

FACULTAD DE INVENIERÍA UNIVERSIDAD NACIONAL DE  
MAR DEL PLATA

**SISTEMAS COMPLEJOS, RUIDOS  
DISCRETOS Y SU  
IMPLEMENTACIÓN EN FPGA**

TESIS

PARA OBTENER EL TÍTULO DE  
DOCTOR EN INGENIERÍA CON ORIENTACIÓN EN ELECTRÓNICA  
**MAXIMILIANO ANTONELLI**

MAR DEL PLATA, ARGENTINA

9 DE MARZO DE 2018



*DEDICATORIA*



# **Agradecimientos**

¡Muchas gracias a todos!



# Índice general

<b>1. Introducción</b>	<b>1</b>
<b>2. Sistemas de dinámica compleja</b>	<b>3</b>
2.1. Teoría Cualitativa - Espacio de Fases . . . . .	5
2.2. Sistemas caóticos . . . . .	12
2.3. Mapas caóticos . . . . .	19
2.3.1. Mapas cuadráticos bidimensionales . . . . .	19
<b>3. Cuantificadores de Aleatoriedad</b>	<b>23</b>
3.1. Máximo Exponente de Lyapunov . . . . .	24
3.1.1. Algoritmo evolutivo para la búsqueda de caos . . . . .	27
3.2. Cuantificadores de la teoría de la información . . . . .	34
3.2.1. Entropía de Shannon y Complejidad Estadística . . . . .	36
3.2.2. Determinación de la distribución de probabilidad . . . . .	38
3.2.3. Planos de doble entropía y entropía-complejidad . . . . .	42
3.2.4. Entropías diferenciales . . . . .	44
3.2.5. Cuantificador de entropías implementado en FPGA . . . . .	48
3.2.6. Dinámica de los ITQ's con AWGN y banda limitada . . . . .	56
3.3. Conclusiones . . . . .	64
<b>4. Generadores de Números Aleatorios Usando Caos</b>	<b>67</b>
4.1. Caos en redes neuronales . . . . .	69
4.1.1. El modelo de Hopfield . . . . .	70
4.1.2. Estudio de la RNA en función de un parámetro . . . . .	72
4.2. Cripto-codificación caótica variante en el tiempo . . . . .	75

4.2.1. Implementación . . . . .	78
4.2.2. Resultados . . . . .	81
4.3. Implementación de atractor Determinístico - Estocástico . . . . .	82
4.3.1. Discretización temporal del oscilador de Lorenz . . . . .	84
4.3.2. Discretización de las variables de estado . . . . .	85
4.3.3. Resultados . . . . .	88
4.4. Mapas cuadráticos 2-D implementados en punto fijo . . . . .	92
4.4.1. Resultados . . . . .	94
4.5. Conclusiones . . . . .	102
<b>5. Mapas conmutados en precisión finita</b>	<b>105</b>
5.1. Introduction . . . . .	105
5.2. Resultados . . . . .	107
5.2.1. Período $T$ en función de $B$ . . . . .	111
5.2.2. Cuantificadores de mapas simples . . . . .	112
5.2.3. Cuantificadores de mapas combinados . . . . .	119
5.3. Conclusiones . . . . .	123
<b>6. Generadores de TRNG usando ROs en FPGA</b>	<b>129</b>
6.1. Introduction . . . . .	129
6.2. Determinación del <i>jitter</i> en <i>RO's</i> . . . . .	131
6.2.1. Resultados . . . . .	133
6.2.2. Conclusiones . . . . .	141
6.3. Implementación y análisis estadístico de <i>TRNG</i> basado en <i>ROs</i> . . . . .	142
6.3.1. Resumen . . . . .	142
6.3.2. Introducción . . . . .	142
6.3.3. Implementación en Hardware . . . . .	143
6.3.4. Resultados . . . . .	146
6.4. Conclusiones . . . . .	148
<b>Bibliografía</b>	<b>151</b>

# Capítulo 1

## Introducción

Los números aleatorios constituyen una de las bases del desarrollo tecnológico, han sido utilizados exitosamente en una gran variedad de aplicaciones como juegos, criptografía, modelado de sistemas físicos, sistemas biológicos, etc. Éstos pueden ser generados a partir de fuentes de aleatoriedad de naturaleza física (TRNG) o a partir de generadores algorítmicos (PRNG). En esta tesis se propone reemplazar los generadores algorítmicos por sistemas caóticos, aunque las secuencias generadas por estos últimos deben ser postprocesadas para randomizarlas.

Esta tesis se centra en la implementación en hardware electrónico de RNGs, particularmente se trata de responder dos preguntas principales: ¿Cómo varían las propiedades estadísticas de los sistemas caóticos cuando son implementados en hardware digital? y, ¿Es posible implementar un generador físico de ruido en hardware? La primer pregunta está directamente relacionada con generadores PRNG, la segunda apunta a la posibilidad de implementar un TRNG (analógico) en hardware digital.

Para estudiar los RNGs, se utilizaron cuantificadores de la teoría de la información, por un lado basados en entropías de valores y por otro en entropías de patrones de orden. Estas dos entropías son complementarias y cubren los dos principales aspectos a considerar: estocasticidad de los valores generados e independencia estadística de valores consecutivos. Además se utilizan exponentes de Lyapunov para evaluar la caoticidad de los sistemas implementados en hardware.

Cuando un sistema es calculado en aritmética discreta, el resultado de cada iteración se sustituye por el valor representable más cercano, lo que desvía su trayectoria de la que

tendría utilizando números reales. La inherente sensibilidad a las condiciones iniciales que presentan los sistemas caóticos hace que estas perturbaciones se vean amplificadas con cada iteración (vía el máximo exponente de Lyapunov) y el sistema resultante pueda tener poco que ver con el original. En el mejor de los casos el sistema pasa a ser pseudocaótico y sus propiedades como estocasticidad, mezcla, período y exponente de Lyapunov se ven degradadas. Uno de los aportes de esta tesis es el estudio de esta degradación en función de la granularidad de la aritmética representada en un sistema electrónico digital.

Por el lado de los TRNG, está bien establecido que un oscilador en anillo (RO) presenta fluctuaciones de fase (jitter) que depende de procesos puramente físicos como gradientes durante el proceso de difusión en la fabricación del circuito integrado, gradientes en la temperatura de trabajo, ruido térmico en las junturas semiconductoras, etc. Como los ROs son comúnmente utilizados como generadores de señales de reloj para sincronizar sistemas el jitter suele ser un problema, sin embargo en esta tesis son la fuente de aleatoriedad física que aprovechamos para generar señales estocásticas. Se propuso un método basado en entropías diferenciales que permite extraer un valor que indica la aleatoriedad de una serie binaria y, por lo tanto, puede indicar el nivel de jitter que contiene. Este método es útil para catalogar un dado RO como bueno para generar ruido o como señal de reloj. Además, se implementó un TRNG basado en ROs mediante la mezcla de varios osciladores.

Esta tesis se basa en doce trabajos originales, nueve de ellos publicados como trabajos completos de congresos con referato y tres publicados en revistas indexadas de los cuales soy el primer autor de dos de ellos [?]. Estos trabajos están ordenados en los últimos cuatro capítulos de esta tesis.

El primer capítulo (cap. 2) es una introducción a los sistemas dinámicos caóticos utilizados a lo largo de la tesis. El segundo capítulo (cap. 3) contiene, por un lado una introducción a los cuantificadores de aleatoriedad que se utilizan para medir los generadores de números, y por otro, algunos avances en la implementación de estos cuantificadores en hardware electrónico (FPGA). El capítulo 4 presenta algunos avances en generadores de números aleatorios utilizando sistemas caóticos y sus aplicaciones. En cap. 5 se estudia la degradación estadística de los mapas caóticos cuando son implementados en aritmética discreta. Y por último en el capítulo 6, primero se propone la utilización de cuantificadores de la teoría de la información para medir la mezcla y estocasticidad de la fuente de incertezas en RO's, luego se muestran los resultados de la implementación en FPGA de un TRNG utilizando RO's.

## Capítulo 2

# Sistemas de dinámica compleja

Ha quedado claro que existen sistemas deterministas que rompen con el preconcepto de que los sistemas físicos pueden clasificarse en dos conjuntos disjuntos: sistemas deterministas y sistemas estocásticos. En esa concepción antigua un sistema determinista es aquél para el cual conocemos el modelo y por lo tanto es posible predecir con exactitud la evolución de sus variables de estado. Se utilizan en su descripción ecuaciones diferenciales o de recurrencia. Por otra parte un sistema estocástico es aquél para el cual el modelo no se conoce o se lo supone sumamente complejo como para ser obtenido, de modo que se adopta la estrategia de estudiar sus variables de estado en forma estadística. Se utilizan entonces en la descripción ecuaciones diferenciales o de recurrencia estocásticas.

El caos determinista demostró que complejidad en la evolución temporal no es sinónimo de complejidad en el modelo, cuando hay no linealidad: modelos deterministas muy simples originan señales de aspecto estocástico. La sensibilidad a las condiciones iniciales hace que en estos sistemas la predictibilidad sea a corto plazo (luego de un tiempo finito es imposible predecir la evolución) lo que ubica a estos sistemas en una posición intermedia entre determinista y estocástico.

Como consecuencia se desarrollaron en los últimos años un número creciente de aplicaciones de los sistemas caóticos, empleándolos principalmente como generadores de ruido controlado, generadores de números pseudoaleatorios, portadoras de señales, sistemas de encriptado, etc.

Hoy en día, los sistemas dinámicos son un objeto de estudio interdisciplinario, aunque originalmente fue una rama de la física. Todo comenzó a mediados del 1600, cuando

Newton inventó las ecuaciones diferenciales, descubriendo sus leyes del movimiento de gravedad universal, y las combinó con las leyes de Kepler sobre el movimiento planetario. Específicamente, Newton resolvió el problema de los dos cuerpos (por ejemplo el sistema tierra-sol).

Subsecuentes generaciones de matemáticos y físicos intentaron extender los métodos analíticos de Newton al problema de los tres cuerpos (por ejemplo luna-tierra-sol), pero curiosamente para resolver este problema se necesitó mucho más esfuerzo. Luego de décadas, se dieron cuenta de que el problema de los tres cuerpos era esencialmente imposible de resolver, en el sentido de obtener las fórmulas explícitas.

La ruptura vino con el trabajo de Poincaré a finales del 1800. Él introdujo un nuevo punto de vista que enfatizaba las cuestiones cualitativas más que las cuantitativas (por ejemplo, ¿es estable el sistema luna-tierra-sol?). Poincaré desarrolló una poderosa aproximación geométrica que es usada hoy para estudiar sistemas dinámicos y también fue el primero en vislumbrar la posibilidad del caos, en el cual un sistema determinístico exhibe un comportamiento aperiódico que depende sensiblemente de las condiciones iniciales, haciendo así imposible la predicción a largo plazo.

Pero el caos se mantuvo en segundo plano hasta la segunda mitad del 1900, en donde los osciladores no lineales jugaron un rol vital en el desarrollo de tecnologías de radio, radar, lazos de enganche de fase y láser. Por el lado matemático, los osciladores no lineales también estimularon la invención de nuevas técnicas matemáticas. Los métodos geométricos de Poincaré se fueron extendiendo para producir un conocimiento mucho más profundo de la mecánica clásica.

La invención de la computadora por el 1950 fue una línea divisoria en la historia de los sistemas dinámicos. La computadora nos permite experimentar con ecuaciones en una forma que antes era imposible, y así desarrollar alguna intuición acerca de los sistemas no lineales. Estos experimentos llevaron a Lorenz a descubrir en 1963 el movimiento caótico de un atractor extraño, mientras estudiaba un modelo simplificado de la circulación de convección para comprender mejor la notoria impredecibilidad del clima. Lorenz encontró que la solución a sus ecuaciones nunca caían al equilibrio o a un estado periódico. Además, si comenzaba sus simulaciones de dos condiciones iniciales ligeramente diferentes, los comportamientos resultantes pronto serían totalmente diferentes. Como consecuencia de ello, el sistema es inherentemente impredecible, pequeños errores en las mediciones del estado actual de la atmósfera (o cualquier sistema caótico) sería amplificado rápidamente.

Pero Lorenz también mostró que había estructura en el caos, cuando las soluciones fueron dibujadas en tres dimensiones, las soluciones a sus ecuaciones cayeron sobre un conjunto de puntos en forma de mariposa. Él sostuvo que este sistema tenía que ser “un infinito complejo de superficies”, lo que hoy podríamos considerar como un ejemplo de fractal.

El trabajo de Lorenz tuvo un pequeño impacto hasta 1970, los años del boom del caos. Se desarrollaron teorías completamente nuevas basadas en consideraciones sobre atractores caóticos, como turbulencia de fluidos y biología de las poblaciones y se encontraron comportamientos caóticos en reacciones químicas, circuitos electrónicos, osciladores mecánicos, semiconductores y oscilaciones biológicas como el ritmo cardíaco y circadiano. Hoy, la teoría del caos es un herramienta más para el estudio de sistemas dinámicos y los sistemas caóticos forman parte de una gran cantidad de dispositivos.

En este capítulo revisamos los conceptos de espacio de fases, pasando por las soluciones típicas de sistemas de ecuaciones diferenciales, para luego poder entrar a la descripción de sistemas caóticos. Primero abordamos los sistemas caóticos continuos con derivada continua y presentamos tres ejemplos clásicos en la literatura. Luego hacemos una reseña a los mapas caóticos, en donde presentamos los mapas cuadráticos bidimensionales, los cuales usaremos en algunas secciones subsiguientes.

## 2.1. Teoría Cualitativa - Espacio de Fases

En algunas aplicaciones puede interesar, más que conocer las ecuaciones explícitas de las soluciones de un sistema, poder analizar sus propiedades cualitativas, tales como la periodicidad, el comportamiento cuando crece la variable independiente (la que se supone que es el tiempo), si es constante, o si se aproxima a una solución conocida, etc. Una herramienta útil en este sentido es el diagrama de fase. El espacio de fase es el lugar geométrico que ocupan las posibles soluciones del sistema de ecuaciones diferenciales, en él se dibujan las trayectorias que son solución a un sistema de ecuaciones. La teoría cualitativa intenta clasificar los sistemas en función del tipo de trayectorias que poseen, en lugar de intentar resolver las ED's.

Se denomina punto crítico de un sistema de ecuaciones diferenciales, al punto del espacio de estados que satisface

$$X' = 0 \quad (2.1)$$

es el punto del espacio de estados a partir del cual el sistema no evoluciona.

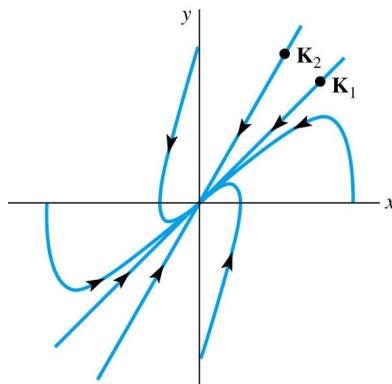


Figura 2.1: Nodo estable

Para sistemas homogéneos de ED lineales, el único punto crítico es el origen de coordenadas. Para sistemas no homogéneos de ED lineales, el punto crítico puede ser cualquier punto del espacio. Para sistemas no lineales, pueden existir varios puntos críticos, o ninguno.

Para un sistema planar, pueden darse las siguientes trayectorias respecto de los dos autovalores.

**Nodo estable** Si ambos autovalores son negativos, la solución se acerca al origen asintóticamente. Las trayectorias de las soluciones son asintóticas a los autovalores de la matriz de coeficientes  $A$ , excepto las soluciones con condiciones iniciales que pertenecen a las direcciones propias, entonces el sistema evoluciona sobre ellas.

**Nodo inestable** Si ambos autovalores son positivos, la solución se aleja del origen. Las trayectorias de las soluciones son asintóticas a los autovalores de la matriz de coeficientes  $A$ , excepto las soluciones con condiciones iniciales que pertenecen a las direcciones propias, entonces el sistema evoluciona sobre ellas.

**Punto silla** Si los autovalores tienen signos opuestos, la solución se aleja del origen asintóticamente a uno de los autovectores y se approxima a él asintóticamente al otro, excepto las soluciones con condiciones iniciales que pertenecen a las direcciones propias, entonces el sistema evoluciona sobre ellas.

**Nodos degenerados** Aparecen en los casos en que los autovalores o autovectores sean iguales. Para iguales autovalores, pueden generarse todas las trayectorias radiales por

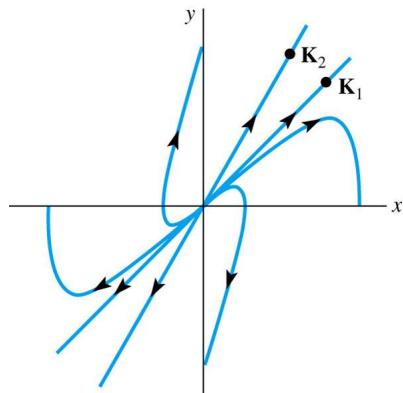


Figura 2.2: Nodo inestable

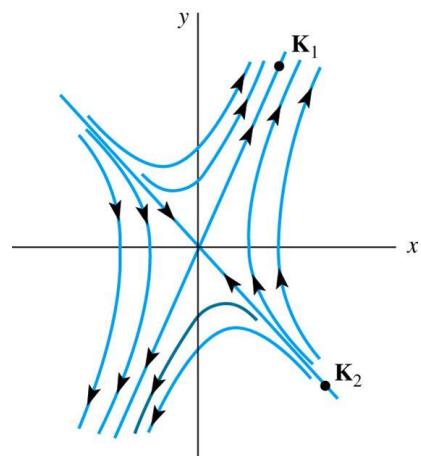


Figura 2.3: Punto silla

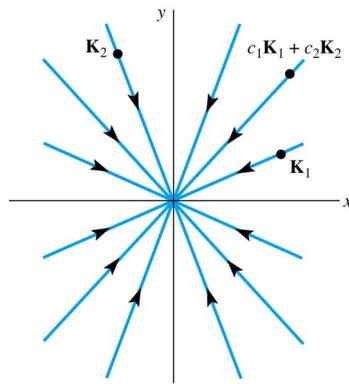


Figura 2.4: Nodo estable degenerado con autovalores negativos

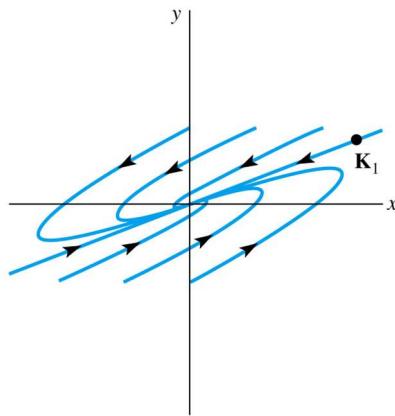


Figura 2.5: Nodo estable degenerado con autovalores negativos y un solo autovector

combinación lineal de los autovectores. La forma de la solución sería

$$X(t) = (c_1 K_1 + c_2 + K_2) e^{\lambda t}$$

Si los autovalores son negativos, la solución se acerca al origen en forma radial y el nodo resulta ser estable, de lo contrario será inestable. Si además tenemos iguales autovectores, la forma de la solución sería

$$X(t) = (c_1 K + t C_2 K + c_2 P) e^{\lambda t}$$

Si los autovalores son negativos, la solución se acerca al origen y el nodo resulta ser estable, de lo contrario será inestable.

