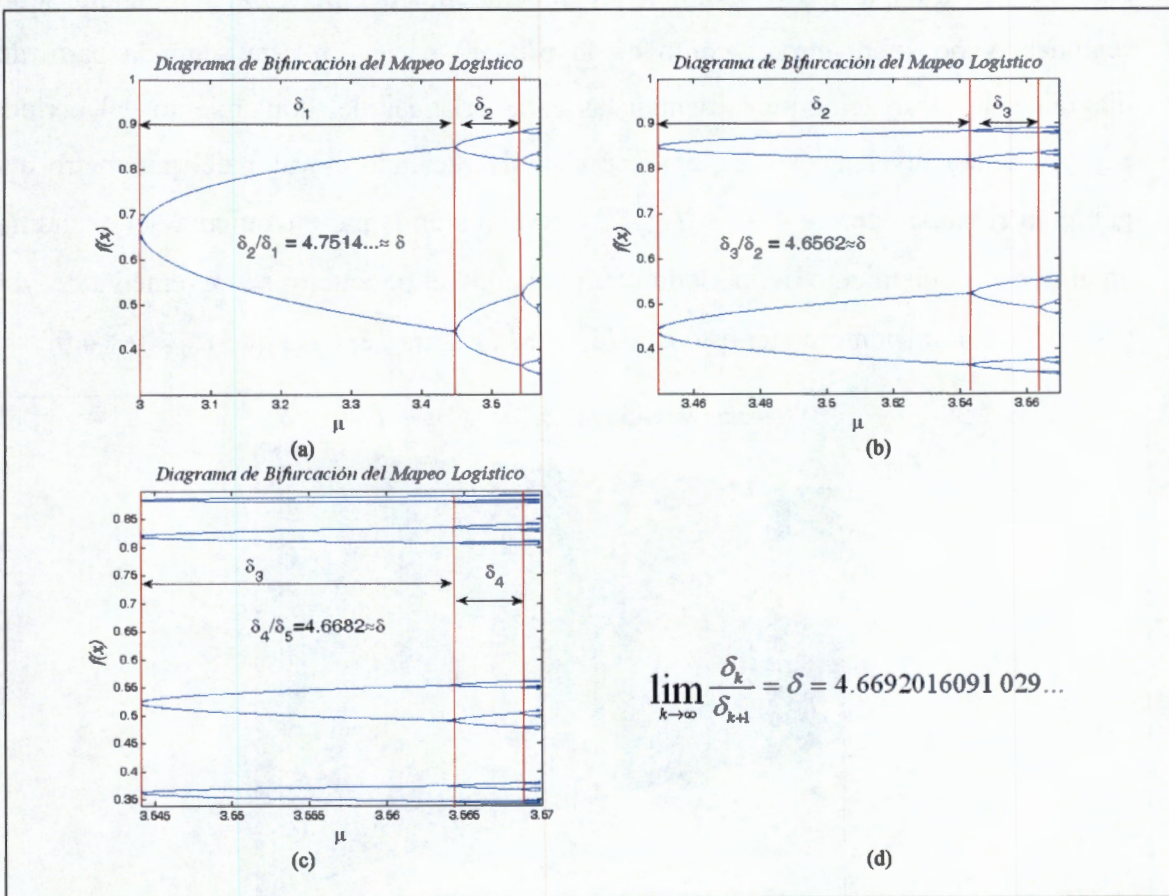


Figura 21. Interpretación de la constante de Feigenbaum

### Doblamiento del periodo en distribuciones

Tradicionalmente se dice que el doblamiento del periodo en el *Mapeo* Logístico ocurre desde  $\mu = 0$  hasta  $\mu_{\infty}$ , y es un fenómeno en cascada que termina cuando  $\mu = \mu_{\infty}$  [45]. Esto es, cuando el *mapeo* entra al caos [86]. Sin embargo, en este apartado se muestra que hay otro fenómeno del doblamiento del periodo que ocurre desde  $\mu = 4$  hasta  $\mu_{\infty}$ , y también es un fenómeno en cascada que termina cuando el *mapeo* sale del caos.

Para observar esto, se debe analizar la segunda parte del diagrama de bifurcación, en el cual se muestra que existe también un doblamiento del periodo, pero ahora sobre regiones, y no sobre curvas como en la primera parte. En esta segunda parte del diagrama de bifurcación se presentan las características del doblamiento del periodo pero en orden inverso; esto es, aparece al ir decreciendo el valor del parámetro que gobierna el *mapeo* de  $\mu = 4.0 \rightarrow \mu = \mu_{\infty}$ , y no como en la parte izquierda del diagrama, en el que el doblamiento del periodo ocurre cuando el parámetro se incrementa de  $\mu = 0 \rightarrow \mu = \mu_{\infty}$ . Para comprender esto considérese la Figura 22, en la que  $\mu_{\infty} < \mu < 4.0$ .

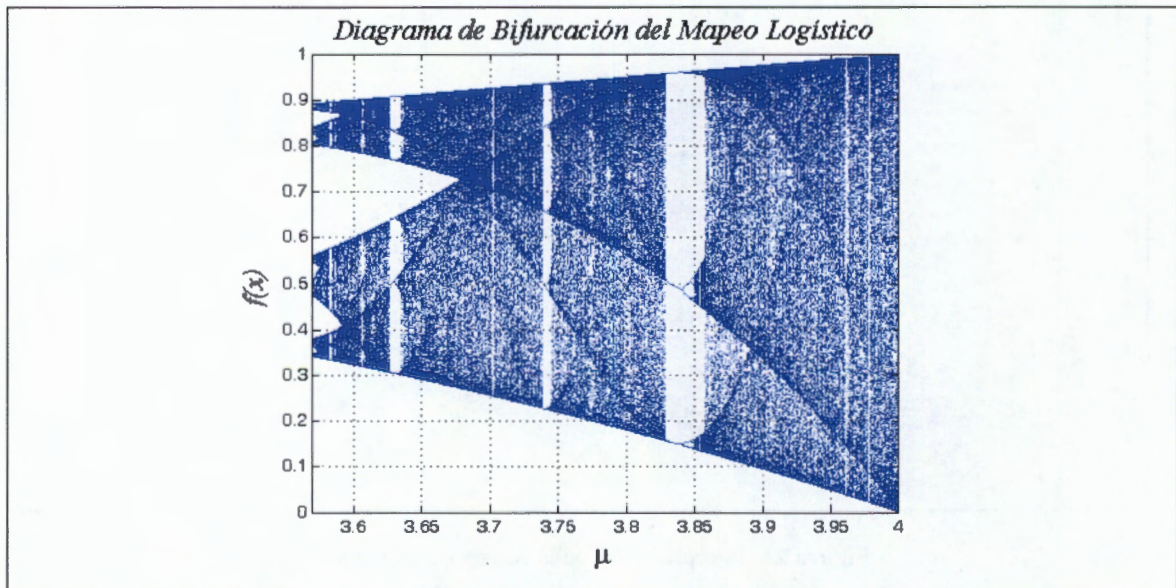


Figura 22. Diagramas de Bifurcación para el *Mapeo* Logístico de  $\mu = \mu_{\infty}$  a  $\mu = 4.0$ .



Lo primero que se debe reconocer es que para el *Mapeo* Logístico existen ciertos intervalos para  $\mu$  en los que aparece un comportamiento no caótico; esto es, el caos se interrumpe por ventanas de orden, en las que el comportamiento se colapsa a unos cuantos puntos que dan lugar a órbitas periódicas. A estas ventanas de orden también se les conoce como islas de estabilidad. Estas islas de estabilidad se han identificado en las gráficas de la Figura 23 y en ellas es posible encontrar secuencias las secuencias de Sharkovskii descritas en el apartado “Diagrama de Bifurcación” de la Sección 2.1 de esta tesis. En estas islas de estabilidad ocurren nuevamente órbitas periódicas y a este fenómeno se le llama intermitencia [89][90][91]. Es posible encontrar este fenómeno en otros *mapeos* caóticos y no únicamente en el *Mapeo* Logístico [92].

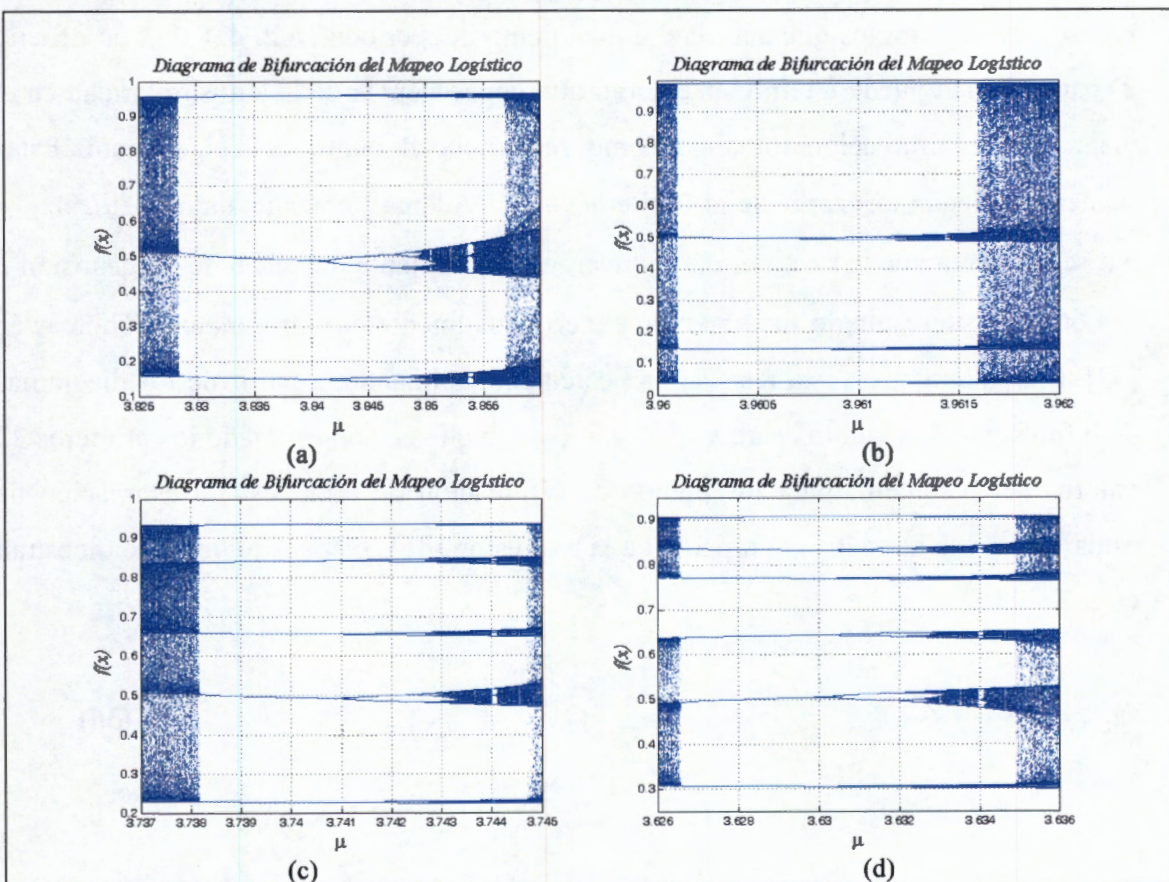


Figura 23. Diagrama de Bifurcación en la isla de estabilidad para  $R = 3, 4, 5$  y  $6$ .

Otro aspecto que se debe analizar es que parece existir una estructura en las bandas de caos que existen entre las islas de estabilidad. La estructura de esas bandas parece no tener una distribución uniforme de sus puntos. Los puntos parecen condensarse a ciertas líneas que encapsulan la dinámica caótica del *mapeo*. Solamente para  $\mu = 4.0$  hay una banda que se extiende a todo el intervalo unitario. Conforme  $\mu$  decrece, esta banda se hace más angosta, hasta el punto etiquetado como  $m_1$  la región se divide en dos, luego en  $m_2$  estas dos regiones se dividen en cuatro, en  $m_3$  se dividen en ocho y en  $m_4$  se divide en dieciséis. Las gráficas de la Figura 24 muestran este fenómeno de doblamiento de periodo de las regiones del diagrama de bifurcación en donde existe caos. De la misma manera que antes, existe un número infinito de valores del parámetro  $m_1, m_2, m_3, \dots$  para los que ocurre el doblamiento del periodo en 2, 4, 8, ..., en general  $2^k$  bandas. Esto puede interpretarse como otra consecuencia de la autosimilaridad en el diagrama de bifurcación tomando como referencia el punto de Feigenbaum. Estas secuencias llegan exactamente al límite  $m_\infty = \mu_\infty$ . Además, considerando que  $d_k = m_{k+1} - m_k$ , se confirma que la razón  $d_k/d_{k+1}$  converge a la constante universal de Feigenbaum  $\delta = 4.669\dots$  Este resultado fue obtenido experimentalmente por Großmann y Thomas en [33]. Sin embargo, en esta tesis se han calculado estimando, a partir de los diagramas de bifurcación, los valores para  $m_1, m_2$  y  $m_3$ , y con ello se han estimado los primeros 22 valores del parámetro para los puntos de bifurcación de regiones. La estimación de estos valores se ha realizado a partir de la expresión (36). Estos resultados se muestran en la Tabla 2.

$$m_{k+2} = \frac{m_{k+1} - m_k}{\delta} + m_{k+1} \quad (36)$$

$\delta = 4.669201609102900$			
$i$	$m_i$	$i$	$m_i$
1	3.678500000000000	12	3.570230574584320
2	3.592500000000000	13	3.570230571031190
3	3.575000000000000	14	3.570230570270220
4	3.571252035901410	15	3.570230570107240
5	3.570449336765160	16	3.570230570072330
6	3.570277423191180	17	3.570230570064860
7	3.570240604568140	18	3.570230570063260
8	3.570232719146570	19	3.570230570062910
9	3.570231030330750	20	3.570230570062840
10	3.570230668638120	21	3.570230570062830
11	3.570230591174630	22	3.570230570062820

Tabla 2. Valores del parámetro en los que ocurre la bifurcación de regiones.

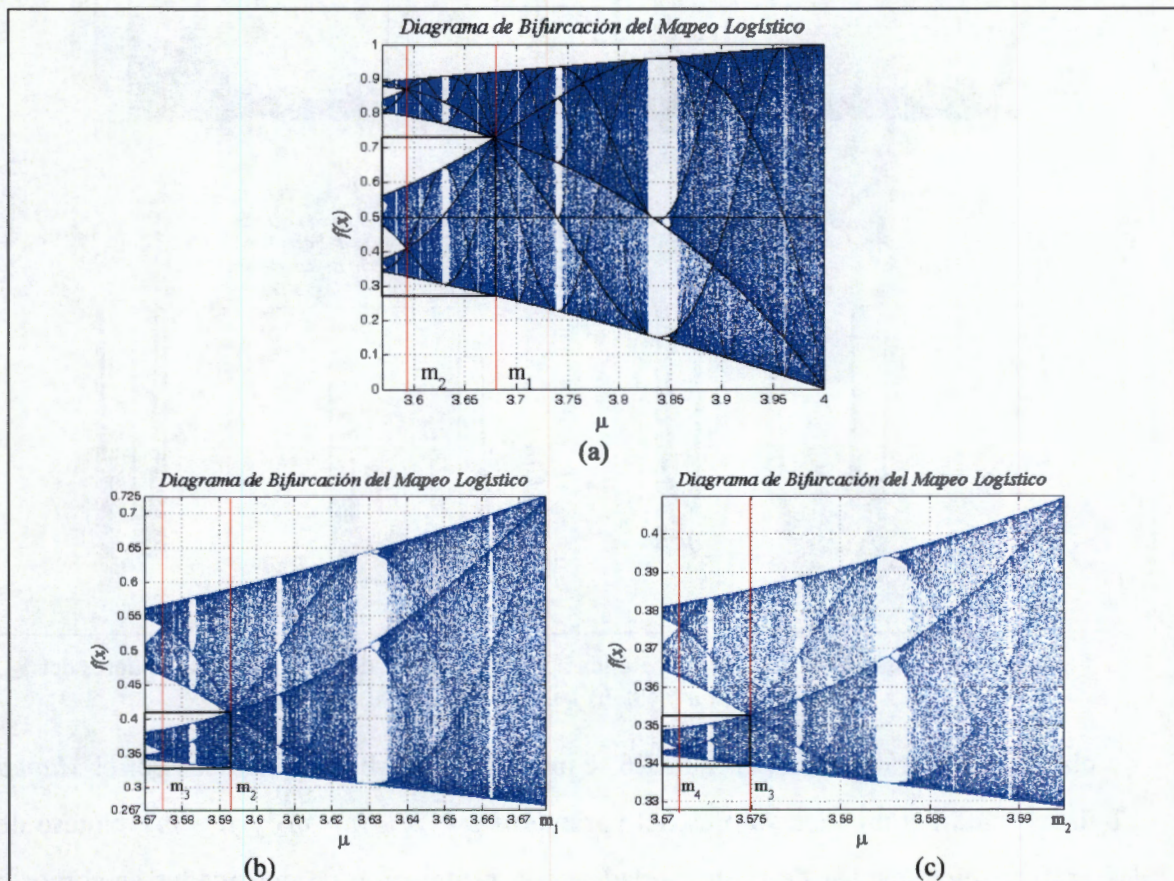


Figura 24. Diagramas de Bifurcación para el Mapeo Logístico de  $\mu = \mu_\infty$  a  $\mu = 4.0$ .

Este mismo comportamiento se puede notar de las gráficas de densidad de probabilidad generadas a partir de una distribución inicial de condiciones iniciales para el *mapeo* y usando los respectivos valores del parámetro que gobierna su comportamiento.

A continuación, en las gráficas de la Figura 25 se muestra la densidad de probabilidad de la órbita para valores del parámetro  $\mu = m_1$ ,  $\mu = m_2$  y  $\mu = m_3$ .

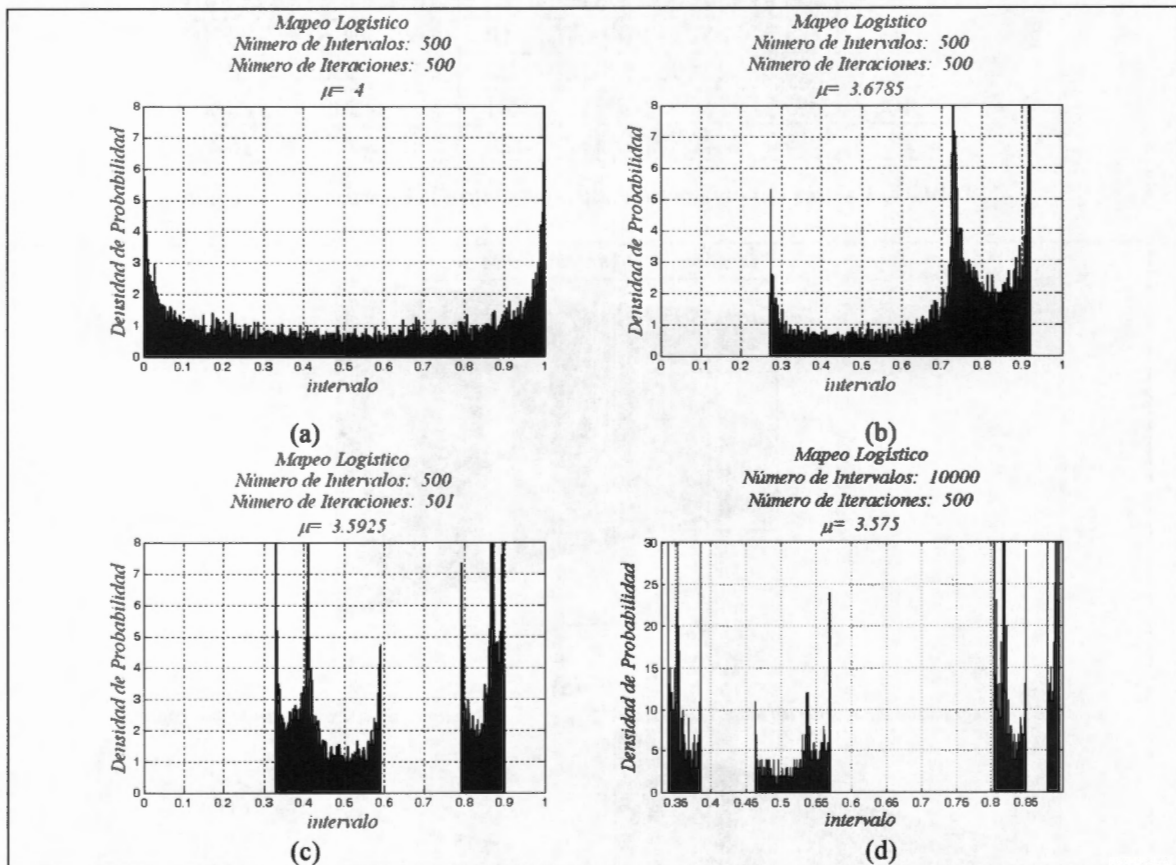
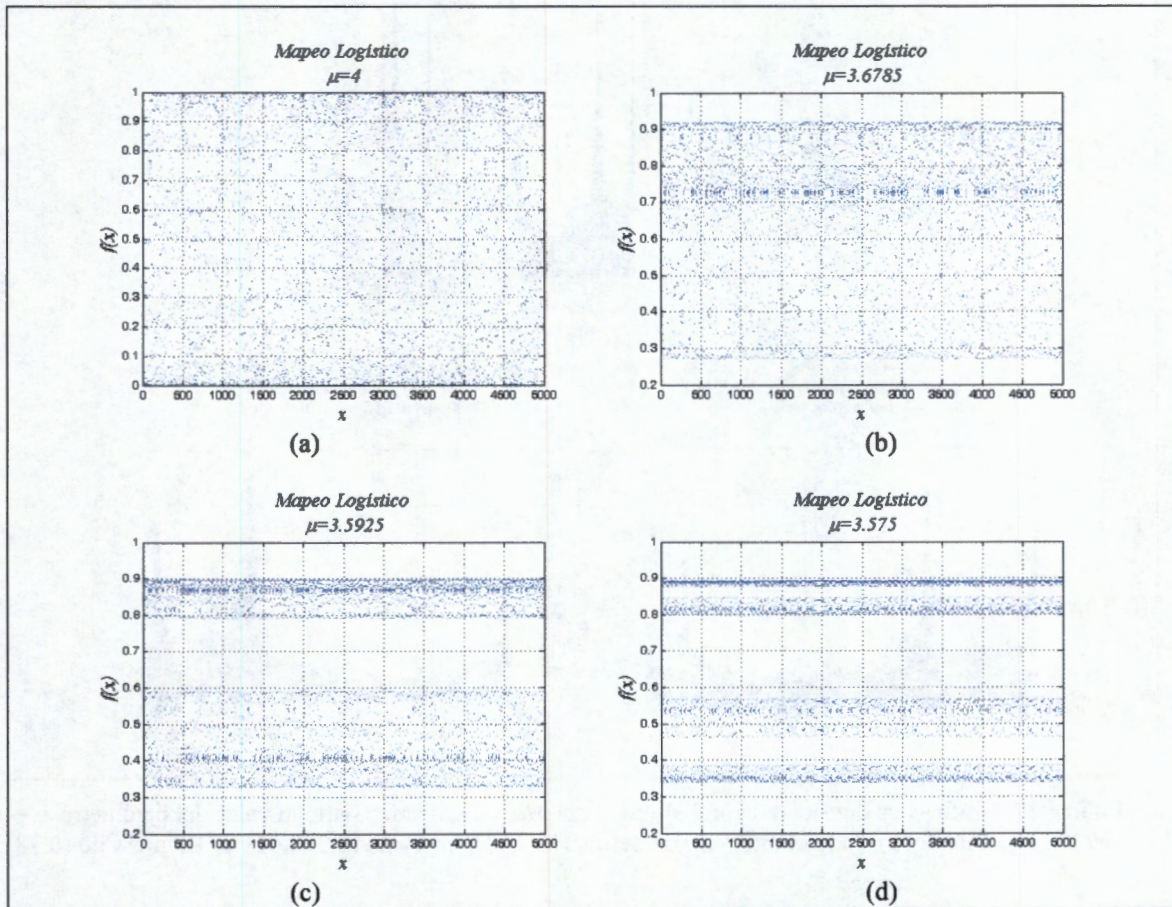


Figura 25. Gráficas de densidad de probabilidad del *Mapeo* Logístico para diferentes valores del parámetro. a)  $\mu = 4.0$  b)  $\mu = m_1$ . c)  $\mu = m_2$ . b)  $\mu = m_3$

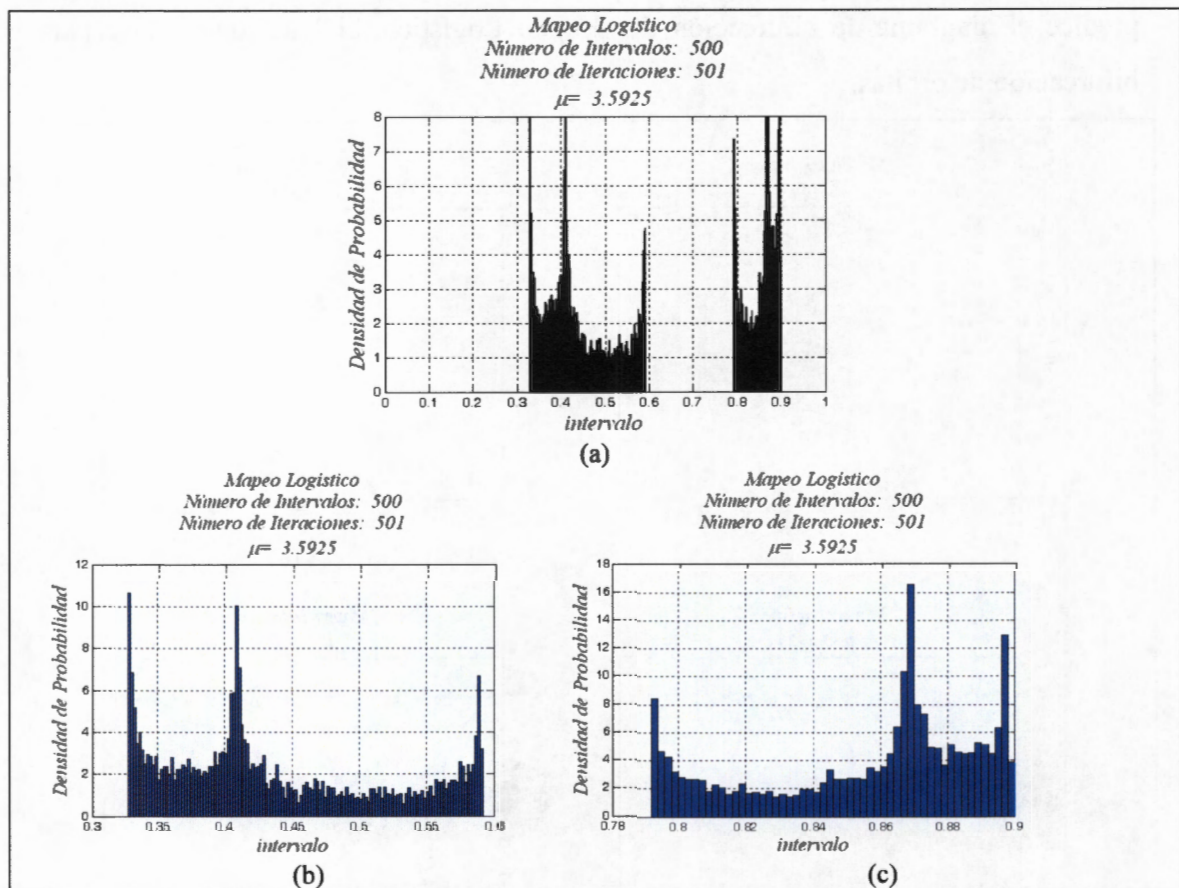
También, en las gráficas de la Figura 26 se muestran las órbitas generadas por el *Mapeo* Logístico para los mismos valores del parámetro  $\mu = m_1$ ,  $\mu = m_2$  y  $\mu = m_3$ . Nótese de las gráficas de densidad de probabilidad que la bifurcación de densidades es como lo

predice el diagrama de bifurcación del *Mapeo Logístico*, al igual que ocurre para la bifurcación de órbitas.

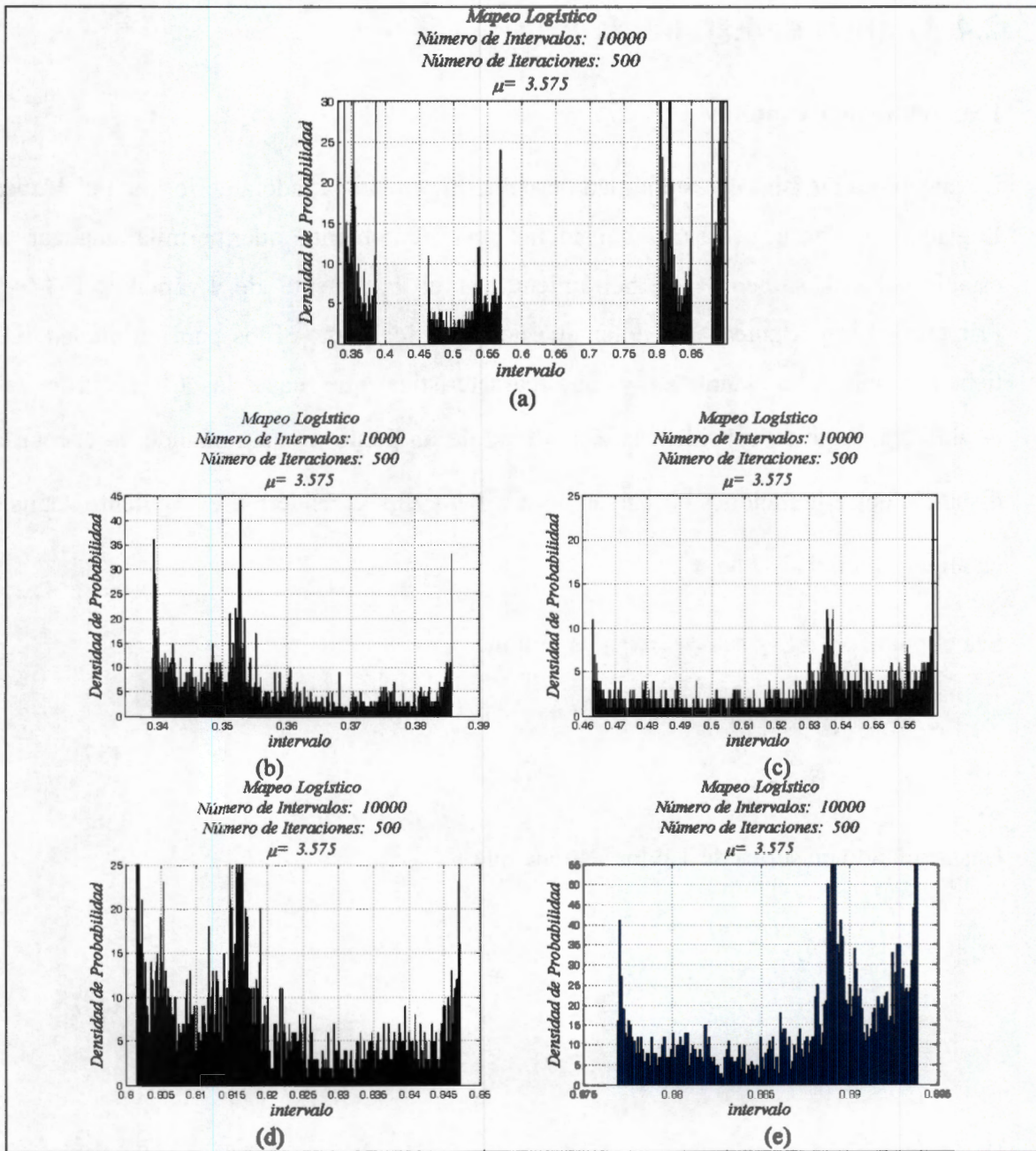


**Figura 26.** Gráficas de las órbitas del *Mapeo Logístico* para diferentes valores del parámetro. a)  $\mu = 4.0$   
b)  $\mu = m_1$ . c)  $\mu = m_2$ . b)  $\mu = m_3$

Las gráficas de la Figura 27 y de la Figura 28 muestran el detalle del comportamiento de las funciones de densidad de probabilidad para  $\mu = m_1$  y  $\mu = m_2$ , respectivamente. En cada una de estas figuras se muestra que las distribuciones se bifurcan en otras dos distribuciones más, siguiendo el mismo comportamiento. Para verificar esto se ha considerado la observación de distintas porciones del intervalo de definición del *mapeo*.