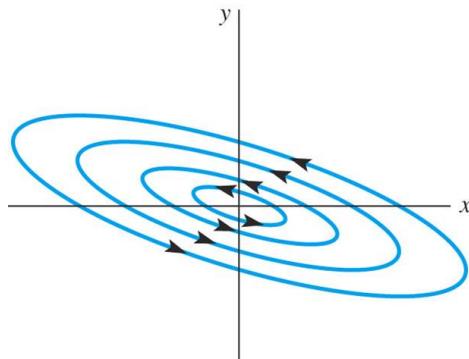


Figura 2.6: Centro

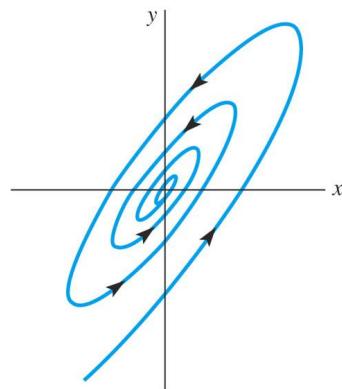


Figura 2.7: Foco estable

**Centro** Si los autovalores son imaginarios puros, la solución describe elipses concéntricas que pasan por el valor inicial.

**Foco estable** Si los autovalores son complejos con parte real negativa, la solución es una combinación de los casos anteriores. Será periódica conforme su parte imaginaria y se aproximará a cero según su parte real.

**Foco inestable** Si los autovalores son complejos, la solución será periódica conforme su parte imaginaria y se aproximará tenderá a infinito según su parte real.

Para cualquier sistema de ED, primero se deben hallar todos los puntos críticos del sistema. Luego, se linealiza en torno a cada uno mediante el primer término de la serie de Taylor obteniendo tantos sistemas de ecuaciones como puntos críticos tenga el sistema. Estos sistemas son válidos en un entorno suficientemente pequeño del punto crítico.

Por ejemplo, supongamos que se necesita trazar el diagrama de fase para el péndulo

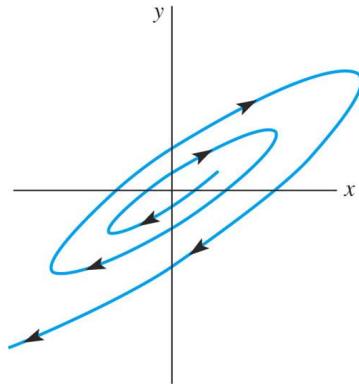


Figura 2.8: Foco inestable

físico de la figura 2.9.

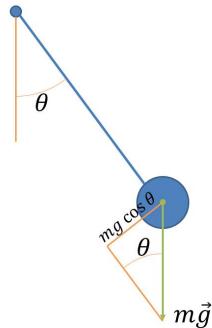


Figura 2.9: Péndulo físico ideal.

Primero hallamos la ecuación de la aceleración, según la figura, la componente tangencial de la gravedad es la que acelera al cuerpo. Tomando como referencia positiva el sentido dextrógiro, queda

$$a = mg \cos \theta - \mu v$$

en donde  $\mu$  es el coeficiente de roce viscoso con el aire y  $v$  la velocidad. Pero como nos interesa la aceleración angular  $\alpha$  y la velocidad angular  $\omega$

$$\alpha = a/l; \quad \omega = v/l$$

siendo  $l$  la longitud de la cuerda.

La aceleración angular  $\alpha$  es la derivada de la velocidad angular  $\omega$  que a su vez es la

derivada del ángulo  $\theta$

$$\alpha = \omega' = \theta''$$

entonces el sistema de ecuaciones queda

$$\begin{cases} \theta' = \omega \\ \omega' = \frac{mg}{l} \cos \theta - \frac{\mu}{l} \omega \end{cases}$$

Una vez planteado el sistema de ecuaciones, el primer paso es hallar los puntos críticos del sistema.

$$\begin{cases} 0 = \omega \\ 0 = \frac{mg}{l} \cos \theta - \frac{\mu}{l} \omega \end{cases} \rightarrow \begin{cases} 0 = \omega \\ \theta = (2n-1)\frac{\pi}{2} \quad n \notin \mathbb{Z} \end{cases}$$

Ahora estamos en condiciones de linealizar el sistema en torno de los puntos críticos.

$$\begin{cases} \theta' = \omega \\ \omega' = \left. \frac{\partial(\frac{mg}{l} \cos \theta)}{\partial \theta} \right|_{\theta=(2n-1)\frac{\pi}{2}} \theta - \frac{\mu}{l} \omega \end{cases} = \begin{cases} \theta' = \omega \\ \omega' = -\frac{mg}{l} \sin(\theta) \left. \right|_{\theta=(2n-1)\frac{\pi}{2}} \theta - \frac{\mu}{l} \omega \end{cases}$$

Según  $n$  sea par (incluyendo el cero) o impar, la ecuación lineal que representa al sistema será diferente.

Si  $n$  es par o cero

$$\begin{cases} \theta' = \omega \\ \omega' = \frac{mg}{l} \theta - \frac{\mu}{l} \omega \end{cases} \rightarrow A = \begin{pmatrix} 0 & 1 \\ \frac{mg}{l} & -\frac{\mu}{l} \end{pmatrix}$$

$$\det(A - \lambda I) = \begin{vmatrix} -\lambda & 1 \\ \frac{mg}{l} & -\frac{\mu}{l} - \lambda \end{vmatrix} = \lambda^2 + \frac{\mu}{l} \lambda - \frac{mg}{l}$$

los autovalores son reales y de distinto signo (punto silla).

Si  $n$  es impar

$$\begin{cases} \theta' = \omega \\ \omega' = -\frac{mg}{l} \theta - \frac{\mu}{l} \omega \end{cases}$$

$$\det(A - \lambda I) = \begin{vmatrix} -\lambda & 1 \\ -\frac{mg}{l} & -\frac{\mu}{l} - \lambda \end{vmatrix} = \lambda^2 + \frac{\mu}{l} \lambda + \frac{mg}{l}$$

los autovalores son complejos conjugados con parte real negativa (foco estable).

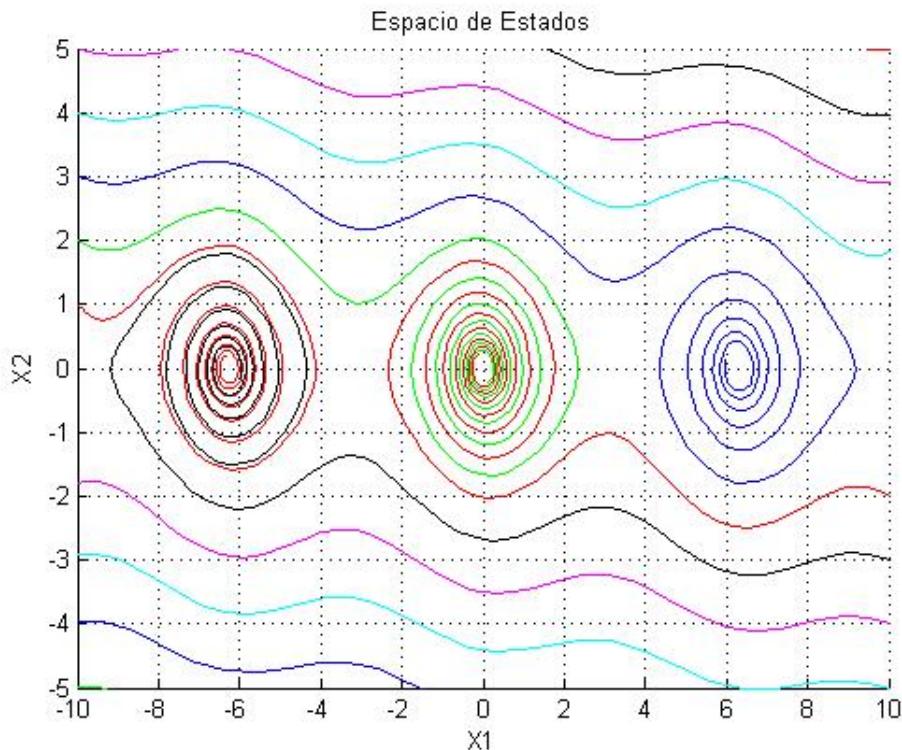


Figura 2.10: Diagrama de fase del péndulo físico real

La resolución numérica en Matlab (figura 2.10, muestra las soluciones al sistema elíptico en el espacio de estados. Puede verse que en los puntos críticos, la solución se aproxima a un foco o a un punto silla, según el valor de  $n$ .

## 2.2. Sistemas caóticos

Cuando se miden variables físicas, no es muy extraño encontrar que el plano de fases tiene un comportamiento similar al de la figura 2.11. Puede verse que las trayectorias se cortan en el plano de fases, lo que indica que el sistema tiene un orden mayor que dos. Otra observación que se puede hacer es que las trayectorias no se repiten, es decir que, aunque la oscilación persiste, no aparece un ciclo con trayectoria definida. Esta última propiedad clasifica al sistema que se está midiendo como caótico.

El teorema de existencia y unicidad de las soluciones a un sistema de ecuaciones garantiza que si  $f$  es continuamente diferenciable, los campos vectoriales sobre el espacio

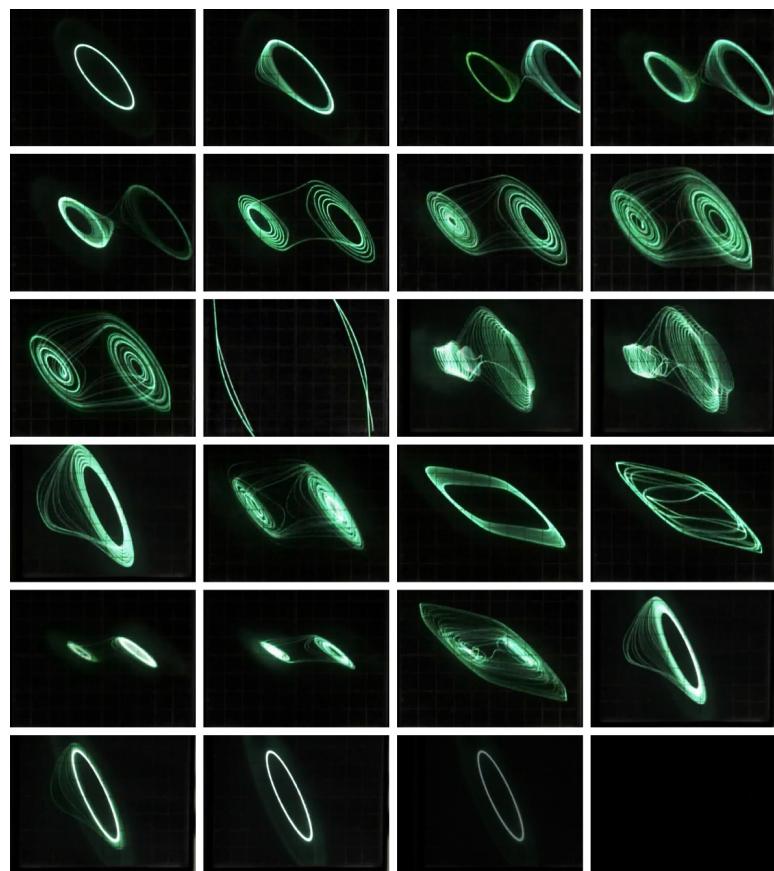


Figura 2.11: Salidas de tensión de dos variables de un circuito oscilador

de fases son suaves y cada punto de este espacio tiene solución única. La existencia de este teorema tiene un corolario importante: trayectorias diferentes nunca se intersectan. Como consecuencia de esto, las trayectorias sobre el plano de fases quedan restringidas a: un nodo estable o inestable, centro, foco estable o inestable y puerto. Entonces queda claro que un sistema continuo con derivada continua debe tener dimensión mayor o igual a tres para que pueda ser caótico, además, la trayectoria en el espacio de fases debe ocupar un dominio restringido.

Para describir analíticamente el comportamiento de este tipo de sistemas en torno a ciertos puntos de interés podemos hacer uso del álgebra lineal. Lo que sigue son tres ejemplos de aplicaciones para atractores caóticos.

El primer y más común ejemplo es el sistema de Lorenz, que está descrito por el siguiente sistema de ecuaciones diferenciales [1]

$$\begin{cases} x'_1 &= \sigma(x_1 - x_2) \\ x'_2 &= -x_1x_3 + \rho x_3 - x_2 \\ x'_3 &= x_1x_2 - \beta x_3 \end{cases} \quad (2.2)$$

El sistema de Lorenz tiene tres puntos de equilibrio,  $E$ ,  $E^+$  y  $E^-$ : el primer punto de equilibrio  $E$  está situado en el origen  $(0,0,0)$  y los otros dos tienen respectivamente como coordenadas,

$$(x_1^\pm, x_2^\pm, x_3) = (\pm\sqrt{\beta(\rho-1)}, \pm\sqrt{\beta(\rho-1)}, \rho-1)$$

El comportamiento físico interesante de este sistema ocurre cuando variamos el parámetro de control  $\rho$ . Cuando  $\rho < 1$ , todas las órbitas del campo vectorial dado por 2.2 tienden al punto fijo situado en el origen. A medida que se va incrementando más allá de la unidad, el origen pasa a ser inestable dando lugar a dos puntos fijos, estables, y simétricos  $E^+$  y  $E^-$ . Para todo  $\rho < 1$ , la geometría del comportamiento asintótico del sistema es la misma ya que todas las condiciones iniciales tienden al origen E.

Para  $\rho > 1$ , se observan dos comportamientos. El primero, asociado a valores de  $\rho$  menores que un cierto valor de umbral  $\rho_h = (\sigma(\sigma+\beta)+3\sigma)/(\sigma-\beta-1)$ , valor para el cual los puntos de equilibrio  $E^+$  y  $E^-$  pierden su estabilidad. Dentro de este rango de valores del parámetro todas las órbitas terminan en uno de los dos puntos de equilibrio dependiendo de las condiciones iniciales.

Cuando  $\rho > \rho_h$ , la situación cambia drásticamente. Los dos puntos fijos pasan a ser

inestables y nuevos comportamientos pueden surgir. Para estudiar estos comportamientos se considera el análisis dinámico del sistema 2.2. La linealización del sistema 2.2 en la proximidad del origen nos proporciona los siguientes autovalores:

$$\lambda = -\beta; \lambda_{\pm} = \frac{1}{2} \left( -(\sigma + 1) \pm \sqrt{(\sigma + 1)^2 + 4\sigma(\rho - 1)} \right)$$

asociados a la matriz Jacobiana

$$\begin{pmatrix} -\sigma & \sigma & 0 \\ \rho & -1 & 0 \\ 0 & 0 & -\beta \end{pmatrix}$$

Los autovalores  $\lambda$  y  $\lambda_-$  son siempre negativos; el autovalor  $\lambda_+$  cambia de negativo a positivo cuando  $\rho$  pasa por el valor 1.

De modo similar, la linealización del sistema 2.2 en la proximidad del punto de equilibrio  $E^+$  nos proporciona los siguientes autovalores:

$$\lambda^3 + \lambda^2(\sigma + \beta + 1) + \lambda\beta(\sigma + \rho) + 2\sigma\beta(\rho - 1) = 0$$

asociados a la matriz Jacobiana

$$\begin{pmatrix} -\sigma & \sigma & 0 \\ \rho - x_3 & -1 & -x_1 \\ x_2 & x_1 & -\beta \end{pmatrix}$$

tiene un autovalor real negativo  $\lambda$  combinado con dos autovalores imaginarios puros,  $\lambda_{\pm} = \pm j\alpha$ , si  $\rho < \rho_h$

La linealización del sistema 2.2 en la proximidad del punto de equilibrio  $E^+$  es un problema simétrico a este.

En la figura 2.12 pueden verse la evolución de las soluciones al sistema de Lorenz.

El sistema de Rössler está descrito por el siguiente sistema de ecuaciones diferenciales

$$\begin{cases} x'_1 &= x_2 - x_3 \\ x'_2 &= x_1x_3 + ax_2 \\ x'_3 &= b + (x_1 + c)x_3 \end{cases} \quad (2.3)$$

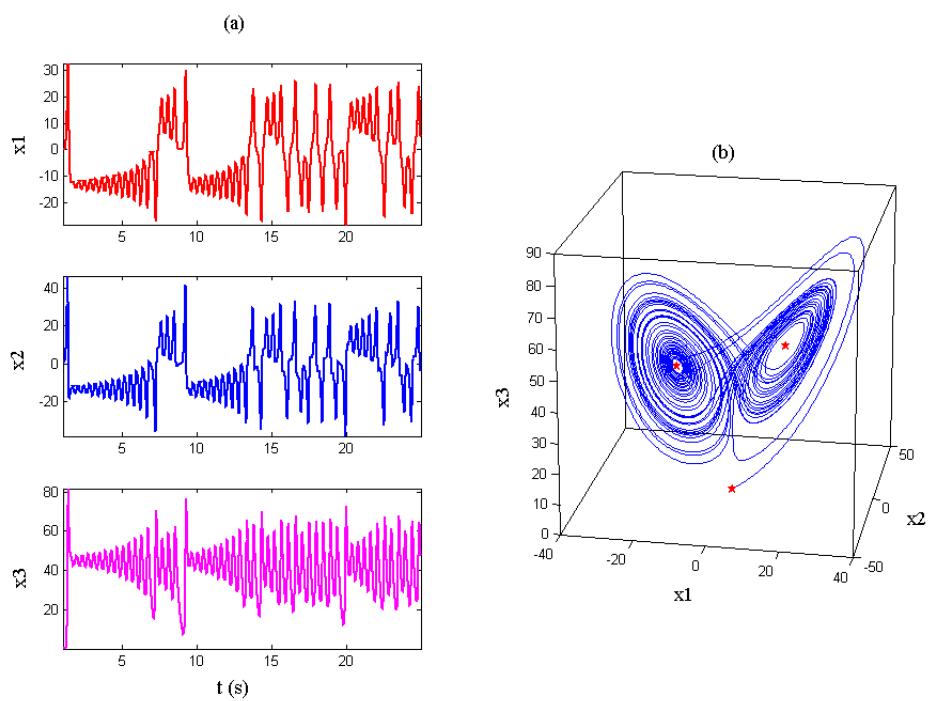


Figura 2.12: (a) Evolución temporal de las tres variables del sistema de Lorenz.(b) Disposición de sus puntos de equilibrio (estrellas rojas) con respecto a su atractor en el espacio de estados.

Este sistema tiene dos puntos de equilibrio,  $E^+$  y  $E^-$  que existen solo cuando  $\Delta = c^2 - 4ab > 0$  y cuyas coordenadas están dadas respectivamente por,

$$(x_1^\pm, x_2^\pm, x_3^\pm) = \left( \frac{1}{2}(c \pm \sqrt{\Delta}), -\frac{1}{2a}(c \pm \sqrt{\Delta}), \frac{1}{2a}(c \pm \sqrt{\Delta}) \right)$$

La linealización del sistema 2.3 en la proximidad de los puntos de equilibrio proporciona los siguientes autovalores:

$$a\lambda^3 - \lambda^2 a(x_1 - c) - \lambda(x_3 - 1) + ax_3 + (x_1 - c) = 0$$

asociados a la matriz Jacobiana

$$\begin{pmatrix} 0 & 1 & -1 \\ 1 & a & 0 \\ x_3^\pm & 0 & x_1^\pm - c \end{pmatrix}$$

de donde se deduce que fijando los parámetros  $a$  y  $b$  y variando  $c$  nos encontramos con dos escenarios diferentes, podemos tener un autovalor real negativo y dos complejos conjugados con parte real positiva, o un autovalor real negativo y dos complejos conjugados con parte real negativa. Para valores pequeños de  $c$ , el atractor de Rössler consiste en una órbita periódica o ciclo límite que tiene un sólo mínimo local. A medida que vamos incrementando el parámetro  $c$ , el ciclo límite va duplicando su periodo y como consecuencia, sus mínimos locales hasta alcanzar un límite en el cual las trayectorias nunca se repiten lo que corresponde al atractor caótico de Rössler.

En la figura 2.13 pueden verse la evolución de las  $x_1$  y  $x_2$  al sistema de Rössler para distintos valores del parámetro  $c$ . En la figura 2.14, la evolución de las tres variables para un parámetro fijo.

El sistema de Chua está descrito por el siguiente sistema de ecuaciones diferenciales

$$\begin{cases} x'_1 &= \alpha x_2 - \alpha x_1^3 - \alpha c x_1 \\ x'_2 &= x_1 + x_3 - x_2 \\ x'_3 &= -\beta x_2 \end{cases} \quad (2.4)$$

Tiene tres puntos de equilibrio,  $E$ ,  $E^+$  y  $E^-$ : el primer punto de equilibrio  $E$  está situado

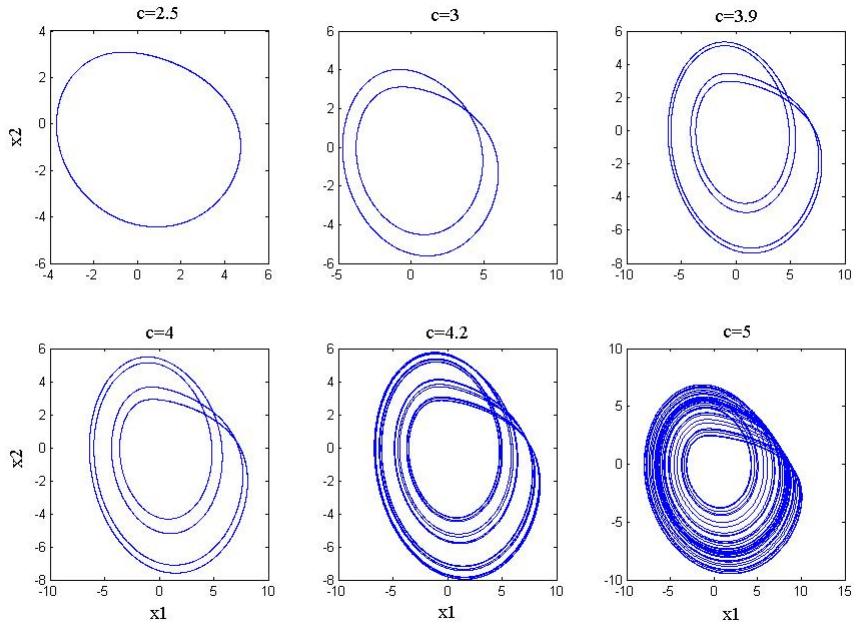


Figura 2.13: Proyecciones del atractor de Rössler en el plano para diferentes valores del parámetro  $c$ .

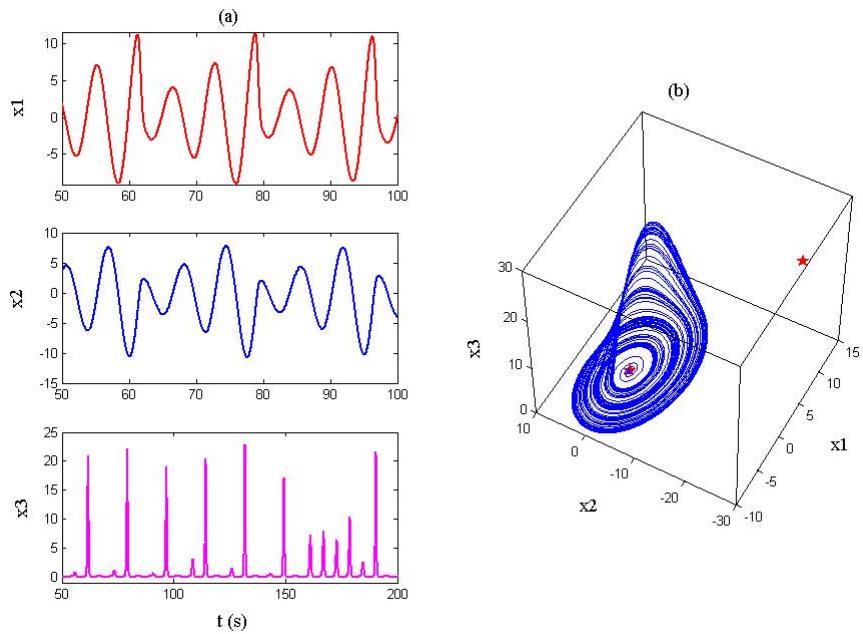


Figura 2.14: (a) Evolución temporal de las tres variables del sistema de Rössler. (b) Disposición de sus puntos de equilibrio (estrellas rojas) con respecto a su atractor en el espacio de estados.

en el origen  $(0,0,0)$  y los otros dos tienen respectivamente como coordenadas,

$$(x_1^\pm, x_2^\pm, x_3) = (\pm\sqrt{-c}, 0, \pm\sqrt{-c})$$

Los puntos de equilibrio existen sólo para valores positivos del parámetro  $c$ .

La linealización del sistema 2.4 en la proximidad de los puntos de equilibrio proporciona los siguientes autovalores:

$$\lambda^3 + \lambda^2 \alpha(\alpha c + 1) + \lambda(\alpha c - \alpha + \beta) + \alpha x_3 + \alpha \beta c = 0$$

asociados a la matriz Jacobiana

$$\begin{pmatrix} -\alpha c & \alpha & 0 \\ 1 & -1 & 1 \\ 0 & -\beta & 0 \end{pmatrix}$$

donde podemos detectar un punto de bifurcación para  $\alpha = 0$  en el cual el autovalor real negativo pasa a ser positivo provocando la inestabilidad del punto de equilibrio  $E$  que permanece inestable para una amplia gama de valores del parámetro  $\alpha$ .

En la figura 2.15, puede verse la evolución de las tres variables de estado para este sistema.

## 2.3. Mapas caóticos

|||||||||||||||Hablar de mapas como Logístico, tent, etc..!!!!!!!!!!!!!!

### 2.3.1. Mapas cuadráticos bidimensionales

La familia de mapas cuadráticos bidimensionales que estudiamos aquí es modelada por un par de ecuaciones cuadráticas acopladas:

$$\begin{cases} x_{n+1} = a_1 + a_2 x_n + a_3 x_n^2 + a_4 x_n y_n + a_5 y_n + a_6 y_n^2 \\ y_{n+1} = a_7 + a_8 x_n + a_9 x_n^2 + a_{10} x_n y_n + a_{11} y_n + a_{12} y_n^2 \end{cases} \quad (2.5)$$

donde  $\{x, y\}$  son las variables de estado y  $A = \{a_i, i = 1, \dots, 12\}$  son los parámetros. La principal característica de este sistema es que presenta múltiples atractores caóticos en

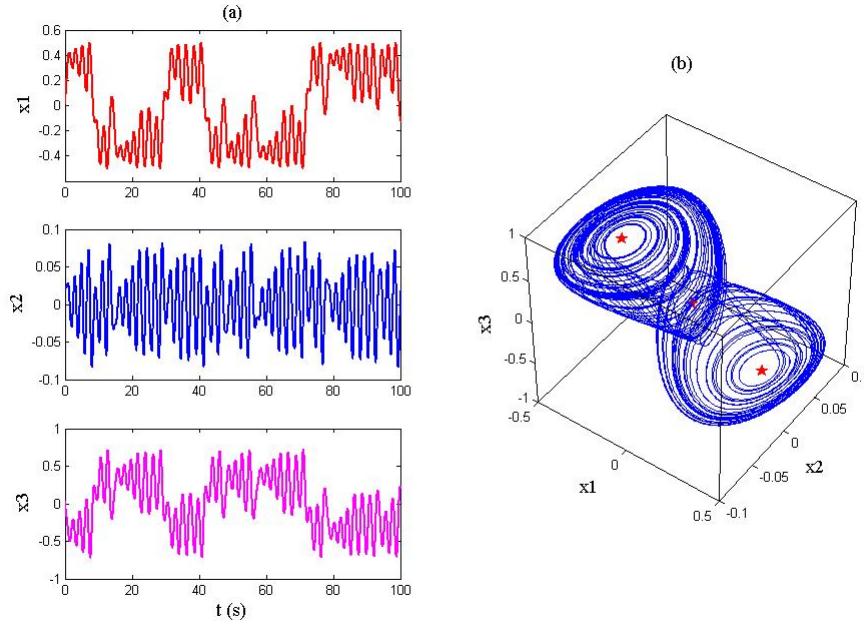


Figura 2.15: (a) Evolución temporal de las tres variables del sistema de Chua. (b) Disposición de sus puntos de equilibrio (estrellas rojas) con respecto a su atractor en el espacio de estados.

función del punto seleccionado en el espacio del parámetros. El espacio de parámetros de  $12D$  generado por los coeficientes  $A$  es muy difícil de explorar.

Las razones para estudiar este sistema en particular son dobles:

1. Usando la aritmética de punto flotante con un barrido automático de parámetros  $a_i$  y una gran cantidad de puntos en el espacio del parámetro (alrededor de  $6 \cdot 10^{16}$ ), Sprott pudo detectar varios atractores en régimen caótico permanente. Es decir, tienen la característica de modificar su atractor según los valores que tomen sus 12 coeficientes reales. Él también encontró una relación entre la dimensión de correlación y los exponentes de Lyapunov, con su estética visual, un tema interesante para la generación automática de arte.
2. Es posible emplear estos atractores en una amplia variedad de aplicaciones electrónicas, como la generación de nuevos sistemas de encriptación, ya sea reemplazando el S-box en AES [?, ?], o incluso desarrollando nuevos algoritmos [?, ?].

Tres de estos atractores caóticos se muestran juntos en la figura 2.16. Sus juegos de

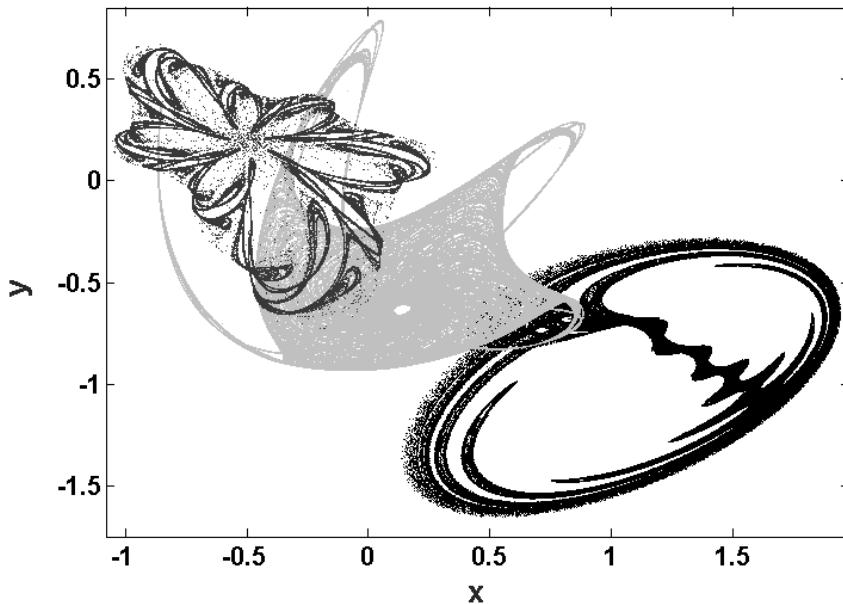


Figura 2.16: Tres atractores para tres juegos de parámetros distintos.

parámetros  $A_i$  son:

$$\begin{aligned}
 A_1 &= \{-0,7, -0,4, 0,5, -1,0, -0,9, -0,8, 0,5, 0,5, 0,3, 0,9, -0,1, -0,9\}, \\
 A_2 &= \{-0,6, -0,1, 1,1, 0,2, -0,8, 0,6, -0,7, 0,7, 0,7, 0,3, 0,6, 0,9\}, \\
 A_3 &= \{-0,1, 0,8, -0,7, -1,1, 1,1, -0,7, -0,4, 0,6, -0,6, -0,3, 1,2, 0,6\}.
 \end{aligned} \tag{2.6}$$

Como se puede ver en la figura, es posible obtener salidas muy diferentes simplemente modificando el valor de los parámetros y manteniendo la estructura del sistema. En una implementación electrónica, esto sería equivalente a poder variar la salida manteniendo la estructura del hardware y modificando los parámetros a través de, por ejemplo, una entrada.

Las figuras 2.17.a a 2.17.d muestran los mismos tres atractores  $A_1$  a  $A_3$  de la Fig. 2.16 junto a un atractor con  $A_4 = \{-1,0,9,0,4, -0,2, -0,6, -0,5, 0,4, 0,7, 0,3, -0,5, 0,7, -0,8\}$ , superpuestos con sus regiones de atracción (en gris). Las áreas blancas de cada figura corresponden a aquellas condiciones iniciales que generan trayectorias divergentes del sistema (semillas inútiles con respecto a su uso como PRNG).

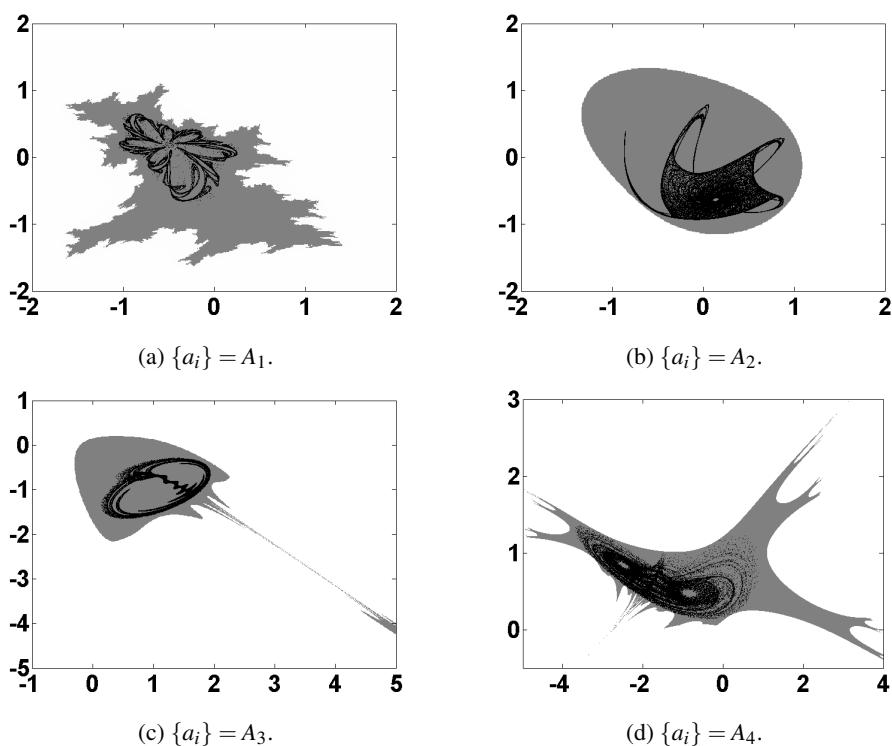


Figura 2.17: Cuatro atractores caóticos y sus respectivos dominios de atracción.