**Figura 27.** Gráficas de densidad de probabilidad del *Mapeo Logístico* para un valor del parámetro  $\mu = 3.5925$ ., observando a) Todo el intervalo de definición, b) El intervalo (0.3, 0.6) y c) El intervalo (0.78, 0.90).



**Figura 28.** Densidad de probabilidad del *Mapeo Logístico* para un valor del parámetro  $\mu = 3.5925$ . Observando a) Todo el intervalo de definición, b) El intervalo (0.33, 0.39). c) El intervalo (0.46, 0.57), d) El intervalo (0.80, 0.85). e) El intervalo (0.875, 0.895).

## 2.4 Análisis de Estabilidad

### Exponente de Lyapunov

De acuerdo a las islas de estabilidad descubiertas en el apartado anterior para el *Mapeo* Logístico, se hace necesario considerar una herramienta que permita analizar la estabilidad del *mapeo*. Esta herramienta es el Exponente de Lyapunov [93-94]. Primero, es importante hacer notar que no todos los puntos fijos para un *mapeo* 1-D tienen propiedades idénticas y una característica que hace la diferencia es su estabilidad. Aquí se considera la estabilidad de un punto fijo  $x^*$  tomando en cuenta la distancia entre iteraciones sucesivas de  $x^*$ . Para ello, considérese el siguiente análisis en alguna vecindad  $U$  de  $x^*$ .

Sea el punto  $x_n \in U$  y sea  $\delta_n = x_n - x^*$ , entonces,

$$\begin{aligned} |\delta_{n+1}| &= |x_{n+1} - x^*| = |\tau_\mu(x_n) - x^*| \\ &= |\tau_\mu(x^* + \delta_n) - x^*| \end{aligned} \quad (37)$$

Desarrollando en series de Taylor se tiene que,

$$\begin{aligned} |\delta_{n+1}| &= \left| \tau_\mu(x^*) + \delta_n \left. \frac{d\tau_\mu(x)}{dx} \right|_{x^*} - x^* \right| \\ &= \left| \frac{d\tau_\mu(x)}{dx} \right|_{x^*} |\delta_n| \end{aligned} \quad (38)$$

De lo anterior se desprende que  $|\delta_{n+1}| < |\delta_n|$  si y solo si  $|d\tau_\mu(x^*)/dx| < 1$ . Por lo que en este caso se trata de un punto fijo atractor. Así que para cuando  $|\delta_{n+1}| > |\delta_n|$  se tendrá un punto fijo repulsor. Nótese que para llegar a esta conclusión lo único que se usó fue la



cercanía del *mapeo* al punto fijo. Además, se dice que si  $|d\tau_\mu(x^*)/dx| \neq 1$ , entonces el punto fijo  $x^*$  es considerado un punto fijo hiperbólico.

Un *mapeo* puede exhibir órbitas aperiódicas para ciertos valores del parámetro, pero surge la pregunta, ¿Cómo se puede estar seguros de que esta condición es realmente caos? Para que un sistema se llame caótico debería mostrar dependencia sensitiva a condiciones iniciales, en el sentido de que dos órbitas muy cercanas se separen rápidamente, en promedio, en forma exponencial. Una forma de cuantificar esta dependencia es usando el exponente de Lyapunov.

Para mostrar esto considere alguna condición inicial  $x_0$ , ahora considere un punto cercano,  $x_0 + \delta_0$ , donde la separación inicial  $\delta_0$  es extremadamente pequeña. Sea  $\delta_n$  la separación después de  $n$  iteraciones. Si  $|\delta_n| \approx |\delta_0|e^{n\lambda}$ , entonces  $\lambda$  es el exponente de Lyapunov. Un exponente positivo es signo de caos.

Una fórmula precisa y computacionalmente útil se obtiene considerando que  $|\delta_n| = |f^n(x_0 + \delta_0) - f^n(x_0)|$ , y tomando el límite cuando  $\delta_0 \rightarrow 0$ .

$$\begin{aligned} \lambda &= \frac{1}{n} \ln \left| \frac{\delta_n}{\delta_0} \right| \\ &= \frac{1}{n} \ln |(f^n)'(x_0)| \end{aligned} \tag{39}$$

El término dentro del logaritmo puede expandirse, de modo que:

$$(f^n)'(x_0) = \prod_{i=0}^{n-1} f'(x_i) \tag{40}$$

De manera que el exponente de Lyapunov puede aproximarse por la siguiente expresión:

$$\lambda \approx \frac{1}{n} \sum_{i=0}^{n-1} \ln |f'(x_i)| \quad (41)$$

Si esta expresión tiene límite cuando  $n \rightarrow \infty$ , entonces el exponente de Lyapunov para la órbita que inicia en  $x_0$  queda determinado por:

$$\lambda = \lim_{n \rightarrow \infty} \left\{ \frac{1}{n} \sum_{i=0}^{n-1} \ln |f'(x_i)| \right\} \quad (42)$$

Note que  $\lambda$  depende de  $x_0$ . Sin embargo, es la misma para todas las  $x_0$  en la cuenca de atracción de un atractor dado. Para puntos y ciclos estables,  $\lambda$  es negativo. Para atractores caóticos es positivo.

Para el *Mapeo* Logístico, un punto fijo está dado por  $x^* = \mu x^*(1-x^*)$ , cuyas soluciones son  $x_1^* = 0$  y  $x_2^* = 1 - \frac{1}{\mu}$ , además para este *mapeo*  $f'_\mu(x) = \mu(1-2x)$ . Ahora bien,

Dado que el criterio de estabilidad dice que un punto fijo es estable si  $|f'_\mu(x^*)| < 1$  y es inestable si  $|f'_\mu(x^*)| > 1$ , entonces para cuando  $x_1^* = 0$  el punto fijo es estable si  $|f'_\mu(x_1^* = 0)| < 1$  y en consecuencia  $0 < \mu < 1$ . Pero es inestable si  $|f'_\mu(x_1^* = 0)| > 1$ , y por lo tanto,  $1 < \mu < 4$ . Sin embargo, cuando  $x_2^* = 1 - \frac{1}{\mu}$  y

$$f'_\mu \left( x^* = 1 - \frac{1}{\mu} \right) = \mu \left( 1 - 2 + \frac{2}{\mu} \right) = 2 - \mu, \text{ se tiene que el punto fijo es estable si } |2 - \mu| < 1,$$

o de forma equivalente si  $1 < \mu < 3$ , y es inestable si  $\mu > 3$ . Los resultados encontrados con este análisis indican que ambos puntos fijos son inestables para  $\mu > 3$ .

Las gráficas de la Figura 29 muestran el comportamiento del exponente de Lyapunov para el *Mapeo* Logístico, y la entrada al caos es cuando por primera vez  $\lambda$  se hace positivo, esto es,  $\mu = \mu_\infty$  y se incrementa cuando  $\mu > \mu_\infty$ , excepto para unos pequeños

intervalos en donde existe un comportamiento periódico a los que se les llama islas de estabilidad (fenómeno de intermitencia). En la Figura 29c se puede apreciar que  $\mu_{co} = 3.5695$  y en la Figura 29d se aprecian las islas de estabilidad. Las amplias se localizan aproximadamente en los siguientes intervalos  $\alpha_1 \in (3.6266, 3.6328)$ ,  $\alpha_2 \in (3.7382, 3.743)$  y  $\alpha_3 \in (3.8284, 3.8495)$ .

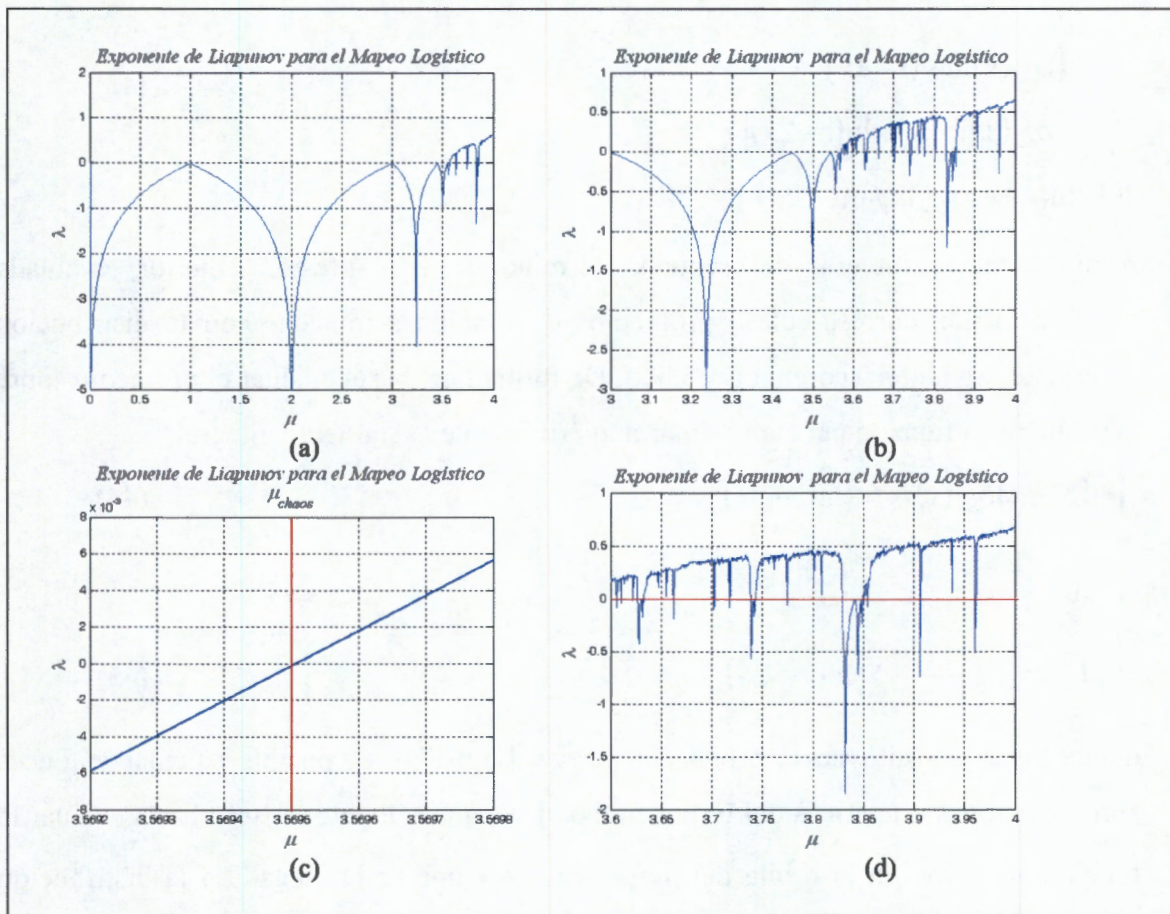


Figura 29. Exponente de Lyapunov para el Mapeo Logístico. a)  $\mu \in (0, 4)$ . b)  $\mu \in (3, 4)$

### Cálculo Numérico del Exponente de Lyapunov

El exponente de Lyapunov para el *Mapeo* Logístico se puede calcular numéricamente empleando para ello, el Teorema de Ergódico de Birkhoff. A partir de la ecuación (42), y considerando que para el *Mapeo* Logístico  $f'_\mu(x) = \mu(1-2x)$ , se tiene que:

$$\begin{aligned} \lambda &= \lim_{n \rightarrow \infty} \left\{ \frac{1}{n} \sum_{i=0}^{n-1} \ln |f'(x_i)| \right\} \\ &= \int \rho_{est}(x) \ln |\mu(1-2x)| \\ &= \int \rho_{est}(x) [\ln(\mu) + \ln(1-2x)] \\ &= \ln(\mu) + \int \rho_{est}(x) \ln(1-2x) \end{aligned} \quad (43)$$

Ahora bien, la integral del segundo término de la expresión anterior, evaluada numéricamente, corresponde a promedios de funciones tomadas con la distribución invariante usando el Teorema Ergódico. De forma que, basta evaluar el promedio sobre la órbita de la función para aproximar numéricamente la siguiente integral,

$$\int \ln(1-2x) \rho_{est}(x) dx = \langle \ln(1-2x) \rangle \quad (44)$$

siendo

$$\langle \ln(1-2x) \rangle \cong \frac{1}{N+1} \sum_{i=1}^N \ln(1-2x_i) \quad (45)$$

donde las  $x_j$  constituyen la órbita del *Mapeo* Logístico, es posible calcular entonces aproximaciones numéricas del Exponente de Lyapunov. Para ello, solo basta evaluar la función  $\ln|1-2x|$  en la órbita del *mapeo* una vez que se ha llegado a la distribución invariante (estacionaria). De este modo, el Exponente de Lyapunov se puede estimar de acuerdo con la siguiente expresión:

$$\begin{aligned}\lambda &= \lim_{n \rightarrow \infty} \left\{ \frac{1}{n} \sum_{i=0}^{n-1} \ln |f'(x_i)| \right\} \\ &= \ln(\mu) + \frac{1}{N+1} \sum_{i=1}^N \ln(1-2x_i)\end{aligned}\quad (46)$$

Otra manera de estimarlo es considerando que para la ecuación (44) se puede calcular la  $\rho_{est}$ , de acuerdo con la expresión (43) y asumiendo una partición regular del intervalo, de modo que  $\Delta x_i = x_{i+1} - x_i = \Delta x$ .

$$\rho_{est} = \sum_{i=1}^M \rho(x_i) D\left(\frac{x-x_i}{\Delta x}\right) \quad (47)$$

De esta manera, la expresión (44) se transforma en

$$\langle \ln(1-2x) \rangle = \sum_{i=1}^M \rho(x_i) \left\{ \int \ln(1-2x) D\left(\frac{x-x_i}{\Delta x}\right) dx \right\} \quad (48)$$

Ahora, considerando que,

$$\begin{aligned}\int \ln(1-2x) D\left(\frac{x-x_i}{\Delta x}\right) dx &= \int_{x_i}^{x_i+\Delta x} \ln(1-2x) dx \\ &= \ln(1-2\bar{x}_i) \Delta x\end{aligned}\quad (49)$$

siendo  $\bar{x}_i$  el valor medio del intervalo  $(x_i, x_i + \Delta x)$  y

$$D\left(\frac{x-x_i}{\Delta x}\right) = \begin{cases} 1 & x \in (x_i, x_i + \Delta x) \\ 0 & x \notin (x_i, x_i + \Delta x) \end{cases} \quad (50)$$

Se tiene que

$$\langle \ln(1-2x) \rangle = \sum_{i=1}^M \rho(x_i) \ln(1-2\bar{x}_i) \Delta x \quad (51)$$

Entonces, el Exponente de Lyapunov, además de poderse calcular con la expresión (46) se puede calcular numéricamente como sigue:

$$\lambda = \lim_{n \rightarrow \infty} \left\{ \frac{1}{n} \sum_{i=0}^{n-1} \ln |f'(x_i)| \right\} \quad (52)$$

$$= \ln(\mu) + \sum_{i=1}^M \rho(x_i) \ln(1 - 2\bar{x}_i) \Delta x$$

## 2.5 Sensitividad ante condiciones iniciales.

Se dice que un *mapeo* posee sensibilidad ante las condiciones iniciales si existen puntos arbitrariamente cercanos,  $x$  y  $x+\delta$ , que al aplicarles el *mapeo*, generan un par de órbitas que eventualmente se separan, sin importar que tan pequeño sea el valor de  $\delta$ .

Además del tratamiento que se hace de la sensibilidad ante condiciones iniciales hecho con el Exponente de Lyapunov en la sección 2.4, a continuación se muestra de manera práctica lo que ocurre, en este sentido, con el *Mapeo* Logístico para 40 iteraciones para  $x_0 = 0.24$  y  $\delta = 10^{-6}$ . Así, la Figura 30 muestra las órbitas generadas para ambas condiciones iniciales, esto es,  $x_0 = 0.24$  y  $x_\delta = 0.240001$ , usando  $\mu = 4.0$  y  $\mu = 3.9$  como valores del parámetro del *mapeo*. Nótese que en la Figura 30.a, cuando  $\mu = 4.0$ , a partir de la iteración 15 es apreciable la diferencia entre ambas órbitas, y en la Figura 30.b, cuando  $\mu = 3.9$ , a partir de la iteración 20 es donde comienza la diferencia apreciable.

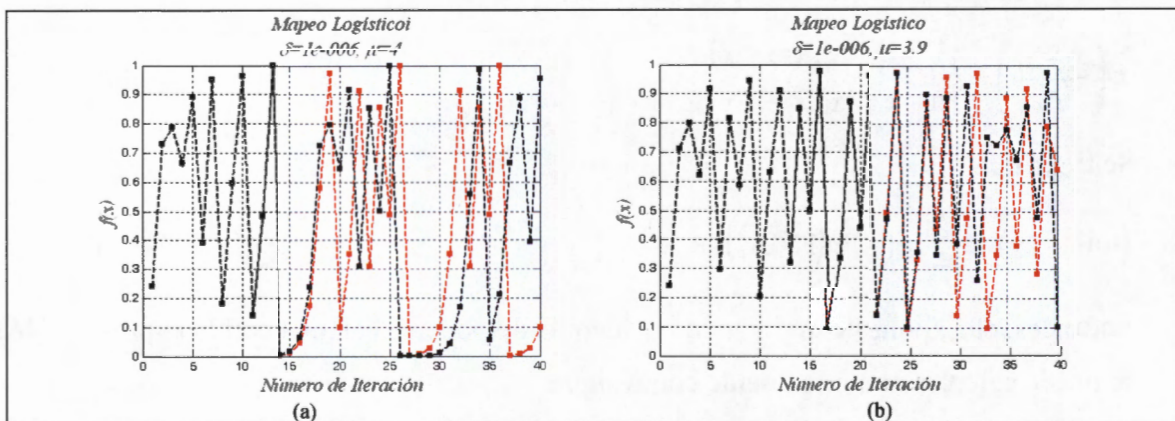
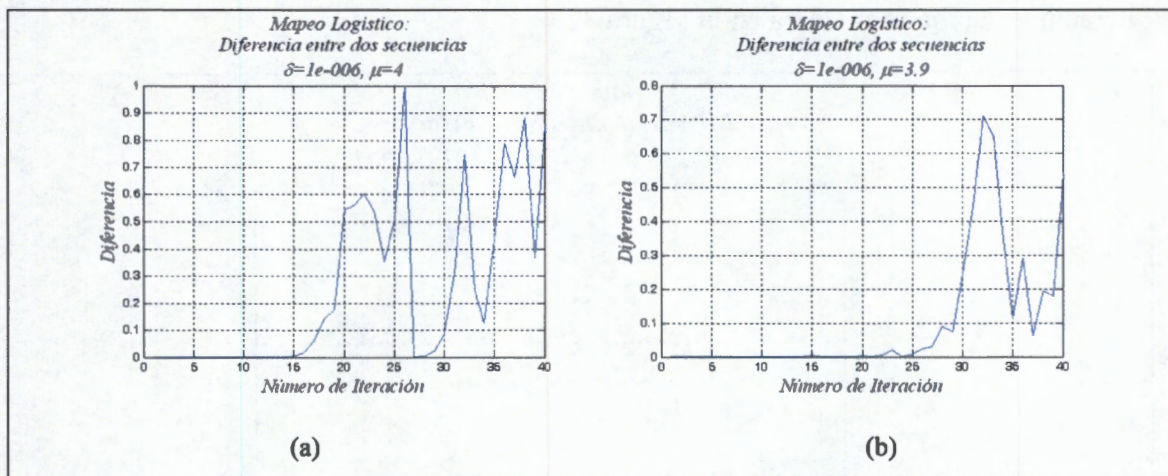


Figura 30. Órbitas generadas con el *Mapeo* Logístico usando dos condiciones iniciales muy cercanas  $x_0 = 0.24$  y  $x_\delta = 0.240001$ . a)  $\mu = 4.0$  y b)  $\mu = 3.9$ .

La Figura 31 muestra la diferencia en valor absoluto entre estas dos órbitas. Nótese en la Figura 31a ( $\mu = 4.0$ ) que después de la iteración 15 la diferencia comienza a ser cada vez mayor, aumentando rápidamente para iteraciones mayores. Lo mismo pasa en la Figura 31b ( $\mu = 3.9$ ), después de la iteración 20 la diferencia entre las dos órbitas se hace apreciable y aumenta rápidamente para iteraciones mayores. Así, un pequeño error en la selección de la condición inicial es amplificado de tal forma que resulta imposible predecir la órbita a largo plazo. De manera que el determinismo no es equivalente a la predictibilidad.



**Figura 31.** Diferencia entre las órbitas generadas con el *Mapeo* Logístico usando dos condiciones iniciales muy cercanas  $x_0 = 0.24$  y  $x_\delta = 0.240001$ . a)  $\mu = 4.0$  y b) para  $\mu = 3.9$ .

## 2.6 Mezclado y Dispersión

### Propiedad de Mezclado

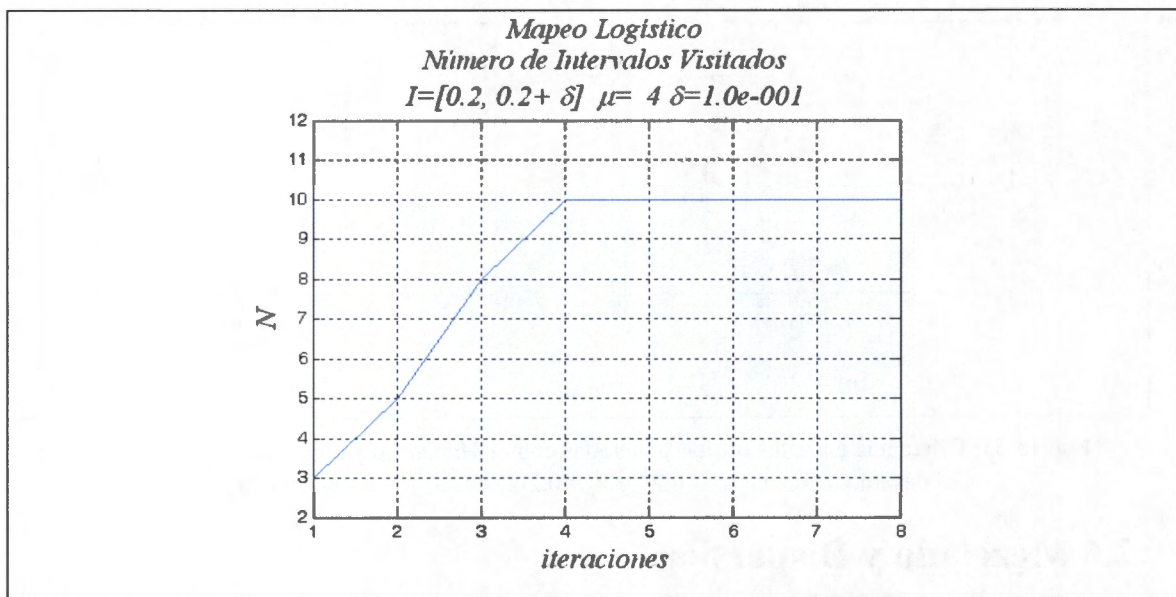
Se ha mostrado en la Figura 30 y en la Figura 31 que una pequeña diferencia en dos condiciones iniciales es amplificada conforme se itera el *mapeo*. Sin embargo, este comportamiento se puede interpretar de una manera distinta. Esto es, un conjunto de condiciones iniciales muy cercanas entre sí, las cuales se encuentran dentro de un

intervalo pequeño arbitrario, llegan a dispersarse sobre el intervalo unitario total dada la sensibilidad del *mapeo* ante condiciones iniciales.

Para verificar este comportamiento en el *Mapeo* Logístico se ha considerado como valor del parámetro  $\mu = 4.0$  y una partición del intervalo unitario en 10 subintervalos de longitud 0.1, esto es,

$$I_k = \left[ \frac{k-1}{10}, \frac{k}{10} \right], \quad k = 1, \dots, 10 \quad (53)$$

Iniciando con el intervalo  $I_3 = [0.2, 0.3]$  es posible cubrir el intervalo completo en 4 iteraciones como se muestra en la Figura 32.



**Figura 32.** Número de intervalos alcanzados en función del número de iteraciones del *Mapeo* Logístico para una partición de 10 subintervalos con  $\mu = 4.0$ .

Los intervalos que son alcanzados en cada iteración se indican en la Tabla 3, considerando el número de elementos en cada uno de los intervalos para la órbita de cada iteración. Los intervalos  $I_7, I_8$  e  $I_9$  se alcanzan en la iteración 1, con 2636, 4945 y 2419 elementos respectivamente; luego en la iteración 2 se alcanzan los intervalos  $I_6, I_7, I_8, I_9$  e  $I_{10}$ , y en la iteración 3 se alcanzan los mismos intervalos que en la iteración 2



más los intervalos  $I_3$ ,  $I_4$  e  $I_5$ . Finalmente, en la iteración 4 se cubre todo el intervalo unitario sin llegar a tener una distribución estacionaria, ya que el número de órbitas existentes en cada uno de los intervalos difieren entre sí. La distribución estacionaria se alcanza hasta después de la iteración 9 como se indica en la Figura 33, ya que  $\varepsilon$ , la distancia entre distribuciones, se ha estabilizado a un valor. Es posible mostrar que se obtienen resultados similares si se inicia con cualquier otro subintervalo dentro de la misma partición, o si tomamos una partición distinta, digamos de 100 o de 1000 intervalos.

Iteración	Intervalos Alcanzados									
	$I_1$	$I_2$	$I_3$	$I_4$	$I_5$	$I_6$	$I_7$	$I_8$	$I_9$	$I_{10}$
0	0	0	10000	0	0	0	0	0	0	0
1	0	0	0	0	0	0	2636	4945	2419	0
2	0	0	0	0	0	1465	2391	2419	2960	765
3	0	0	119	1061	1078	1043	1091	1187	1539	2882
4	1016	799	666	623	548	553	546	573	1312	3364

Tabla 3. Intervalos alcanzados en función del número de iteraciones del Mapeo Logístico para una partición de 10 subintervalos con  $\mu = 4.0$ .

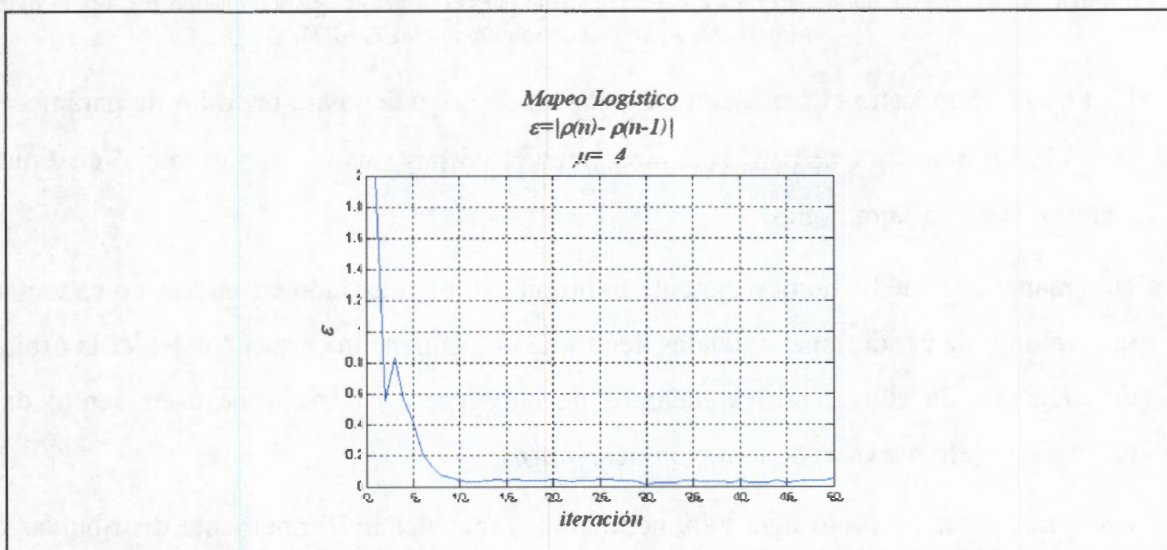
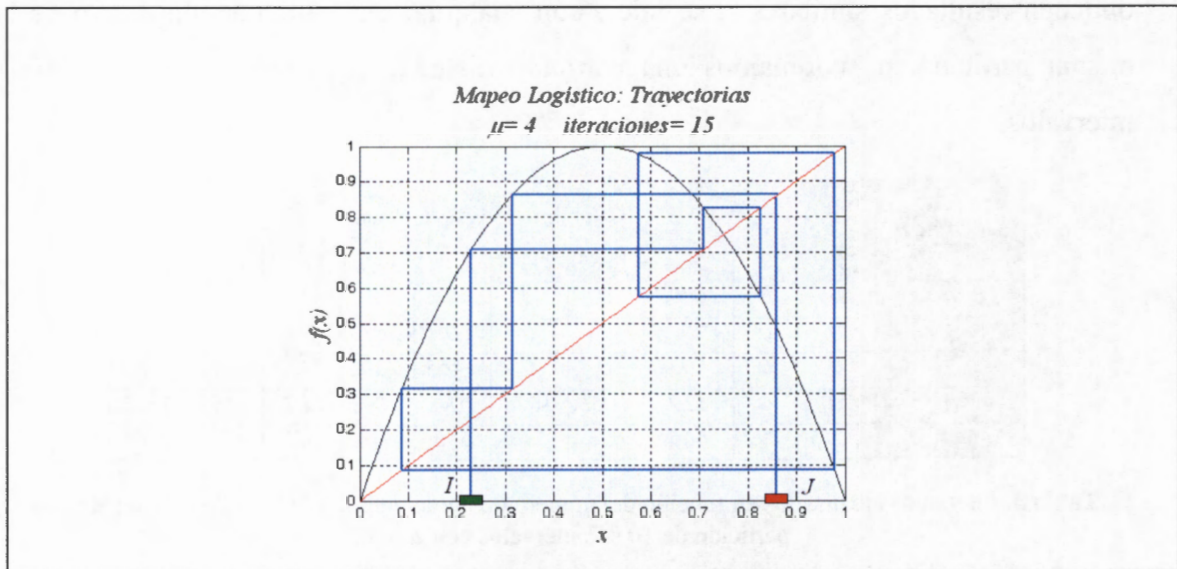


Figura 33. Comportamiento de  $\varepsilon_n$  para el Mapeo Logístico cuando  $\mu = 4.0$ .