## Capítulo 3

# Cuantificadores de Aleatoriedad

Los sistemas dinámicos son sistemas que evolucionan en el tiempo. En la práctica, solo es posible medir una serie de tiempo escalar  $X(t)$  la cual puede ser función de las variables  $V = \{v_1, v_2, \dots, v_k\}$  que describe la dinámica subyacente (por ejemplo  $dV/dt = f(V)$ ). Tratamos de inferir propiedades de un sistema no conocido a partir del análisis de los datos guardados de variables observacionales. ¿Cuanta información revelan estos datos sobre la dinámica del sistema o procesos subyacentes?

El contenido de información de un sistema se evalúa típicamente mediante una función de distribución de probabilidad (PDF)  $P$  que describe la distribución de alguna cantidad mensurable o observable, generalmente una serie de tiempo  $X(t)$ . Podemos definir los cuantificadores de la Teoría de la Información como medidas capaces de caracterizar las propiedades relevantes de las PDFs asociadas a estas series temporales, y de esta manera debemos extraer juiciosamente información sobre el sistema dinámico en estudio. Estos cuantificadores representan métricas en el espacio de PDFs para conjuntos de datos, permitiendo comparar diferentes conjuntos y clasificarlos de acuerdo a sus propiedades de procesos subyacentes, de manera amplia, estocástica vs. determinística.

En nuestro caso, nos interesa la dinámica caótica. Por lo tanto, nos centramos en las métricas que toman en cuenta el orden temporal de las observaciones de forma explícita; es decir, el enfoque es fundamentalmente de naturaleza *causal* y *estadística* en la naturaleza. En un enfoque puramente estadístico, las correlaciones entre los valores sucesivos de las series temporales se ignoran o simplemente se destruyen a través de la construcción del PDF; mientras que un enfoque causal se centra en las PDFs de secuencias de datos. Además,

los exponentes de Lyapunov permiten analizar los datos de un punto de vista topológico y brindan una valiosa información acerca de la caoticidad del sistema.

En este capítulo primero se presenta al Máximo Exponente de Lyapunov (MLE) como un detector de caos, para luego presentar un caso de aplicación de un algoritmo de búsqueda de caos. Este algoritmo fue presentado en [?] y muestra la factibilidad de la búsqueda automática de caos con algoritmos eurísticos basados en el MLE. Después se presenta una implementación en FPGA del mismo algoritmo pero aplicado a los mapas cuadráticos bidimensionales presentados en 2.3.1, esta implementación ya cuenta con cierto grado de avance.

En la segunda sección de este capítulo se presentan una serie cuantificadores de aleatoriedad provenientes de la teoría de la información. Estos cuantificadores se utilizan luego a través del resto de esta tesis como una herramienta de análisis, con ella se evalúa la calidad de los generadores de números aleatorios. Después mostramos los resultados presentados en [?], en donde se implementaron estas herramientas en FPGA. La implementación de estos cuantificadores surge como una solución práctica, así es posible medir la calidad de los generadores en la misma plataforma, sin la necesidad de extraer los datos y medirlos en una computadora. Aprovechando la disponibilidad de entradas analógicas en el kit de desarrollo, al diseño se le agregó la posibilidad de medir señales analógicas externas. Cuando se midieron señales de prueba bien conocidas, los resultados mostraron ciertos corrimientos de los valores esperados debido a la contaminación con ruido aditivo (AWGN) y a la limitación en la banda de paso inherentes a todo sistema analógico. Esto abre la inquietud de caracterizar el comportamiento de los cuantificadores frente a estos dos factores, en la sección 3.2.6 se realiza un estudio al respecto.

### 3.1. Máximo Exponente de Lyapunov

¿Qué es lo que diferencia a un ciclo límite o una órbita cerrada de una órbita caótica? Una órbita caótica (atractor caótico) es aperiódica, es decir que nunca se repite exactamente y la oscilación persiste para  $t \rightarrow \infty$ . El movimiento sobre un atractor exhibe una dependencia sensible a las condiciones iniciales. Esto significa que dos trayectorias que comienzan muy cercanas, rápidamente divergen una de otra, por lo que tendrán futuros muy diferentes. La implicación práctica de esto es que la predicción a largo plazo se vuelve imposible en un sistema como este, en donde pequeñas incertezas son amplificadas rápidamente.

Hagamos estas ideas un poco más precisas. Supongamos que te tenemos una trayectoria sobre el atractor y un punto  $x(t)$  perteneciente a dicha trayectoria en un instante  $t$ , ahora consideremos un punto vecino  $x(t) + \delta_0$ , en donde  $\delta_0$  es una pequeña separación inicial. Ahora veamos como evoluciona esta separación  $\delta(t)$ . Encontramos que

$$\|\delta(t)\| \sim \|\delta_0\| e^{\lambda t} \quad (3.1)$$

Por lo tanto, trayectorias vecinas se separan a un ritmo exponencial. El número  $\lambda$  es llamado exponente de Lyapunov. Cuando este exponente es positivo, se dice que el sistema tiene un horizonte de tiempo  $t_h$  más allá del cual la predicción falla por una tolerancia  $a$ , de modo que

$$t_h \sim O\left(\frac{1}{\lambda} \ln \frac{a}{\|\delta_0\|}\right) \quad (3.2)$$

Como este sistema presenta un horizonte de tiempo, puede decirse que es sensible a las condiciones iniciales, su exponente de Lyapunov es positivo y resulta ser caótico.

Los exponentes de Lyapunov son quantificadores que caracterizan como evoluciona la separación entre dos trayectorias [2]. En general es bien conocido que el comportamiento caótico está principalmente caracterizado por los números de Lyapunov de la dinámica del sistema.

Venimos llamando al número  $\lambda$  exponente de Lyapunov, sin embargo este es un uso poco riguroso de este término, por dos razones: Primero,  $\lambda$  depende de la trayectoria que estamos estudiando, deberíamos promediar sobre muchos puntos sobre la misma trayectoria para obtener su verdadero valor. Segundo, realmente hay tantos exponentes de Lyapunov como dimensiones tenga el sistema. Supongamos la evolución de una esfera infinitesimal de condiciones iniciales en el espacio de estados de tres dimensiones. Durante esta evolución la esfera se vuelve un elipsoide infinitesimal con tres ejes principales  $\lambda_1$ ,  $\lambda_2$  y  $\lambda_3$ , siendo estos tres los exponentes de Lyapunov del sistema. El caos está definido por el máximo exponente de Lyapunov, a partir de ahora MLE, entonces basta que uno de los tres exponentes sea positivo para que el sistema sea caótico. Si uno o más números de Lyapunov es mayor que cero, entonces el sistema se comporta caóticamente, de otra forma el sistema es estable.

El Máximo Exponente de Lyapunov (MLE) caracteriza que tan rápido se apartan dos trayectorias inicialmente vecinas. Si esta velocidad es exponencial, se dice que el sistema es caótico, por lo que este exponente es conocido como un detector de "caoticidad", [3, 4, 2].

Más adelante, el MLE fue utilizado en diversas aplicaciones de muy distintas áreas. Sólo por mencionar algunas, en [5] el MLE es usado para medir una señal muy débil en un gas ideal utilizando criterios caóticos. En [6], se estudia si es posible predecir un cambio en la probabilidad de caída para un modelo simple de caminante humano a partir del *MLE*.

Sabemos que el sistema en tiempo continuo es una idealización, por lo que se usa el exponente de Lyapunov para tiempo discreto:

$$L = \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{i=1}^n \log_2 J_F(x, y, z) \quad (3.3)$$

en donde  $L$  es un vector columna de tres dimensiones que contiene los tres exponentes de Lyapunov y  $J_F(x, y, z)$  es la matriz jacobiana de la función  $F$  para las variables  $(x, y, z)$ . El logaritmo es en base dos para estimar la velocidad de apartamiento en bits. Con estas dos consideraciones (tiempo discreto y base numérica binaria finita) la distancia entre dos trayectorias cambia en  $2^{MLE}$  por cada iteración, en promedio. Si el  $MLE < 0$  las trayectorias se aproximan, esto puede deberse a un punto fijo. Si el  $MLE = 0$  las trayectorias mantienen su distancia, esto puede deberse a un ciclo límite. Si el  $MLE > 0$  la distancia entre las trayectorias es creciente, lo que es un indicador de caos.

Calcular  $L$  con la ecuación 3.3 tiene dos problemas: Se necesitan infinitas iteraciones para hallar los exponentes de Lyapunov. Trabajar con el jacobiano puede ser computacionalmente pesado, o éste puede no existir. Afortunadamente existe un algoritmo no analítico por aproximaciones sucesivas que converge al máximo exponente de Lyapunov. Las entradas y las salidas de un sistema deben ser accesibles para poder utilizarlo. El procedimiento es el siguiente: el sistema debe ser iniciado desde dos puntos cercanos en el plano de fase, llamémoslos  $(x_a, y_a)$  y  $(x_b, y_b)$ . A medida que el sistema es iterado se mide la distancia euclídea entre las dos trayectorias ( $d_n$  en la muestra  $n_{th}$ ) (eq. 3.4), y la trayectoria  $b$  es relocalizada en cada iteración (eq. 3.6) obteniendo los puntos  $(x_{br}, y_{br})$  para realimentar el sistema. Entonces, el MLE puede ser calculado como se muestra en la ecuación 3.5. El proceso puede verse en la Fig. 3.1.

$$\begin{aligned} d_{0(i-1)} &= \sqrt{(x_{a(i-1)} - x_{br(i-1)})^2 + (y_{a(i-1)} - y_{br(i-1)})^2} \\ d_{1(i)} &= \sqrt{(x_{a(i)} - x_{b(i)})^2 + (y_{a(i)} - y_{b(i)})^2} \end{aligned} \quad (3.4)$$

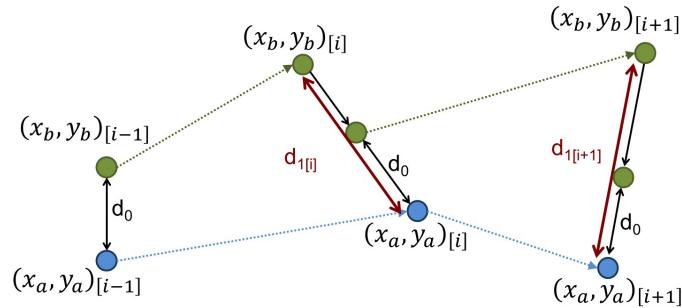


Figura 3.1: Algoritmo para calcular el MLE.

$$MLE = \frac{1}{n} \sum_{i=2}^n \log_2 \frac{d_{1(i)}}{d_{0(i-1)}} \quad (3.5)$$

$$\begin{aligned} x_{br(i)} &= x_{a(i)} + (x_{b(i)} - x_{a(i)})d_{o(i-1)}/d_{1(i)} \\ y_{br(i)} &= y_{a(i)} + (y_{b(i)} - y_{a(i)})d_{o(i-1)}/d_{1(i)} \end{aligned} \quad (3.6)$$

### 3.1.1. Algoritmo evolutivo para la búsqueda de caos

Se propuso emplear un método eurístico para buscar parámetros del sistema implementado de tal forma que se maximice la caoticidad de su salida. Este algoritmo tiene la ventaja que realiza una búsqueda inteligente mediante el empleo de un algoritmo genético, lo que minimiza el tiempo de cómputo.

Un algoritmo evolutivo es un método de búsqueda dirigido basado en la probabilidad. Un juego de entidades que representan posibles soluciones compite con otros, evolucionando en mejores soluciones [7].

Las entidades que representan posibles soluciones al problema son llamados *cromosomas* y el grupo de cromosomas es llamados *población inicial*.

Desde la población inicial, o los primeros padres, se genera un hijo mediante el cruce entre ellos. Luego, ellos son mutados en forma aleatoria para crear la próxima generación. Cada generación es comparada con la previa para descartar los “peor adaptados” así los coeficientes (cromosomas) mutan hacia los “mejor adaptados”.

Cuando se aplican estos algoritmos en funciones continuas, siempre convergen hacia el máximo local. Sin embargo, si el espacio de coeficientes es fractal, existen áreas bien definidas en donde la función objetivo es positiva, negativa, cero o no existente. Este es el caso si la función a maximizar es el MLE y el espacio de exploración es el de parámetros.

## Resultados

Para evaluar la viabilidad del método, se generó el siguiente algoritmo y se probó sobre el mapa logístico.

En la figura 3.2 podemos ver el diagrama de flujo principal. El bloque *Evolution* fue descompuesto en otro sub-diagrama para simplificar la descripción. Este segundo diagrama puede verse en la figura 3.3, esta surutina maneja la evolución de los parámetros.

El algoritmo inicia con una inicialización general de parámetros como el número máximo de generaciones *max\_gen*, el número máximo de mutaciones *max\_mut* y el número máximo de cambios en cada mutación *max\_stem*. Luego se definen los primeros dos padres, ellos definirán los márgenes de búsqueda. Además se calcula su *fitness function* *Fp*. A partir de este punto se itera la segunda generación, se elige en forma aleatoria un valor de parámetro *r* con una distribución aleatoria entre los primeros dos padres, generando un nuevo hijo. Luego este hijo entra en la subrutina *Evolution* cuya salida es el valor de *r* evolucionado y su correspondiente *Fc*.

Luego se evalúa si este hijo avolucionó muy cerca de sus padres o no. Si la distancia entre ellos es más grande que el parámetro *max\_hop*, entonces este hijo es considerado como adulto, en caso contrario debe competir con su padre más cercano sobreviviendo el más apto.

Este proceso se repite hasta que se llega al máximo número de generaciones *max\_gen*. El grupo final de adultos es la solución al problema de buscar los máximos MLE locales.

La subrutina *Evolution* de la figura 3.3 es un algoritmo muy simple basado en mutaciones. El primer paso es generar una mutación del hijo con una probabilidad uniformemente distribuida entre  $\pm max\_step$ , tambien se calcula su *fitness function* *Fm*, que se compara con la del individuo original *Fc*. Entonces sobrevive el mejor adaptado para dar lugar a la siguiente mutación. Este procedimiento se repite hasta que se llega al máximo número de mutaciones *max\_mut*.

Como resultado podemos ver el *MLE* del mapa logístico en función de su único parámetro *r* en la figura 3.4. La línea continua muestra el *MLE* en pasos continuos de *r*, mientras

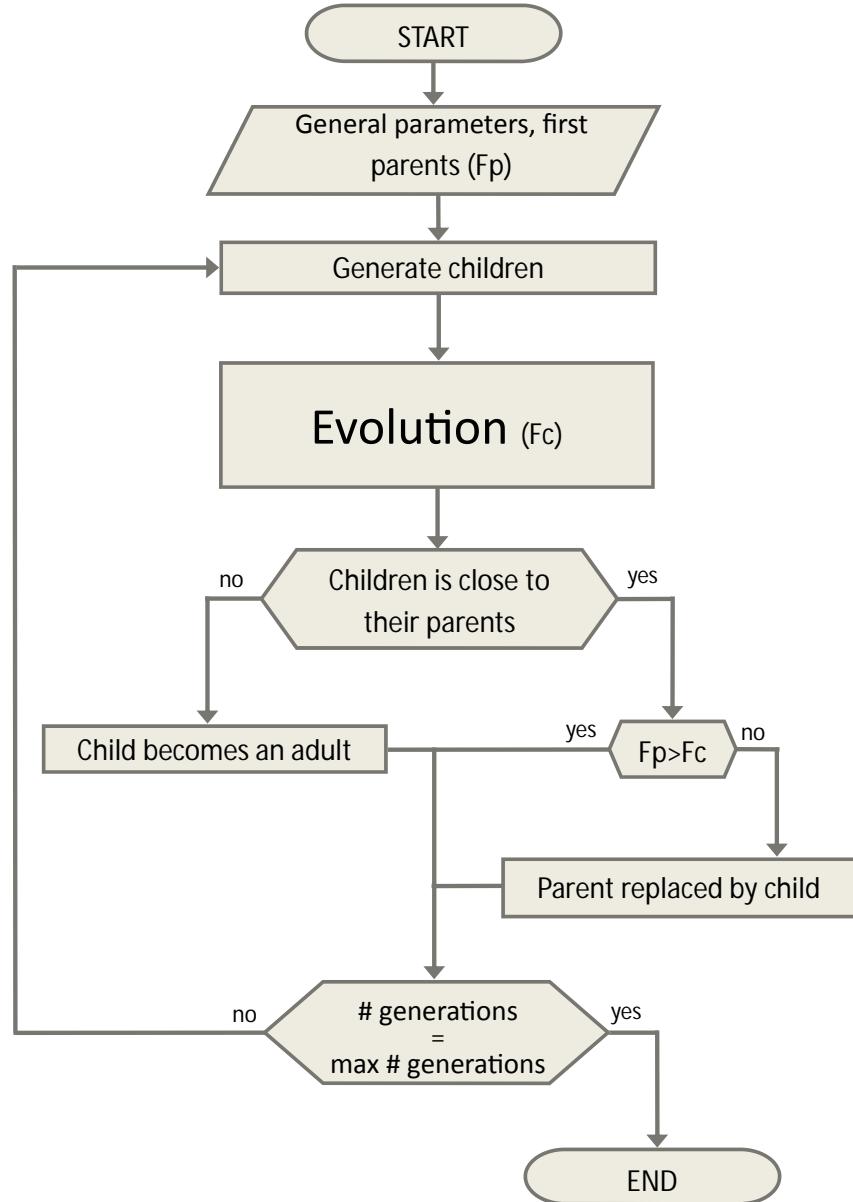


Figura 3.2: Diagrama de flujo principal.

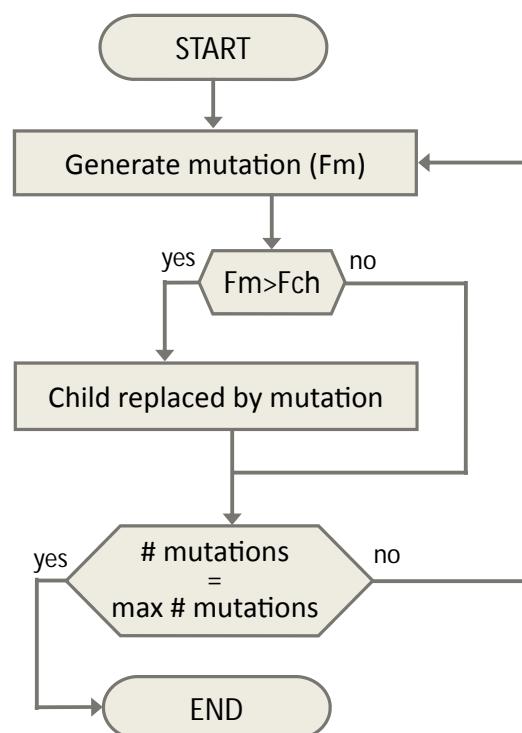


Figura 3.3: Diagrama de flujo del bloque *Evolution*.

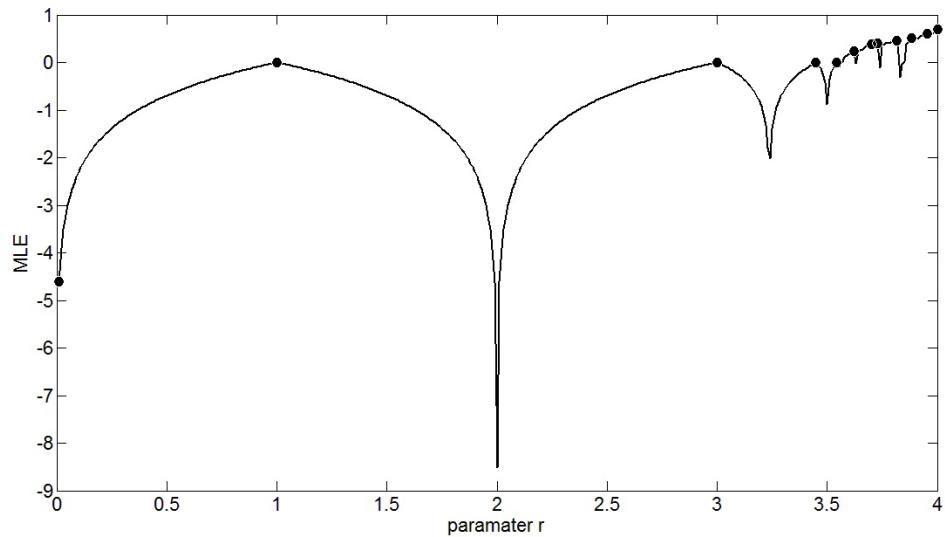


Figura 3.4: Resultados del algoritmo evolutivo para el mapa logístico, los puntos son los resultados del algoritmo.

que los puntos destacados son el resultado del algoritmo propuesto.

El bloque que calcula el *MLE* fue sintetizado y verificado experimentalmente en un Altera CYCLONE III FPGA y los resultados de la compilación mostrados en la figura 3.5. Los resultados del *Timing Analysis* reportan que la máxima frecuencia es de  $84,95MHz$ . El reporte de compilación muestra que la utilización de la lógica no excede el 20%, es decir un total de 20307 de elementos lógicos, 54 % de los bits de memoria totales y 8 % de los multiplicadores embebidos.

En la figura 3.6 se muestra la salida del Signal Tap. La señal *salida* es la suma de los *MLE* luego de cada iteración. La segunda señal llamada *cuenta\_sal* corresponde a la sumatoria actual. Finalmente, cada flanco descendente de la señal *listoD1* indica que la salida es un dato válido. La salida fué procesada con Matlab para obtener la curva mostrada en la figura 3.7. El valor del *MLE* en la iteración 250000 es 0,1415, lo que es consistente con el *MLE* obtenido con Matlab.

### Estado actual del avance

Actualmente estamos en etapa de desarrollo de la implementación en hardware de este algoritmo. En este segundo caso, el sistema bajo prueba es la familia de mapas cuadráticos bidimensionales descriptos en la sección 2.3.1.

Flow Summary	
Flow Status	Successful - Fri Apr 19 10:20:17 2013
Quartus II 32-bit Version	12.1 Build 177 11/07/2012 SJ Web Edition
Revision Name	CalculaLyap
Top-level Entity Name	TOP
Family	Cyclone III
Device	EP3C120F780C7
Timing Models	Final
Total logic elements	29,307 / 119,088 ( 25 % )
└ Total combinational functions	26,048 / 119,088 ( 22 % )
└ Dedicated logic registers	18,014 / 119,088 ( 15 % )
Total registers	18014
Total pins	197 / 532 ( 37 % )
Total virtual pins	0
Total memory bits	2,133,356 / 3,981,312 ( 54 % )
Embedded Multiplier 9-bit elements	48 / 576 ( 8 % )
Total PLLs	1 / 4 ( 25 % )

Figura 3.5: Compilation report of the *MLE* calculator.

Type	Alias	Name	4096	sal0484	4096	-3584	-3072	-2560	-2048	-1536	-1024	-512	0	512	1024	1536	2048	2560	3072	3584	4096	
E	salida	1171430159	1171430159	1171430159	1171430159	1171430159	1171430159	1171430159	1171430159	1171430159	1171430159	1171430159	1171430159	1171430159	1171430159	1171430159	1171430159	1171430159	1171430159	1171430159	1171430159	
I	cuenta_sal	95475	95475	95476	95476	95477	95477	95478	95478	95479	95479	95480	95481	95482	95483	95484	95485	95486	95487	95488	95489	95490
out	listo1	1																				

Figura 3.6: Salida del Signal Tap.

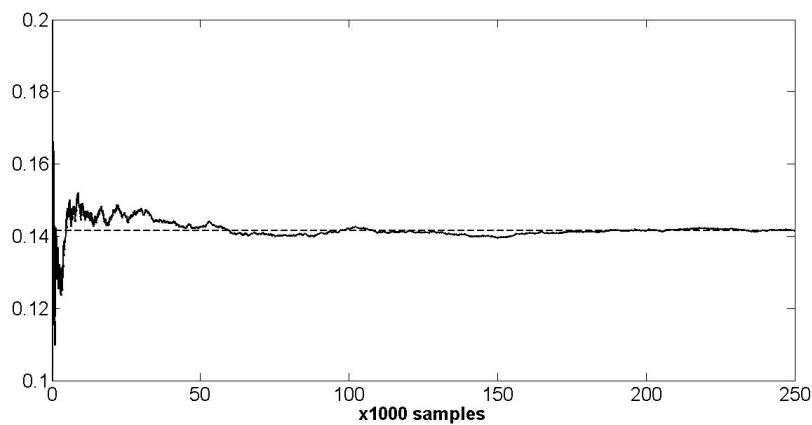


Figura 3.7: Convergencia del algoritmo que calcula el MLE.

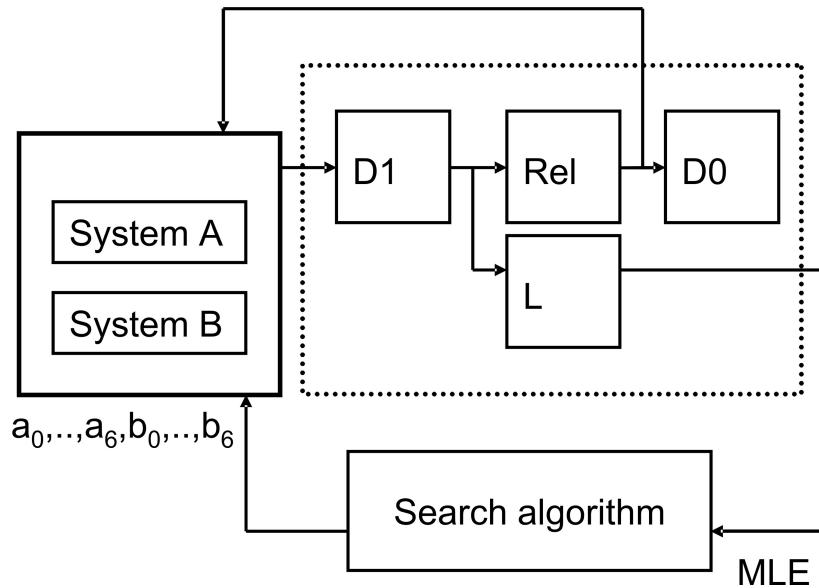


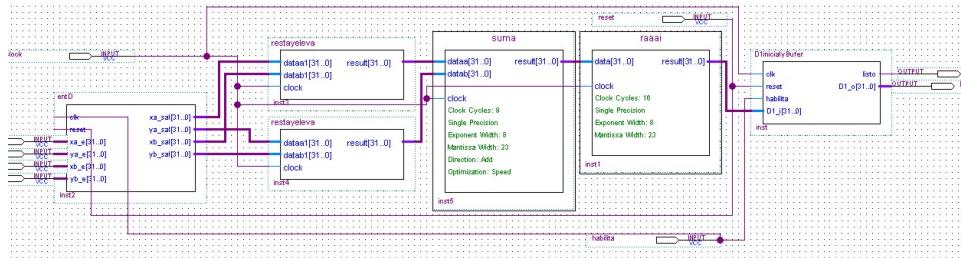
Figura 3.8: Diagrama en bloques del sistema implementado en FPGA.

La población inicial es de 12 coeficientes iniciales del mapa caótico empleado. En la figura 3.8 puede verse un diagrama en bloques general del sistema. Este consiste en dos bloques principales conectados al sistema caótico bajo prueba a través de una interface wishbone. Esto independiza el sistema del cuantificador y permite cambiar fácilmente el sistema bajo prueba.

El sistema caótico es duplicado en dos bloques, *SystemA* y *SystemB*. Cada uno de ellos es inicializado con los puntos en el espacio de fases  $(x_{a(i-1)}, y_{a(i-1)})$  y  $(x_{br(i-1)}, y_{br(i-1)})$  respectivamente. Cuando los sistemas caóticos terminan de calcular sus salidas, la señal digital *habilita* se pone en cero y el bloque *D1* es habilitado para calcular la distancia euclídea entre las salidas  $(x_{a(i)}, y_{a(i)})$  y  $(x_{br(i)}, y_{br(i)})$ .

Luego se habilitan los bloques concurrentes *L* y *Rel*. Los puntos relocalizados que alimentan al bloque *SystemB* son calculados por el bloque *Rel*. Este bloque solo necesita los valores actuales de  $d_1$  los valores previos de  $d_0$ , como se muestra en la ecuación 3.6. Cuando los puntos relocalizados  $x_{br(i)}$  y  $y_{br(i)}$  están disponibles, los bloques *SystemA* y *SystemB* se habilitan para obtener la siguiente iteración. También se habilita el bloque *D0* para calcular el valor actual de  $d_{0(i)}$ , que se utilizará en la siguiente iteración.

Finalmente, el bloque *L* realiza la división entre  $d_0$  y  $d_1$  para luego calcular el valor absoluto y el logaritmo de esta división. El mapa es iterado  $N = 250000$  veces y el resultado de la sumatoria dividido por  $N$  para asegurar la convergencia del método.

Figura 3.9: Bloque  $D_1$ .

Cada bloque fue implementado utilizando lenguaje VHD e IP *cores* provistos por *Altera* (*megafunctions*) cada vez que fue posible, debido a que estos *cores* están optimizados para este dispositivo. Las operaciones de punto flotante como las sumas, multiplicaciones, valores absolutos y logaritmos fueron calculadas con dichas *megafunctions*.

La figura 3.9 muestra la implementación del bloque  $D_1$  en el entorno gráfico Quartus. Los puntos de salida y entrada  $a$  y  $b$ , son tomados luego de que la señal *habilita* se pone en cero. Entonces, las señales son procesadas de acuerdo a la ecuación 3.4 para calcular la distancia euclídea  $d_1$ .

La lógica del algoritmo genético fue implementada en lenguaje VHD. Esta lógica junto con el registro de los 12 coeficientes se muestran en la figura 3.10. También se muestran los resultados de la compilación en la figura 3.11. Puede verse que esta implementación ocupa pocos recursos del dispositivo.

### 3.2. Cuantificadores de la teoría de la información

Dada una fuente de símbolos cuya salida es un vector de símbolos  $X$ , existen diferentes procedimientos para obtener una PDF [8, 9, 10, 11, 12, 13]. La determinación de la mejor PDF  $P$  es un problema fundamental porque  $P$  y el espacio de muestra  $X$  están inextricablemente vinculados. Su aplicabilidad depende de las características particulares de los datos, tales como estacionariedad, duración de la serie temporal, variación de los parámetros, nivel de contaminación de ruido, etc.

Los cuantificadores seleccionados se basan en el recuento de símbolos y en la estadística de patrones de orden. Las métricas a utilizar pueden clasificarse de forma amplia en dos categorías: las que cuantifican el *contenido de información* de los datos en comparación con los relacionados con su *complejidad*. Obsérvese que aquí nos estamos refiriendo al espacio

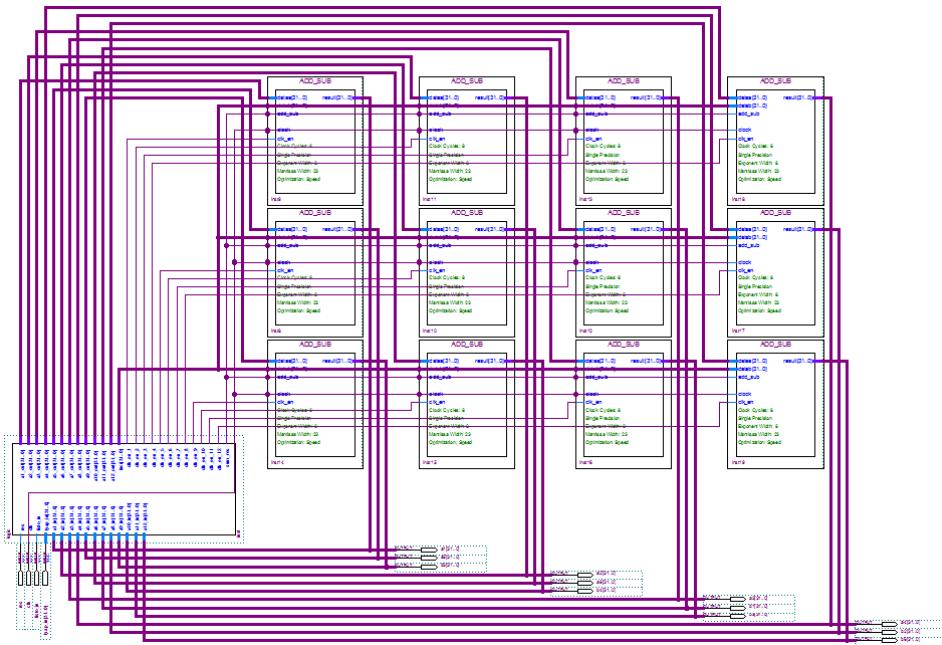


Figura 3.10: Circuito del algoritmo evolutivo. Cada uno de los 12 bloques ADD\_SUB guarda el valor de uno de los coeficientes  $a_i$ .

Flow Summary	
Flow Status:	Successful - Mon Apr 22 11:03:28 2013
Quartus II 64-Bit Version	12.1 Build 243 01/31/2013 SP 1 SJ Web Edition
Revision Name	feedback
Top-level Entity Name	feedback
Family	Cyclone III
Device	EP3C120F780C7
Timing Models	Final
Total logic elements	10,136 / 119,088 ( 9 % )
Total combinational functions	9,700 / 119,088 ( 8 % )
Dedicated logic registers	5,093 / 119,088 ( 4 % )
Total registers	5093
Total pins	419 / 532 ( 79 % )
Total virtual pins	0
Total memory bits	432 / 3,981,312 ( < 1 % )
Embedded Multiplier 9-bit elements	0 / 576 ( 0 % )
Total PLLs	0 / 4 ( 0 % )

Figura 3.11: Compilation report del algoritmo evolutivo.

de funciones de densidad de probabilidad, no al espacio físico. Para clarificar y simplificar, introducimos solamente los cuantificadores de la Teoría de la Información que se definen en PDFs discretas, ya que solo estamos tratando con datos discretos (series temporales). Sin embargo, todos los cuantificadores también tienen definiciones para el caso continuo [14].

### 3.2.1. Entropía de Shannon y Complejidad Estadística

La entropía es una cantidad básica que puede considerarse como una medida de la incertidumbre asociada (información) al proceso físico descrito por  $P$ . Al tratar con el contenido de la información, la entropía de Shannon se considera a menudo como la fundamental y más natural [14]. Considerada como una medida de la incertidumbre, es el ejemplo más paradigmático de estos cuantificadores de información.

Sea  $P = \{p_i; i = 1, \dots, N\}$  con  $\sum_{i=1}^N p_i = 1$ , una distribución de probabilidad discreta, con  $N$  el número de estados posibles del sistema bajo estudio. La medida de la información logarítmica de shannon se denota como

$$S[P] = - \sum_{i=1}^N p_i \ln [p_i] . \quad (3.7)$$

Si  $S[P] = S_{\min} = 0$ , estaremos en posición de predecir con total certeza cuáles de los posibles resultados  $i$ , cuyas probabilidades están dadas por  $p_i$ , tendrán lugar realmente. Nuestro conocimiento del proceso subyacente descrito por la distribución de probabilidad es máximo en este caso. Por el contrario, nuestro conocimiento es mínimo para una distribución uniforme  $P_e = \{p_i = 1/N; i = 1, \dots, N\}$  dado que cada resultado exhibe la misma probabilidad de ocurrencia, y la incertidumbre es máxima, es decir,  $S[P_e] = S_{\max} = \ln N$ . Estas dos situaciones son casos extremos, por lo tanto nos centramos en la entropía de Shannon "normalizada",  $0 \leq H \leq 1$ , dada como

$$H[P] = S[P]/S_{\max} . \quad (3.8)$$

Contrariamente al contenido de la información, no existe una definición universalmente aceptada de complejidad. Aquí, nos centramos en describir la *complejidad de las series temporales* y no nos referimos a la complejidad de los *sistemas* subyacentes. Un sistema complejo no genera necesariamente una salida compleja. De hecho, los modelos "simples" pueden generar datos complejos, mientras que los sistemas "complicados" pueden

producir datos de salida de baja complejidad [?].