El comportamiento que se ha descrito es la esencia de la propiedad de mezclado, la cual se puede definir como sigue: “Para cualesquiera dos intervalos abiertos  $I$  y  $J$ , los cuales pueden ser arbitrariamente pequeños, pero de longitud distinta de cero, es posible encontrar valores iniciales en  $I$ , los cuales, cuando se itera el *mapeo*, caerán eventualmente a puntos dentro del intervalo  $J$ ”.



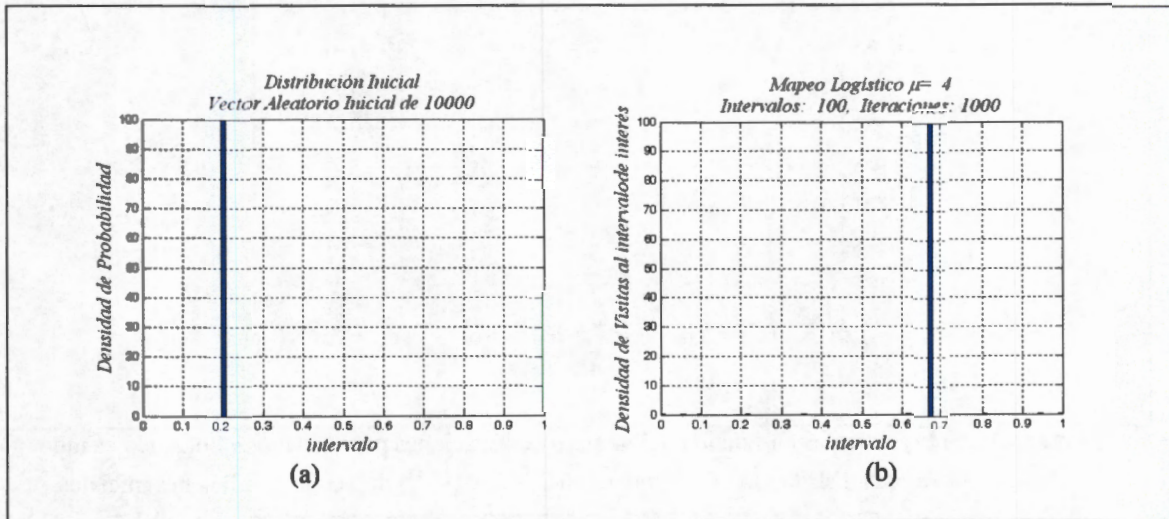
**Figura 34.** Manifestación de la Propiedad de Mezclado para el *Mapeo* Logístico cuando  $\mu = 4.0$ , usando los intervalos  $I$  y  $J$ , una condición inicial  $x_0=0.23$ .

La Figura 35 muestra el mezclado para el *Mapeo* Logístico para un valor de parámetro  $\mu = 4.0$ . Se muestra que para cualquier intervalo  $J$  hay una condición inicial en  $I$  que alcanza  $J$  con 15 iteraciones.

Una manera de medir numéricamente la propiedad de mezclado en un *mapeo* es tomar un conjunto de condiciones iniciales dentro de un pequeño intervalo  $I$ , calcular la órbita de cada una de ellas, verificar cuantos de ellos caen y cuantos no caen dentro del intervalo objetivo  $J$  en cada iteración del *mapeo*.

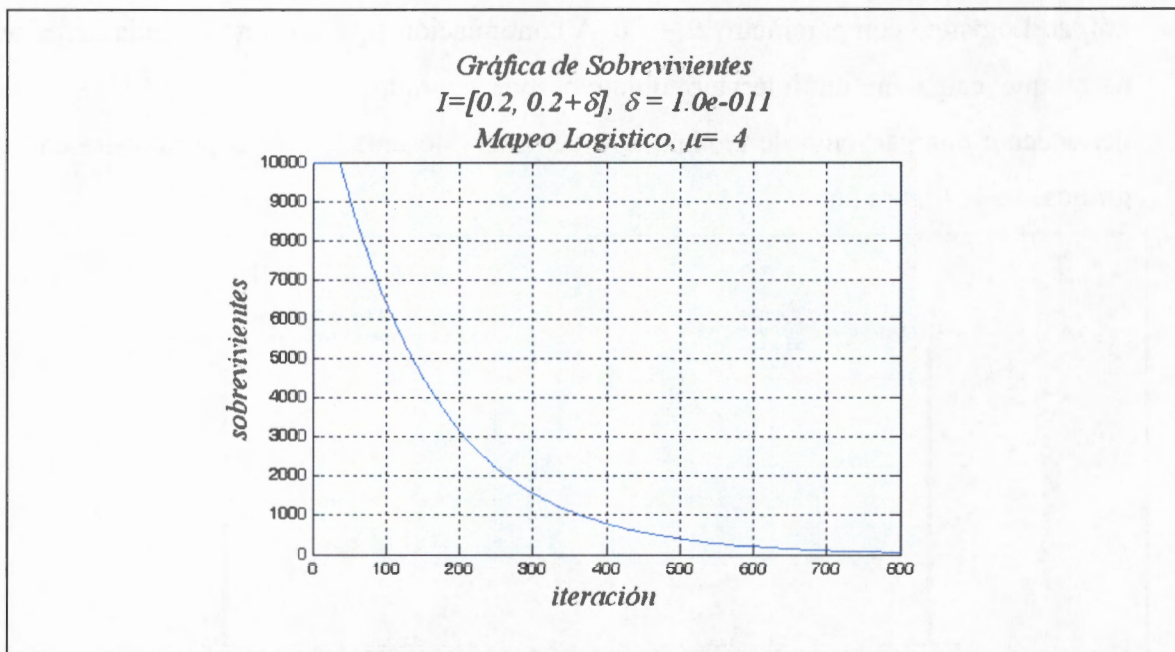
Considérese un conjunto de 10000 condiciones iniciales uniformemente distribuidas e igualmente espaciadas en el intervalo origen  $I = [0.2, 0.2+1 \times 10^{-11}]$ , e itérese el

*Mapeo* Logístico con parámetro  $\mu = 4.0$ , A continuación siga la órbita de cada iteración hasta que caiga en un intervalo objetivo, por ejemplo,  $J = [0.68, 0.69]$ , el cual pertenece a una partición de tamaño 100 del intervalo unitario. Esto se muestra en las gráficas de la Figura 36.



**Figura 35.** Densidad de la distribución inicial uniforme en  $I = [0.2, 0.2+1 \times 10^{-11}]$  y distribución final en el intervalo objetivo  $J = [0.68, 0.69]$  para el *Mapeo* Logístico cuando  $\mu = 4.0$  con 100 iteraciones.

Cuando la órbita cae en el intervalo objetivo se descarta. A las órbitas que no se descartan después de cada iteración se les llama sobrevivientes. La Figura 36 muestra que durante las primeras 36 iteraciones ninguna de las 10000 condiciones iniciales alcanzan el intervalo objetivo  $J$ ; luego, en la iteración 37 existen 60 órbitas que finalmente caen en el intervalo objetivo; en la iteración 38 otras 48 órbitas caen en el intervalo objetivo, para un acumulado de 108 órbitas. Luego, en la iteración 39 caen otras 54 órbitas, para un acumulado de 162. Así para la iteración 40, caen otras 70 para un acumulado de 232 órbitas que caen en el intervalo objetivo, etc. La Tabla 4 muestra una relación de las órbitas sobrevivientes en función del número de iteraciones, la cual es consistente con la Figura 36.



**Figura 36.** Sobrevivientes en función del número de iteraciones para el *Mapeo Logístico* cuando  $\mu = 4.0$ , usando una distribución uniforme en  $(0.2, 0.2 \times 10^{-11})$  de 10000 condiciones iniciales.

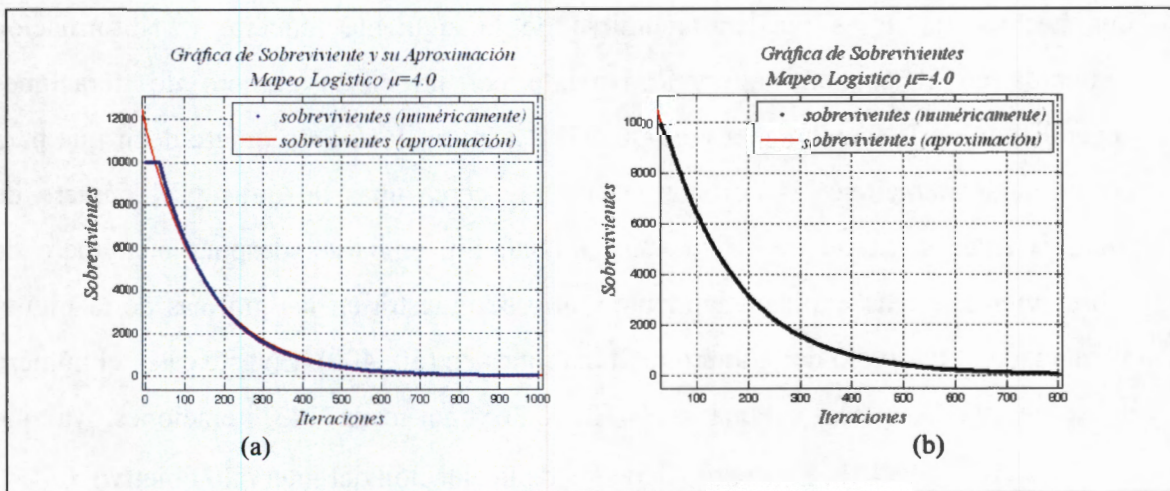
# Iteración	Órbitas Sobrevivientes	Órbitas en el Intervalo Objetivo por iteración	Órbitas en el Intervalo Objetivo acumuladas
36	10000	0	0
37	9940	60	60
38	9892	48	108
39	9838	54	162
40	9768	70	232
41	9717	51	283
42	9636	81	364
43	9571	65	429
44	9508	63	492
45	9453	55	547
46	9398	55	602
47	9320	78	680
48	9234	86	766
49	9171	63	829
50	9101	70	899
51	9027	74	973
52	8966	61	1034
53	8900	66	1100
54	8833	67	1167
55	8768	65	1232
56	8688	80	1312
57	8646	42	1354
58	8579	67	1421
59	8524	55	1476
60	8474	50	1526

**Tabla 4.** Sobrevivientes en función del número de iteraciones para el *Mapeo Logístico* cuando  $\mu = 4.0$ , usando una distribución uniforme en  $(0.2, 0.2 \times 10^{-11})$  de 10000 condiciones iniciales, para la iteración 36 a la 60.

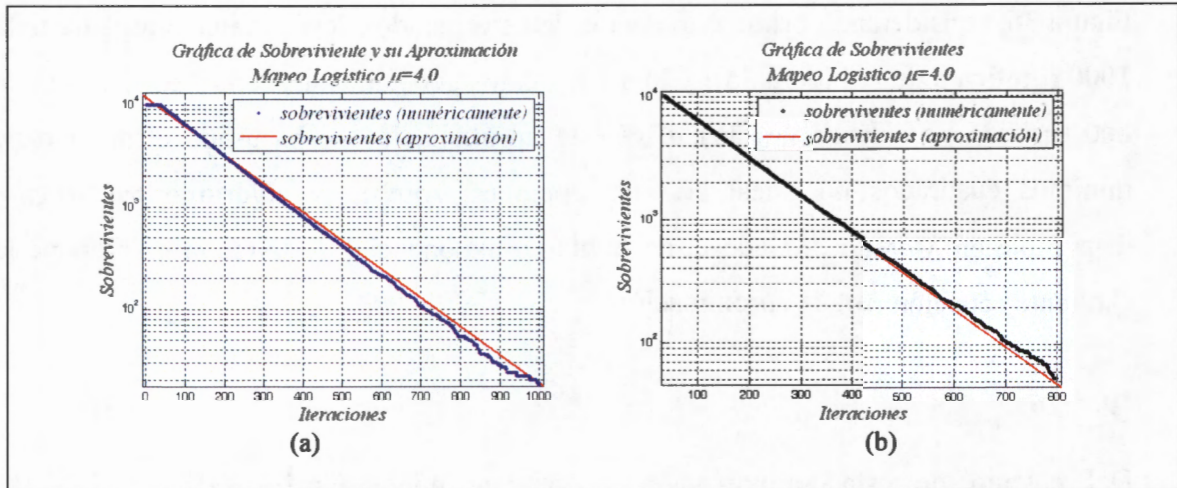
En las gráficas a y b de la Figura 37 se ha realizado una aproximación a la curva de la Figura 36, considerando primero todos los datos generados desde la iteración 1 hasta la 1000 (gráfica a de la Figura 35), y luego los datos generados desde la iteración 36 a la 800 (gráfica b de la Figura 35). Para esta aproximación se ha usado el método de mínimos cuadrados no lineal con las opciones: *robusto* y algoritmo *trust-region* disponible en *MatLab*<sup>TM</sup>. Dado el decaimiento exponencial de la curva se propone la siguiente ecuación para la aproximación:

$$y = ae^{-\frac{n}{\tau}} \quad (54)$$

Del cálculo de esta aproximación se obtiene que  $a = 1.24 \times 10^4$  y  $\tau \approx 148$ , considerando todos los datos generados desde la iteración 1 hasta la 1000 (véase las gráficas a y b de la Figura 37), y se obtiene  $a = 1.26 \times 10^4$  y  $\tau \approx 147$ , considerando de la iteración 36 a la 800. En las gráficas de la Figura 38 se muestran gráficas semilog de las gráficas de la Figura 37.



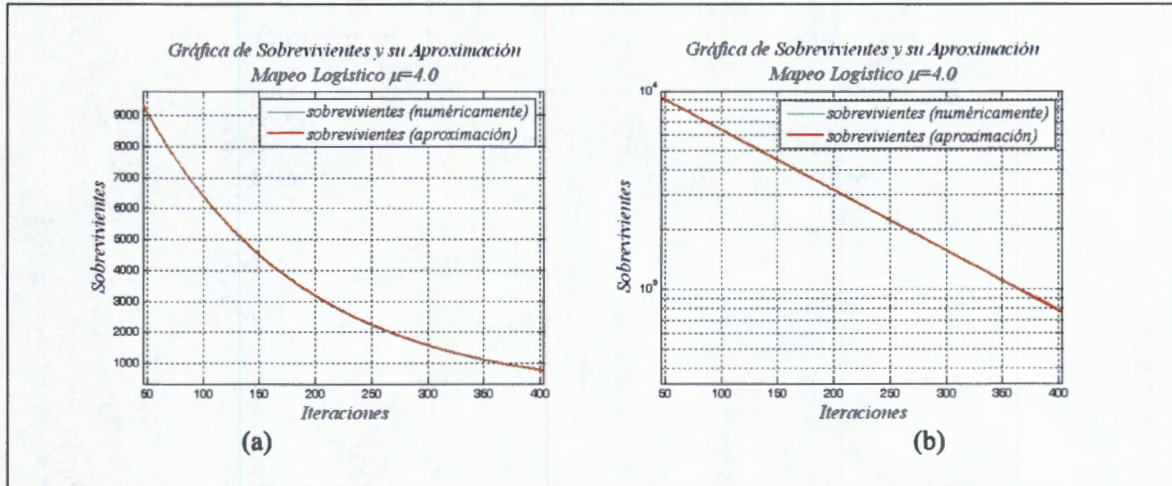
**Figura 37.** Gráfica lineal para el Número de Sobrevivientes en función del número de iteraciones para el Mapeo Logístico cuando  $\mu = 4.0$  y la curva de aproximación con la ecuación (43).



**Figura 38.** Gráfica semilog para el Número de Sobrevivientes en función del número de iteraciones para el Mapeo Logístico cuando  $\mu=4.0$  y la curva de aproximación con la ecuación (43).

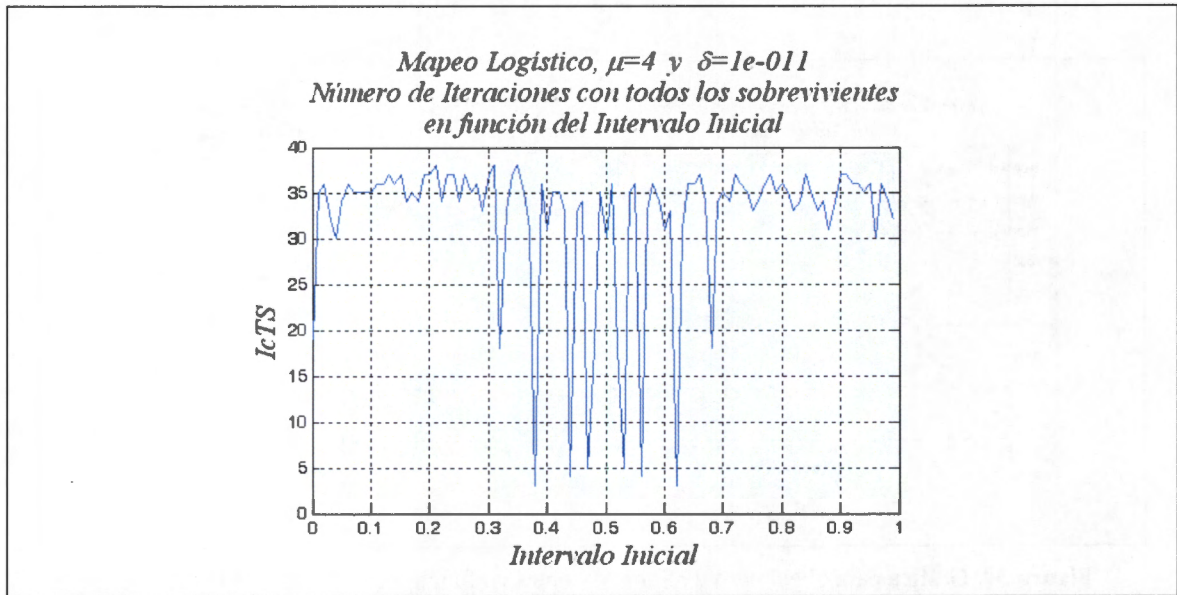
El valor de  $\tau$  se interpreta como un estimado del número de iteraciones que se requieren para reducir el número de sobrevivientes por un factor de  $1/e \approx 0.368$  también se conoce como el tiempo promedio de vida de las órbitas.

Los hechos anteriores pueden resumirse de la siguiente manera. La información contenida en el pequeño intervalo persiste por un cierto número de iteraciones dependiendo de la localización y el tamaño del intervalo  $I$ . Esto quiere decir que para las primeras iteraciones las órbitas están muy cerca unas de otras y el número de sobrevivientes se mantiene en su valor inicial. Sin embargo, después el número de sobrevivientes decae exponencialmente como se muestra en las gráficas de la Figura 39, acotada al intervalo del número de iteraciones en (50, 400). En este caso, el número de sobrevivientes decae a una razón de 0.368 por cada 143 iteraciones, ya que  $a = 1.29 \times 10^4$  y  $\tau \approx 143$ . Esta razón depende de la elección del intervalo objetivo  $J$ .

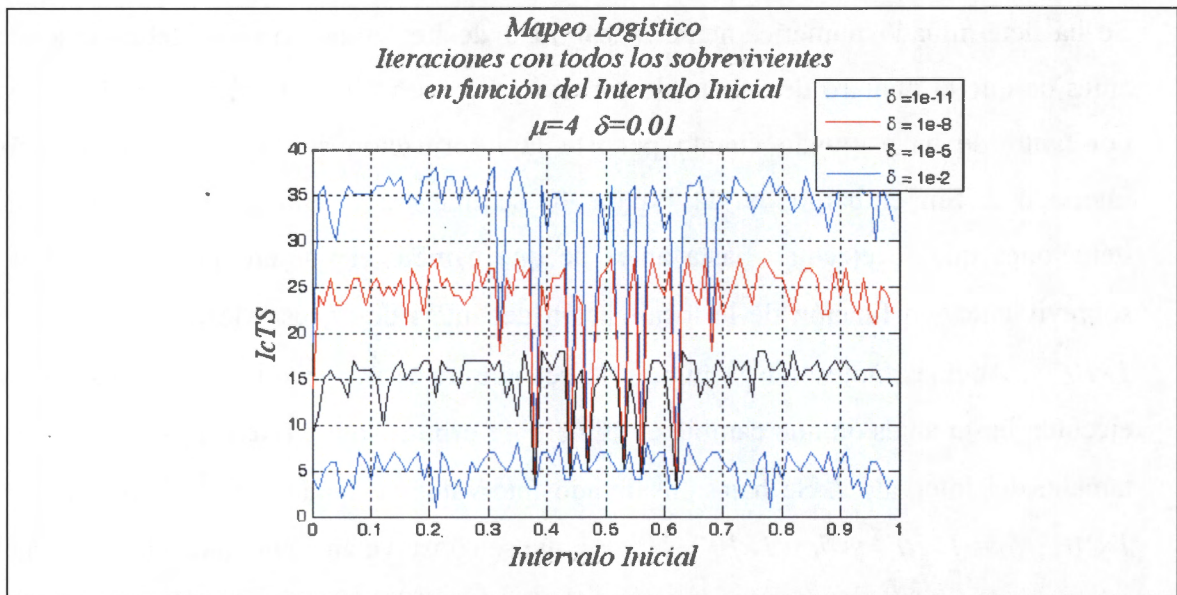


**Figura 39.** Gráfica para el Número de Sobrevivientes en función del número de iteraciones para el Mapeo Logístico cuando  $\mu = 4.0$ , acotado al intervalo de iteraciones (50, 400). a) Lineal. b) Semilog.

Se ha determinado numéricamente la cantidad de iteraciones que se deben ejecutar antes de que el número de órbitas de sobrevivientes sea diferente al número inicial  $y$ , por tanto, se ha estimado cuanto persiste la información contenida en el pequeño intervalo  $I$ . Sin embargo, en la Figura 40 se muestra el límite en el número de iteraciones que se ejecutan hasta antes de que cambie el número inicial de órbitas sobrevivientes en función de la localización del intervalo  $I$ , usando  $\mu = 4.0$  y  $\delta = 1 \times 10^{-11}$ . Además, nótese en la Figura 41 se muestra el número de iteraciones que se ejecutan hasta antes de que cambie el número de órbitas sobrevivientes en función del tamaño del intervalo  $I$ . Se han considerado intervalos de tamaño  $\delta_1 = 1 \times 10^{-11}$ ,  $\delta_2 = 1 \times 10^{-8}$ ,  $\delta_3 = 1 \times 10^{-5}$  y  $\delta_4 = 1 \times 10^{-2}$ . Nótese que se conserva en cada una de las curvas el mismo comportamiento que se presenta en la Figura 38.



**Figura 40.** Sobrevivientes en función de la localización del Intervalo  $I$  para el Mapeo Logístico cuando  $\mu = 4.0$ .



**Figura 41.** Sobrevivientes en función del tamaño del intervalo  $I$  para el Mapeo Logístico cuando  $\mu = 4.0$ .



### Propiedad de Dispersión

Un *mapeo* caótico como el que se analiza en esta tesis, además de exhibir la propiedad de mezclado, exhibe también la propiedad de dispersión. Para mostrar esto considérese un pequeño intervalo arbitrario, dentro del cual, hay un conjunto de condiciones iniciales que se deben iterar usando el *Mapeo* Logístico. Como se muestra en la tabla 4, en cada iteración resultará un nuevo intervalo de diferente tamaño y localización, hasta que se cubre completamente el intervalo unitario. En otras palabras, cualquier punto del intervalo unitario tiene sus pre-imágenes en el pequeño intervalo inicial, o bien, cualquier pequeño intervalo se expandirá completamente al intervalo unitario después de un número de iteraciones. La pregunta que surge en este momento es ¿Cuántas iteraciones es necesario realizar para que partiendo de un ensamble acotado a un pequeño intervalo inicial se cubra el intervalo unitario completamente? La respuesta se deriva del siguiente razonamiento. Se inicia con una partición de tamaño 2 del intervalo unitario. Primero, se considera que el conjunto de condiciones iniciales queda definido dentro del primer intervalo y se itera  $n_1$  veces hasta que se cubra completamente el intervalo unitario; luego, se considera que el conjunto de condiciones iniciales queda definido en el segundo intervalo y nuevamente se itera  $n_2$  hasta que se cubra el intervalo unitario. Finalmente, se obtiene el promedio  $\bar{n}$  entre  $n_1$  y  $n_2$ . Después se duplica la partición a 4, y se calcula considerando separadamente en cada uno de los 4 intervalos de la partición el conjunto de condiciones iniciales, y para cada caso, se itera  $n_i$  veces con  $i = 1, 2, \dots, 4$ , hasta cubrir el intervalo unitario. Si duplicamos una y otra vez el número de intervalos el número promedio de iteraciones necesarias que se deben realizar para cubrir completamente el intervalo unitario queda aproximadamente definido de acuerdo a la siguiente relación,  $N = 2^{\bar{n}}$ , donde  $N$  es el número de intervalos de la partición, siempre y cuando  $\mu = 4.0$ , para otros valores de  $\mu$  se tiene otra relación. La Tabla 5 muestra los valores de  $\bar{n}$  para diferentes valores de  $\mu$ .

$N$	$\bar{n}, \mu = 4.0$	$\bar{n}, \mu = 3.95$	$\bar{n}, \mu = 3.90$	$\bar{n}, \mu = 3.85$	$\bar{n}, \mu = 3.80$	$\bar{n}, \mu = 3.75$
<b>2</b>	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
<b>4</b>	2.5000	2.0000	2.0000	2.0000	2.0000	2.0000
<b>8</b>	3.7500	4.5000	4.5000	15.0000	6.0000	6.7500
<b>16</b>	4.8750	5.8750	6.6875	15.0000	7.6875	8.2500
<b>32</b>	6.1250	7.6875	7.9063	15.0000	9.0938	9.5625
<b>64</b>	7.1563	8.5000	9.0156	15.0000	10.3438	11.5156
<b>128</b>	8.1875	9.7188	10.2109	15.0000	11.5859	12.7891
<b>256</b>	9.1875	10.8438	11.6797	15.0000	13.2422	13.6797
<b>512</b>	10.2305	12.3086	13.0234	15.0000	14.2266	14.4766
<b>1024</b>	13.1016	14.3330	15.0000	15.0000	15.0000	15.0000
<b>2048</b>	15.0000	15.0000	15.0000	15.0000	15.0000	15.0000

**Tabla 5.** Número promedio de iteraciones necesarias para cubrir el intervalo unitario para el *Mapeo* Logístico con diferentes valores del parámetro.

## CAPÍTULO 3: Generación de ruido analógico caótico

### Resumen

Este capítulo presenta el procedimiento que permite diseñar un generador de ruido analógico usando un circuito MOS QT, cuya función de transferencia tiene un comportamiento consistente con el *mapeo* logístico. En este procedimiento, se tiene como criterio principal la distribución invariante del *mapeo*, se hace uso del diagrama de bifurcación y de una generalización del *mapeo* logístico. Se discuten también aspectos relacionados con las implicaciones de la variación del valor del parámetro derivada de procesos de fabricación y realización física de un circuito, en particular, se consideran las variaciones del voltaje de umbral ( $V_{th}$ ) y las dimensiones de los transistores. Al final de este capítulo se presentan los resultados para el análisis de Monte Carlo, usando los parámetros de la fábrica *Austria Micro Systems*.

### 3.1 Antecedentes

De acuerdo con el análisis realizado en el capítulo anterior, el *Mapeo* Logístico es un sistema caótico unidimensional que puede producir señales de ruido o señales periódicas, según sea el valor del parámetro que gobierna su comportamiento. Las herramientas de mecánica estadística que sirvieron para describir y analizar el comportamiento del *Mapeo* Logístico fueron el Teorema Ergódico de Birkhoff, el Diagrama de Bifurcación, la Distribución Estadística y el Exponente de Lyapunov. Con estas herramientas es posible que el ingeniero de diseño electrónico pueda definir y establecer los criterios para que un circuito electrónico, cuya función de transferencia sea una función cuadrática, genere señales de ruido con distribución estadística útil, aprovechando sus propiedades de dispersión mezclado descritas en el capítulo 2 de esta tesis.

Es importante mencionar que además del *Mapeo* Logístico, existen otros *mapeos* como el de Bernoulli y el de la Carpa (tent map) que pueden usarse para la generación de

señales de ruido [95] [96]. Por ejemplo, M. Eisencrafta, y L. Antonio Baccalá buscaron estimar las condiciones iniciales de las órbitas de ruido embebido producido por *mapeos* unidimensionales generales [97]. Otro ejemplo, es el trabajo de A. Mooney et al. [98] en el que se comparan las secuencias pseudo aleatorias con secuencias caóticas generadas por el *mapeo* de carpa aleatorizado (skew tent map). Sin embargo, para propósitos de esta tesis solo se considera el *Mapeo* Logístico; pero, el proceder planteado en el capítulo 2 puede seguirse para la descripción, análisis y utilización de otros *mapeos* como el de Bernoulli y el de carpa.

Una característica importante del *Mapeo* Logístico es, al igual que ocurre para otros *mapeos* unidimensionales como el de Bernoulli y el de carpa, que puede llevarse a la realización en un circuito electrónico con relativa facilidad, empleando para ello circuitos cuya función de transferencia corresponda al *mapeo* que se pretende utilizar.

Para mostrar como se debe aplicar el Teorema Ergódico, la Distribución Invariante, la Dependencia a condiciones iniciales, el Diagrama de Bifurcación y el Exponente de Lyapunov para establecer los criterios de diseño de un generador de ruido analógico, se ha seleccionado un circuito electrónico que tiene un modelo de comportamiento consistente con el *Mapeo* Logístico. El circuito electrónico que se usa es el MOS Translineal Cuadrático (MOS-QT) de Wiegerink [99]. Se usa este circuito debido a que basa su comportamiento en la ley cuadrática de un transistor MOS (congruente con el *mapeo* logístico) y debido a su insensibilidad a variaciones de temperatura y del proceso de fabricación [100]; además, este circuito multiplicador tiene un amplio ancho de banda (se encuentra reportado un valor de 50 MHz con transistores de 10 $\mu$ m).

Para tener una implementación del generador de señales de ruido basado en el circuito MOS-QT de Wiegerink se debe considerar que el *Mapeo* Logístico se encuentra definido para el intervalo (0, 1) y que los circuitos electrónicos actuales manejan niveles de corriente del orden de las micras o menos. Por lo tanto, se hace necesario el

uso de un *Mapeo* Logístico Generalizado que permita asociar la función de transferencia del circuito de Wiegerink con el *mapeo* logístico, y así tener la posibilidad de manejar los niveles de corriente y voltaje congruentes con la realidad en el diseño de circuitos electrónicos.

Es importante mencionar que existen trabajos similares que procuran la generación de señales de ruido empleando sistemas caóticos con implementaciones basadas en transistores MOS, pero en ninguno de ellos se hace mención del uso de las herramientas de mecánica estadística (el Teorema Ergódico, el Diagrama de Bifurcación, la Distribución Estadística y el Exponente de Lyapunov) para establecer los criterios de diseño en el comportamiento estadístico del circuito, tal y como se hace en este trabajo. En el apartado “1.4 Justificación” de esta tesis se mencionan algunos ejemplos de trabajos similares que usan tecnología CMOS.

Así, en esta tesis se muestra el diseño de un generador analógico de ruido caótico a partir de una generalización del *Mapeo* Logístico y se estudian sus características en función de las nuevas variables incluidas en el modelo y se presenta un análisis de Monte Carlo considerando variaciones en el voltaje de umbral ( $V_{th}$ ) y variaciones en las dimensiones de los transistores MOS que constituyen el circuito. Después se muestra el procedimiento de diseño de un generador analógico de ruido caótico que emplea como circuito base el MOS-QT de Wiegerink.

A partir de la discusión anterior, en las siguientes secciones de este capítulo se describe el *Mapeo* Logístico Generalizado que se usa y el circuito MOS-QT de Wiegerink, respectivamente. Después se presenta el procedimiento de diseño precisando la manera en que se deben aplicar las herramientas de mecánica estadística descritas en el capítulo anterior.

## 3.2. Mapeo Logístico Generalizado.

### Modelos Generalizados

Se han propuesto diferentes modelos que hacen una generalización del *Mapeo Logístico*. Por ejemplo, K. Kubota et al. reportan en [101] en el año 2000 un estudio de la dinámica de *Mapeo Logístico Generalizado* que se describe de acuerdo a la siguiente expresión:  $x_{n+1} = \beta\{4x_n(1-x_n)\}^q$ . Establecen diferentes valores de  $q$  para su análisis y determinan la existencia de *Caos Intermitente* en este *mapeo*. Otro ejemplo de una generalización del *Mapeo Logístico* se encuentra en [102], donde M. C. Shastry et al. propusieron en julio de 2006 el *Mapeo B-Exponencial* como una generalización del *Mapeo Logístico* y su aplicación a la generación de números pseudo aleatorios. Shastry et al. encuentran en esta generalización que la familia de *mapeos* producen y exhiben caos robusto para todo valor real del parámetro  $\beta \geq e^{-4}$ ; además, presentan resultados que muestran que las secuencias de números aleatorios generadas pasan (cumplen satisfactoriamente) las pruebas estadísticas tales como ENT [103], NIST [104] y Diehard [105]. Un ejemplo más se tiene con el trabajo reportado por R. Tonelli y M. Coraddu en julio de 2006 [106], en el cual se comparan tres diferentes tipos de entrada al caos en el *Mapeo Logístico* y el *Mapeo Logístico generalizado*: el atractor de Feigenbaum al final del doblamiento del periodo en el diagrama de bifurcación, la bifurcación tangente al borde de la isla de estabilidad para el periodo 3, y la transición al caos en el *Mapeo Logístico Generalizado* con inflexión  $1/2$  ( $x_{n+1} = 1 - \mu x_n^{1/2}$ ), en el cual la cascada de bifurcación colapsa a un punto único. Sin embargo, para propósitos de este trabajo es necesario considerar un modelo del *Mapeo Logístico* que permita diseñar un circuito que genere una señal analógica de ruido caótico, considerando para ello que los niveles de señal (corriente o voltaje) que se requiere son cantidades cuya

magnitud es mucho más pequeña que el intervalo de definición del *Mapeo* Logístico clásico. A continuación, se presenta la propuesta de este *Mapeo* Generalizado.

### Modelo de R. Mathews

El *Mapeo* Logístico clásico está confinado al intervalo de los números reales cuya dimensión es menor o igual al intervalo unitario. Es posible plantear un modelo diferente para el *Mapeo* Logístico que resulte, en términos de la aplicación [107] [108], un modelo generalizado. En este caso, se ha tomado como base el modelo sugerido por R. Mathews en 1989 [109].

$$x_{n+1} = C\mu((x_n + d)(M - (x_n + d)) - e) \quad (55)$$

donde  $C$  y  $M$  modifican la escala del *mapeo* logístico, las variables  $d$  y  $e$  son cantidades usadas como desplazamiento de la variable independiente de la función logística.

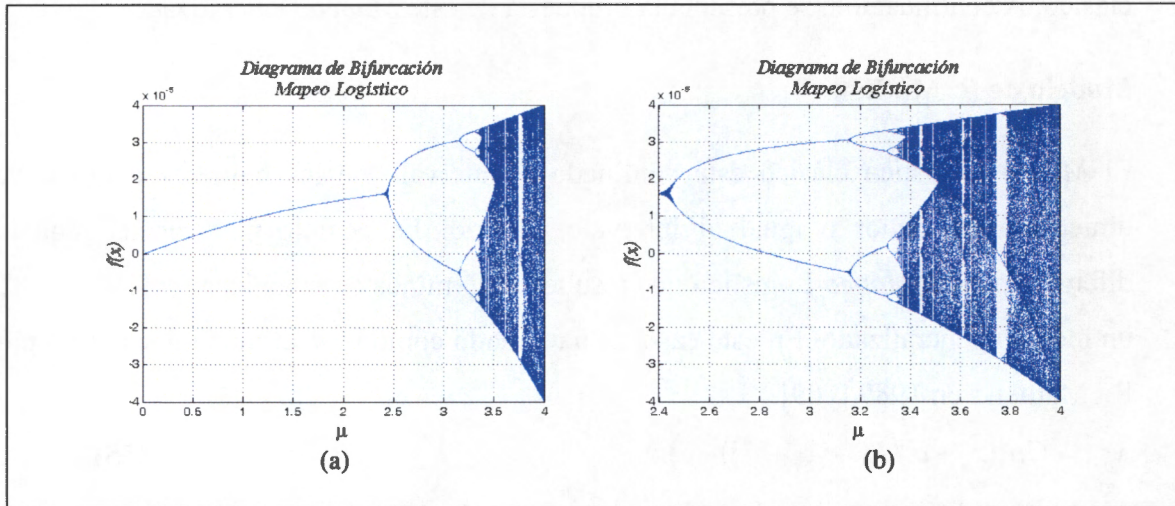
Las raíces de la ecuación (55) son  $x^+ = -d$  y  $x^- = M - d - e$ , en las cuales el *mapeo* generalizado tiene su cruce por cero. En consecuencia  $-d \leq x_n \leq M - d - e$  y su valor máximo está en:

$$x_{Max} = \frac{M - e}{2} - d \quad (56)$$

La ecuación (55) puede ser usada en el diseño de generadores de ruido analógico caótico, de modo que puede reescribirse de la siguiente manera para poder ser asociada a la función de transferencia cuadrática del circuito:

$$x_{n+1} = -C\mu x_n^2 + C\mu(M - 2d - e)x_n + C\mu(dM - de - d^2) \quad (57)$$

La Figura 42 muestra el diagrama de bifurcación para la ecuación (57) usando  $C = 12500$ ,  $M = 80 \times 10^{-6}$ ,  $d = 40 \times 10^{-6}$  y  $e = 800 \times 10^{-12}$ . Nótese que  $-40 \times 10^{-6} \leq x_n \leq 40 \times 10^{-6}$ .



**Figura 42.** Diagrama de bifurcación para el *Mapeo Logístico Generalizado*, a)  $\mu \in (0,4)$ . b)  $\mu \in (2.4,4)$

De esta manera, seleccionado adecuadamente, y en términos de la aplicación particular, los valores de  $C$ ,  $M$ ,  $d$  y  $e$  es posible tener un comportamiento caótico para intervalos diferentes de  $x_n$  y de  $\mu$ , tal y como se muestra en la Figura 42.



### 3.3. Circuito MOS QT de Wiegierink

#### Consideraciones

El circuito MOS-QT de Wiegierink fue propuesto en 1991 por Remco J. Wiegierink como un multiplicador analógico de corriente de cuatro cuadrantes basado en tecnología MOS<sup>39</sup> [100]. Un circuito multiplicador es un bloque importante en procesamiento de señales en tiempo continuo. Se pueden emplear para modulación e instrumentación, y en sistemas de control o generación de ruido [110]. Existen muchas técnicas para implementar un multiplicador; las basadas en la propiedad translineal de un transistor bipolar [111], las basadas en las características de ley cuadrática de un transistor CMOS [112] y las basadas en capacitores conmutados [113].

#### Funcionamiento del Circuito de Wiegierink

El circuito de Wiegierink basa su funcionamiento en la característica de *Ley Cuadrática* de un transistor MOS y tiene insensibilidad a variaciones del proceso de fabricación [100]. Además al ser un circuito que opera en modo corriente se puede asumir que posee las ventajas de amplio rango dinámico, ancho de banda amplio (se reporta como un multiplicador con un ancho de banda de 50 MHz con transistores de 10 $\mu$ m), simplicidad del circuito y bajo consumo de potencia [114]. Por tanto, resulta ser un adecuado candidato para mostrar la aplicación de las herramientas de mecánica estadística como criterios de diseño de un generador de ruido. Debido a la ley cuadrática que rige su comportamiento, este circuito sirve de base para el análisis y diseño de un generador analógico de ruido caótico, que en esta tesis se presenta.

---

<sup>39</sup> Los transistores MOS se emplean en circuitos analógicos, debido a dos características importantes: a) **Alta impedancia de entrada**: La compuerta de un transistor MOS viene a ser un pequeño condensador, por lo que no existe corriente de polarización. b) **Reducida resistencia de canal**: Un MOS saturado se comporta como una resistencia cuyo valor depende de la

La Figura 43 muestra el circuito de Translineal cuadrático de Wiegerink, que se ha considerado como pieza principal del generador de ruido analógico caótico. Su función de transferencia está dada por la siguiente ecuación [110],

$$I_o = 2I_b - \frac{I_{in}^2}{8I_b} \quad (58)$$

Esta ecuación es válida solamente si todos los transistores operan en la región de saturación. Esto impone algunas restricciones sobre la corriente de entrada. Si  $I_{in}=0$ , la corriente de drenaje de los transistores M1 a M4 deberán ser igual a  $I_b$ . Si  $I_{in}$  se incrementa en cualquier dirección, la corriente a través de los transistores M1 y M3 permanecerá constante, pero la corriente a través de M2 ó M4 se incrementará mientras la otra decrece. La máxima corriente de entrada se alcanza cuando  $I_2$  ó  $I_4$  llegan a ser cero. Estas corrientes son ambas mayores o iguales a cero si la corriente de entrada está restringida a  $-4I_b \leq I_{in} \leq 4I_b$ .

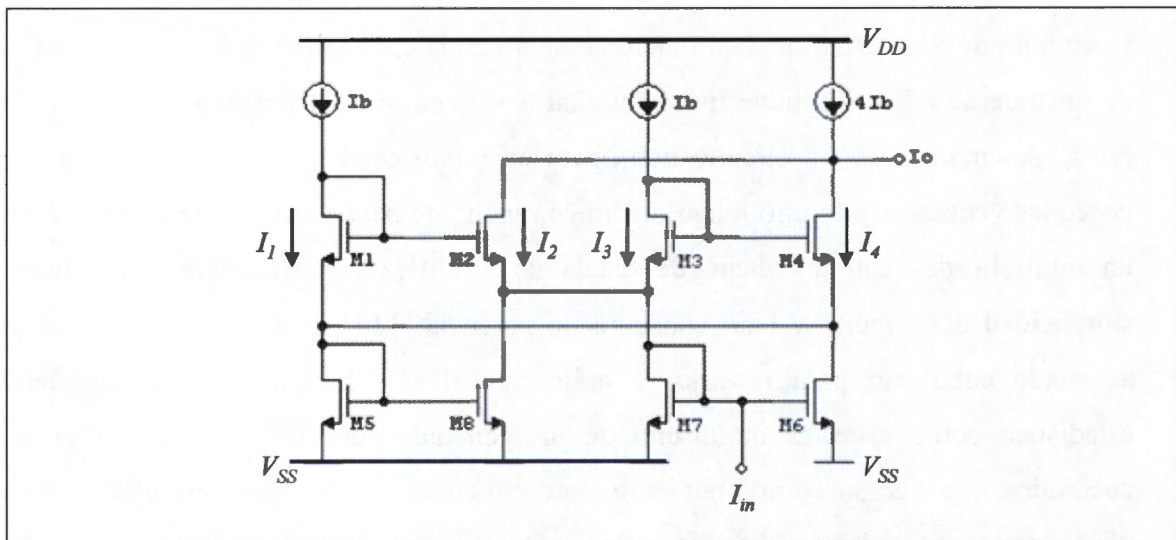


Figura 43. Circuito MOS Cuadrático Translineal de Wiegerink.

superficie del transistor. Es decir, que si se le piden corrientes reducidas, la caída de tensión en el transistor llega a ser muy reducida

### **Función de Transferencia**

Para obtener la función de transferencia del circuito Wiegerink se asume que M1-M8 tienen el mismo voltaje de umbral ( $V_{th}$ ) y la misma relación de dimensiones ( $W/L$ ). La función de transferencia puede obtenerse con el análisis del lazo translineal formado por los transistores M1-M4:

$$\sqrt{I_1} + \sqrt{I_3} = \sqrt{I_2} + \sqrt{I_4} \quad (59)$$

Donde  $I_j$  es la corriente de drenaje de cada transistor  $M_j$ .

Las corrientes  $I_1$  e  $I_3$  se fuerzan a ser igual a la corriente de polarización  $I_b$ , de manera que la ecuación (59) llega a ser:

$$\sqrt{4I_b} = \sqrt{I_2} + \sqrt{I_4} \quad (60)$$

$$4I_b = I_2 + I_4 + 2\sqrt{I_2 I_4} \quad (61)$$

$$4I_2 I_4 = (I_2 + I_4 - 4I_b)^2 \quad (62)$$

$$8I_b(I_2 + I_4) = (I_4 - I_2)^2 + 16I_b^2 \quad (63)$$

$$I_2 + I_4 = 2I_b + \frac{(I_4 - I_2)^2}{8I_b} = 4I_b - I_o \quad (64)$$

La corriente del espejo M7-M6 fuerza la relación:

$$I_m + I_2 + I_3 = I_1 + I_4 \quad (65)$$

Dado que  $I_1$  e  $I_3$  son iguales a  $I_b$  entonces:

$$I_m = I_4 - I_2 \quad (66)$$

Substituyendo (66) en (64), se obtiene la expresión siguiente, la cual corresponde a la ecuación (58):

$$4I_b - I_o = 2I_b + \frac{I_m^2}{8I_b} \quad (67)$$

### 3.4. Generador analógico de ruido

#### El Modelo Generalizado y la Función de Transferencia

Debido a que la implementación del generador analógico de ruido se hace con el circuito de Wiegierink, en este apartado se muestra la asociación de la función de transferencia de dicho circuito (apartado 3.3) con la ecuación del *Mapeo* Logístico Generalizado presentada (apartado 3.2). Esta asociación de ecuaciones hace un escalamiento de la ecuación del *mapeo* logístico original que permite estar en condiciones de diseñar el circuito generador analógico de ruido para los niveles de corriente adecuados (del orden de micro amperes) a la realidad de la tecnología disponible y las distintas aplicaciones posibles. Además, con esta asociación se precisa el intervalo de definición del *mapeo* logístico al rango dinámico que debe tener la señal de salida para una posible aplicación.

Adicionalmente a esta asociación de ecuaciones, se hace necesario iterar la función logística generalizada para que pueda ser posible generar caos; para ello, se requiere de un amplificador de ganancia  $\mu$  en el lazo de retroalimentación entre la salida y la entrada del circuito de Wiegierink. La ganancia de este amplificador corresponde completamente al parámetro  $\mu$  que regula el comportamiento del circuito. La señal de salida del circuito total en lazo cerrado es determinista, y si  $\mu \geq \mu_c$  será impredecible, excepto si cae en alguna de las islas de estabilidad. La señal de salida depende de la condición inicial, esto es, la semilla del generador. La Figura 44 muestra como la salida del circuito de Wiegierink (función logística) se retroalimenta a la entrada para lograr el *mapeo* logístico iterado. En [116] se pueden encontrar circuitos que pueden usarse para iterar la función logística dada por el circuito de Wiegierink.

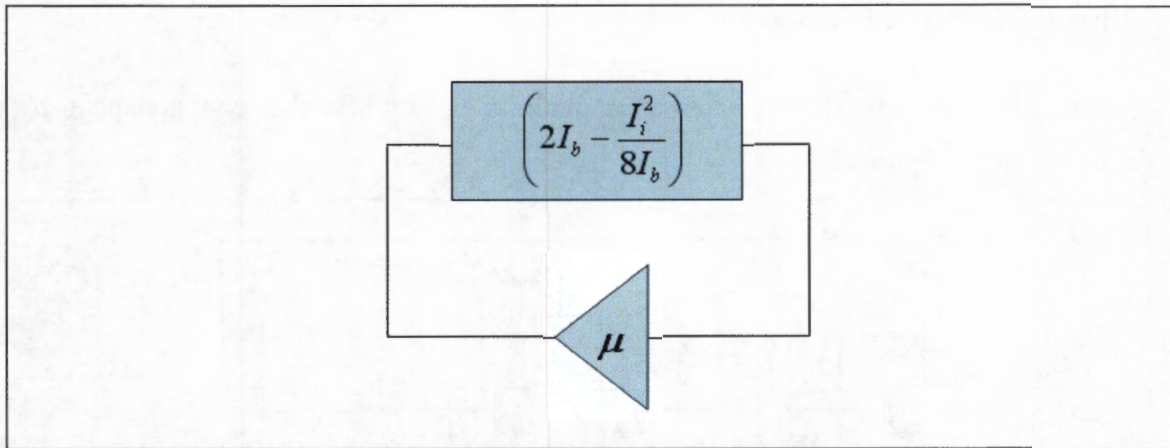


Figura 44. Diagrama a bloques de un circuito retroalimentado para lograr la iteración de la función de transferencia con una línea de retardo.

A partir de lo anterior se asocian entonces las ecuaciones (55) y (58) para diseñar un generador de ruido analógico caótico con el circuito de Wiegierink, y una vez realimentada la señal de salida a través de un punto suma a la entrada, se obtiene la siguiente función iterada para el circuito MOS Cuadrático Translineal:

$$\begin{aligned}
 I_{i+1} &= \mu \left( 2I_b - \frac{I_i^2}{8I_b} \right) \\
 &= -\frac{\mu}{8I_b} I_i^2 + 2\mu I_b
 \end{aligned}
 \tag{68}$$

Entonces usando (55) y (58) se tiene que

$$C = \frac{1}{8I_b}; \tag{69}$$

$$M = 8I_b + e; \tag{70}$$

$$d = 4I_b \tag{71}$$

Adicionalmente, usando  $-d \leq x_n \leq M - d - e$  se selecciona  $e = (20 \times 10^{-6})d$ . De esta manera, el valor del parámetro  $\mu$  debe seleccionarse más allá de las islas de estabilidad que reporta el diagrama de bifurcación.

### Circuito de Retroalimentación

Ahora bien, el circuito empleado para realizar el amplificador con ganancia  $\mu$  se muestra en la Figura 45.

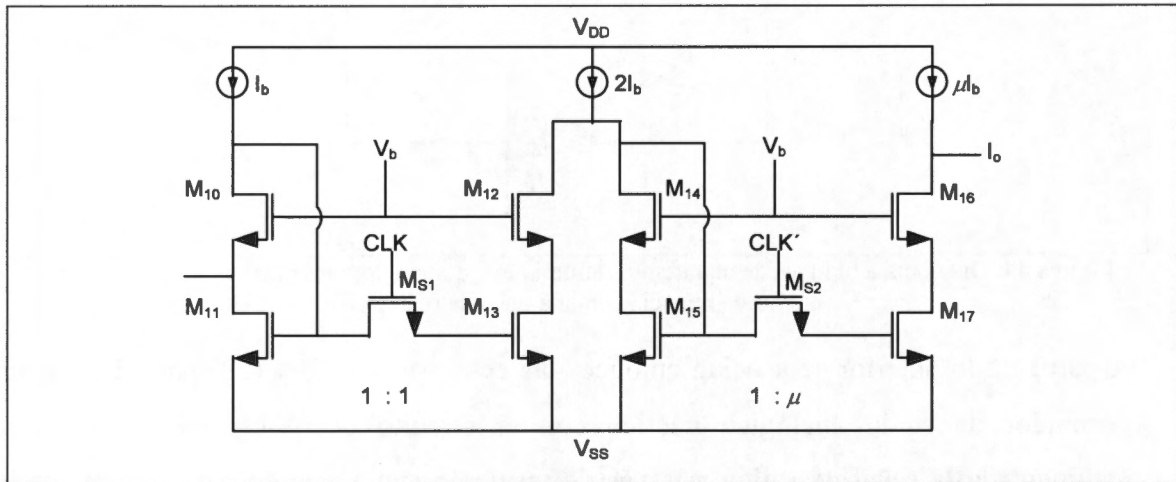


Figura 45. Diagrama del circuito amplificador de ganancia  $\mu$ .

Es importante destacar que la función de transferencia de este amplificador depende de las dimensiones de los transistores que lo constituyen, y está dada esencialmente por los espejos de corriente de relación 1:1 y 1: $\mu$ , y se reduce a la razón de las corrientes de drenaje que pasan por dos transistores  $M_{11}$  y  $M_{17}$  indicados en la figura anterior. Dado que la corriente de drenaje está dada por,

$$I_D = \frac{K_P}{2} \left( \frac{W}{L} \right) (V_{GS} - V_{th})^2 (1 + \lambda(V_{DS} - V_{DS,sat})) \quad (72)$$

La ganancia de este circuito está dada por,

$$\mu = \frac{I_0}{I_{in}} = \frac{\left( \frac{W}{L} \right)_{M_{17}} (1 + \lambda_{(M_{17})} (V_{DS(M_{17})} - V_{DS,sat}))}{\left( \frac{W}{L} \right)_{M_{11}} (1 + \lambda_{(M_{11})} (V_{DS(M_{11})} - V_{DS,sat}))} \quad (73)$$

Asimismo, en este circuito se asume que  $M_{10}=M_{11}=M_{12}=M_{13}=M_{14}=M_{15}=M_A$ ,  $M_{17}=M_{18}=M_B=\mu M_A$ , y  $\lambda$  es la modulación de la longitud de canal. Se asume además que  $\lambda_{(M_A)}=\lambda_{(M_B)}$ . Nótese que si la ganancia  $\mu$  del amplificador se selecciona y controla adecuadamente, entonces al estar integrado al circuito de Wiegink en el lazo de retroalimentación, el circuito total generará señales de ruido o señales periódicas, según se desee, dependiendo del valor que tenga  $\mu$ .

### 3.5. Procedimiento de Diseño

#### Consideraciones del procedimiento

En este procedimiento de diseño se consideran dos aspectos importantes, la determinación del régimen de operación del circuito MOS y la distribución estadística de la señal de salida del generador analógico de ruido caótico. El régimen de operación está relacionado con el principio de transconductancia lineal, comúnmente llamado principio translineal (TLP: TransLinear Principle)<sup>40</sup>. Los circuitos translineales operan en modo corriente y, en general, pueden implementarse en tecnologías CMOS estándar. El principio translineal MOS es una herramienta poderosa para el análisis y síntesis de circuitos analógicos [117-118] y es útil para aplicaciones tales como amplificadores de banda amplia y multiplicadores de cuatro cuadrantes [119-120]. Para transistores MOS este principio fue originalmente formulado en régimen de inversión débil<sup>41</sup>; pero el

<sup>40</sup> Originalmente, el Principio Translineal se basó en una propiedad de los transistores bipolares, llamada transconductancia con la corriente de colector, pero esta propiedad se encontró después en otros dispositivos. Los elementos translineales son dispositivos con una relación lineal entre la transconductancia y la corriente. Por lo tanto, todos los dispositivos con una relación exponencial voltaje-corriente pueden ser utilizados como elementos translineales.

<sup>41</sup> El estado de inversión débil en una superficie de silicio en una estructura MOS se reconoce implícitamente como la región parabólica en los primeros artículos de C. G. Garrett and W.H. Brattain [121][122]. La operación en inversión débil ocurre cuando el voltaje aplicado en la compuerta está por debajo del voltaje de umbral  $V_{th}$  y la superficie del sustrato debajo de la compuerta se invierte débilmente. Por lo anterior, también se conoce como operación en subumbral (subthreshold).

régimen en inversión fuerte<sup>42</sup> se usa debido a que en 1991, E. Seevinck y R.J. Wiegerink hicieron la generalización de este principio. En inversión fuerte la corriente de drenaje en la región lineal puede aproximarse por,

$$I_D = \beta \left( V_{GS} - V_{th} - \frac{V_{DS}}{2} \right) V_{DS} \text{ para } V_{DS} \leq V_{GS} - V_{th} \quad (74)$$

y en la región de saturación por,

$$I_D = \frac{1}{2} \beta (V_{GS} - V_{th})^2 \text{ para } V_{DS} \geq V_{GS} - V_{th} \quad (75)$$

Siendo,

$$\beta = \frac{W}{L} \frac{K_P}{2}. \quad (76)$$

La ecuación (75) es equivalente a la (72) considerando para propósitos de diseño que  $\lambda(V_{DS} - V_{DS,sat}) \ll 1$ .

En este caso, se usa el modelo del transistor MOS operando bajo el principio translineal en modo corriente, en inversión fuerte en la región de saturación, según lo expresan las ecuaciones (75) y (76).

### Distribución Estadística de la Señal de Salida

La distribución estadística de la señal de salida del generador analógico de ruido caótico está relacionada, como se describió en el capítulo 2 con el valor del parámetro que regula la función logística, que de acuerdo con el apartado 3.4 de esta tesis, depende de la ganancia del amplificador de retroalimentación del circuito generador de ruido y de la condición inicial con que comience a funcionar el circuito. Para determinar la distribución estadística de la señal de salida en el generador analógico de

<sup>42</sup> El estado de inversión fuerte ocurre cuando el voltaje de compuerta es mayor que el voltaje de umbral. En este estado la densidad de electrones en el canal en el equilibrio térmico es mayor que la densidad de agujeros.



ruido caótico se deben precisar dos aspectos. Primero, el valor del parámetro que regula el comportamiento cuadrático de la función logística a partir del diagrama de bifurcación; y segundo, los intervalos de operación caótica usando el Exponente de Lyapunov. Con estas precisiones es posible, entonces, calcular numéricamente en una computadora la distribución estadística aprovechando la propiedad de mezclado del *mapeo* logístico y el Teorema Ergódico de Birkhoff, de acuerdo con lo expuesto en el capítulo 2 de esta tesis.

Entonces, precisando el régimen de operación del circuito MOS, y la distribución estadística deseada o requerida de la señal de salida en el generador de ruido, se puede describir el siguiente procedimiento de diseño, que si bien tratar de ser general, se hace para el circuito cuadrático translineal MOS propuesto por R.J. Wiegerink in 1993 y descrito en el apartado 3.2 de esta tesis; y para el cual se ha mostrado que es posible obtener una función de transferencia cuadrática que puede relacionarse con el *mapeo* logístico. Así, el circuito a diseñar deberá operar como un generador de ruido si trabaja en régimen de inversión fuerte en la región de saturación, cuando el parámetro que regula el comportamiento de este circuito es mayor que el valor de entrada al caos ( $\mu_{\infty} = 3.5699456\dots$ ) para el *mapeo* logístico, pero evitando al mismo tiempo las islas de estabilidad descritas en el capítulo 2.

### Descripción del Procedimiento

El procedimiento de diseño para el circuito de la Figura 44, construido con el circuito de la Figura 43 y por el circuito de la Figura 45 puede describirse de la siguiente manera:

1. Determinación de la distribución estadística de la señal de salida.
  - 1.1. Construir el diagrama de bifurcación del *mapeo* logístico generalizado y en el seleccionar como valor del parámetro un valor  $\mu > \mu_{\infty}$ .
  - 1.2. Con ayuda del Exponente de Lyapunov determinar los intervalos en el valor del parámetro  $\mu$ , en los que el *mapeo* logístico tendrá un comportamiento caótico, evitando las islas de estabilidad. Esto es, para aquellos intervalos de  $\mu$  en los que el Exponente de Lyapunov sea mayor que cero. Preferentemente usar aquellas regiones en las que el valor del parámetro  $\mu$ , que regula el comportamiento logístico, sea mayor a aquellos valores en los que se presenta la isla de estabilidad de ciclo 3, ya que de acuerdo al teorema de Sharkovskii es la última isla de estabilidad que se presenta dentro de la región de comportamiento caótico.
  - 1.3. Para los valores de  $\mu$  seleccionados, determinar numéricamente la distribución estadística de la señal de salida usando un programa de cómputo desarrollado en lenguaje "C" o MatLab<sup>TM</sup>, aprovechando la propiedad de mezclado del *Mapeo* Logístico y el Teorema Ergódico de Birkhoff. Para ello, emplear un ensemble de condiciones iniciales con una distribución inicial uniforme, con el cual se habrá de iterar el *mapeo* logístico hasta que se cumpla con el criterio de convergencia estadística fuerte ó el de divergencia de Kullback-Leibler descritos en la sección 2.2 de esta tesis.

- 1.4. Precisar si la distribución estadística obtenida en el punto anterior es la deseada, de lo contrario regresar al punto 1.1 y repetir los puntos siguientes. En caso de que sea la deseada continuar con el procedimiento.
2. Determinación del rango dinámico de la señal de salida.
  - 2.1. En función de la aplicación y de los requerimientos de diseño y funcionalidad del circuito, definir el intervalo  $(I_{prin}, I_{fin})$  en el cual se desea la señal de ruido caótico, de manera que  $I_{prin} \leq I_o \leq I_{fin}$ .
  - 2.2. Precisar el modelo generalizado del *mapeo* logístico, de manera que se cumpla con el rango dinámico y la distribución estadística deseados. Nótese que el rango dinámico y la distribución estadística de la señal de salida están relacionados por el diagrama de bifurcación del *mapeo* logístico. Considerar que a mayor valor del parámetro que regula el comportamiento logístico mayor amplitud del intervalo que define el rango dinámico de la señal de salida, y si dicho parámetro cambia, cambia entonces la distribución estadística.
  - 2.3. Revisar que lo obtenido hasta este punto sea consistente con lo definido en el punto 1 de este procedimiento.
3. Asociar el modelo del *mapeo* logístico generalizado con la función de transferencia del circuito usado.
  - 3.1. Considerando que  $-d \leq x_n \leq M - d - e$  en el modelo del *mapeo* generalizado, y el criterio del rango dinámico que dice que  $I_{prin} \leq I_o \leq I_{fin}$ , definir  $d$  como  $d = -I_{prin}$ .
  - 3.2. Calcular la corriente de polarización  $I_b$  de acuerdo a la ecuación (71),

4. Definir el régimen de operación de inversión fuerte en la región de saturación de los transistores MOS que conforman el circuito.
  - 4.1. Seleccionar las dimensiones de los transistores de la Figura 43 de acuerdo con la ecuación (72).
  - 4.2. Asegurarse de que el circuito opere en el régimen de inversión fuerte en la región de saturación de acuerdo con la ecuación (75).
  - 4.3. Definir  $\left(\frac{W}{L}\right)_{M1-M8} = \frac{W}{L}$ , para el circuito de la Figura 43, de acuerdo a la consideración hecha para obtener la función de transferencia del circuito MOS QT de Wiegerink de la ecuación (58) y considerando que todos los transistores tiene el mismo  $V_{th}$ .
5. Evaluar la funcionalidad logística del circuito MOS QT de Wiegerink.
  - 5.1. Usar a la entrada del circuito MOS QT de Wiegerink a lazo abierto, una señal analógica con pendiente igual a 1 en el intervalo  $(I_{prin}, I_{fin})$ .
  - 5.2. Verificar que la respuesta del circuito MOS QT de Wiegerink sea igual a una parábola como la mostrada en la Figura 46. El cruce por cero debe estar en  $I_{prin}$  e  $I_{fin}$ , su valor máximo debe estar dado por  $\frac{C}{4}(M-e)^2$  y debe encontrarse localizado en  $x_{max} = \frac{M-e}{2} - d$ .