Una noción intuitiva de una complejidad cuantitativa atribuye valores bajos tanto a datos perfectamente ordenados (es decir, con entropía de Shannon que se va desapareciendo) como a datos aleatorios no correlacionados (con entropía Shannon máxima). Por ejemplo, la complejidad estadística de una simple oscilación o tendencia (ordenada), pero también de ruido blanco no correlacionado (no ordenado) sería clasificada como baja. Entre los dos casos de mínima y máxima entropía, los datos son más difíciles de caracterizar y por lo tanto la complejidad debe ser mayor. Buscamos alguna función  $C[P]$  que cuantifique las estructuras presentes en los datos que se alejan de estos dos casos. Estas estructuras se relacionan con la organización, la estructura correlacional, la memoria, la regularidad, la simetría, los patrones y otras propiedades [15].

Asumimos que el grado de estructuras correlacionales sería capturado adecuadamente por algún funcional  $C[P]$  de la misma manera que la entropía de Shannon  $S[P]$  [14] “captura” la aleatoriedad. Claramente, las estructuras ordinales presentes en un proceso no son cuantificadas por medidas de aleatoriedad y, por consiguiente, son necesarias medidas de complejidad estadística o estructural para una mejor comprensión (caracterización) de la dinámica del sistema representada por sus series temporales [16].

Una medida adecuada de complejidad puede definirse como el producto de una medida de información y una medida de desequilibrio, es decir, algún tipo de distancia de la distribución equiprobable de los estados accesibles de un sistema. En este sentido, en [17] los autores introdujeron una eficaz *Medida de Complejidad Estadística* (SCM)  $C$ , que es capaz de detectar detalles esenciales de los procesos dinámicos subyacentes al conjunto de datos. Basado en el trabajo de López-Ruiz [18], esta medida de complejidad estadística [19, 17] se define a través de la forma del producto

$$C[P] = Q_J[P, P_e] \cdot H[P] \quad (3.9)$$

de la entropía de Shannon normalizada  $H$ , ver eq. (3.8), y el desequilibrio  $Q_J$  definido en términos de la divergencia de Jensen-Shannon  $J[P, P_e]$ . Esto es,

$$Q_J[P, P_e] = Q_0 J[P, P_e] = Q_0 \{S[(P + P_e)/2] - S[P]/2 - S[P_e]/2\}, \quad (3.10)$$

en la divergencia de Jensen-Shannon mencionada arriba,  $Q_0$  es una constante de normaliza-

ción tal que  $0 \leq Q_J \leq 1$ :

$$Q_0 = -2 \left\{ \frac{N+1}{N} \ln(N+1) - \ln(2N) + \ln N \right\}^{-1}, \quad (3.11)$$

y es igual a la inversa del máximo valor posible de  $J[P, P_e]$ . Este valor es obtenido cuando una de las componentes de  $P$ , digamos  $p_m$ , es igual a uno y todos los  $p_j$  restantes son cero.

La divergencia de Jensen-Shannon, que cuantifica la diferencia entre las distribuciones de probabilidad, es especialmente útil para comparar la composición simbólica entre diferentes secuencias [?]. Obsérvese que la SCM introducida anteriormente depende de dos distribuciones de probabilidad diferentes: una asociada con el sistema analizado,  $P$ , y la otra con la distribución uniforme,  $P_e$ . Además, se demostró que para un valor dado de  $H$ , el rango de valores posibles de  $C$  varía entre un mínimo  $C_{min}$  y un máximo  $C_{max}$ , restringiendo los posibles valores del SCM [20].

Por lo tanto, está claro que información adicional importante relacionada con la estructura correlacional entre los componentes del sistema físico se proporciona evaluando la medida de la complejidad estadística.

### 3.2.2. Determinación de la distribución de probabilidad

La evaluación de los cuantificadores derivados de la Teoría de la Información supone algún conocimiento previo sobre el sistema; específicamente para aquellos introducidos previamente (entropía de Shannon y complejidad estadística), una distribución de probabilidad asociada a la serie temporal en análisis debe proporcionarse antes. La determinación del PDF más adecuado es un problema fundamental porque la PDF  $P$  y el espacio de muestra  $\Omega$  están intrincadamente vinculados.

Las metodologías usuales asignan a cada valor de la serie  $X(t)$  (o conjunto de valores consecutivos no superpuestos) un símbolo de un alfabeto finito  $A = \{a_1, \dots, a_M\}$ , creando así una *secuencia simbólica* que puede considerarse como una descripción de la serie cronológica en cuestión. Como consecuencia, las relaciones de orden y las escalas temporales de la dinámica se pierden por completo.

Es importante resaltar que  $P$  en si, no es un objeto con una definición única y existen varias aproximaciones para “asociar” una dada  $P$  con una dada serie de tiempo. Solo para mencionar algunos criterios de extracción utilizados frecuentemente en la literatura: *a*) histogramas de series temporales [21], *b*) dinámica simbólica binaria [10], *c*) análisis de

Fourier [11], *d*) transformadas wavelet [22, 12], *e*) PDF de particiones [23], *f*) PDF de permutaciones [13, 24], *g*) PDF discreta [25], etc. Hay una amplia libertad para elegir entre ellas y la aplicación específica debe ser analizada para hacer una buena elección.

Se puede incorporar debidamente la información causal si se incluye información sobre la dinámica pasada del sistema en la secuencia simbólica, es decir, los símbolos del alfabeto  $A$  se asignan a una porción del espacio de fase o trayectoria. Bandt y Pompe (BP) [?] introdujeron una metodología simbólica simple y robusta que toma en cuenta el ordenamiento temporal de las series temporales comparando valores vecinos en una serie temporal. La propiedad de causalidad de la PDF permite que los cuantificadores (basados en esta PDF) discriminan entre sistemas determinísticos y estocásticos [26]. Los datos simbólicos son: (*i*) creados por la clasificación de los valores de la serie; y (*ii*) definidos por el reordenamiento de los datos embebidos en orden ascendente, lo que equivale a una reconstrucción de espacio de fase con dimensión de embedding (longitud de patrón)  $D$  y retardo de tiempo  $\tau$ . De esta forma, es posible cuantificar la diversidad de los símbolos de ordenación (patrones) derivados de una serie temporal escalar. Obsérvese que la secuencia de símbolos apropiada surge naturalmente de la serie temporal, y no se necesitan suposiciones basadas en modelos. El procedimiento es el siguiente:

- Dada una serie  $\{x_t; t = 0, \Delta t, \dots, N\Delta t\}$ , se genera una secuencia de vectores de longitud  $D$ .

$$(s) \mapsto (x_{t-(d-1)\Delta t}, x_{t-(d-2)\Delta t}, \dots, x_{t-\Delta t}, x_t) \quad (3.12)$$

Cada vector resulta ser la "historia" del valor  $x_t$ . Evidentemente, cuanto más larga sea la longitud de los vectores  $D$ , mayor será la información sobre la historia de los vectores, pero se requiere un valor más alto de  $N$  para tener una estadística adecuada.

- Las permutaciones  $\pi = (r_0, r_1, \dots, r_{D-1})$  de  $(0, 1, \dots, D-1)$  es llamado “patrón de orden” de tiempo  $t$ , definido por:

$$x_{t-r_{D-1}\Delta t} \leq x_{t-r_{D-2}\Delta t} \leq \dots \leq x_{t-r_1\Delta t} \leq x_{t-r_0\Delta t} \quad (3.13)$$

Para obtener un resultado único se considera  $r_i < r_{i-1}$  si  $x_{t-r_i\Delta t} = x_{t-r_{i-1}\Delta t}$ . De esta forma, todas las  $D!$  permutaciones posibles  $\pi$  de orden  $D$ , y la PDF  $P = \{p(\pi)\}$  es

definida como:

$$p(\pi) = \frac{\#\{s | s \leq N - D + 1; (s) \text{ has type } \pi\}}{N - D + 1} \quad (3.14)$$

En estas últimas expresiones, el símbolo  $\#$  denota cardinalidad.

Por lo tanto, una distribución de probabilidad de patrones de orden  $P = \{p(\pi_i), i = 1, \dots, D!\}$  se obtiene de la serie temporal. De esta manera, el vector definido por la ecuación (3.14) se convierte en un símbolo único  $\pi$ . Se establece  $r_i < r_{i-1}$  si  $x_{s-r_i} = x_{s-r_{i-1}}$  para la obtener una única solución. La única condición para la aplicabilidad del método BP es una suposición estacionaria muy débil: para  $k \leq D$ , la probabilidad para  $x_t < x_{t+k}$  no debe depender de  $t$ . Con respecto a la selección de los parámetros, Bandt y Pompe sugirieron trabajar con  $3 \leq D \leq 6$  para longitudes de series de tiempo típicas, y específicamente se consideró un retraso de tiempo  $\tau = 1$  en su publicación principal.

Para destacar la diferencia entre una *P causal* y una *no causal*, consideremos una serie de valores  $X = \{x_i, i = 1, 2, \dots\}$  generada por la función *randn* de Matlab's <sup>©</sup>; consideremos también la serie  $Y = \{y_i, i = 1, 2, \dots\}$  como la resultante de ordenar la serie  $X$  en forma ascendente. Esto se puede ver en el ejemplo en la figura 3.12, en la figura 3.12a se muestran 1000 valores sorteados con una distribución uniforme entre 0 y 1, también mostramos en la figura 3.12b la versión ordenada de la serie de la figura 3.12a, son los mismos valores pero ordenados en forma ascendente. Una *P no causal* es el histograma normalizado que mostramos en las figuras 3.12c y 3.12d, en donde puede verse que  $P(X)$  es idéntica a  $P(Y)$ , por lo que todos los cuantificadores que se calculen a partir de ellas serán idénticos para las dos series. Una *P causal* puede ser obtenida mediante el procedimiento de Bandt & Pompe descripto arriba, en este caso  $P(X)$  de la figura 3.12e es bastante uniforme y  $P(Y)$  de la figura 3.12f tiene una forma tipo delta. En este caso, *P* registra que  $Y$  es monótonamente creciente y presenta un solo patrón de orden.

Recientemente, la entropía de permutación se amplió para incorporar también información de amplitud. Ponderar las probabilidades de patrones individuales de acuerdo a su varianza mitiga los problemas potenciales con respecto a los patrones de "alto ruido, baja señal", porque los patrones de baja varianza que están fuertemente afectados por el ruido se ponderan en las distribuciones de patrones ordinales ponderados resultantes. Por lo tanto, una posible desventaja de las estadísticas de los patrones ordinales, es decir, la pérdida de información de amplitud, se puede abordar mediante la introducción de pesos con el fin de

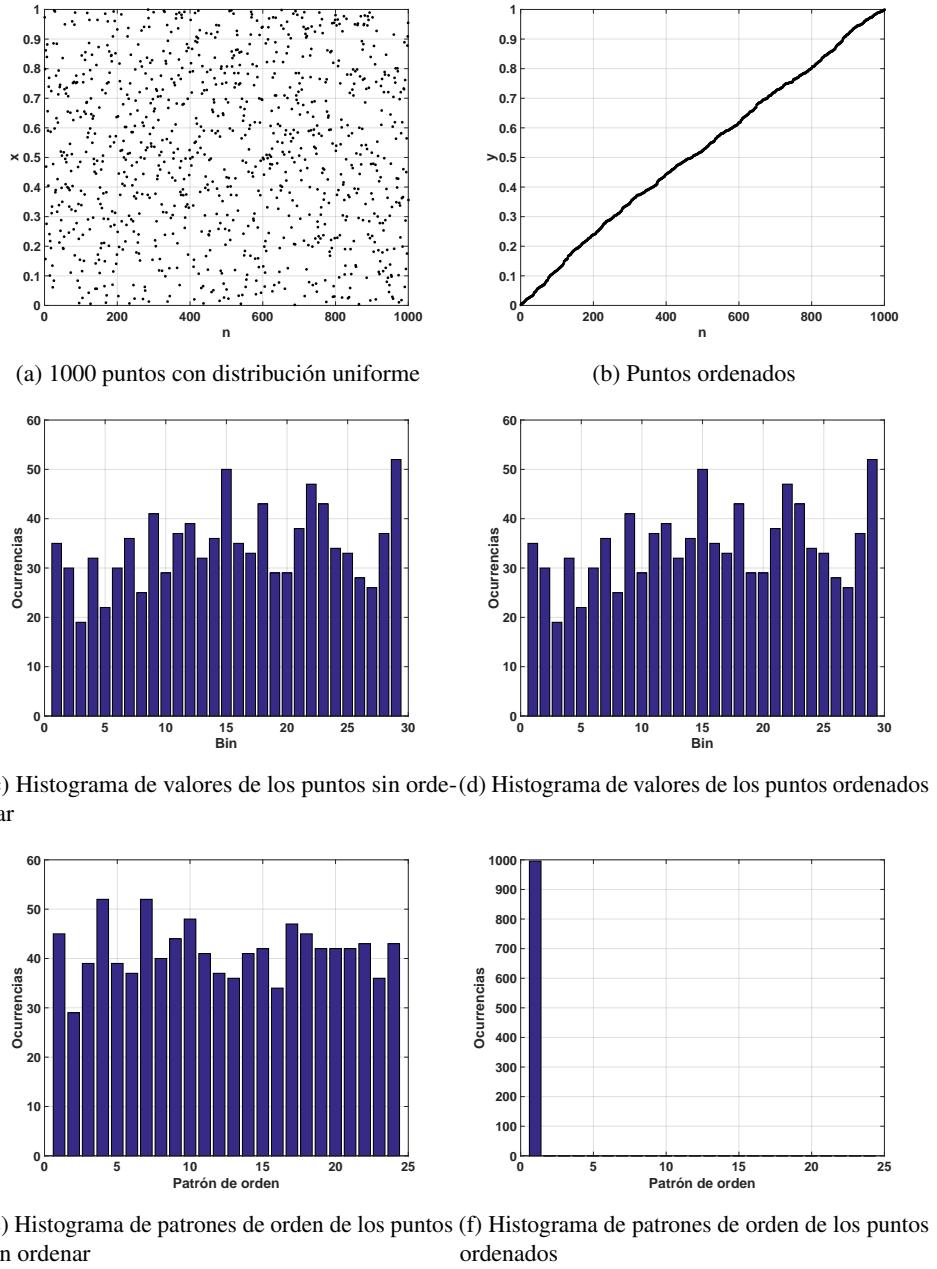


Figura 3.12: Comparación entre histogramas causal y no causal

obtener una .<sup>en</sup>tropía de permutación ponderada (WPE)"[?]. Los pesos no normalizados se calculan para cada ventana temporal para la serie de tiempo  $X$ , tal que

$$w_j = \frac{1}{D} \sum_{k=1}^D \left( x_{j+k-1} - \bar{X}_j^D \right)^2. \quad (3.15)$$

En la ecuación anterior  $x_{j+k-1} - \bar{X}_j^D$  denota la media aritmética del actual vector de embedding de longitud  $D$  y su varianza  $w_j$  se utiliza entonces para ponderar las frecuencias relativas de cada patrón ordinal  $p_j$ . Originalmente, se propuso esta técnica para discriminar patrones sumergidos en un bajo nivel de ruido. Nosotros también aprovechamos el hecho de que los puntos fijos no se computan en el WPE.

Al calcular la entropía de Shannon normalizada  $H$  y la complejidad estadística  $C$  de estas PDFs, y los valores obtenidos se denotan como:

- $H_{hist}$ , es la entropía de Shannon normalizada aplicada a una PDF no causal  $P_{hist}$
- $H_{BP}$ , es la entropía de Shannon normalizada aplicada a una PDF causal  $P_{BP}$
- $H_{BPW}$ , es la entropía de Shannon normalizada aplicada a una PDF causal con contribuciones de amplitud  $P_{BPW}$
- $C_{BP}$ , es la complejidad estadística normalizada aplicada a una PDF causal  $P_{BP}$
- $C_{BPW}$ , es la complejidad estadística normalizada aplicada a una PDF causal con contribuciones de amplitud  $P_{BPW}$

### 3.2.3. Planos doble entropía y entropía-complejidad

Una visualización particularmente útil de los cuantificadores de la Teoría de la Información es su yuxtaposición en los gráficos bidimensionales. Se definen cuatro planos de información:

1. Entropía causal vs. entropía no-causal,  $H_{BP} \times H_{hist}$
2. Entropía causal con contribución de amplitudes vs. entropía no-causal,  $H_{BPW} \times H_{hist}$
3. Complejidad causal vs. entropía causal,  $C_{BP} \times H_{BP}$
4. Complejidad causal con contribución de amplitudes vs. entropía causal con contribución de amplitudes,  $C_{BPW} \times H_{BPW}$

Estas herramientas de diagnóstico demostraron ser particularmente eficientes para distinguir entre el caos determinista y la naturaleza estocástica de una serie de tiempo ya que los cuantificadores de permutación tienen comportamientos distintos para diferentes tipos de procesos.

En la Fig. ?? se muestran los planos  $H_{BP} \times H_{hist}$  y  $H_{BPW} \times H_{hist}$  colapsados en un mismo plano. En este plano un valor más alto en cualquiera de las entropías,  $H_{BP}$ ,  $H_{BPW}$  o  $H_{hist}$ , implica una mayor uniformidad de la PDF implicada. El punto  $(1, 1)$  representa el caso ideal con histograma uniforme y distribución uniforme de los patrones de orden. Mostramos algunos puntos relevantes como ejemplo.