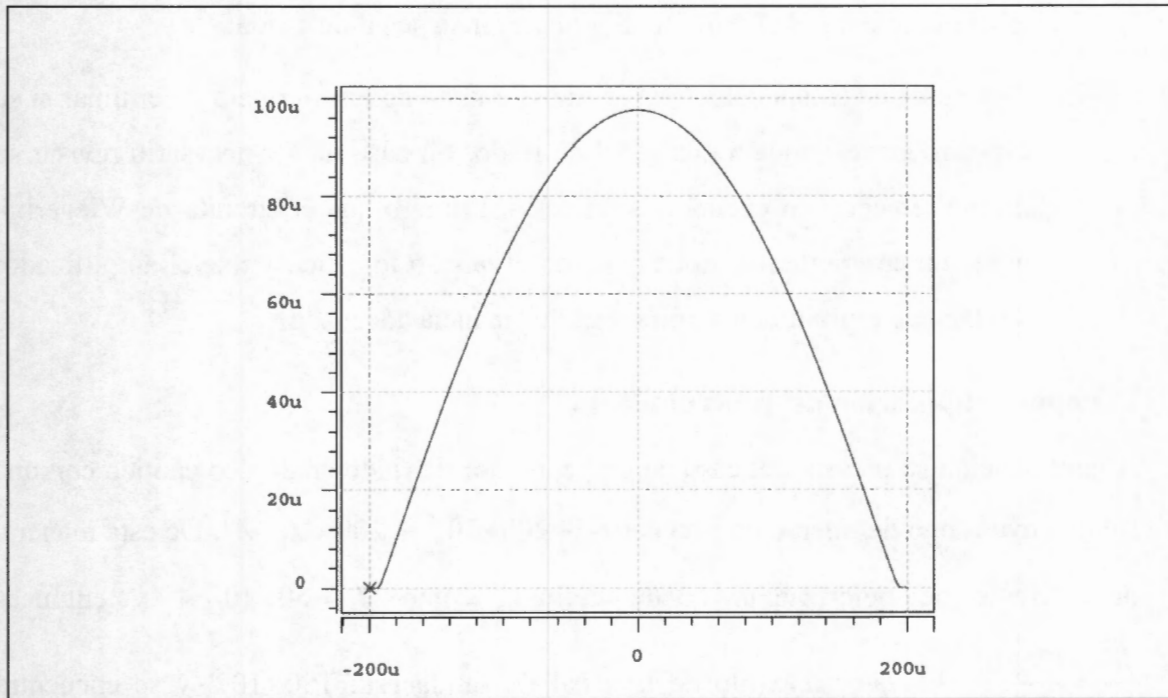


Figura 46. Respuesta en tiempo de un circuito MOS QT de Wiegierink.

6. Diseñar y construir un circuito amplificador de ganancia  $\mu$ .
  - 6.1. Diseñar el circuito amplificador seleccionando el valor  $\mu$  de la ganancia de acuerdo con lo definido en los puntos 2 y 3 de este procedimiento, para que el comportamiento del circuito total cumpla con el rango dinámico y la distribución estadística de la señal de salida.
  - 6.2. Evaluar el circuito amplificador diseñado y precisar el valor de su ganancia. En caso de ser necesario realizar los ajustes al diseño para que cumpla con el valor específico que define el rango dinámico y la distribución estadística de la señal de salida.
  - 6.3. Establecer el lazo de retroalimentación usando el amplificador de ganancia  $\mu$  diseñando.
7. Evaluar la funcionalidad del circuito generador analógico de ruido caótico.

7.1. Hacer funcionar el circuito total y observar su señal de salida.

7.2. A la señal de salida calcularle la transformada de Fourier para determinar si su espectro corresponde a una señal de ruido. En caso de ser necesario revisar su diseño teniendo en cuenta dos aspectos. Primero que el circuito de Wiegink tenga un comportamiento de acuerdo al *mapeo* logístico y que el amplificador del lazo de retroalimentación tenga la ganancia adecuada.

### Ejemplo de aplicación del procedimiento

A continuación se presenta el caso de un generador de ruido analógico caótico con una salida cuyo rango de operación está entre  $(-200 \times 10^{-6} A, 200 \times 10^{-6} A)$ . De esta manera, la corriente de polarización queda definida como  $I_b = 50 \times 10^{-6} A$  y entonces

$\frac{W}{L} = \frac{135 \mu m}{2 \mu m}$ . El valor máximo de la señal de salida está  $100 \times 10^{-6}$  y se encuentra

localizado en 0. En la Figura 47.a se muestra el comportamiento en tiempo del generador analógico de ruido caótico para una  $\mu = 3.2$  y en la Figura 47.b se muestra su comportamiento en frecuencia. De acuerdo al diagrama de bifurcación de la Figura 18, para  $\mu = 3.2$  el sistema se comporta de manera periódica, ya que cae en dos puntos fijos estables.

En la Figura 48.a se presenta el comportamiento en tiempo del circuito generador de ruido para  $\mu = 3.5$  y en la Figura 48.b se muestra su comportamiento en frecuencia. En este caso, el sistema presenta el fenómeno de doblamiento de periodo, por lo que la señal de salida pasa de tener un periodo de orden 2 para convertirse en una señal periódica de periodo 4, habiendo caído en una órbita periódica de orden 4, esto es, 4 puntos fijos estables.

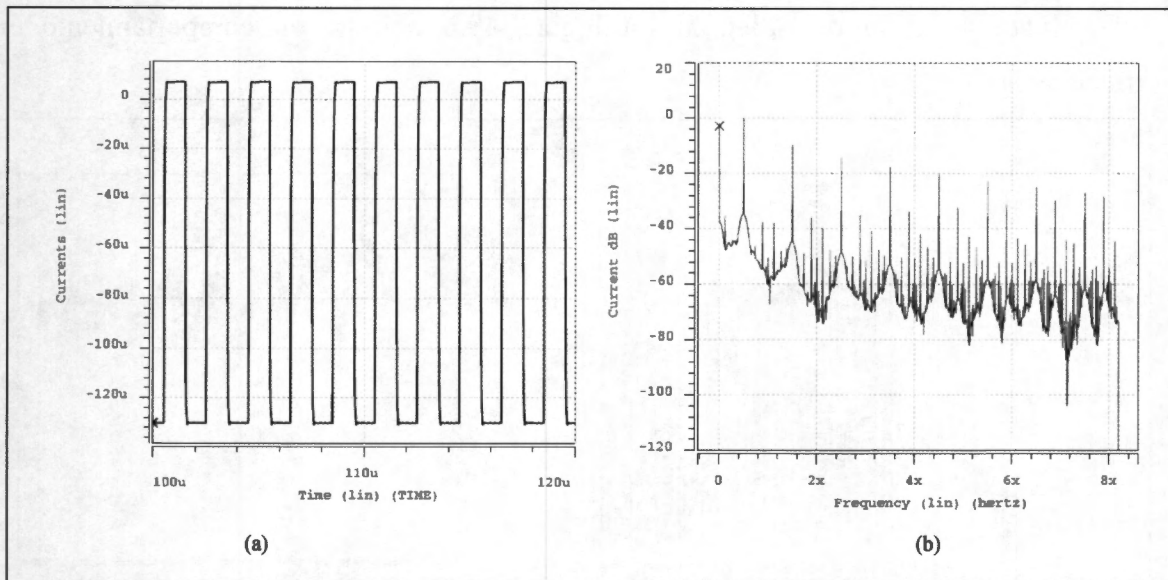


Figura 47. Respuesta en tiempo del circuito generador de ruido para  $\mu=3.2$ .

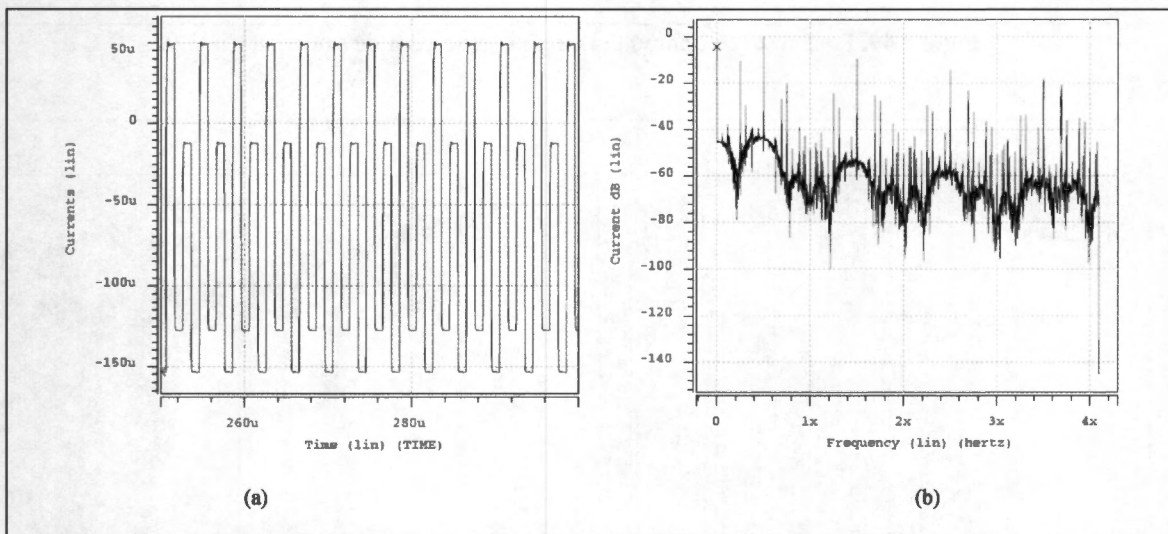


Figura 48. Respuesta en tiempo del circuito generador de ruido para  $\mu=3.5$ .

Finalmente, la Figura 49.a muestra el comportamiento en tiempo del generador analógico de ruido caótico usando un valor de  $\mu = 3.92$ , el cual ha superado la isla de

estabilidad de ciclo de orden 3. La Figura 49.b muestra su comportamiento en frecuencia.

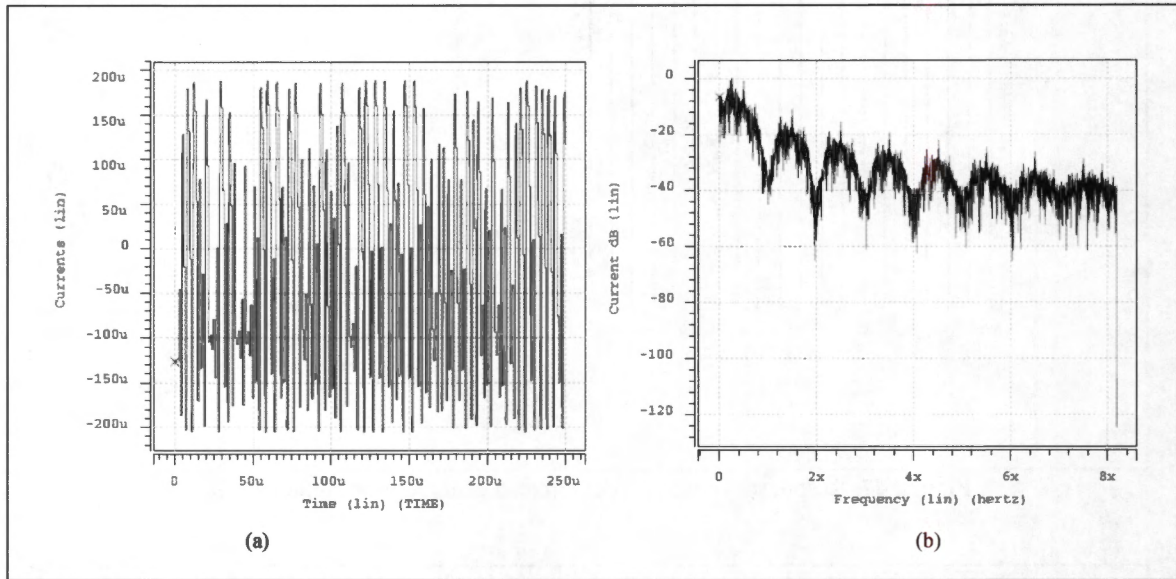


Figura 49. Respuesta en tiempo del circuito generador de ruido para  $\mu=3.92$ .

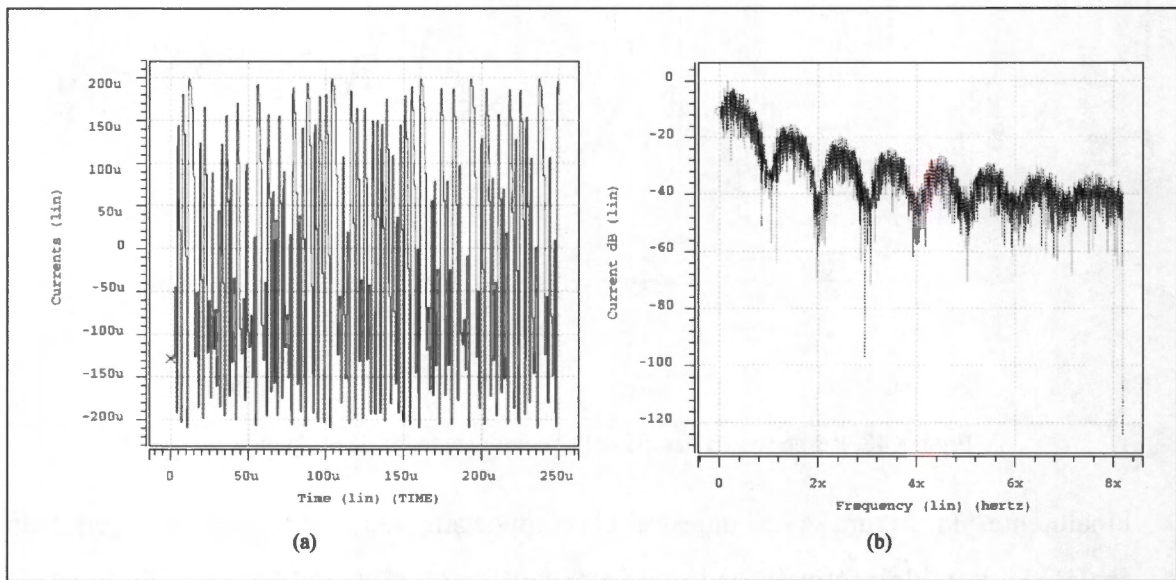


Figura 50. Respuesta en tiempo del circuito generador de ruido para  $\mu=4.0$ .



### 3.6. Consideraciones para su implementación

#### Variaciones del Proceso de Fabricación

En este apartado se presentan los resultados relacionados con el posible cambio de comportamiento del circuito derivado de variaciones en dos condiciones específicas en el proceso de fabricación: voltaje de umbral,  $V_{th}$ , y las dimensiones de los transistores. En este caso se ha empleado tecnología 0.35  $\mu$ mAMS (*Micrómetros de la tecnología Austria Micro Systems*), de la cual se obtienen los parámetros de diseño para ser usados en el simulador circuital HSPICE<sup>TM</sup> y que corresponden al proceso C35, modelo MOS BSIM3v3, revisión 3.1 doc#ENG-182 REV\_3, PMOS y NMOS nivel 49. El voltaje de polarización empleado fue de 3.3 volts, y la ganancia definida para el amplificador del lazo de retroalimentación (parámetro que gobierna el comportamiento del *mapeo*) fue de 3.92. En el Apéndice D se encuentra la definición del circuito realizada para HSPICE<sup>TM</sup>.

Así, de acuerdo a lo indicado en el capítulo 2 de esta tesis, seleccionando y controlando esta ganancia con un valor de  $\mu \geq \mu_{\infty}$  será posible que el circuito pueda operar en la región caótica (excepto para las regiones donde se presentan las islas de estabilidad), y así producir señales de ruido caótico con buenas propiedades estadísticas para ser usado en sistemas de protección de información y en sistemas de comunicaciones. Es importante mencionar que cualquier variación en los valores del parámetro  $\mu$  y de la condición inicial o semilla del generador, tendrán un efecto tal que, el mismo circuito generará señales muy diferentes. En particular, debido a que el parámetro  $\mu$  del sistema analizado es la ganancia del amplificador colocado en el lazo de retroalimentación, y esta ganancia depende de las dimensiones de los transistores y de que estos se encuentren adecuadamente acoplados entre sí, cualquier variación en dichas

dimensiones ocasionará un comportamiento distinto al esperado o al deseado del circuito total. Asimismo, este circuito es sensible a variaciones del  $V_{th}$ .

A partir de lo anterior se hace necesario entonces realizar un análisis de Monte Carlo que permita determinar la desviación en los valores de la ganancia  $\mu$  derivados de las variaciones en las dimensiones de los transistores y en el  $V_{th}$ .

### **Análisis de Monte Carlo.**

Cuando se diseña un circuito electrónico se hace necesario determinar la tolerancia del diseño a variaciones de parámetros debidas a un proceso específico de fabricación. Para analizar y optimizar la producción de circuitos integrados HSPICE<sup>TM</sup> cuenta con una herramienta de análisis estadístico que permite observar los efectos de las variaciones en los elementos y parámetros que definen el modelo que se usa. Cada que se considera la influencia de un parámetro en el comportamiento del circuito, la herramienta de Monte Carlo considera a dicho parámetro como una variable aleatoria con una distribución estadística específica. Dicha distribución se puede precisar a partir de las condiciones impuestas por el proceso específico de fabricación. Por ello, en esta tesis se han considerado las condiciones que se indican en los archivos de referencia de la fábrica AMS (*Austria Micro Systems*). Para los procesos de fabricación de AMS, se considera una distribución estadística Gaussiana<sup>43</sup> de parámetros (*valor\_nominal, desviación\_estándar, intervalo\_confianza*), donde *valor\_nominal* representa el valor nominal de referencia que habrá de usarse en el análisis de Monte Carlo, considerado en muchos casos como la *media* de la variable en cuestión; *desviación\_estándar* hace que el análisis de Monte Carlo considere una variación de +/- el valor indicado en este

---

<sup>43</sup> La distribución gaussiana, también llamada distribución de gauss o distribución normal, es la distribución de probabilidad que con más frecuencia aparece en estadística. Esto se debe a que su función de densidad es simétrica con forma de campana, lo que favorece su aplicación como modelo a gran número de variables estadísticas. Es además, límite de otras distribuciones y aparece relacionada con muchos fenómenos naturales y procesos de fabricación, los cuales pueden ligarse a la teoría de probabilidades gracias a las propiedades matemáticas de esta distribución.

parámetro, e *intervalo\_confianza* especifica el intervalo de confianza que posee el proceso de fabricación y precisa el porcentaje de muestras cuyo parámetro (variable) considerado tiene valores aceptables. Así un valor de *intervalo\_confianza* = 1, precisa el 68% de casos de éxito, *intervalo\_confianza* = 2 precisa el 95% y *intervalo\_confianza* = 3 precisa 99.7%. Para este caso, de acuerdo con los modelos disponibles del fabricante *intervalo\_confianza* = 3.

De esta manera, para el valor del ancho W y largo L del canal del transistor MOS esta distribución es *agauss*(1, 0.01, 3), para el  $V_{th}$  del transistor tipo NMOS es *agauss*(0.4979, 0.01, 3) y para el  $V_{th}$  del transistor PMOS es *agauss*(-0.6915, 0.01, 3).

Para el análisis de Monte Carlo se ha considerado el escenario indicado en la Figura 51, las funciones de distribución indicadas en el párrafo anterior para las variaciones del  $V_{th}$  y las dimensiones (W/L) de los transistores y 50 iteraciones. Para este escenario se tienen en cuenta tres casos. El primer caso se hace considerando solo la variación del voltaje  $V_{th}$  de los transistores, el segundo cuando solamente varían las dimensiones de los transistores y el tercero considera la variación del  $V_{th}$  y de las dimensiones (W/L), simultáneamente. En estos tres casos se calculan las siguientes cantidades:

1. Variación de la función de transferencia del bloque que corresponde al circuito de Wiegierink (función logística) considerando que  $e(t)$  es una rampa que va de 10 a 100 micro amperes.
2. Variación de la función de transferencia del amplificador de ganancia  $\mu$ , considerando que se encuentra conectado al circuito de Wiegierink, y posee a su entrada una señal  $s(t)$  que es la salida del circuito de Wiegierink.

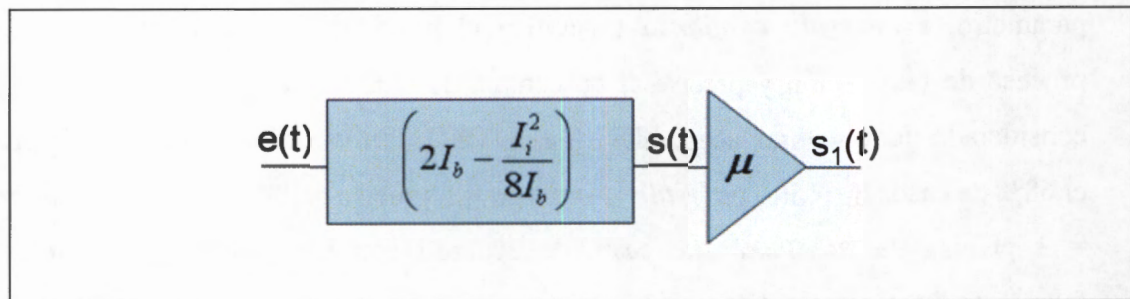
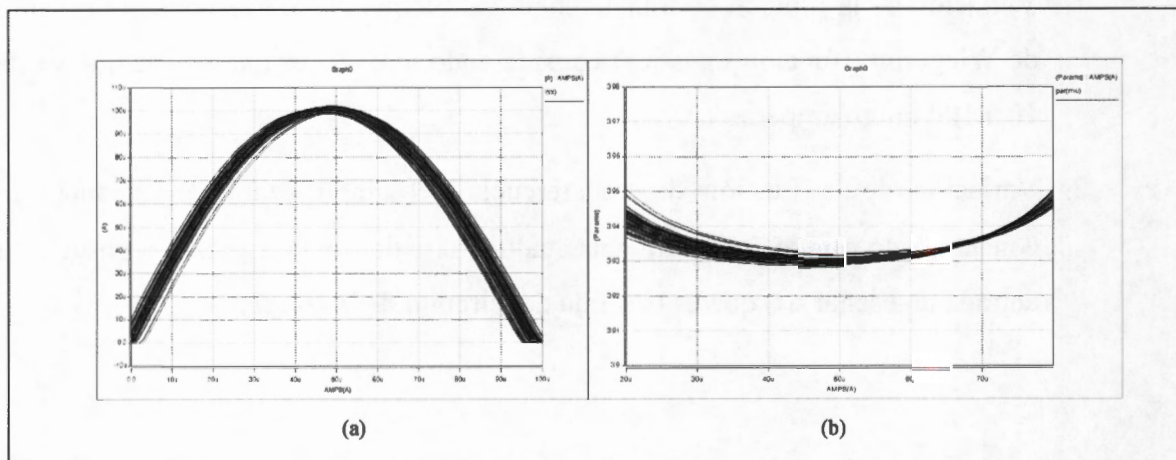


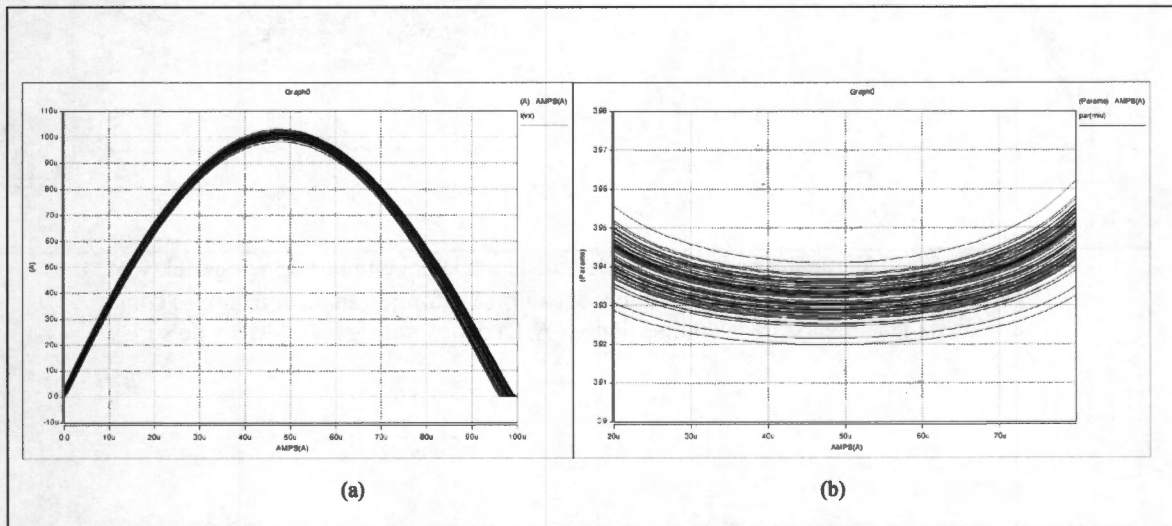
Figura 51. Diagrama a bloques de generador de ruido que describe el escenario para el análisis de Monte Carlo.

Se procedió a realizar el análisis para los bloques conectados de acuerdo con la Figura 51. La Figura 52 muestra las variaciones en la función de transferencia del circuito de Wiegink y las variaciones en la función de transferencia del amplificador de ganancia  $\mu$  de acuerdo con las variaciones en  $V_{th}$  según lo indicado en los párrafos anteriores. Esto es, *agauss* (0.4979, 0.01, 3) para el  $V_{th}$  del transistor tipo NMOS y *agauss*(-0.6915, 0.01, 3) para el  $V_{th}$  del transistor PMOS. La Figura 52 muestra que la variación de  $\mu$  en función de las variaciones de  $V_{th}$  es razonable, ya que el valor de  $\mu$  es siempre mayor que 3.87, por lo que el circuito no caerá en la isla de estabilidad de periodo 3 (ver Figura 18).



**Figura 52.** a) Variación de la función de transferencia del circuito de Wiegerink y b) Variación de la función de transferencia del amplificador de ganancia  $\mu$ , ambas como función de la variación de  $V_{th}$ .

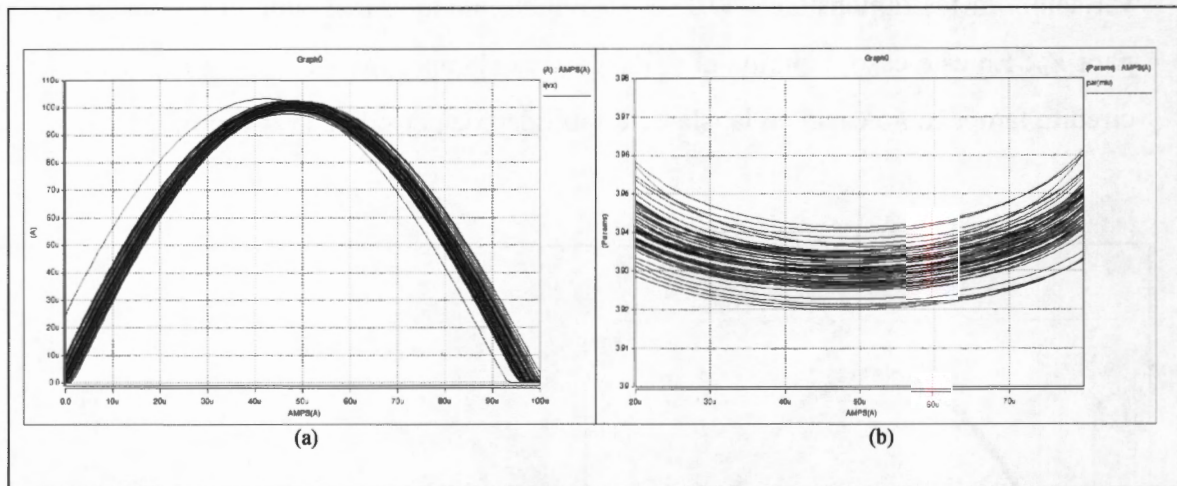
La Figura 53 muestra las variaciones en la función de transferencia del circuito de Wiegerink y las variaciones en la función de transferencia del amplificador de ganancia  $\mu$  de acuerdo con las variaciones en las dimensiones (W/L) según lo indicado en los párrafos anteriores. Esto es, *agauss(1, 0.01, 3)* para el valor del ancho W y largo L del canal del transistor MOS. La Figura 53 muestra que la variación de  $\mu$  en función de la variación en las dimensiones W/L es razonable, aunque más amplia que la variación para  $V_{th}$ . En este caso, también el valor de  $\mu$  es siempre mayor que 3.87, por lo que el circuito tampoco caerá en la isla de estabilidad de periodo 3 (ver Figura 18).



**Figura 53.** a) Variación de la función de transferencia del circuito de Wiegerink y b) Variación de la función de transferencia del amplificador de ganancia  $\mu$ , ambas como función de la variación de las dimensiones (W/L) de los transistores MOS.

La Figura 54 muestra las variaciones en la función de transferencia del circuito de Wiegerink y las variaciones en la función de transferencia del amplificador de ganancia

$\mu$  de acuerdo con las variaciones de ambas variables, las dimensiones (W/L) de los transistores y su  $V_{th}$ . Se consideran las mismas distribuciones indicadas en los párrafos anteriores pero ahora con efecto simultáneo. La Figura 54 muestra que la variación de  $\mu$  en función de las variaciones tanto de  $V_{th}$  como de W/L es razonable, ya que para este caso, el valor de  $\mu$  es siempre mayor que 3.87, por lo que el circuito tampoco caerá en la isla de estabilidad de periodo 3 (ver Figura 18).



**Figura 54.** a) Variación de la función de transferencia del circuito de Wiegerink y b) Variación de la función de transferencia del amplificador de ganancia  $\mu$ , ambas como función de la variación de las dimensiones (W/L) de los transistores MOS y de su  $V_{th}$ .

## CAPÍTULO 4: Comentarios y Conclusiones

### Resumen

Este capítulo presenta de inicio los hechos y consideraciones que se tuvieron en cuenta a lo largo de este trabajo de tesis, para luego presentar las conclusiones más relevantes de este trabajo. Se destaca la importancia del uso de la distribución invariante y el Teorema Ergódico en el diseño de generadores de señales de ruido. Finalmente, se incluye un apartado denominado "Trabajo a futuro" en el que se describe un conjunto de ideas que permiten mostrar que este tema sigue vigente y que el enfoque que se presenta en esta tesis permite la aplicación de esta teoría en otras áreas relacionadas con la protección de la información.

### 4.1 Hechos y Consideraciones

Las conclusiones se han establecido a partir de los siguientes hechos que se han puesto de manifiesto durante el desarrollo de este trabajo de tesis:

- a. Es posible diseñar con criterios objetivos un generador de ruido analógico, a partir de un circuito cuyo comportamiento puede modelarse usando un *mapeo* caótico unidimensional.
- b. Un generador de ruido analógico caótico como el que se presenta en esta tesis permite generar señales analógicas, cuya distribución estadística es tal que pueden usarse como señales de ruido, ya que contienen un número ilimitado de valores dentro del rango dinámico de operación del circuito. Por ello, es posible usarlos en sistemas analógicos de espectro disperso.
- c. Es posible conocer el comportamiento estadístico de estos generadores a través del cálculo numérico de su distribución invariante haciendo uso de la propiedad de mezclado de los *mapeos* caóticos unidimensionales como el *mapeo* logístico, haciendo uso del Teorema Ergódico de Birkhoff.

- d. En el análisis y diseño de un generador caótico de ruido analógico se han considerado como requerimientos el comportamiento estadístico y el rango dinámico de la señal de salida. Dado que en este caso se deben generar señales de ruido, es necesario considerar que el comportamiento estadístico debe tal que la señal de salida tenga una distribución estadística lo más cercano posible a una distribución uniforme. Por otro lado, el rango dinámico de la señal que se genera a la salida del generador caótico de ruido debe seleccionarse con atención y cuidado, pues de ello depende la adecuada interacción con circuitos de las otras etapas que conforman el sistema en el que se habrán de incluir estos generadores.
- e. El punto de partida para el diseño de este tipo de generadores es la posibilidad de seleccionar adecuadamente el valor de la ganancia en el lazo de retroalimentación del circuito. Al seleccionar esta ganancia es posible precisar el valor que tenga el parámetro que gobierna el comportamiento del circuito. Esta selección es posible a través del uso del diagrama de bifurcación y la distribución invariante del modelo matemático que gobierna el comportamiento del circuito.
- f. El Exponente de Lyapunov es una herramienta muy útil que permite determinar la estabilidad del sistema en cuestión. En esta tesis se abordaron dos maneras equivalentes de calcular numéricamente dicho exponente usando el Teorema Ergódico. En el primer caso se evalúa la derivada de la ecuación que describe el *mapeo* y usando para ello la órbita generada por el propio *mapeo*. En el segundo caso se asume que es posible estimar la distribución estadística de la señal de salida y empleando una partición regular. En este caso la función resultante se evalúa en el valor medio de cada intervalo de la partición definida.



## 4.2 Conclusiones finales

- a. En esta tesis se ha usado un circuito MOS translineal cuadrático, el cual rige su comportamiento a través del *mapeo* logístico, y opera en régimen de inversión fuerte en la región de saturación. Además del régimen de operación, el diseño de este circuito tiene como premisa importante el acoplamiento de dimensiones en los transistores MOS que utiliza. Esta premisa permitió obtener la función de transferencia del circuito, la cual se asoció con la ecuación del *mapeo* logístico generalizado. Si en los transistores que conforman el circuito existiera un desacoplamiento la función de transferencia puede ser sustancialmente diferente y no necesariamente seguiría el modelo del *mapeo* logístico.
- b. Siguiendo de manera general el mismo proceder que para el circuito MOS QT es posible usar circuitos cuyo comportamiento pueda modelarse por otros *mapeos* caóticos unidimensionales, identificando las zonas de estabilidad si las hubiere y precisando el comportamiento estadístico deseado y el rango dinámico de operación del circuito a diseñar o a analizar.
- c. Es posible determinar el comportamiento estadístico del circuito con criterios objetivos dados a partir del diagrama de bifurcación, la distribución estadística invariante y un valor apropiado del parámetro que gobierna el circuito. Para ello, una condición importante es evitar las islas de estabilidad, las cuales producen un comportamiento periódico no deseable.
- d. El uso de una generalización del *mapeo* logístico permite fijar el rango dinámico del circuito a su salida y modelar el comportamiento del circuito usando valores de corriente razonables desde el punto de vista de una implementación práctica.

- e. El procedimiento de diseño que se muestra en esta tesis es simple y garantiza la funcionalidad del generador de ruido analógico si se tiene atención en los aspectos de acoplamiento de transistores, rango dinámico y valor del parámetro que gobierna el comportamiento logístico. Sin embargo, cuando se quiere fabricar un circuito como este, se debe tener en cuenta las variaciones del  $V_{th}$  y de las dimensiones de los transistores, debidas al proceso de fabricación, ya que de eso depende, en este caso, el valor del parámetro que gobierna el comportamiento estadístico del circuito. En el apartado 3.6 de esta tesis se han mostrado los resultados obtenidos del análisis de Monte Carlo teniendo en cuenta los parámetros recomendados por la empresa *Austria Micro Systems*, y considerando variaciones sobre  $V_{th}$  y las dimensiones de los transistores. Estos resultados muestran que el valor de  $\mu$  que se seleccione debe estar muy por encima del valor superior de la isla de estabilidad de periodo 3, al menos en 0.04, ya que según el Teorema de Sharkowskii después de esa isla de estabilidad no habrá más regiones estables que generen señales periódicas. Estas variaciones definitivamente influyen en el comportamiento estadístico del circuito, el cual depende de la ganancia  $\mu$  del amplificador del lazo de retroalimentación.
- f. El diseño ciego y el diseño con predicción del comportamiento tienen problemas que pueden ser superados empleando las herramientas de la Mecánica Estadística con las que se analizan los sistemas dinámicos.
- g. El Diagrama de Bifurcación, el Teorema Ergódico, la Distribución Invariante y el Exponente de Lyapunov son las herramientas de la Mecánica Estadística que han resultado ser efectivas en el análisis y diseño de generadores caóticos de ruido analógico, ya que permiten establecer criterios objetivos.

- h. El diagrama de Bifurcación permite identificar las regiones en las que se producen señales no periódicas (caóticas) con una distribución de apariencia aleatoria. Además de que permite identificar los valores del parámetro para los cuales ocurre una bifurcación de funciones. Las vecindades de estas regiones se deben evitar ya que una pequeña variación en el parámetro que gobierna el comportamiento del circuito ocasionaría un cambio radical en la distribución estadística invariante del circuito, lo cual en la mayoría de los casos no es deseable que ocurra.
- i. El Exponente de Lyapunov determina con mayor precisión las islas de estabilidad y las regiones de comportamiento periódico, las cuales son no deseables en este caso. Sin embargo, es posible que en otros casos estas regiones sean de interés como en el caso en el que se pretenda diseñar un generador de funciones periódicas.
- j. Haciendo uso del Teorema Ergódico de Birkhoff es posible obtener las distribuciones estadísticas invariantes que el sistema puede producir, de manera que se puedan establecer los límites aceptables de variación debidos a los procesos de fabricación de los circuitos integrados y a las variaciones de los valores de los componentes.
- k. La propiedad de mezclado de un *mapeo* caótico unidimensional y la aplicación del Teorema Ergódico de Birkhoff permiten calcular numéricamente la distribución estadística invariante a partir de un ensemble arbitrario.
- l. El Exponente de Lyapunov y el Diagrama de Bifurcación permiten establecer los valores (intervalos) prohibidos que debe evitar el valor del parámetro del *mapeo*. Sin embargo, también pueden ayudar a construir un generador de señales arbitrarias, ya sea periódicas o aperiódicas.

- m. Se deben usar circuitos que siguiendo un comportamiento de acuerdo al *mapeo* logístico y con una estructura distinta, garanticen que serán superados los problemas derivados de la potencial falta de simetría (acoplamiento de transistores) en el circuito.
- n. Si se emplea un circuito que tenga un comportamiento que siga otro *mapeo* unidimensional caótico, como el *mapeo* de Bernoulli, es posible garantizar que una vez entrando al caos, el sistema no caerá en islas de estabilidad, aún a pesar de las variaciones en los componentes que conforman el circuito debidas al proceso de fabricación.

Finalmente, con esta tesis se ha mostrado también que las herramientas de mecánica estadística con las que se ha analizado el *Mapeo* Logístico (Diagrama de Bifurcación, Diagrama de Trayectorias y Exponente de Lyapunov) son útiles para determinar los criterios o premisas de diseño de circuitos generadores de ruido caótico.

### 4.3 Trabajo a Futuro

Considerando el diseño del generador analógico de ruido caótico realizado en esta tesis, es posible abordar la realización de generadores basados en otros *mapeos* caóticos como el *mapeo* de Bernoulli, el *mapeo* de carpa (tent map) o el *mapeo* senoidal, entre otros. El proceder sería el mismo que aquel que se presenta en esta tesis. Esto es, se analizaría detalladamente el *mapeo* en cuestión, a partir de herramientas tales como el diagrama de bifurcación, la distribución estadística, el Teorema Ergódico de Birkhoff y el Exponente de Lyapunov; después se buscaría un circuito electrónico que tenga una función de transferencia congruente con el *mapeo* que se utiliza, precisando sus condiciones de polarización y rango dinámico. Con esto, se procedería a escalar el *mapeo* con un modelo generalizado que permita diseñar un circuito que opere en condiciones reales de voltaje y corriente. Finalmente se aplicarían los criterios de

convergencia fuerte o divergencia de Kullback-Leibler para determinar, haciendo uso del Teorema Ergódico de Birkhoff, la distribución estadística de la señal producida por el generador de ruido.

Por otro lado, el estudio detallado para el *Mapeo* Logístico, presentado en el capítulo 2 de esta tesis, permite establecer nuevas líneas de investigación relacionadas con la protección de la información y no necesariamente relacionadas con la generación de ruido. Estas líneas de investigación pueden ser consideradas para abordarse en un futuro. Por ejemplo, se pueden aprovechar las características de dispersión que sobre una distribución inicial ejerce el *mapeo* logístico, o algún otro *mapeo*, para producir señales de espectro disperso o señales con marcas de agua. En este caso, un tema importante es aquel que se relaciona con la definición de las condiciones que permitan precisar la sincronía de los generadores de ruido que se ocupan en el transmisor y el receptor para un sistema de comunicaciones de espectro disperso, o aquellos que se usan en la etapa de inserción y extracción para los sistemas de marcas de agua.

También, los *mapeos* caóticos unidimensionales, dada su condición de unidireccionalidad, se pueden utilizar como funciones unidireccionales en las conocidas redes de Feistel que constituyen los cifradores de bloque. El uso de *mapeos* caóticos en cifradores de bloque permite contar con un parámetro adicional a la llave de cifrado. Este nuevo parámetro en el cifrador de bloque puede ser el parámetro que gobierna el comportamiento caótico del *mapeo*, pues de él depende la salida de la función unidireccional. Cabe hacer mención que para que este tipo de *mapeos* se puedan utilizar en cifradores de bloque se requiere de emplear un modelo discretizado y escalado del *mapeo*, lo que se traduce en la necesidad de realizar un estudio ampliado de los *mapeos*, ya que su intervalo de definición se debe escalar y precisar al conjunto de los números ASCII. En este caso, se debe considerar que el *mapeo* requerido para el cifrador de bloques es una aproximación al *mapeo* en cuestión, por lo que se debe tener en cuenta

el error que esta condición introduce sobre la generación de la órbita del *mapeo* y, por lo tanto, sobre el comportamiento caótico que tenga. Así, se debe calcular el diagrama de bifurcación y el Exponente de Lyapunov para esta aproximación del *mapeo* en cuestión. Resulta claro que el diagrama de bifurcación y el Exponente de Lyapunov serán una función de la aproximación con que se represente un número en una computadora.

Con lo discutido en esta sección se consideran tres posibles líneas de investigación como trabajo a futuro:

- a. **Diseño de generadores de ruido** basados en *mapeos* caóticos unidimensionales distintos al *mapeo* logístico. En particular, se considera de mucho interés el diseño de generadores de ruido basados en *mapeos* caóticos unidimensionales que no tengan islas de estabilidad, como el *mapeo* de Bernoulli. Este caso es de interés dadas las ventajas pudiera representar ante las variaciones de los circuitos y sus parámetros derivadas de los procesos de fabricación, y al no existir islas de estabilidad se evita el riesgo de que el generador de ruido genere, ante una pequeña variación en el circuito, un comportamiento periódico en lugar de un comportamiento caótico.
- b. **Diseño de sistemas de espectro disperso** para sistemas de comunicaciones y marcas de agua, aprovechando la condición de dispersión y mezclado de los *mapeos* caóticos unidimensionales.
- c. **Diseño de cifradores de bloque**, en los cuales existan redes de Feistel cuyas funciones unidireccionales sean *mapeos* caóticos unidimensionales. Para esta línea de investigación se hace necesario abordar el estudio de las aproximaciones discretizadas y escaladas de dichos *mapeos*.

## Bibliografía

1. M. Schroeder; "Fractals, Chaos, Power Laws: Minutes from an Infinite Paradise"; W.H. Freeman & Co., 1991, pp. 264-265.
2. Levine and Steinhardt; "Quasicrystals I, definitions and Structure"; Phys.Rev B34 (2), pp 596; 1986
3. Socolar and Steinhardt; "Quasicrystals II, unit cell configurations", Physic. Rev B 34 (2), pp 617; 1986
4. Preneel B., El estado de las funciones hash, Criptología y Seguridad de la Información, VI RECSI, Editorial Ra-ma, Tenerife, Islas Canarias, pag 3-37, Septiembre 2000.
5. Merkle R., One way hash functions and DES, Advances in Cryptology-Crypto 89 Proceedings, Lecture Notes in Computer Science Vol. 435, G. Brassard ed., Springer-Verlag, 1989.
6. Pieprzyk J., Sadeghiyan Babak, Design of hashing algorithms, Lecture Notes in Computer Science 756, Springer-Verlang, Berlin Heidelberg, Germany, 1993.
7. Devaney, R.L. "An Introduction to Chaotic Dynamical Systems", Addison-Wesley, Second Edition, 1989.
8. L. Cong and S. Songgeng: "Chaotic Frequency Hopping Sequences", IEEE Transactions on Communications, Vol. 46, No. 11, Nov. 1998. pp 1433-1437.
9. A. Tefas, A. Nikolaidis, N. Nikolaidis, V. Solachidis, S. Tsekeridou, I. Pitas: "Statistical Analysis Of Markov Chaotic Sequences For Watermarking Applications", Department of Informatic in Aristotle University of Thessaloniki, Grecia (2001).

10. N. Matsuda and K. Aihara, "Cryptosystems with discretized Chaotic Maps", IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications, Vol 49, No. 1, January 2002, 28-40
11. S. Tsekeridou, V. Solachidis, N. Nikolaidis, A. Nikolaidis, A. Tefas and I. Pitas, "Theoretic Investigation on the use of Watermak Signals Derived from Bernoulli Chaotic Sequences", Department of Informatic in Aristotle University of Thessaloniki, Grecia 2003.
12. Z. Li, K. Li, C. Wen and Y. Chai Soh: "A New Chaotic Secure Communication System", IEEE Transactions on Communications, Vol 51, No. 8, August 2003, 1306-1312.
13. Ninan Sajeeth P. and K. Babu J., "Chaos for Stream Cipher", Department of Phisycs, Cochin University of Science and Technology, Kochi, India, 2004
14. J. Szczepanski, J. M. Amigó T. Michalek and L. Kocarev, "Cryptographically Secure Substitutions based on the Approximation of Mixing Maps", IEEE Transactions on Circuits and Systems.I: Regular papers, Vol 52, No. 2, February 2005, 443-453.
15. A. Tsuneda, "Design of Binary Sequences with tunable Exponential Autocorrelations and Run Statistics Based on One-Dimensional Chaotic Maps", IEEE Transactions on Circuits and Systems.I: Regular papers, Vol 52, No. 2, February 2005, 454-462.
16. A. G. Radwan, A. M. Soliman and A. El-Sedeek, "MOS realization of the modified Lorenz chaotic system", Chaos, Solitons & Fractals, Elsevier, Vol. 21, Issue 3, pp. 553-561, July 2004.



17. H. Tanaka, S. Sato and K. Nakajima, "Integrated Circuits of Map Chaos Generators", *Analog Integrated Circuits and Signal Processing*; Springer Netherlands, Vol. 25, No. 3, Dec. 2000, pp. 329-335, on line Oct. 28, 2004.
18. Q. Ding, Y. Zhu, F. Zhang and X. Peng, "Discrete Chaotic Circuit and the Property Analysis of Output Sequence", *Proc. of ISCIT 2005*, pp. 1009-1012, IEEE 2005.
19. A. Fort, F. Cortigiani, S. Rocchi and V. Vignoli, "Very High Speed True Random Noise Generator, *Analog Integrated Circuits and Signal Processing*", 34, pp. 97-105, Kluwer Academic Publisher, 2003.
20. A. Rodríguez-Vázquez, J.L. Huertas, A. Rueda and B. Pérez-Verdú: "Chaos from Switched-Capacitor Circuits: Discrete Maps", *Proc. of the IEEE*, Vol. 75, pp. 1090-1106, Aug. 1987.
21. A. Rodríguez-Vázquez, S. Espejo, J.L. Huertas and J.D. Martín: "Analog Building Blocks for Noise and Truly Random Number Generation in CMOS VLSI", *Proc. of the Solid-State Circuits Conference*, pp. 229-232, Frontières, Sept. 1992.
22. A. Rodríguez-Vázquez, M. Delgado-Restituto, S. Espejo and J.L. Huertas: "Switched-Capacitor Broadband Noise Generator for CMOS VLSI", *Electr. Lett.*, Vol. 27, pp. 1913-1915, Oct. 1991.
23. M. Delgado-Restituto, A. Rodríguez-Vázquez, S. Espejo and J.L. Huertas: "A Chaotic Switched-Capacitor Circuit for  $1/f$  Noise Generation", *IEEE Trans. Circuits and Systems*, Vol. 39, pp. 325-328, April 1992.

24. R. M. May and G. F. Oster, "Bifurcation and Dynamic Complexity in Simple Ecological Models", *American Naturalist*, Vol. 110, Issue 974, Jul-Aug, 1976, pp. 573-599, <http://www.jstor.org>.
25. R. M. May "Simple Mathematical Models with very complicated dynamics", *Nature*, Vol. 261, June 10, 1976, pp. 459-467.
26. Delmas, Bernard, "Pierre-François Verhulst and the logistic law of population", *Mathematics and Social Science* No. 167, 2004.
27. Raymond Pearl and Lowell J. Redd, "On the Rate of Growth of the Population of the United States since 1790 and its Mathematical Representation", *Proceedings of the National Academy of Sciences*, Vol 6, No. 6. June 15, 1920, pp 275-288.
28. von Neumann J. "Various Techniques used in Connection with Random Digits. In A.S. Householder, G.E. Forsythe, and H.H. Germond, eds., *Monte Carlo Method*, Applied Mathematics Series, 12, US National Bureau of Standards, pp 36-38.
29. S. L. Ulam and J. von Neumann, "On combination of stochastic and deterministic processes", *Bull. Amer. Math. Soc.* 53 (1947) 1120.
30. Ricker, W.E. 1954, "Stock and recruitment", *J. Fisheries Res. Board Can* 11: 559-623.
31. Paul R. Stein and Stanislaw Ulam, "Non-linear transformation studies on electronic computers" \* *Rozprawy Matematyczne* 39 (1963): 1-66. URL: <http://content.cdlib.org/xtf/view?docId=ft9g50091s&chunk.id=d0e575&toc.id=d0e32079&brand=eschol>.

32. N. Metropolis, M. L. Stein, P. R. Stein: On Finite Limit Sets for Transformations on the Unit Interval. *J. Comb. Theory, Ser. A*, 15 (1973), pp. 25-44.
33. S. Grossmann and S. Thomaes, Invariant distribution and Stationary correlation functions of the one dimensional discrete processes, *Zeitschrift für Naturforschg.* 32 A (1977) 1353-1363.
34. Feigenbaum, M. J. "Quantitative Universality for a Class of Non-Linear Transformations." *J. Stat. Phys.* 19, 25-52, 1978
35. Feigenbaum, M. J. "The Metric Universal Properties of Period Doubling Bifurcations and the Spectrum for a Route to Turbulence", *Ann. New York. Acad. Sci.* 357, pp. 330-336, 1980.
36. Gerald Schueler, "Chaos Theory: Interface with Jungian Psychology: The Order/Chaos Relationship in Complex Systems", 1997. URL: <http://www.schuelers.com/chaos/chaos1.htm>
37. Torres Agudo, J., Física No lineal : Caos y Universalidad, Universidad de Granada, España, Grupo de Neurofísica, <http://www.ugr.es/~jtorres/FNtema41.pdf>, pp 1-48.
38. HN Nuñez Yépez et al., Chaos in Dripping Faucet, *Eur. J. Phys.* 10, 99-105, 1989.
39. Ayer, Elizabeth, and Carter Butts. 1993. Finding Order in Chaos. *Vertices* 9(2): 14-17. URL: <http://www.duke.edu/vertices/spr93/chaos.html>.
40. E. Piña, "Order in the Chaotic Region", *Lecture Notes in Physics* Vol. 189 (1983) pp 402-415, Book Chapter, DOI: 10.1007/3-540-12730-5\_23, Book: *Nonlinear Phenomena*, Edited by B. Wolf, Springer Verlag, Berlin.

41. Berge, P., Pomeau, Y., and Vidal, C. Order within Chaos: towards a deterministic approach to Turbulence, New York: Wiley, 1986
42. R. L. Devaney, An introduction to chaotic dynamical systems, second edition (Addison-Wesley: New York, 1989).
43. E. Ott, "Chaos in Dynamical Systems", Cambridge University Press, 2002.
44. A. González, "Dynamical behaviour arising in the adaptive control of the generalized logistic map", Chaos, Solitons & Fractals, Elsevier, Vol. 8, Issue 9, pp. 1485-1488, Sept. 1997.
45. Feigenbaum, M. J. "Home Page", The Rockefeller University, 2007, URL: <http://www.rockefeller.edu/research/abstract.php?id=38>.
46. Feigenbaum M. J. Universal behavior in nonlinear systems. *Universality in chaos. Bristol: Adam Hilger.. 1984. 49-84.*
47. Feigenbaum, M. J. "The Universal Metric Properties of Nonlinear Transformations." J. Stat. Phys. 21, 669-706, 1979.
48. Munafo, R. "Mandelbrot Set Glossary and Encyclopedia", <http://ww.mrob.com>, 1996-2008. s.13.
49. Eric W. Weisstein, "Feigenbaum Constant", Math World, National Science Foundation's National Science Digital Library, Wikipedia (2007) URL: [http://en.wikipedia.org/wiki/Feigenbaum\\_constants](http://en.wikipedia.org/wiki/Feigenbaum_constants).
50. Briggs, K. "Simple experiments in chaotic dynamics", Am. J. Phys. 55, 1083-1089.
51. Jensen, H.D.; Larsen, A. and Mygind J.; "Mutual locking, chaos and devils staircase in two Josephson tunnel junction with a common resistive shunt"; IEEE Transaction on Magnetics, Vol. 25, No. 2, March 1989, pp 1412-1415.

52. Cvitanovic P. "Universality in Chaos", NORDITA, 2a Edition, ISBN10 0852742606, ISBN13 9780852742600, 1989.
53. Briggs, K. "A Precise Calculation of the Feigenbaum Constants." Math. Comput. 57, 435-439, 1991.
54. Briggs, K "Feigenbaum Scaling in Discrete Dynamical Systems", Department of Physics of the University of Western Australia, 1997.
55. David Broadhurst, "Feigenbaum constants to 1018 decimal places, March 22, 1999, collection of math constants server, Plouffe's Inverter, URL: <http://pi.lacim.uqam.ca/piDATA/feigenbaum.txt>.
56. Cullen, H. F., "Introduction to General Topology". Boston, MA: Heath, pp. 78-81, 1968.
57. Medio A. and Linez M. "Nonlinear Dynamics: A premier", Cambridge University Press, ISBN 0 521 55186 2, 2001, pp 216-217.
58. Thom, R., "Topological models in biology", Topology 8: 313-335, (1969)
59. Thom, R. F., "Topological models in biology", In Waddington, Towards a Theoretical Biology, vol. 3, 89—116 (1970).
60. Rene Thom, "Catastrophe Theory," Nature Vol. 270, No. 5639, pp 658 (22 Dec 1977) doi:10.1038/270658a0 and Nature 270, No. 5636, Letters, 381-4 (1 Dec 1977)
61. Chris C. King, "Fractal and Chaotic Dynamics in Nervous Systems", 1991 Progress in Neurobiology 36 279-308
62. Birkhoff, G. D. "Proof of the Ergodic Theorem", Proc. of the Nat Acad. Sci. USA 17 (1931), pp 656-660.

63. Boyarsky, A. and Gora, P. "Laws of Chaos: Invariant Measures and Dynamical Systems in One Dimension", Birkhäuser Boston, 1997, pp. 40-41.
64. Rudolph, D. J. "Fundamentals of measurable dynamics: Ergodic theory on Lebesgue spaces", Oxford Science Publications, The Clarendon Press, Oxford University Press, New York, 1990.
65. Birkhoff, G. D. "Proof of the Ergodic Theorem", Proc. of the Nat Acad. Sci. USA 17 (1931), pp 656-660.
66. Barbashin, E.A, Krasovskii, N. N. , On the stability of motion as a whole, (Russian), Dokl. Akad. Nauk, 86, pp.453-456, 1952.
67. Krasovskii, N. N. Problems of the Theory of Stability of Motion, (Russian), 1959. English translation: Stanford University Press, Stanford, CA, 1963.
68. Lasalle, J.P. Some extensions of Lyapunov's second method, IRE Transactions on Circuit Theory, CT-7, pp. 520-527, 1960.
69. A. Lassota and M.C. Mackey, "Chaos Fractals and Noise: Stochastic Aspects of Dynamics", Springer Verlag 1994, Second Edition, 1985, ISBN 0-387-94049-9
70. Ruelle, D. "*Chance and chaos*", Princeton, NJ: Princeton University Press, (1991).
71. Wiener, N., "The homogeneous chaos", Am. J. Math. 60 (1938), 897-936.
72. Wiener, N. and Wintner A. "The discrete chaos", Am. J. Math. 65, 279-298; Math. Rev. 4 (1943), 220.
73. Shaposhnikova T., Polyshchuk E., "Jacques Hadamard, Nauka, Leningrad", 1990.

74. Maz'ya V., Shaposhnikova T., "Jacques Hadamard, a Universal Mathematician", American Mathematical Society and London Mathematical Society, 1998.
75. Kellert, S.H., "*In the wake of chaos: Unpredictable order in dynamical systems*", Chicago: The University of Chicago Press, (1993).
76. Packard, Norman, "Adaption Toward the Edge of Chaos", 1988
77. Waldrop, M. M., "*Complexity: The emerging science at the edge of order and chaos*", New York: Simon & Schuster, (1992).
78. Annick Lesne; "Renormalization Methods: Critical Phenomena, Chaos, Fractal Structures"; John Wiley & Sons Ltd. 1998.
79. Smith, P., "Explaining Chaos", Cambridge University Press, 1999, ISBN 0 521 47747 6.
80. Eckmann, J. P. , Thomas, L., Wittwer, P.; "Intermittency in the presence of Noise"; Journal of Physics A: Mathematical and General, Vol. 14, Issue 12, pp 3153-3168, 1981.
81. A. S. Pikosvky; "A new type of intermittent transition to chaos"; Journal of Physics A: Mathematical and General, Vol. 16, Issue 4, 1983, pp L109.
82. Rand D., Ostlund S., Sethna J. And Siggia E., "Universal transition from quasiperiodicity to chaos in dissipative systems", Phys. Rev. Lett., 49, pp 132, 1982.
83. M. Xua, "Property of period-doubling bifurcation cascades of discrete dynamical systems", Chaos, Solitons & Fractals; Elsevier, Vol. 33, Issue 2, pp. 455-462, July 2007, Available online 28 Feb. 2006.

84. Briggs, K. "How to Calculate the Feigenbaum Constants on Your PC." Austral. Math. Soc. Gaz. 16, pp. 89-92, 1989.
85. Feigenbaum, M. J. "The Universal Metric Properties of Nonlinear Transformations", J. Stat. Phys. 21, pp. 669-706, 1979.
86. G. Elert, "Measuring Chaos", The Chaos Hypertextbook, 2005.
87. Dewdney, A. K. "Mathematical Recreations: Leaping into Lyapunov Space", Sci. American, Sept. 1991.
88. Hofstadter, Douglas R. "Metamagical Themas: Questing for the Essence of Mind and Pattern", New York: Basic Books, 1985.
89. A. Pikovsky and M. Rosenblum, "Comment on Intermittency in Chaotic Rotations", Phys. Rev. E 64, 058203, 2001.
90. J. San Martín, "Intermittency cascade", Chaos, Solitons & Fractals, Elsevier, Vol. 32, Issue 2, pp. 816-831, April 2007.
91. C. Jeffries and J. Perez, "Observation of a Pomeau-Manneville intermittent route to chaos in a nonlinear oscillator", Phys. Rev. A 26, pp. 2117-2122, 1982.
92. H.L. Yang and E.J. Ding, "On-off intermittency in random map lattices", Phys. Rev. E 50, R3295 - R3298, 1994.
93. Y. B. Pesin, Characteristic Lyapunov Exponents and Smooth Ergodic Theory, Russian Math. Surveys, 32 (1977), 4, 55-114
94. Salman Habib and Robert D. Ryne. "Symplectic Calculation of Lyapunov Exponents". Physical Review Letters 74: 70-73, (1995).



95. T. Hondou and Y. Sawada “Dynamical Behavior of a Dissipative Particle in a Periodic Potential Subject to Chaotic Noise: Retrieval of Chaotic Determinism with Broken Parity”, *Phys. Rev. Lett.* 75, pp. 3269 - 3272, Issue 18, Oct. 1995.
96. Goloubentsev, A.F.; Anikin, V.M.; Barulina, Y.A. “Chaotic maps generating white noise”; *Proc. of the Int. Conf. on Phys. and Control*, Vol. 2, Issue 20-22, pp. 452–455, 2003.
97. M. Eisencrafta and L. Antonio Baccalá, “The Cramer-Rao bound for initial conditions estimation of chaotic orbits”, *Chaos, Solitons & Fractals*, Elsevier, April 2007.
98. A. Mooneya, J. G. Keatinga, and I. Pitasb; “A comparative study of chaotic and white noise signals in digital watermarking”; *Chaos, Solitons & Fractals*, Elsevier, July 2006.
99. R. J. Wiegierink, “Analysis and synthesis of MOS translinear circuits”, Kluwer Academic Publishers: USA, 1993, pp. 109-113. ISBN 0-7923-9390-2.
100. R. J. Wiegierink, “A CMOS Four-Quadrant Analog Current Multiplier”, *IEEE ISCAS –Conference*, Singapore, June 1991, pp. 2244-2247.
101. K. Kubota et al. “Logistic Generalized Map”, <http://www.usrv.rdu/Kubota.htm>, Oct. 2007.
102. Mahesh C Shastry, “The B-Exponential Map: A Generalization of the Logistic Map and Its Applications In Generating Pseudo-random Numbers”; available at [http://arxiv.org/PS\\_cache/cs/pdf/0607/0607069v2.pdf](http://arxiv.org/PS_cache/cs/pdf/0607/0607069v2.pdf), July 17, 2006.
103. John Walker; “ENT: A Pseudorandom Number Sequence Test Program”; <http://www.fourmilab.ch/random/>, consultado en Noviembre de 2007.

104. A Rukhin et. al.; "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications"; NIST Special Publication 800-22, with revisions dated May 15, 2001
105. G Marsaglia; "The Diehard Battery of Tests of Randomness", available online at: <http://www.csis.hku.hk/~diehard/index.html>, Nov. 2007.
106. R. Tonelli and M. Coraddu, "Numerical Study of the Oscillatory Convergence to the Attractor at the Edge of Chaos"; Vol. 50, No. 1-2, pp. 355-359, Springer Berlin/Heidelberg, March, 2006.
107. K. Kazuomi , M. Yoichi and A. Kazuyuki, "A Study on the Dynamics of a Generalized Logistic Map"; IEICE Trans. on Fund. of Electr., Comms. and Comp. Sci., Vol.E83-A, No.3 (20000325), pp. 524-531, IEICE, ISSN:09168508.
108. K. Yoshida and S. Saito, "Analytical Study of the Julia Set of a Coupled Generalized Logistic Map"; eprint arXiv:solv-int/9805001; ARXIV, 1998.
109. R. Matthews, "On the derivation of a Chaotic Encryption Algorithm", Cryptology, Vol. XIII, No. 1, 1989 - Taylor & Francis, pp. 29-42.
110. Leenaerts, D.M.W, G.H.M Joordens and J. A. Hegt, "A 3.3V 625kHz switched-current multiplier", IEEE J. Solid State Circuits, 1996. 31: pp 1340-1343.
111. Gilbert, B.; "A precise four quadrant multiplier with subnanosecond response", IEEE J. Solid- State Circuits, 1968, SC-3: pp 365-375.
112. Pena-Finol, J.S. and J.A. Connelly, "A MOS four-quadrant analog multiplier using quarter-square technique", IEEE J. Solid-State Circuits. SC-22: pp 1064-1073, 1987.