El ruido aleatorio blanco ideal con distribución uniforme da un punto en  $(H_{hist}, H_{BP}) = (1, 1)$  representado por un círculo azul, un círculo rojo en la misma posición muestra los resultados cuando se incluyen las contribuciones de amplitud  $(H_{hist}, H_{BPW}) = (1, 1)$ . Si ordenamos el vector ideal con distribución uniforme de forma ascendente, los puntos resultantes se muestran con un cuadrado azul  $(H_{hist}, H_{BP}) = (1, 0)$  y un cuadrado rojo  $(H_{hist}, H_{BPW}) = (1, 0)$ , este ejemplo ilustra la complementariedad de  $H_{hist}$  y  $H_{BP}$ .

Las estrellas azules y rojas muestran  $(H_{hist}, H_{BP})$  y  $(H_{hist}, H_{BPW})$  respectivamente aplicadas a una señal de diente de sierra. Los valores están perfectamente distribuidos en todos los intervalos, pero sólo aparecen unos pocos patrones de orden, esto explica el alto  $H_{hist}$  y bajo  $H_{BP}$ . La frecuencia de aparición de patrones de baja amplitud es mayor que los patrones de alta amplitud, entonces la PDF con contribuciones de amplitud es más uniforme y  $H_{BPW}$  es un poco más alto que  $H_{BP}$ . Cuando la señal de diente de sierra está contaminada con ruido blanco, se incrementan  $H_{BP}$  y  $H_{BPW}$  como se muestra con triángulos azules y rojos. Es evidente que aparecen nuevos patrones de orden y tanto  $H_{BP}$  como  $H_{BPW}$  muestran valores más altos que los casos no contaminados, sin embargo el incremento de  $H_{BPW}$  es menor que  $H_{BP}$  mostrando que la técnica de registrar contribuciones de amplitud añade alguna inmunidad al ruido.

Finalmente, se evaluaron los cuantificadores de una secuencia de un mapa logístico que converge a un punto fijo, en todos los casos la longitud del vector de datos permanece constante y la longitud de transitorio es variable. Los resultados obtenidos sin las contribuciones de amplitud se representan en puntos azules, convergen a  $(H_{hist}, H_{BP}) = (0, 0)$  a medida que la longitud de transitorio se hace más corta, sin embargo  $H_{BPW}$  (puntos rojos) permanece constante para todos los casos. El último punto en  $(H_{hist}, H_{BP}) = (0, 0)$  corresponde a un vector de ceros, en este caso el histograma de patrones de orden con

contribuciones de amplitud es también un vector nulo y  $H_{BPW}$  no se puede calcular. A través de este último ejemplo, mostramos que la convergencia a un punto fijo puede ser detectada por la información conjunta de  $H_{BP}$  y  $H_{BPW}$ .

En la figura 3.14 se muestra el plano causal  $H_{BP} \times C_{BP}$ . Podemos ver que no toda la región  $0 < H_{BP} < 1$ ,  $0 < C_{BP} < 1$  es alcanzable, de hecho, para cualquier PDF los pares  $(H, C)$  de valores posibles caen entre dos curvas extremas en el plano  $H_{BP} \times C_{BP}$  cite Anteneodo1996. Los mapas caóticos tienen entropía intermedia  $H_{BP}$ , mientras que su complejidad  $C_{BP}$  alcanza valores mayores, muy cercanos a los del límite de complejidad superior [?, ?]. Para procesos regulares, la entropía y la complejidad tienen valores pequeños, cercanos a cero. Los procesos estocásticos no correlacionados se ubican en la localización planar asociada con  $H_{BP}$  cerca de uno y  $C_{BP}$  cerca de cero. Los sistemas aleatorios ideales que tienen un Bandt & Pompe PDF uniforme, están representados por el punto  $(1, 0)$  citeGonzalez2005 y una PDF tipo delta corresponde al punto  $(0, 0)$ .

En la figura 3.14 mostramos  $H_{BP} \times C_{BP}$  con y sin contribuciones de amplitud. Se muestran los mismos puntos de muestra para ilustrar las posiciones planas para diferentes vectores de datos.

En ambos planos de información  $H_{BP} \times H_{hist}$  en la Fig. 3.13 y  $H_{BP} \times C_{BP}$  en Fig. 3.14, los datos estocásticos, caóticos y deterministas están claramente localizados en diferentes posiciones planares.

También usamos el número de patrones perdidos MP como un cuantificador [27]. Como mostraron recientemente Amigó y colaboradores [28, 25, 29, 30], en el caso de mapas deterministas, no todos los patrones de orden posibles pueden materializarse efectivamente en órbitas. De hecho, la existencia de estos patrones de orden faltantes se convierte en un hecho persistente que puede considerarse como una nueva propiedad dinámica. Por lo tanto, para una longitud de patrón fija (dimensión de embedding  $D$ ) el número de patrones perdidos de una serie temporal (patrones no observados) es independiente de la longitud de la serie  $N$ . Obsérvese que esta independencia no caracteriza otras propiedades de la serie como la proximidad y la correlación [25, 30].

### 3.2.4. Entropías diferenciales

La entropía de Shannon  $S(P)$  es el punto de partida para otros cuantificadores.

!!!!HABLAR DE LOS CONJUNTOS DE PARTICIONES Y NO SE QUE!!!

Para medir la entropía de una serie binaria es necesario

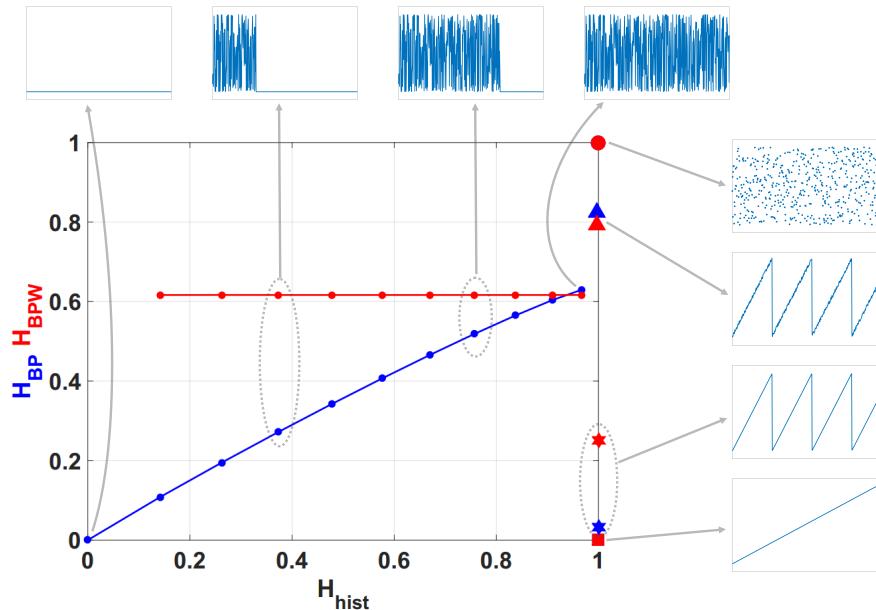


Figura 3.13: Causal-Non causal Entropy plane.

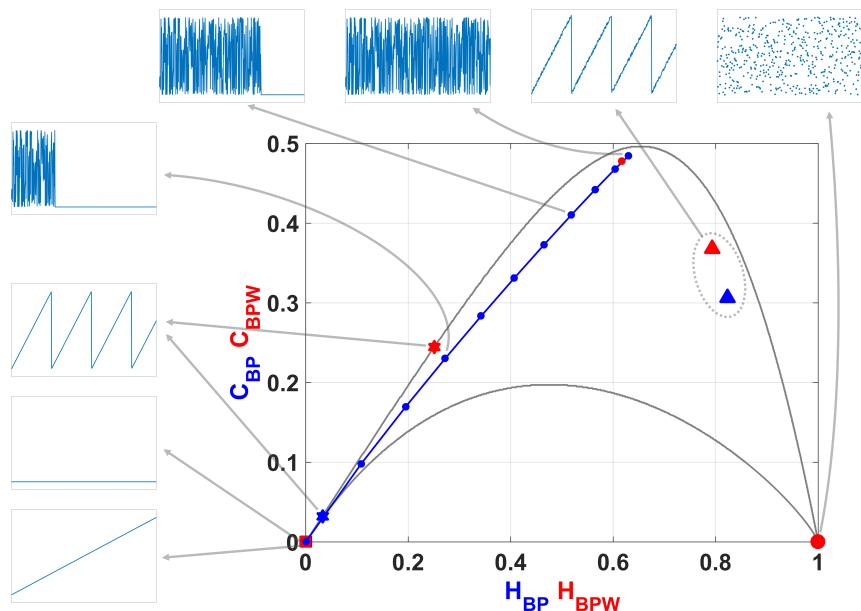


Figura 3.14: Causal Entropy-Complexity plane.

!!!FIN DE HABLAR DE LOS CONJUNTOS DE PARTICIONES Y NO SE QUE!!!

1. Entropía normalizada  $H(P)$ : es la entropía de Shannon dividida por su valor máximo.

Por ejemplo, si usamos  $S_2$  (ver arriba), se obtiene la entropía máxima para equiprobabilidad entre dos símbolos. Su valor es  $S_{max} = -1/2\log(1/2) - 1/2\log(1/2) = \log(2) = 1$ ; entonces, la entropía normalizada es  $H_2 = S_2$ . Si usamos  $S_W$  la equiprobabilidad entre las  $2^W$  posibles palabras (números decimales de  $W$ -bits) produce  $S_{max} = W$  y  $H_W = S_W/W$ . Finalmente, para  $S_{BP}^{(D)}$  la equiprobabilidad entre los  $D!$  patrones de orden produce  $S_{max} = \log(D!)$  y  $H_{BP}^{(D)} = S_{BP}^{(D)}/\log(D!)$ .

2. Entropía diferencial o condicional  $h$  y  $h^*$  son:

$$h = S_{W+1} - S_W \quad (3.16)$$

$$h^* = S_{BP}^{(D+1)} - S_{BP}^{(D)} \quad (3.17)$$

En las expresiones de arriba  $W = 1, 2, \dots$  y  $D = 2, 3, \dots$ ,  $S_0 = 0$  y  $S_{BP}^{(1)} = 0$ . Esta entropía diferencial o condicional da la cantidad promedio de información requerida para predecir el símbolo ( $W + 1$ ) (o ( $D + 1$ )), dado los  $W$  (o  $D$ ) símbolos precedentes.

3. Finalmente, las *rate entropies*  $h_0$  y  $h_0^*$  [23, 31] son dadas por:

$$h_0 = \lim_{W \rightarrow \infty} h = \lim_{W \rightarrow \infty} S_W/W \quad (3.18)$$

$$h_0^* = \lim_{D \rightarrow \infty} h^* = \lim_{D \rightarrow \infty} S_{BP}^{(D)}/(D - 1) \quad (3.19)$$

Enfatizemos algunas cuestiones importantes involucradas en los cálculos de las entropías binarias mencionadas anteriormente:

1. La entropía binaria  $S_2$  es no causal, mientras que ambas, la entropía de bloque  $S_W$  y la entropía Bandt & Pompe  $S_{BP}^{(D)}$ , son causales.
2. La entropía de bloque  $S_W$  tiene en cuenta las correlaciones entre  $W$  bits consecutivos. La entropía Bandt & Pompe  $S_{BP}^{(D)}$  tiene en cuenta las correlaciones entre  $D$  consecutivas palabras de longitud  $W$ . Ambos procedimientos de agrupación (números decimales de  $W$  bits y patrones de permutación de  $D$  números decimales) pueden realizarse con o sin superposición. La cantidad de datos requeridos para obtener buenas estadísticas es diferente dependiendo de que los procedimientos de agrupación se realicen.

3. Para  $S_W$  solo hay un proceso de agrupación ( $W$  bits agrupados para obtener una serie de números decimales  $Y$ ). Definamos  $\alpha$  como un parámetro de calidad estadística, dado por el cociente entre el número de elementos en la serie de tiempo simbólica  $Y$  y la cantidad de símbolos en el alfabeto. En este documento, no aceptaremos  $\alpha < 10$ .

Obviamente, el factor de calidad  $\alpha$  aumenta con la longitud de la serie temporal:

- a) si el agrupamiento de  $W$  bits está hecho con, dos palabras consecutivas de longitud  $W$  comparten  $W - 2$  bits. En consecuencia, comenzando con un archivo con una longitud de  $N$  bits obtenemos  $N - W + 1$  palabras. Además, hay símbolos  $2^W$  en el alfabeto y  $\alpha = (N - W + 1)/(2^W)$ .
  - b) Si  $S_W$  se evalúa sin superposición la cantidad de palabras de longitud  $W$  es  $\lfloor N/W \rfloor$  y el parámetro de calidad se calcula como  $\alpha = \lfloor N/W \rfloor / (2^W)$ . Si  $N \gg W$  el factor de calidad estadística es  $W$  veces más bajo que el usado con superposición.
4. En el caso de  $S_{BP}^{(D)}$ , hay dos procesos de agrupación involucrados.
- a) Si ambos procesos de agrupamiento se realizan con superposición obtenemos  $NW - D + 2$  elementos comenzando con un archivo  $N$  bits de longitud, y el factor de calidad es  $\alpha = (NW - D + 2)/D!$ . En este caso  $S_{BP}^{(D)}$  tiene en cuenta las correlaciones entre  $W + D$  bits consecutivos.
  - b) Si el proceso de agrupación de  $W$  bits se realiza sin superposición pero la agrupación de números decimales  $D$  se realiza con superposición obtenemos  $\lfloor N/W \rfloor - D + 1$  elementos y el parámetro de calidad estadística es  $\alpha = (\lfloor N/W \rfloor - D + 1)/D!$ . En este caso  $S_{BP}^{(D)}$  incluirá correlaciones entre  $WD$  bits consecutivos.
  - c) Si el proceso de agrupación de  $W$  bits se realiza con superposición y la agrupación de números decimales  $D$  se realiza sin superposición, obtenemos  $\lfloor (N - W + 1)/D \rfloor$  elementos a partir de un archivo de  $N$  bits. El factor de calidad estadística es  $\alpha = \lfloor (N - W + 1)/D \rfloor / D!$  y  $S_{BP}^{(D)}$  tiene en cuenta correlaciones de  $W + D - 1$  bits.
  - d) Si ambos procesos de agrupación se realizan sin superposición, obtenemos  $\lfloor \lfloor N/W \rfloor / D \rfloor$  elementos a partir de un archivo de longitud de  $N$  bits.

El factor de calidad estadística es  $\alpha = \text{floor}\{\text{floor}\{N/W\}/D\}/D!$  y  $S_{BP}^{(D)}$  tiene en cuenta las correlaciones entre  $WD$  bits consecutivos.

### 3.2.5. Cuantificador de entropías implementado en FPGA

En esta sección se describe la implementación de un sistema de medición de entropías. El diseño fue optimizado para ser implementado en un microcontrolador simple y pequeño, conservando una precisión aceptable. El sistema permite medir entropías a señales generadas internamente por código y a señales externas analógicas muestreadas. Se utilizó la placa de desarrollo *MIAFS-embedded kit* de ACTEL. En la FPGA (*Field Programmable Gate Array*) se instanció un microcontrolador 8051 al que se programó en lenguaje C. Se detalla el diseño del *hardware* y *software* y los resultados obtenidos.

Este trabajo se enmarca en un proyecto más ambicioso, que se propone el desarrollo e implementación en *hardware* de herramientas para el análisis de sistemas alineales. Contar con estas herramientas supondrá un avance significativo en el campo de la implementación de los sistemas no lineales. Permitiría comprender y describir con mayor precisión el comportamiento de la versión digital de este tipo de sistemas. El paquete completo de herramientas que nos proponemos implementar consta de:

- funcionales de la distribución de probabilidad: entropía de Shannon, desequilibrio estadístico y complejidad estadística;
- cuantificadores de la serie temporal, en especial exponentes de Lyapunov, autocorrelación, correlación cruzada y dimensiones fractales;
- operador de Perron Frobenius, y cuantificadores de diagramas de recurrencias;
- tests estadísticos propuestos en los bancos estandarizados para el estudio de generadores de números aleatorios (Marsaglia, NIST, etc.).

Al momento hay muy poca bibliografía sobre implementaciones en *hardware* de estas herramientas[32].

En el caso particular de la entropía es empleada en diversas aplicaciones, como por ejemplo, en la detección de anomalías en flujos de datos IP [33, 34]. En [35] se presentó un diseño y simulación en FPGA de un cuantificador de entropía, sin embargo actualmente no hay disponibles implementaciones en *hardware* de este cuantificador.

Dentro del proyecto mencionado, en este trabajo se implementa un sistema que calcula la entropía para la distribución de probabilidades (*PDF*) asociada a una serie de datos. Se analizan *PDF*'s causales y no causales. Los datos pueden tener un origen digital (generados mediante códigos), o bien provenir del muestreo de señales analógicas. Se utilizó la placa de desarrollo *MIAFS-embedded kit*, basado en el chip *MIAFS1500* que se destaca por tener un bloque analógico embebido en el mismo encapsulado de la FPGA. Luego, se verifica la exactitud numérica del cuantificador implementado comparando sus resultados con un programa patrón. A partir del máximo error detectado se determina la exactitud numérica del sistema.

### ***Hardware Implementado***

El diseño del *hardware* se basó en el que provee ACTEL en [36], basado en el microcontrolador 8051, interfaces y periféricos. Fue realizado con el paquete de programas *Libero Soc v11.3<sup>®</sup>* de ACTEL. Se utilizó la placa de desarrollo *MIAFS-EMBEDDED-KIT* que contiene una FPGA *MIAFS1500* de ACTEL y periféricos [37]. El chip *MIAFS1500* contiene embebido un bloque analógico que consiste en nueve adaptadores direccionables de cuatro entradas cada uno, un multiplexor analógico de 32 entradas y un conversor analógico-digital configurable.