113. Yamasuto, M. and T. Enomoto, "Integrated MOS Four-quadrant analog multiplier using switched-capacitor technique", *Electronics Letters* 18: pp 769-771, 1982.
114. Tomazou, C.F., F.J. Lidgely, and D.G. Haigh; "Analogue IC design: the current-mode approach", London: Peter Peregrinus, 1990.
115. Vázquez-Medina, R.; Díaz-Méndez, A.; Del Río-Correa, J.L; López-Hernández, J; "Designo f Chaotic Analog Noise Generators Witg Logistic Map and MOS QT Cirtcuits"; *Chaos, Solitons & Fractals* (2007), doi:10.1016/j.chaos.2007.09.088.
116. López-Hernández, J.; Díaz-Méndez, J. A. and Reyes-García, C. A. "Logmap Based Analog Random Number Generator," *Circuit and Systems*, 2006. MWSCAS'06, San Juan de Puerto Rico. 49th IEEE International Midwest Symposium. 6-9 August 2006, Vol. 1, pp 327-330. ISSN 1548-3746, ISBN 1-4244-0173-9, DOI: 10.1109/MWSCAS.2006.382063.
117. E. Seevinck, "Analysis and Synthesis of Translinear Integrated Circuits", Elsevier Science Publishers, Amsterdam, 1988.
118. A. G. Andreou and K. A. Boahen, "Translinear Circuits in Subthreshold MOS", *Analog Integrated Circuits and Signal Processing*, Springer Netherlands, Vol. 9, pp. 141-166, 1996.
119. J. A de Lima, "Desing of a micropower CMOS four-quadrant multiplier based on the translinear principle", *Proc. of the ESSCIRC*, 1989, pp. 260-263.

120. B. Gilbert, "Translinear Circuits: An Historical Overview", Analog Integrated Circuits and Signal Processing, 9, Kluwer Academic Publishers, pp. 95-118, 1996.
121. C. G. Garrett and W.H. Brattain "Self-Powered Semiconductor Amplifier" Physical Review 95, pp 1091-1092. 1954.
122. C. G. Garrett and W.H. Brattain "Physical Theory of Semiconductor Surfaces" Physical Review 99, pp 376-387. 1955.

## Índice de figuras

	Página
Figura 1. Diagrama a bloques de un cifrador de flujo.....	23
Figura 2. Diagrama a bloques de sistemas de comunicaciones de Espectro Disperso Secuencia Directa.	23
Figura 3. Diagrama a bloques de sistemas de comunicaciones de Espectro Disperso por Salto de Frecuencias. ....	24
Figura 4. Diagrama a bloques de un sistema de marcas de agua. ....	24
Figura 5. Familia de curvas para el <i>Mapeo</i> Logístico para parámetros desde $\mu = 1$ hasta $\mu = 4$ .....	31
Figura 6. Comportamiento de la órbita con dos condiciones iniciales con $\delta=0.3$ para el <i>Mapeo</i> Logístico .....	35
Figura 7. Diagrama de Bifurcación del <i>Mapeo</i> Logístico .....	35
Figura 8. Comportamiento de $\varepsilon_n$ y $\varepsilon_{2n}$ para el <i>Mapeo</i> Logístico cuando $\mu = 3.75$ .....	49
Figura 9. Media y desviación estándar de $\varepsilon_n$ para el <i>Mapeo</i> Logístico cuando $\mu = 3.75$ .....	50
Figura 10. Distribución Invariante para el <i>Mapeo</i> Logístico cuando $\mu = 3.75$ .....	50
Figura 11. Divergencia de Kullback-Leibler para el <i>Mapeo</i> Logístico cuando el valor del parámetro es $\mu = 3.75$ . (a) Divergencia de Kullback-Leibler entre la distribución de la iteración $n-1$ , $\rho_{n-1}$ , y la distribución de la iteración $n-2$ , $\rho_{n-2}$ . (b) Divergencia de Kullback-Leibler entre la distribución de la iteración $n-2$ , $\rho_{n-2}$ , y la distribución de la iteración $n-1$ , $\rho_{n-1}$ . ....	54
Figura 12. Gráficas del <i>Mapeo</i> Logístico para $\mu=2.5$ : (a) Diagrama de Trayectorias, (b) Diagrama de bifurcación y (c) Densidad de Probabilidad.....	56
Figura 13. Gráficas del <i>Mapeo</i> Logístico para $\mu=3.2$ : (a) Diagrama de Trayectorias, (b) Diagrama de bifurcación y (c) Densidad de Probabilidad.....	57
Figura 14. Gráficas del <i>Mapeo</i> Logístico para $\mu=3.5$ : (a) Diagrama de Trayectorias, (b) Diagrama de bifurcación y (c) Densidad de Probabilidad.....	58
Figura 15. Gráficas del <i>Mapeo</i> Logístico para $\mu=3.56$ : (a) Diagrama de Trayectorias, (b) Diagrama de bifurcación y (c) Densidad de Probabilidad.....	59
Figura 16. Gráficas del <i>Mapeo</i> Logístico para $\mu=4.0$ : (a) Diagrama de Trayectorias para 1000 iteraciones, (b) Diagrama de Trayectorias para 5000 iteraciones, (c) Diagrama de bifurcación y (d) Densidad de Probabilidad. ....	60
Figura 17. Idea intuitiva del proceso de bifurcación y cambio de la condición de los conjuntos atractores estables a conjuntos inestables .....	63
Figura 18. Diagrama de Bifurcación del <i>Mapeo</i> Logístico para $\mu \in (2.8, 4.0)$ .....	65
Figura 19. Órbitas generadas por el <i>Mapeo</i> Logístico para diferentes valores del parámetro $\mu$ .....	66
Figura 20. Acercamientos en el diagrama de bifurcación para apreciar el comportamiento autosimilar..	67
Figura 21. Interpretación de la constante de Feigenbaum.....	69
Figura 22. Diagramas de Bifurcación para el <i>Mapeo</i> Logístico de $\mu = \mu_\infty$ a $\mu = 4.0$ . ....	70
Figura 23. Diagrama de Bifurcación en la isla de estabilidad para $R = 3, 4, 5$ y $6$ . ....	71
Figura 24. Diagramas de Bifurcación para el <i>Mapeo</i> Logístico de $\mu = \mu_\infty$ a $\mu = 4.0$ . ....	73
Figura 25. Gráficas de densidad de probabilidad del <i>Mapeo</i> Logístico para diferentes valores del parámetro. a) $\mu = 4.0$ b) $\mu = m_1$ . c) $\mu = m_2$ . b) $\mu = m_3$ .....	74
Figura 26. Gráficas de las órbitas del <i>Mapeo</i> Logístico para diferentes valores del parámetro. a) $\mu = 4.0$ b) $\mu = m_1$ . c) $\mu = m_2$ . b) $\mu = m_3$ .....	75

Figura 27. Gráficas de densidad de probabilidad del <i>Mapeo</i> Logístico para un valor del parámetro $\mu = 3.5925$ , observando a) Todo el intervalo de definición, b) El intervalo (0.3, 0.6) y c) El intervalo (0.78, 0.90).	76
Figura 28. Densidad de probabilidad del <i>Mapeo</i> Logístico para un valor del parámetro $\mu = 3.5925$ . Observando a) Todo el intervalo de definición, b) El intervalo (0.33, 0.39). c) El intervalo (0.46, 0.57), d) El intervalo (0.80, 0.85). e) El intervalo (0.875, 0.895).	77
Figura 29. Exponente de Lyapunov para el <i>Mapeo</i> Logístico. a) $\mu \in (0, 4)$ . b) $\mu \in (3, 4)$ .	81
Figura 30. Órbitas generadas con el <i>Mapeo</i> Logístico usando dos condiciones iniciales muy cercanas.	84
Figura 31. Diferencia entre las órbitas generadas con el <i>Mapeo</i> Logístico usando dos condiciones iniciales muy cercanas $x_0 = 0.24$ y $x_\delta = 0.240001$ . a) $\mu = 4.0$ y b) para $\mu = 3.9$ .	85
Figura 32. Número de intervalos alcanzados en función del número de iteraciones del <i>Mapeo</i> Logístico para una partición de 10 subintervalos con $\mu = 4.0$ .	86
Figura 33. Comportamiento de $\varepsilon_n$ para el <i>Mapeo</i> Logístico cuando $\mu = 4.0$ .	87
Figura 34. Manifestación de la Propiedad de Mezclado para el <i>Mapeo</i> Logístico cuando $\mu = 4.0$ , usando los intervalos $I$ y $J$ , una condición inicial $x_0 = 0.23$ .	88
Figura 35. Densidad de la distribución inicial uniforme en $I = [0.2, 0.2 + 1 \times 10^{-11}]$ y distribución final en el intervalo objetivo $J = [0.68, 0.69]$ para el <i>Mapeo</i> Logístico cuando $\mu = 4.0$ con 100 iteraciones.	89
Figura 36. Sobrevivientes en función del número de iteraciones para el <i>Mapeo</i> Logístico cuando $\mu = 4.0$ , usando una distribución uniforme en $(0.2, 0.2 \times 10^{-11})$ de 10000 condiciones iniciales.	90
Figura 37. Gráfica lineal para el Número de Sobrevivientes en función del número de iteraciones para el <i>Mapeo</i> Logístico cuando $\mu = 4.0$ y la curva de aproximación con la ecuación (43).	91
Figura 38. Gráfica semilog para el Número de Sobrevivientes en función del número de iteraciones para el <i>Mapeo</i> Logístico cuando $\mu = 4.0$ y la curva de aproximación con la ecuación (43).	92
Figura 39. Gráfica para el Número de Sobrevivientes en función del número de iteraciones para el <i>Mapeo</i> Logístico cuando $\mu = 4.0$ , acotado al intervalo de iteraciones (50, 400). a) Lineal. b) Semilog.	93
Figura 40. Sobrevivientes en función de la localización del Intervalo $I$ para el <i>Mapeo</i> Logístico cuando $\mu = 4.0$ .	94
Figura 41. Sobrevivientes en función del tamaño del intervalo $I$ para el <i>Mapeo</i> Logístico cuando $\mu = 4.0$ .	94
Figura 42. Diagrama de bifurcación para el <i>Mapeo</i> Logístico Generalizado, a) $\mu \in (0, 4)$ . b) $\mu \in (2.4, 4)$ .	102
Figura 43. Circuito MOS Cuadrático Translineal de Wiegierink.	104
Figura 44. Diagrama a bloques de un circuito retroalimentado para lograr la iteración de la función de transferencia con una línea de retardo.	107
Figura 45. Diagrama del circuito amplificador de ganancia $\mu$ .	108
Figura 46. Respuesta en tiempo de un circuito MOS QT de Wiegierink.	115
Figura 47. Respuesta en tiempo del circuito generador de ruido para $\mu = 3.2$ .	117
Figura 48. Respuesta en tiempo del circuito generador de ruido para $\mu = 3.5$ .	117
Figura 49. Respuesta en tiempo del circuito generador de ruido para $\mu = 3.92$ .	118
Figura 50. Respuesta en tiempo del circuito generador de ruido para $\mu = 4.0$ .	118
Figura 51. Diagrama a bloques de generador de ruido que describe el escenario para el análisis de Monte Carlo.	122
Figura 52. a) Variación de la función de transferencia del circuito de Wiegierink y b) Variación de la función de transferencia del amplificador de ganancia $\mu$ , ambas como función de la variación de $V_{th}$ .	123

Figura 53. a) Variación de la función de transferencia del circuito de Wiegerink y b) Variación de la función de transferencia del amplificador de ganancia  $\mu$ , ambas como función de la variación de las dimensiones (W/L) de los transistores MOS..... 123

Figura 54. a) Variación de la función de transferencia del circuito de Wiegerink y b) Variación de la función de transferencia del amplificador de ganancia  $\mu$ , ambas como función de la variación de las dimensiones (W/L) de los transistores MOS y de su  $V_{th}$ ..... 124

Figura 55. Diagrama de bifurcación del *Mapeo* Logístico para valores de parámetro entre 2.8 y 4.0.... 154

Figura 56. Diagrama de bifurcación del *Mapeo* Senoidal para valores de parámetro entre 0.7 y 1.0..... 154





## Índice de Tablas

	<b>Página</b>
Tabla 1. Valores de $\mu$ para los que ocurre el doblamiento del periodo.....	38
Tabla 2. Valores del parámetro en los que ocurre la bifurcación de regiones.....	73
Tabla 3. Intervalos alcanzados en función del número de iteraciones del <i>Mapeo</i> Logístico para una partición de 10 subintervalos con $\mu = 4.0$ .....	87
Tabla 4. Sobrevivientes en función del número de iteraciones para el <i>Mapeo</i> Logístico cuando $\mu = 4.0$ , usando una distribución uniforme en $(0.2, 0.2 \times 10^{-11})$ de 10000 condiciones iniciales, para la iteración 36 a la 60.....	90
Tabla 5. Número promedio de iteraciones necesarias para cubrir el intervalo unitario para el <i>Mapeo</i> Logístico con diferentes valores del parámetro.....	96



## ANEXO A. Diagramas de Bifurcación de dos mapeos unimodales

Este anexo muestra las semejanzas y diferencias entre los diagramas de bifurcación de dos *mapeos* unimodales, el *mapeo* logístico y el *mapeo* senoidal. La Figura 55 muestra el diagrama de bifurcación para el *mapeo* logístico y la Figura 56 lo muestra para el *mapeo* senoidal. Ambos diagramas son muy semejantes. Note que ambos diagramas tienen la misma escala en el eje vertical, pero note que el eje horizontal del diagrama para el *mapeo* senoidal está afectado por un factor de 4. Esta normalización es apropiada dado que el valor máximo del *mapeo* senoidal dado por  $x_{n+1}=r\sin(\pi x_n)$ , es  $r$ , mientras que para el *mapeo* logístico dado por  $x_{n+1}=r x_n (1-x_n)$  es  $r/4$ .

Estas figuras muestran que las dinámicas cuantitativas de los dos *mapeos* son idénticas. Así que ambos *mapeo* experimentan una ruta al caos por doblamiento del periodo, seguida por ventanas de comportamiento periódico con bandas perfectamente identificables en el interior de la zona caótica. Todavía más notable, las ventanas periódicas ocurren en el mismo orden y con las mismas medidas relativas. Para el caso de la ventana de periodo 3, es la más amplia en ambos casos, y las siguientes ventanas en tamaño que le preceden son las de periodo 5 y 6.

También hay diferencias cuantitativas que deben resaltarse. Por ejemplo, la bifurcación por doblamiento del periodo ocurre más tarde en el *mapeo* logístico y las ventanas periódicas en él son más angostas.

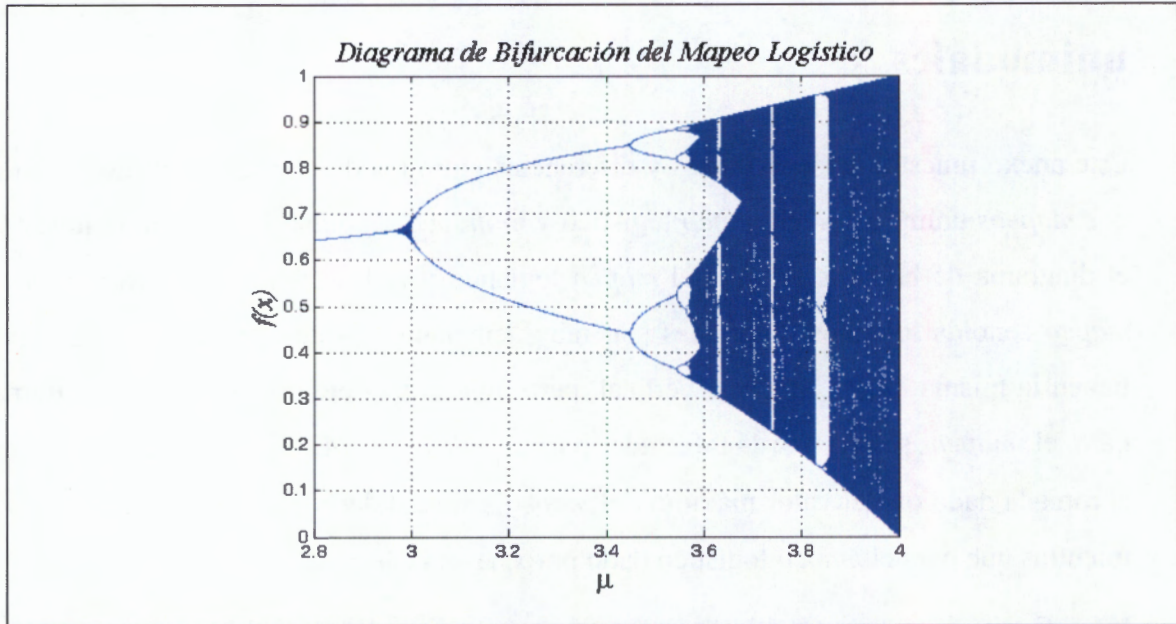


Figura 55. Diagrama de bifurcación del *Mapeo* Logístico para valores de parámetro entre 2.8 y 4.0.

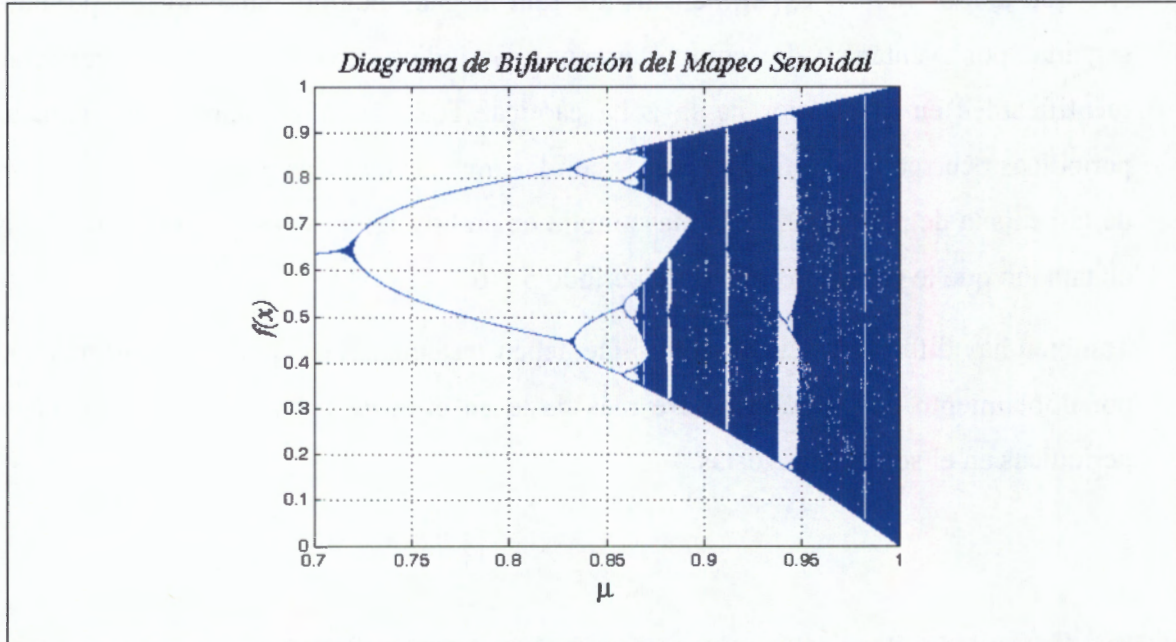


Figura 56. Diagrama de bifurcación del *Mapeo* Senoidal para valores de parámetro entre 0.7 y 1.0.

## ANEXO B. Mapeos Caóticos Unidimensionales

Un *mapeo* caótico unidimensional (1-D), es un sistema dinámico caótico (SDC) que está dado por la siguiente transformación,

$$x_{n+1} = \tau_{\mu}(x_n), \quad n = 0, 1, 2, \dots \quad (\text{B. 1})$$

con

$$x_n = \tau_{\mu}^n(x_0) \in I, \quad n = 0, 1, 2, \dots \quad (\text{B. 2})$$

De acuerdo con R.L. Devaney, un sistema dinámico caótico debe cumplir con la siguiente definición:

Sea  $I$  un conjunto, se dice que  $\tau : I \rightarrow I$  es caótico sobre  $I$  si:

- ✚  $\tau$  tiene dependencia sensitiva de las condiciones iniciales.
- ✚  $\tau$  es topológicamente transitiva.
- ✚ los puntos periódicos son densos en  $I$

La transformación  $\tau_{\mu}(\cdot) : I \rightarrow I$  es un *mapeo* no lineal,  $I$  denota el intervalo dentro del cual queda definido y  $n$  indica el índice de la iteración actual de la función  $\tau_{\mu}(\cdot)$ , comenzando con la condición inicial  $x_0$  y usando el parámetro  $\mu$ .

Estos *mapeos* producen órbitas, las cuales quedan definidas por,

$$\phi(x_0) = \{x_0, x_1, x_2, \dots, x_n, \dots\} = \{x_n\}_{n=0}^{\infty}, \quad (\text{B. 3})$$

Cada una de estas órbitas depende de la condición inicial  $x_0$  impuesta para el *mapeo*.

Es posible que estas órbitas tiendan a uno o más valores, en tal caso, estos valores constituyen los puntos fijos atractores ú órbitas estables del *mapeo*. Pero también es posible que existan otros valores de los que se alejan las órbitas, siendo estos los puntos

fijos repulsores ú órbitas inestables del *mapeo*. Ahora bien, la condición que hace que un punto fijo sea atractor o repulsor depende del valor que tenga el parámetro  $\mu$ . Un punto fijo de una función se define por,

$$\tau_{\mu}(x_1^*) = x_1^* \quad (\text{B. 4})$$

Y será estable si

$$\lim_{n \rightarrow \infty} \tau_{\mu}^n(x_0) = x_1^* \quad (\text{B. 5})$$

Sin embargo, en un *mapeo* 1-D pueden existir órbitas estables, que corresponden a puntos fijos de la función  $\tau_{\mu}^{2^n}(x)$ ; así, una órbita estable de periodo 2, es de la forma:

$$\phi_2(x_0) = \{x_0, x_1, x_2, \dots, x_1^*, x_2^*, x_1^*, x_2^*, x_1^*, \dots\} \quad (\text{B. 6})$$

donde  $x_1^*$  y  $x_2^*$  son puntos fijos de  $\tau_{\mu}^2(x)$ , esto es,

$$\begin{aligned} \tau_{\mu}(x_1^*) &= x_2^*, \\ \tau_{\mu}(x_2^*) &= x_1^* \end{aligned} \quad (\text{B. 7})$$

Por lo que,

$$\begin{aligned} \tau_{\mu}^2(x_1^*) &= x_1^*, \\ \tau_{\mu}^2(x_2^*) &= x_2^* \end{aligned} \quad (\text{B. 8})$$

De igual forma, para una órbita estable de periodo 4, la secuencia producida por el *mapeo* 1-D sería,

$$\phi_4(x_0) = \{x_0, x_1, x_2, \dots, x_0^*, x_1^*, x_2^*, x_3^*, x_0^*, x_1^*, x_2^*, x_3^*, \dots\} \quad (\text{B. 9})$$

Con lo que,

$$\begin{aligned} \tau_{\mu}(x_0^*) &= x_1^*, \\ \tau_{\mu}(x_1^*) &= x_2^*, \\ \tau_{\mu}(x_2^*) &= x_3^*, \\ \tau_{\mu}(x_3^*) &= x_0^* \end{aligned} \quad (\text{B. 10})$$

De la misma forma que para una órbita de periodo 2, en la órbita de periodo 4 es posible llegar a un mismo punto fijo a través de aplicar cuatro veces el *mapeo*. Es decir,

$$\begin{aligned} \tau_{\mu}^4(x_0^*) &= x_0^*, & \tau_{\mu}^4(x_2^*) &= x_2^*, \\ \tau_{\mu}^4(x_1^*) &= x_1^*, & \tau_{\mu}^4(x_3^*) &= x_3^*, \end{aligned} \quad (\text{B. 11})$$

De este planteamiento, se pueden resaltar tres aspectos importantes,

- i. La órbita depende del valor inicial.
- ii. La órbita también depende del parámetro  $\mu$ ,
- iii. Pueden existir órbitas estables de periodo  $p = 2^k, k \in \mathbb{Z}^+$

- Para una órbita estable de periodo 1,

$$\lim_{n \rightarrow \infty} x_n = x^* \text{ con } \tau_{\mu}(x^*) = x^*,$$

Por lo que,

$$\phi_1(x_0) \rightarrow \left\{ \overline{x^*} \right\}_{\mu} \text{ con } \mu \in (c_1, c_2).$$

- Para una órbita estable de periodo 2,

$$\lim_{n \rightarrow \infty} x_n = \begin{cases} x_1^* \\ x_2^* \end{cases} \text{ con } \tau_{\mu}^2(x_i^*) = x_i^*,$$

Por lo que

$$\phi_2(x_0) \rightarrow \left\{ \overline{x_1^*, x_2^*} \right\}, \text{ con } \mu \in (c_2, c_3)$$

- Para una órbita estable de periodo 4,

$$\lim_{n \rightarrow \infty} x_n = \begin{cases} x_0^* \\ x_1^* \\ x_2^* \\ x_3^* \end{cases}, \text{ con } \tau_{\mu}^4(x_i^*) = x_i^*,$$

Por lo que,

$$\phi_4(x_0) \rightarrow \left\{ \overline{x_0^*, x_1^*, x_2^*, x_3^*} \right\}_\mu, \text{ con } \mu \in (c_3, c_4)$$

- En general para una órbita estable de periodo  $2^k$ ,

$$\lim_{n \rightarrow \infty} x_n = \begin{cases} x_0^* \\ x_1^* \\ \vdots \\ x_{2^k}^* \end{cases}, \quad \text{con } \tau_\mu^{2^k}(x_i^*) = x_i^*,$$

Por lo que,

$$\phi_{2^k}(x_0) \rightarrow \left\{ \overline{x_0^*, x_1^*, \dots, x_{2^k}^*} \right\}_\mu, \text{ con } \mu \in (c_{2^k-1}, c_{2^k})$$

De esta forma, se puede construir una secuencia periódica que depende del parámetro  $\mu$ , por lo que es necesario establecer un parámetro crítico,  $\mu_{\text{critico}}$ , a partir de cual es posible generarla. Es decir,

$$\lim_{n \rightarrow \infty} \tau_{\mu_{\text{critico}}}^{2^k}(x_i^*) = x_i^*, \quad (\text{B. 12})$$

De este modo, antes del primer punto fijo se encuentra la secuencia,

$$x_0, x_1, x_2, \dots, x_n \quad (\text{B. 13})$$

y después es posible tener la secuencia periódica

$$x_0^*, x_1^*, \dots, x_n^* \quad (\text{B. 14})$$

Lo anterior es llamado bifurcaciones del periodo, que fueron encontradas por primera vez para el Mapeo Logístico [25].



## ANEXO C. Sentido del Teorema Ergódico

El Teorema Ergódico de Birkhoff es uno de los mayores resultados en la Teoría Ergódica, fue probado por primera vez en 1931 por G.D. Birkhoff, y desde entonces ha habido varios autores que lo han probado, la prueba mas reciente fue realizada por Rudolph en 1990.

Para entender este teorema considere que  $\tau: (X, B, \rho) \rightarrow (X, B, \rho)$  es una transformación de medida  $\rho$  invariante (measure preserving) y  $E \in B$ , con las siguientes definiciones.

$(X, B, \rho)$  constituye el espacio de medida (measure space),  $X$  es un conjunto,  $B$  es una familia de subconjuntos de  $X$  y  $\rho$  es una función  $\rho: B \rightarrow \mathfrak{R}^+$  que se considera la medida de  $B$  debido a que para conjuntos mensurables y disjuntos  $B_n \in B$ ,  $n = 1, 2, \dots$ ,

$$\rho\left(\bigcup_{n=1}^{\infty} B_n\right) = \sum_{n=1}^{\infty} \rho(B_n) \quad (\text{D.1})$$

Si  $X$  es una unión contable de conjuntos de medida  $\rho$  finita, entonces decimos que  $\rho$  es una medida  $\sigma$ -finita.

Una  $\tau: X \rightarrow X$  transformación es mensurable si  $\tau^{-1}(B) \in B$ , i.e.  $B \in B \Rightarrow \tau^{-1}(B) \in B$ , donde  $\tau^{-1}(B) = \{x \in X : \tau(x) \in B\}$  y es de medida  $\rho$  invariante o que  $\rho$  es  $\tau$ -invariant si  $\rho(\tau^{-1}(B)) = \rho(B)$  para todo  $B \in B$ .

Finalmente, considere la función de pertenencia:

$$\chi_E(x) = \begin{cases} 1, & \text{si } x \in E \\ 0, & \text{si } x \notin E \end{cases} \quad (\text{D.2})$$

Así, para  $x \in X$ , una pregunta de interés físico es, ¿Con qué frecuencia los puntos de la órbita  $\{x, \tau(x), \tau^2(x), \tau^3(x), \dots\}$  ocurren en el conjunto  $E$ ? Entonces,  $\tau^i(x) \in E$  si y solo si  $\chi_E(\tau^i(x)) = 1$ , entonces, el número de puntos de  $\{x, \tau(x), \tau^2(x), \tau^3(x), \dots\}$  en  $E$  es igual a,

$$\sum_{k=0}^n \chi_E(\tau^k(x)) \quad (\text{D.3})$$

y la frecuencia relativa es

$$\frac{1}{n+1} \sum_{k=0}^n \chi_E(\tau^k(x)) \quad (\text{D.4})$$

Con estos elementos decimos que el Teorema Ergódico de Birkhoff supone que si  $\tau: (X, B, \rho) \rightarrow (X, B, \rho)$  es una transformación de medida invariante (measure preserving) donde  $(X, B, \rho)$  es un  $\sigma$ -finite, y  $f: X \rightarrow \mathfrak{R}$  es un función medible ( $\forall c \in \mathfrak{R}, f^{-1}(c, \infty) \in B$ ) que satisfacen  $\int_X |f(x)| d\rho < \infty$ , i.e.  $f \in L^1(\rho)$ , entonces existe una función estacionaria  $f^* \in L^1(\rho)$  tal que,

$$\lim_{n \rightarrow \infty} \frac{1}{n+1} \sum_{k=0}^n f(\tau^k(x)) = f^*, \quad \rho - a.e. \quad (\text{D.5})$$

Además,  $f^* \circ \tau = f^*$ ,  $\rho - a.e.$  y si  $\rho(X) < \infty$ , entonces,

$$\int_X f^* d\rho = \int_X f d\rho \quad (\text{D.6})$$

En particular, si para cualquier  $B \in B$ ,  $\tau^{-1}(B) = B$ ,  $\rho(B) = 0$ , tal que la  $\tau$ -invariant de  $f^*$  implica que sea constante casi en todas partes, y esta constante debe ser la integral de  $f^*$ , significa que  $\tau$  es ergódico, entonces,

$$\lim_{n \rightarrow \infty} \frac{1}{n+1} \sum_{k=0}^n f(\tau^k(x)) = \int_X f^* d\rho, \quad \rho - a.e. \quad (\text{D.7})$$

Por lo que considerando la ecuación (D.6), la ecuación (D.7) se convierte en,

$$\lim_{n \rightarrow \infty} \frac{1}{n+1} \sum_{k=0}^n f(\tau^k(x)) = \int_x f d\rho \quad (\text{D.8})$$

Para casi cualquier  $x$ . Esto es frecuentemente interpretado de la siguiente forma, para una transformación ergódica, el promedio estadístico es seguramente igual al promedio aritmético. En general el promedio estadístico y el promedio aritmético son diferentes, pero si la transformación es ergódica y la medida invariante, son iguales casi siempre.

El término del lado izquierdo de la expresión (D.8) corresponde al promedio aritmético  $\overline{f(x)}$  definido (si existe) como el promedio sobre las iteraciones de  $\tau$  comenzando de alguna condición inicial  $x$ . El término del lado derecho de la expresión (D.8) corresponde al promedio estadístico,  $\langle f(x) \rangle$  o promedio fase de  $f$ . De esta manera la expresión (D.8) puede escribirse como,

$$\overline{f(x)} = \langle f(x) \rangle \quad (\text{D.9})$$

Ahora bien, dado que los *mapeos* caóticos unidimensionales son SDC y estos son ergódicos, entonces para ellos se satisface el Teorema Ergódico de Birkhoff, de manera que si  $\rho_{st}(x)$  es la medida (distribución estacionaria) del *mapeo* en cuestión, se tiene que,

$$\int f(x) \rho_{st}(x) dx \approx \frac{1}{n+1} \sum_{j=0}^n f(x_j) \quad (\text{D.10})$$

donde las  $x_j$  generadas constituyen la órbita del *mapeo*  $\tau(x)$ . Este resultado permite calcular aproximaciones numéricas a integrales difíciles de resolver por métodos analíticos. Para ello, solo basta evaluar la función a integrar en la órbita del *mapeo* una vez que se ha llegado a la distribución estacionaria.



## ANEXO D. Generador de Ruido en HSPICE™

### D.1. Circuito Generador de Ruido

```

*****
.option MODMONTE=0          ABSMOS=11E-15
.param  vton_par=agauss(0.4979, 0.01, 3)      vtop_par=agauss(-0.6915, 0.01, 3)      wpar=1  lpar=1
*       wpar=agauss(1, 0.01, 3)              lpar=agauss(1, 0.01, 3)
*       vton_par=agauss(0.4979, 0.01, 3)      vtop_par=agauss(-0.6915, 0.01, 3)
.dc     li      0u      100u  1u      sweep monte=50
.print  dc      miu=par'(-1)*i(VI)/i(Vx)'
*****

.include bias.sp
.include quad.sp
.include s&h.sp
.global vdd      vss      bias1      bias2      bias3
*****
Vdd     vdd      0      1.65
Vss     vss      0      -1.65

Vclk    vclk     0      -1.65
Mclk1   clk      vclk    vss      vss      NMOS    L='2u*Ipar'      W='2.8u*wpar'
Mclk2   clk      vclk    vdd     vdd     PMOS    L='2u*Ipar'      W='10.4u*wpar'
Mclk3   clk      vclk    vss     vss     NMOS    L='2u*Ipar'      W='2.8u*wpar'
Mclk4   clk      vclk    vdd     vdd     PMOS    L='2u*Ipar'      W='10.4u*wpar'

li      ii      vss     PWL(    0      0      10u     100u   20u     0      R)
Mi1     ii      ii      vdd     vdd     PMOS    L='2u*Ipar'      W='10.4u*wpar'
Mi2     3      ii      vdd     vdd     PMOS    L='2u*Ipar'      W='41.6u*wpar'
Mi3     3      vdd     ii1     vss     NMOS    L='2u*Ipar'      W='10.4u*wpar'
*****
Xbias   bias1    bias2    bias3    bias
Xquad   iq1     ii1     quad
Vx      iq1     0       0
Fx      vdd     iq2     Vx       1
Xs&h    iq2     vq      s&h
*VI     iq2     0       0
VI      vq      0       0
*****

.MODEL NNMOS NMOS LEVEL=49
*-----
***** SIMULATION PARAMETERS *****
*-----
* format : HSPICE
* model   : MOS BSIM3v3
* process : C35
* revision : 3.1;
* extracted : B10866 ; 2002-12; ese(487)
* doc#    : ENG-182 REV_3
*-----
*
* TYPICAL MEAN CONDITION
*-----
*
* *** Flags ***
+MOBMOD =1.000e+00 CAPMOD =2.000e+00

```

```
+NOIMOD=3.000e+00
+VERSION=3.11
* *** Threshold voltage related model parameters ***
+K1 =5.0296e-01
+K2 =3.3985e-02 K3 =-1.136e+00 K3B =-4.399e-01
+NCH =2.611e+17 VTH0 =4.979e-01
+VOFF =-8.925e-02 DVTO =5.000e+01 DVT1 =1.039e+00
+DVT2 =-8.375e-03 KETA =2.032e-02
+PSCBE1=3.518e+08 PSCBE2=7.491e-05
+DVTOW =1.089e-01 DVT1W =6.671e+04 DVT2W =-1.352e-02
* *** Mobility related model parameters ***
+UA =4.705e-12 UB =2.137e-18 UC =1.000e-20
+U0 =4.758e+02
* *** Subthreshold related parameters ***
+DSUB =5.000e-01 ETA0 =1.415e-02 ETAB =-1.221e-01
+NFACTOR=4.136e-01
* *** Saturation related parameters ***
+EM =4.100e+07 PCLM =6.948e-01
+PDIBLC1=3.571e-01 PDIBLC2=2.065e-03 DROUT =5.000e-01
+A0 =2.541e+00 A1 =0.000e+00 A2 =1.000e+00
+PVAG =0.000e+00 VSAT =1.338e+05 AGS =2.408e-01
+B0 =4.301e-09 B1 =0.000e+00 DELTA =1.442e-02
+PDIBLCB=3.222e-01
* *** Geometry modulation related parameters ***
+W0 =2.673e-07 DLC =3.0000e-08
+DWC =9.403e-08 DWB =0.000e+00 DWG =0.000e+00
+LL =0.000e+00 LW =0.000e+00 LWL =0.000e+00
+LLN =1.000e+00 LWN =1.000e+00 WL =0.000e+00
+WW =-1.297e-14 WWL =-9.411e-21 WLN =1.000e+00
+WWN =1.000e+00
* *** Temperature effect parameters ***
+TNOM =27.0 AT =3.300e+04 UTE =-1.800e+00
+KT1 =-3.302e-01 KT2 =2.200e-02 KT1L =0.000e+00
+UA1 =0.000e+00 UB1 =0.000e+00 UC1 =0.000e+00 PRT =0.000e+00
* *** Overlap capacitance related and dynamic model parameters ***
+CGDO =1.200e-10 CGSO =1.200e-10 CGBO =1.100e-10
+CGDL =1.310e-10 CGSL =1.310e-10 CKAPPA =6.000e-01
+CF =0.000e+00 ELM =5.000e+00
+XPART =1.000e+00 CLC =1.000e-15 CLE =6.000e-01
* *** Parasitic resistance and capacitance related model parameters ***
+RDSW =3.449e+02
+CDSC =0.000e+00 CDSCB =1.500e-03 CDSCD =1.000e-03
+PRWB =-2.416e-01 PRWG =0.000e+00 CIT =4.441e-04
* *** Process and parameters extraction related model parameters ***
+TOX =7.575e-09 NGATE =0.000e+00
+NLX =1.888e-07
+XL =0.000e+00 XW =0.000e+00
* *** Substrate current related model parameters ***
+ALPHA0=0.000e+00 BETA0 =3.000e+01
* *** Noise effect related model parameters ***
+AF =1.507e+00 KF =2.170e-26 EF =1.000e+00
+NOIA =1.121e+19 NOIB =5.336e+04 NOIC =-5.892e-13
* *** Common extrinsic model parameters ***
+ACM =2
+RD =0.000e+00 RS =0.000e+00 RSH =7.000e+01
+RDC =0.000e+00 RSC =0.000e+00
```

```
+LINT =-5.005e-08 WINT =9.403e-08
+LDIF =0.000e+00 HDIF =8.000e-07 WMLT =1.000e+00
+LMLT =1.000e+00 XJ =3.000e-07
+JS =1.000e-05 JSW =0.130e-09 IS =0.000e+00
+N =1.000e+00 NDS =1000.
+VNDS =-1.000e+00 CBD =0.000e+00 CBS =0.000e+00 CJ =9.400e-04 CJSW =2.500e-10
+FC =0.000e+00 MJ =3.400e-01 MJSW =2.300e-01
+XTI =2.026e+00 TT =0.000e+00
+PB =6.900e-01 PHP =6.900e-01
```

```
* -----
* Owner: austriamicrosystems
* HIT-Kit: Digital
```

```
.MODEL PPMOS PMOS LEVEL=49
```

```
* -----
***** SIMULATION PARAMETERS *****
```

```
* -----
* format : HSPICE
* model : MOS BSIM3v3
* process : C35
* revision : 3.1;
* extracted : C64685 ; 2002-12; ese(487)
* doc# : ENG-182 REV_3
* -----
```

```
***** TYPICAL MEAN CONDITION *****
```

```
* *** Flags ***
+MOBMOD =1.000e+00 CAPMOD =2.000e+00
+NOIMOD =3.000e+00
+VERSION=3.11
* *** Threshold voltage related model parameters ***
+K1 =5.9959e-01
+K2 =-6.038e-02 K3 =1.103e+01 K3B =-7.580e-01
+NCH =9.240e+16 VTH0 =-6.915e-01
+VOFF =-1.170e-01 DVT0 =1.650e+00 DVT1 =3.868e-01
+DVT2 =1.659e-02 KETA =-1.440e-02
+PSCBE1 =5.000e+09 PSCBE2 =1.000e-04
+DVT0W =1.879e-01 DVT1W =7.335e+04 DVT2W =-6.312e-03
* *** Mobility related model parameters ***
+UA =5.394e-10 UB =1.053e-18 UC =1.000e-20
+U0 =1.482e+02
* *** Subthreshold related parameters ***
+DSUB =5.000e-01 ETA0 =2.480e-01 ETAB =-3.917e-03
+NFACTOR=1.214e+00
* *** Saturation related parameters ***
+EM =4.100e+07 PCLM =3.184e+00
+PDIBLC1=1.000e-04 PDIBLC2=1.000e-20 DROUT =5.000e-01
+A0 =5.850e-01 A1 =0.000e+00 A2 =1.000e+00
+PVAG =0.000e+00 VSAT =1.158e+05 AGS =2.468e-01
+B0 =8.832e-08 B1 =0.000e+00 DELTA =1.000e-02
+PDIBLCB=1.000e+00
* *** Geometry modulation related parameters ***
+W0 =1.000e-10 DLC =2.4500e-08
+DWC =3.449e-08 DWB =0.000e+00 DWG =0.000e+00
+LL =0.000e+00 LW =0.000e+00 LWL =0.000e+00
+LLN =1.000e+00 LWN =1.000e+00 WL =0.000e+00
```

```
+WW =1.894e-16 WWL =-1.981e-21 WLN =1.000e+00
+WWN =1.040e+00
* *** Temperature effect parameters ***
+TNOM =27.0 AT =3.300e+04 UTE =-1.300e+00
+KT1 =-5.403e-01 KT2 =2.200e-02 KT1L =0.000e+00
+UA1 =0.000e+00 UB1 =0.000e+00 UC1 =0.000e+00 PRT =0.000e+00
* *** Overlap capacitance related and dynamic model parameters ***
+CGDO =8.600e-11 CGSO =8.600e-11 CGBO =1.100e-10
+CGDL =1.080e-10 CGSL =1.080e-10 CKAPPA =6.000e-01
+CF =0.000e+00 ELM =5.000e+00
+XPART =1.000e+00 CLC =1.000e-15 CLE =6.000e-01
* *** Parasitic resistance and capacitance related model parameters ***
+RDSW =1.033e+03
+CDSC =2.589e-03 CDSCB =2.943e-04 CDSCD =4.370e-04
+PRWB =-9.731e-02 PRWG =1.477e-01 CIT =0.000e+00
* *** Process and parameters extraction related model parameters ***
+TOX =7.754e-09 NGATE =0.000e+00
+NLX =1.770e-07
+XL =0.000e+00 XW =0.000e+00
* *** Substrate current related model parameters ***
+ALPHA0 =0.000e+00 BETA0 =3.000e+01
* *** Noise effect related model parameters ***
+AF =1.461e+00 KF =1.191e-26 EF =1.000e+00
+NOIA =5.245e+17 NOIB =4.816e+03 NOIC =8.036e-13
* *** Common extrinsic model parameters ***
+ACM =2
+RD =0.000e+00 RS =0.000e+00 RSH =1.290e+02
+RDC =0.000e+00 RSC =0.000e+00
+LINT =-7.130e-08 WINT =3.449e-08
+LDIF =0.000e+00 HDIF =8.000e-07 WMLT =1.000e+00
+LMLT =1.000e+00 XJ =3.000e-07
+JS =9.000e-05 JSW =0.610e-09 IS =0.000e+00
+N =1.000e+00 NDS =1000.
+VNDS =-1.000e+00 CBD =0.000e+00 CBS =0.000e+00 CJ =1.360e-03 CJSW =3.200e-10
+FC =0.000e+00 MJ =5.600e-01 MJSW =4.300e-01
+XTI =1.973e+00 TT =0.000e+00
+PB =1.020e+00 PHP =1.020e+00
*
* Owner: austriamicrosystems
* HIT-Kit: Digital
*****

.MODEL NMOS NMOS LEVEL=49
*
***** SIMULATION PARAMETERS *****
*
* format : HSPICE
* model : MOS BSIM3v3
* process : C35
* revision : 3.1;
* extracted : B10866 ; 2002-12; ese(487)
* doc# : ENG-182 REV_3
*
* TYPICAL MEAN CONDITION
*
* *** Flags ***
```



```
+MOBMOD=1.000e+00 CAPMOD=2.000e+00
+NOIMOD=3.000e+00
+VERSION=3.11
* *** Threshold voltage related model parameters ***
+K1 =5.0296e-01
+K2 =3.3985e-02 K3 =-1.136e+00 K3B =-4.399e-01
+NCH =2.611e+17 VTH0 =vton_par
*4.979e-01
+VOFF =-8.925e-02 DVTO =5.000e+01 DVT1 =1.039e+00
+DVT2 =-8.375e-03 KETA =2.032e-02
+PSCBE1=3.518e+08 PSCBE2=7.491e-05
+DVTOW=1.089e-01 DVT1W=6.671e+04 DVT2W=-1.352e-02
* *** Mobility related model parameters ***
+UA =4.705e-12 UB =2.137e-18 UC =1.000e-20
+UO =4.758e+02
* *** Subthreshold related parameters ***
+DSUB =5.000e-01 ETA0 =1.415e-02 ETAB =-1.221e-01
+NFACTOR=4.136e-01
* *** Saturation related parameters ***
+EM =4.100e+07 PCLM =6.948e-01
+PDIBLC1=3.571e-01 PDIBLC2=2.065e-03 DROUT =5.000e-01
+A0 =2.541e+00 A1 =0.000e+00 A2 =1.000e+00
+PVAG =0.000e+00 VSAT =1.338e+05 AGS =2.408e-01
+B0 =4.301e-09 B1 =0.000e+00 DELTA =1.442e-02
+PDIBLCB=3.222e-01
* *** Geometry modulation related parameters ***
+W0 =2.673e-07 DLC =3.0000e-08
+DWC =9.403e-08 DWB =0.000e+00 DWG =0.000e+00
+LL =0.000e+00 LW =0.000e+00 LWL =0.000e+00
+LLN =1.000e+00 LWN =1.000e+00 WL =0.000e+00
+WW =-1.297e-14 WWL =-9.411e-21 WLN =1.000e+00
+WWN =1.000e+00
* *** Temperature effect parameters ***
+TNOM =27.0 AT =3.300e+04 UTE =-1.800e+00
+KT1 =-3.302e-01 KT2 =2.200e-02 KT1L =0.000e+00
+UA1 =0.000e+00 UB1 =0.000e+00 UC1 =0.000e+00 PRT =0.000e+00
* *** Overlap capacitance related and dynamic model parameters ***
+CGDO =1.200e-10 CGSO =1.200e-10 CGBO =1.100e-10
+CGDL =1.310e-10 CGSL =1.310e-10 CKAPPA =6.000e-01
+CF =0.000e+00 ELM =5.000e+00
+XPART =1.000e+00 CLC =1.000e-15 CLE =6.000e-01
* *** Parasitic resistance and capacitance related model parameters ***
+RDSW =3.449e+02
+CDSC =0.000e+00 CDSCB =1.500e-03 CDSCD =1.000e-03
+PRWB =-2.416e-01 PRWG =0.000e+00 CIT =4.441e-04
* *** Process and parameters extraction related model parameters ***
+TOX =7.575e-09 NGATE =0.000e+00
+NLX =1.888e-07
+XL =0.000e+00 XW =0.000e+00
* *** Substrate current related model parameters ***
+ALPHA0=0.000e+00 BETA0 =3.000e+01
* *** Noise effect related model parameters ***
+AF =1.507e+00 KF =2.170e-26 EF =1.000e+00
+NOIA =1.121e+19 NOIB =5.336e+04 NOIC =-5.892e-13
* *** Common extrinsic model parameters ***
+ACM =2
```

```
+RD =0.000e+00 RS =0.000e+00 RSH =7.000e+01
+RDC =0.000e+00 RSC =0.000e+00
+LINT =-5.005e-08 WINT =9.403e-08
+LDIF =0.000e+00 HDIF =8.000e-07 WMLT =1.000e+00
+LMLT =1.000e+00 XJ =3.000e-07
+JS =1.000e-05 JSW =0.130e-09 IS =0.000e+00
+N =1.000e+00 NDS =1000.
+VNDS =-1.000e+00 CBD =0.000e+00 CBS =0.000e+00 CJ =9.400e-04 CJSW =2.500e-10
+FC =0.000e+00 MJ =3.400e-01 MJSW =2.300e-01
+XTI =2.026e+00 TT =0.000e+00
+PB =6.900e-01 PHP =6.900e-01
```

```
* Owner: austriamicrosystems
* HIT-Kit: Digital
```

```
.MODEL PMOS PMOS LEVEL=49
```

```
***** SIMULATION PARAMETERS *****
```

```
* format : HSPICE
* model : MOS BSIM3v3
* process : C35
* revision : 3.1;
* extracted : C64685 ; 2002-12; ese(487)
* doc# : ENG-182 REV_3
```

```
TYPICAL MEAN CONDITION
```

```
*** Flags ***
+MOBMOD =1.000e+00 CAPMOD =2.000e+00
+NOIMOD =3.000e+00
+VERSION=3.11
*** Threshold voltage related model parameters ***
+K1 =5.9959e-01
+K2 =-6.038e-02 K3 =1.103e+01 K3B =-7.580e-01
+NCH =9.240e+16 VTH0 = vtop_par
*-6.915e-01
+VOFF =-1.170e-01 DVT0 =1.650e+00 DVT1 =3.868e-01
+DVT2 =1.659e-02 KETA =-1.440e-02
+PSCBE1 =5.000e+09 PSCBE2 =1.000e-04
+DVTOW =1.879e-01 DVT1W =7.335e+04 DVT2W =-6.312e-03
*** Mobility related model parameters ***
+UA =5.394e-10 UB =1.053e-18 UC =1.000e-20
+U0 =1.482e+02
*** Subthreshold related parameters ***
+DSUB =5.000e-01 ETA0 =2.480e-01 ETAB =-3.917e-03
+NFACTOR=1.214e+00
*** Saturation related parameters ***
+EM =4.100e+07 PCLM =3.184e+00
+PDIBLC1=1.000e-04 PDIBLC2=1.000e-20 DROUT =5.000e-01
+A0 =5.850e-01 A1 =0.000e+00 A2 =1.000e+00
+PVAG =0.000e+00 VSAT =1.158e+05 AGS =2.468e-01
+B0 =8.832e-08 B1 =0.000e+00 DELTA =1.000e-02
+PDIBLCB=1.000e+00
*** Geometry modulation related parameters ***
+W0 =1.000e-10 DLC =2.4500e-08
```

```

+DWC =3.449e-08 DWB =0.000e+00 DWG =0.000e+00
+LL =0.000e+00 LW =0.000e+00 LWL =0.000e+00
+LLN =1.000e+00 LWN =1.000e+00 WL =0.000e+00
+WW =1.894e-16 WWL =-1.981e-21 WLN =1.000e+00
+WWN =1.040e+00
* *** Temperature effect parameters ***
+TNOM =27.0 AT =3.300e+04 UTE =-1.300e+00
+KT1 =-5.403e-01 KT2 =2.200e-02 KT1L =0.000e+00
+UA1 =0.000e+00 UB1 =0.000e+00 UC1 =0.000e+00 PRT =0.000e+00
* *** Overlap capacitance related and dynamic model parameters ***
+CGDO =8.600e-11 CGSO =8.600e-11 CGBO =1.100e-10
+CGDL =1.080e-10 CGSL =1.080e-10 CKAPPA =6.000e-01
+CF =0.000e+00 ELM =5.000e+00
+XPART =1.000e+00 CLC =1.000e-15 CLE =6.000e-01
* *** Parasitic resistance and capacitance related model parameters ***
+RDSW =1.033e+03
+CDSC =2.589e-03 CDSCB =2.943e-04 CDSCD =4.370e-04
+PRWB =-9.731e-02 PRWG =1.477e-01 CIT =0.000e+00
* *** Process and parameters extraction related model parameters ***
+TOX =7.754e-09 NGATE =0.000e+00
+NLX =1.770e-07
+XL =0.000e+00 XW =0.000e+00
* *** Substrate current related model parameters ***
+ALPHA0 =0.000e+00 BETA0 =3.000e+01
* *** Noise effect related model parameters ***
+AF =1.461e+00 KF =1.191e-26 EF =1.000e+00
+NOIA =5.245e+17 NOIB =4.816e+03 NOIC =8.036e-13
* *** Common extrinsic model parameters ***
+ACM =2
+RD =0.000e+00 RS =0.000e+00 RSH =1.290e+02
+RDC =0.000e+00 RSC =0.000e+00
+LINT =-7.130e-08 WINT =3.449e-08
+LDIF =0.000e+00 HDIF =8.000e-07 WMLT =1.000e+00
+LMLT =1.000e+00 XJ =3.000e-07
+JS =9.000e-05 JSW =0.610e-09 IS =0.000e+00
+N =1.000e+00 NDS =1000.
+VNDS =-1.000e+00 CBD =0.000e+00 CBS =0.000e+00 CJ =1.360e-03 CJSW =3.200e-10
+FC =0.000e+00 MJ =5.600e-01 MJSW =4.300e-01
+XTI =1.973e+00 TT =0.000e+00
+PB =1.020e+00 PHP =1.020e+00
* -----
* Owner: austriamicrosystems
* HIT-Kit: Digital
.end

```

## D.2. Circuito de Polarización

```

*****
.subckt bias bias1 bias2 bias3
M1 bias1 bias1 vdd vdd PPMOS L=2u W=10.4u
M2 bias1 bias1 vss vss NNMOS L=2u W=2.8u
M3 bias2 bias2 vdd vdd PPMOS L=2u W=10.4u
M4 bias2 bias2 bias3 vss NNMOS L=2u W=58.8u
M5 bias3 bias3 vss vss NNMOS L=2u W=58.8u
.ends

```

\*\*\*\*\*  
**D.3. Circuito Multiplicador**  
\*\*\*\*\*

```
.subckt quad ii io

M1 1 bias2 vdd vdd PMOS L='2u*lpar' W='5.2u*wpar'
M2 2 bias2 vdd vdd PMOS L='2u*lpar' W='5.2u*wpar'
M3 ii bias2 vdd vdd PMOS L='2u*lpar' W='20.8u*wpar'
M4 1 1 3 vss NMOS L='2u*lpar' W='58.8u*wpar'
M5 3 3 vss vss NMOS L='2u*lpar' W='58.8u*wpar'
M6 ii 1 io vss NMOS L='2u*lpar' W='58.8u*wpar'
M7 io 3 vss vss NMOS L='2u*lpar' W='58.8u*wpar'
M8 2 2 io vss NMOS L='2u*lpar' W='58.8u*wpar'
M9 io io vss vss NMOS L='2u*lpar' W='58.8u*wpar'
M10 ii 2 3 vss NMOS L='2u*lpar' W='58.8u*wpar'
M11 3 io vss vss NMOS L='2u*lpar' W='58.8u*wpar'
M12 io bias3 vss vss NMOS L='2u*lpar' W='117.6u*wpar'

.ends
```

\*\*\*\*\*  
**D.4. Circuito Muestreo y Retención**  
\*\*\*\*\*

```
.subckt s&h 1 vo

Vb vb 0 0
lbi vdd i 100u
lbo vdd vo 392u
M2 i vb 1 vss NMOS L='2u*lpar' W='100u*wpar'
M3 1 i vss vss NMOS L='2u*lpar' W='100u*wpar'
M4 vo vb 2 vss NMOS L='2u*lpar' W='392u*wpar'
M5 2 i vss vss NMOS L='2u*lpar' W='392u*wpar'

*lop1 vdd op1 400u
*lop2 vdd op2 400u
*Mop1 op1 1 op3 vss NMOS L=2u W=300u
*Mop2 op2 2 op3 vss NMOS L=2u W=300u
*lop3 op3 vss 800u

.ends
```

## ANEXO E. Publicaciones en revistas

### I. Artículos publicados en Revista Internacional

- ✚ “Chaotic Noise MOS Generator based on Logistic Map”, A. Díaz-Méndez, J. V. Marquina-Pérez, M. Cruz-Irisson, **R. Vázquez-Medina**, J. L. Del-Río-Correa; *Microelectronics Journal* (2008), DOI: 10.1016/j.mejo.2008.06.042. Aceptado el 22 de febrero de 2008 para ser publicado. Article in Press.
- ✚ “Design of Chaotic Analog Noise Generators with Logistic Map and MOS QT Circuits”, **R. Vázquez-Medina**, A. Díaz-Méndez, J. L. del Río-Correa and J. López-Hernández; *Chaos, Solitons & Fractals* (2007): The Interdisciplinary Journal of Nonlinear Science, Nano and Quantum Technology. DOI:10.1016/j.chaos.2007.09.088. Aceptado el 16 de septiembre de 2007 para ser publicado. Article in Press.
- ✚ “Non Classical Difusión Boxes using the Golden Binary Self Similar Sequence”; **R. Vázquez-Medina**, H. M. Pérez-Meana and J. L. del-Río-Correa; *Journal of Telecommunications and Radio Engineering*; Vol.56, Issue 1, pp 18-36, 2001. ISSN: 0040-2508, Begell House Inc.; <http://www.begellhouse.com/journals/0632a9d54950b268,5d2ce61c0e461b2b,4980f1572573449d.html>.
- ✚ “Self-similar Sequences: Spread Spectrum Application in the WLAN”, **R. Vázquez-Medina**, J. L. del-Río-Correa, G. I. Duchén-Sánchez and O. Téllez-Analco, *Telecommunications and Radio Engineering*; Vol 56, Issue 4&5, 2001. pp 186-194. ISSN: 0040-2508, Begell House Inc.; <http://www.begellhouse.com/journals/0632a9d54950b268,422345a314832522,7ce9e047074bd282.html>.

- ✚ “Secuencias Cifrantes de Números Metálicos a partir de Fracciones Continuas,” F. J. Romero-Ibarra y **R. Vázquez-Medina**, Revista Iberoamericana de Computación: Computación y Sistemas, número 4 del volumen 7 (abr-jun 2004). PP 272-284, ISSN 1405-5546
- ✚ “Evaluación y Análisis de Secuencias cifrantes Irracionales usando la Prueba Universal de Maurer,” F.J. Romero-Ibarra y **R. Vázquez-Medina**, Revista Científica de Ingeniería Electrónica, Automática y Comunicaciones, Vol. XXV, no.1, pp 67-72, Cuba, 2004. ISSN 0258-5944.

## II. Artículos publicados en Revista Nacional en el Padrón de CONACYT

- ✚ “Aplicación de las Secuencias Autosimilares a las Cajas de Dispersión”; **Rubén Vázquez Medina**, José Luis del Río Correa y Héctor Manuel Pérez Meana; Aceptado en Diciembre 2000, Revista Científica No. 23 Septiembre Octubre del 2000. Escuela Superior de Ingeniería Mecánica y Eléctrica, IPN.
- ✚ “Un Algoritmo de Dispersión del Espectro usando la Teoría de los Cuasicristales”; Oreste Téllez Analco, **Rubén Vázquez Medina**, Gonzalo I. Duchén Sánchez y José Luis del Río Correa; Revista Científica; Mayo Junio 1998. Escuela Superior de Ingeniería Mecánica y Eléctrica, IPN.

## ANEXO F. Publicaciones en congresos

### I. Artículos en Extenso en Memorias de Congreso Internacional

- ✚ “Numerical calculation of the Lyapunov exponent for the logistic map” R. Vázquez-Medina, E. Ibarra Olivares, M. Cruz-Irisson and J. L. Del-Río-Correa; 12 th International Conference on Mathematical Methods in Electromagnetic Theory, MMET 08, June 29 to July 2, 2008; Odesa Ukraine. IEEE: CFP08761-PRT, ISBN: 978-1-4244-2284-5, pp 409-411.
- ✚ “Algoritmo de Cifrado usando *Mapeos* Caóticos”, **Rubén Vázquez-Medina**, Eric Ibarra Olivares, y Sebastián Gutiérrez Flores, Tercer Congreso Internacional en Matemáticas Aplicadas 2007, APPLEIDMATH3, 2007, 9 al 12 de octubre de 2007, México, pp 311-320. ISBN 978-970-36-0442-5
- ✚ “Noise Sequences using Chaotic Maps”, **Rubén Vázquez-Medina**, José Luis Del Río-Correa and Alejandro Díaz-Méndez, Mexican Conference On Informatics Security MCIS 2006, november 14-17, 2006, México. Organizado por The Institute of Electrical and Electronics Engineers Puebla Section.
- ✚ “File Encryption with Silver Numbers And Quasicrystals”; **Rubén Vázquez Medina**, José Luis Del Río Correa y Héctor Manuel Pérez Meana; International Symposium on Information Theory and its Applications, ISITA '98; México; Oct, 1998.

### II. Artículos en Extenso en Memorias de Congreso Nacional

- ✚ “La Secuencia de Fibonacci y su Aplicación a las Redes Locales Inalámbricas”; Oreste Téllez Analco, **Rubén Vázquez Medina**, Gonzalo I. Duchén Sánchez y José Luis del Río Correa; 9º. Congreso Internacional de

Electrónica, Comunicaciones y Computadoras; Universidad de las Américas Puebla; Marzo de 1999.

### III. Trabajos presentados en Congreso Internacional

- ✚ “Quasicrystals and its Applications to File Encryption”; **Rubén Vázquez Medina**, José Luis Del Río Correa y Héctor Manuel Pérez Meana; International Conference on Coding Theory, Cryptography and Related Areas, UAM-IPN, Guanajuato, Guanajuato; 20 al 24 de abril de 1998.

### IV. Trabajos presentados en Congreso Nacional

- ✚ “Pseudo Ruido con *Mapeos* Caóticos”; **Rubén Vázquez Medina** y José Luis Del Río Correa; VII Coloquio Nacional de Códigos, Criptografía y Áreas Relacionadas, Universidad Autónoma del Estado de México, Toluca, Estado de México; 7 al 9 de junio de 2006.
- ✚ “Criptografía con Secuencias Autosimilares”; **Rubén Vázquez Medina**, José Luis Del Río Correa y Héctor Manuel Pérez Meana; II Coloquio de Códigos, Criptografía y Áreas Relacionadas, Dirección General de Cómputo Académico de la UNAM, UAM e IPN, 26 de Junio de 1998 pp-6.