El sistema implementado puede dividirse en tres etapas principales como se muestra en la Fig. 3.15: una primer etapa de Adquisición de datos, que convierte a palabras digitales las señales del mundo analógico, una Lógica de Cálculo, que se vale de la memoria SRAM para llevar a cabo los cálculos y coordinar las interfaces y una etapa de Presentación de resultados, que envía los resultados de la medición a una computadora a través de la interfaz *USB-to-UART*.

#### *1. Etapa de Adquisición:*

Para ingresar los datos analógicos a ser evaluados utilizamos la entrada de tensión AV2 del *Analog Quad 2* del bloque analógico. Se encuentra direccionada en el canal siete del multiplexor analógico y fue configurada para un rango de tensiones de entrada de 0 V a 4 V. El conversor analógico-digital se configuró con una resolución de 12 bits. En este primer prototipo la frecuencia de muestreo máxima alcanzada fue de 16 ks/s limitada por el retardo necesario en el procesamiento de la lógica.

#### *2. Lógica de cálculo:*

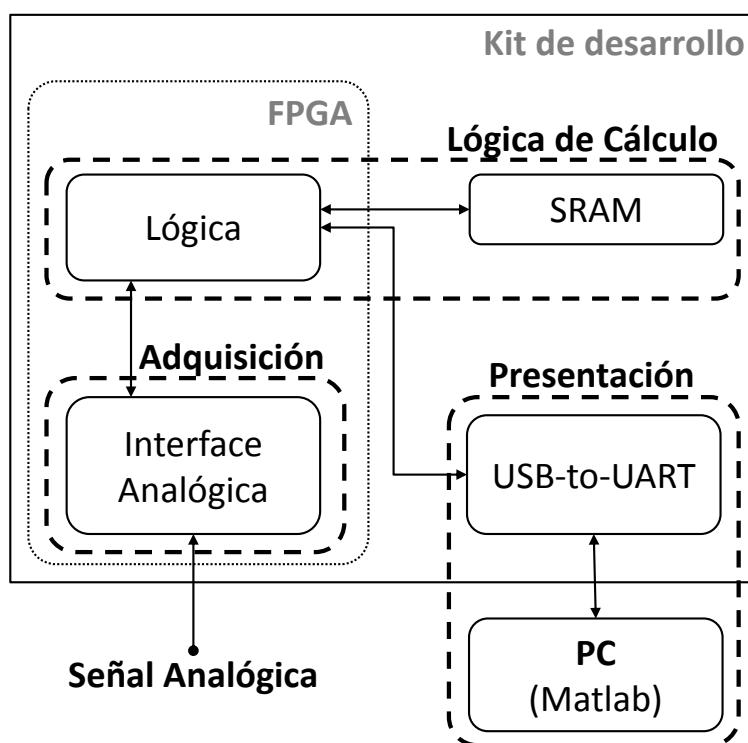


Figura 3.15: Esquema del sistema completo.

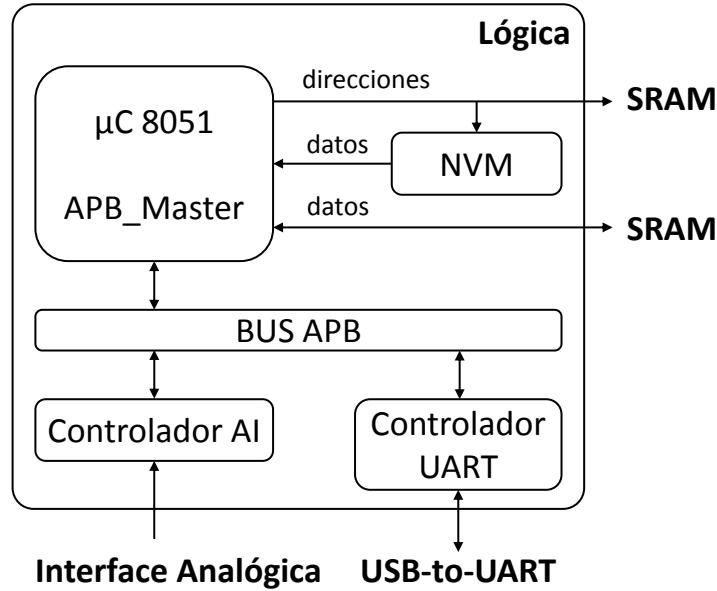


Figura 3.16: Detalle de la lógica de cálculo.

En esta etapa se realizan los cálculos y la sincronización entre periféricos. En la Fig. 3.16 pueden verse los bloques principales que la componen.

El núcleo de la implementación es un *Core 8051* que provee ACTEL en su catálogo de librerías. Se trata de un microcontrolador que contiene la lógica principal del microprocesador 8051 de Intel, sin sus periféricos. Este micro tiene una arquitectura Von Newman con un bus de direcciones de 16 bits, lo que limita nuestro diseño a 64 KB de memoria de código y 64 KB de memoria de datos.

Sobre este microcontrolador corre el programa que realiza los cálculos presentados en la sección 3.2. Se encarga de, a partir de los datos de entrada, obtener las PDFs (*BP e hist*) y de realizar los cálculos para la obtención de las entropías, según la ec. ???. El *software* implementado se describe más detalladamente en la sección 3.2.5.

La memoria de código es una memoria no volátil (NVM) implementada con los bloques flash internos de la FPGA. Ocupa las direcciones desde 0x0000 hasta 0xFFFF y se escribe con el contenido de un archivo en formato hexadecimal durante la compilación.

Las funcionalidades del sistema son ampliadas mediante la conexión de periféricos a través de la interfaz APB.

Para realizar la comunicación con la PC utilizamos el *Controlador UART*. La salida de este bloque es dirigida hacia afuera de la FPGA y se conecta a un chip *USB-to-UART* que se encuentra soldado a la placa del kit de desarrollo.

El bloque analógico es controlado por el *Controlador AI*, que direcciona y sincroniza sus entradas.

### 3. Presentación:

La etapa de Presentación de los datos involucra al chip adaptador *USB-to-UART* que se encuentra en la placa de desarrollo y es manejado tanto por el programa que corre en la FPGA como por el *software* que corre sobre la PC. El chip adaptador *USB-to-UART* es el responsable de adaptar la entrada-salida UART de la lógica a una entrada-salida USB estándar mediante la cual es posible interactuar con la PC. Por otra parte el programa que corre en la PC se encarga de la interfaz con el usuario y es descripto en detalle en la siguiente sección.

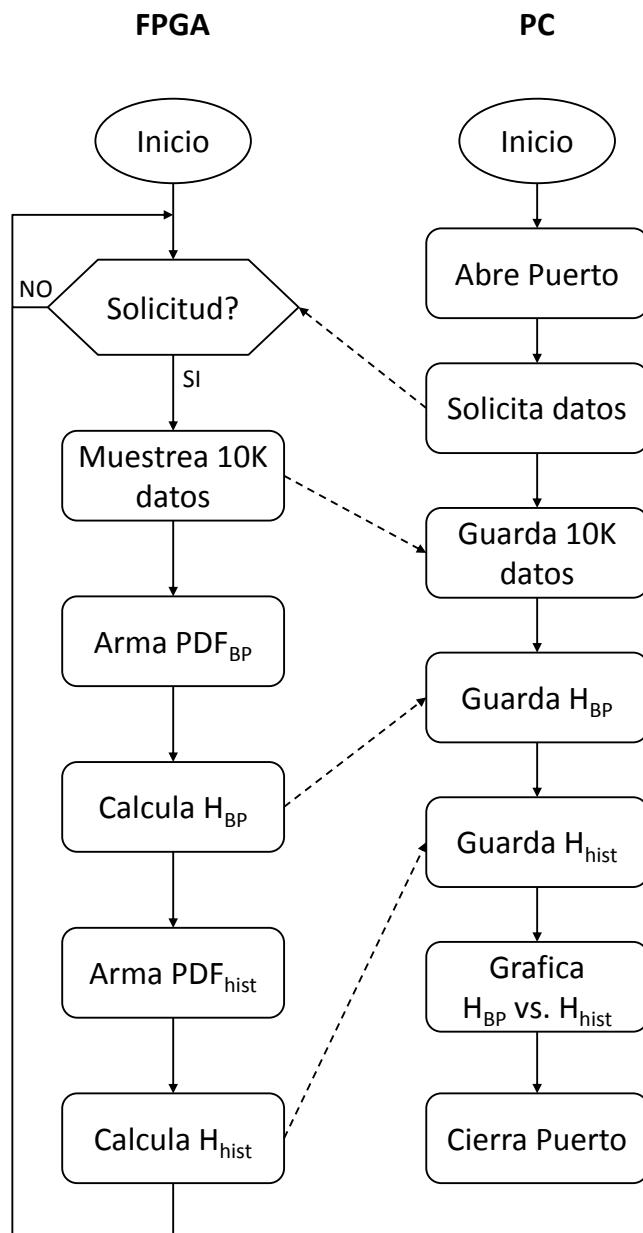
### **Software Implementado**

El funcionamiento del sistema se logra mediante la interacción de dos programas. Uno corriendo en la PC y otro en el microcontrolador implementado en la FPGA. Puede verse un diagrama de flujo de ambos programas y la interacción entre ellos en la Fig. 3.17.

En la PC corre un *script* de *Matlab*<sup>©</sup> que se encarga de abrir el puerto serie en donde se encuentra mapeado el USB, solicitar los datos, tomar los resultados del mismo puerto, graficarlos en un plano  $H_{BP}$  vs.  $H_{hist}$  y cerrar el puerto.

Sobre el microcontrolador en la FPGA corre un programa escrito en lenguaje C y compilado para el microcontrolador 8051 utilizando la herramienta *SoftConsole IDE v3.4*<sup>©</sup>. El firmware es una modificación del usado en [38]. Cuando se presenta una solicitud de datos por el puerto UART, se guardan los datos muestreados de la entrada analógica. Luego, se recorre este vector generando las  $PDF_{hist}$  y  $PDF_{BP}$ , a las que se les calcula sus respectivas entropías  $H_{hist}$  y  $H_{BP}$ . Estos resultados son enviados a la PC mediante el mismo puerto.

Con el fin de validar el sistema, el programa en la FPGA envía a *Matlab*<sup>©</sup> el vector de datos muestreados, para que se puedan calcular en la PC sus entropías y compararlas con los resultados del sistema implementado.

Figura 3.17: Diagrama de flujo del *software* implementado.

Generador	Origen	Error $H_{BP}$	Error $H_{hist}$
Rand	Digital	$1,7421E^{-6}$	$2,6977E^{-6}$
Logístico	Digital	$0,4256E^{-6}$	$94,693E^{-6}$
Triangular	Analógico	$6,3445E^{-6}$	$2,0028EE^{-6}$
Senoidal	Analógico	$6,3151E^{-6}$	$5,6506E^{-6}$
Cuadrada	Analógico	$0,1797E^{-6}$	$1,9930EE^{-6}$
Rampa	Analógico	$245,00E^{-6}$	$1,0876E^{-6}$

Cuadro 3.1: Error de los cuantificadores evaluados en la FPGA con respecto a los resultados calculados por el programa patrón.

## Resultados

Como se dijo, para testear el sistema se compararon los resultados obtenidos por el sistema implementado y por un programa patrón que corre en la PC. Para esto, se generaron 10 000 muestras de señales con distintas formas de onda tanto externas (analógicas) como internas (digitales).

Las señales digitales fueron generadas por código en el microcontrolador, una corresponde a la función `rand()` de C y la otra al mapa caótico logístico con parámetro  $r=4$ .

Las señales analógicas fueron generadas con el generador de funciones *HP33120A*. Tienen una amplitud de 4 Vpp y un nivel de continua de 2 V de forma de aprovechar todo el rango del conversor analógico-digital y aumentar la relación señal-ruido. En los cuatro casos la frecuencia de las señales fue de 100 Hz y la velocidad de muestreo de 16 ks/s.

El cuadro 4.3 muestra el error absoluto entre los resultados de los cuantificadores calculados en la FPGA comparados con los resultados calculados con el programa patrón sobre los mismos datos.

La Fig. 3.18 muestra los valores entregados por la FPGA en el plano  $H_{BP}$  vs.  $H_{hist}$ .

Los resultados de la compilación nos permite conocer los recursos de la FPGA utilizados por el sistema completo y la cantidad de memoria ocupada por el *software* que corre en el microcontrolador. Recordemos que esta es una implementación de *hardware* rígida, es decir primero se arma el circuito en la FPGA (microcontrolador, periféricos, etc.) y luego se carga el *software* sobre él.

El reporte de la compilación de *hardware* devuelto el *Place and Route* se muestra en la Fig. 3.19. Podemos ver que la implementación utiliza un 19 % de los recursos lógicos de la FPGA, el 21 % de las celdas de entrada-salida y el 28 % de los bloques de memoria.

El reporte de la compilación de *software* se muestra en la Fig. 3.20. Podemos ver que la memoria FLASH no volátil se encuentra ocupada al 15,4 %. Por otro lado, de las 65536

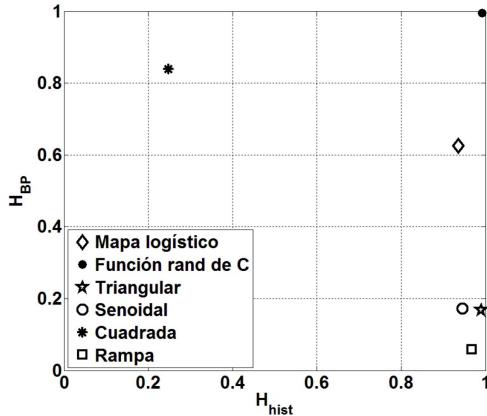


Figura 3.18: Resultados de las mediciones.

```
Core Cells : 7349 of 38400 (19%)
IO Cells : 53 of 252 (21%)
```

```
RAM/ROM Usage Summary
Block Rams : 17 of 60 (28%)
```

Figura 3.19: Recursos empleados por el *hardware* del sistema.

direcciones la memoria SRAM tenemos disponibles 61440 dado que parte de esta memoria es utilizada por el bus APB, por lo que se utiliza el 76,7% de la memoria disponible.

Name	Start	End	Size	Max
PAGED EXT. RAM			0	256
EXTERNAL RAM	0x0000	0xb828	47145	65536
ROM/EPROM/FLASH	0x0000	0x276e	10095	65536

Figura 3.20: Recursos empleados por el *software* del sistema.

El programa debió ser adaptado al microcontrolador instanciado en la FPGA. Estas modificaciones hacen que la salida del sistema implementado no sea igual a la de un programa que corre en la PC, al cual tomamos como programa o patrón. Por esto se testeó el error cometido, para tener una cota y determinar si los resultados de los cuantificadores son correctos. El programa patrón utiliza aritmética de 64 bits en punto flotante norma IEEE754-64 bits y emplea la librería math.h [39]. Para el algoritmo en la FPGA se disminuyó la aritmética a 32 bits de punto flotante norma IEEE754-32 bits. También se requirió el cálculo de la función logaritmo, que se implementó mediante un algoritmo de CORDIC. En el cuadro 4.3 se ve que el error absoluto no supera los  $245E^{-6}$ . Esto indica que se detecta diferencia recién a partir del quinto dígito decimal.

En la Fig. 3.18 puede verse como los cuantificadores  $H_{BP}$   $H_{hist}$  diferencian claramente

las propiedades estadísticas de las series de datos analizadas. Las señales Senoidal, Rampa y Triangular presentan un valor alto de  $H_{hist}$  porque tienen casi todos los valores que es capaz de generar el conversor Analógico-Digital. Sin embargo, la mezcla de estos datos es mala por tratarse de una señales periódicas totalmente predecibles, esto se ve en el bajo valor de  $H_{BP}$ . Un caso interesante de analizar es la señal Cuadrada. El efecto del ruido aditivo es especialmente notable en las zonas en donde el valor de la señal debería ser constante. Se generan dos Gaussianas muy finas en torno a los valores ideales en la  $PDF_{hist}$ , esto no afecta demasiado el valor calculado  $H_{hist}$ , sin embargo para la  $PDF_{BP}$ , se calcula el patrón de orden directamente a la señal ruidosa, por lo que el valor de  $H_{BP}$  es más alto que el esperado. La señal generada mediante la función rand de C, presenta las mejores propiedades estadísticas ubicándose en el punto  $\sim (1, 1)$ .

### 3.2.6. Dinámica de los ITQ's con AWGN y banda limitada

En esta sección exploramos la respuesta de un sistema de medición de entropías en presencia de ruido aditivo y señales filtradas. Esta inquietud surge como resultado de la implementación detallada en la sección 3.2.5. El filtrado es inherente al ancho de banda del sistema de medición y las señales a medir siempre están contaminadas con ruido, por lo tanto es necesario caracterizar la respuesta de nuestro sistema de medición ante estos dos procesos. Este trabajo es complementario al desarrollo de un sistema de medición de entropías implementado en FPGA.

#### Filtrado digital

Ya sea en la elección de un filtro como en cualquier problema de diseño en ingeniería, generalmente no es posible dar una respuesta posible acerca de cual es al mejor solución. Se discute la posibilidad de la implementación de distintos filtros porque no hay un solo método de diseño ni un solo tipo de filtro mejor para todas las circunstancias. La elección del tipo de filtro depende de la importancia de sus ventajas aplicadas a cada problema.

Un filtro ideal es aquel en el que la respuesta en frecuencia es unitaria en el rango de las frecuencias de paso, cero en la banda de rechazo y no posee banda de transición. Dada la inherente periodicidad de la respuesta en frecuencia para tiempo discreto esta tiene la apariencia de un tren rectangular en frecuencias, sin embargo en este trabajo solo se muestra la frecuencia normalizada en el intervalo  $(0; 1)$ . Entonces la transferencia de un pasabajos

ideal en frecuencia normalizada quedaría:

$$H_{LP} = \begin{cases} 1, & |f - 0,5| > f_c \\ 0, & |f - 0,5| < f_c \end{cases} \quad (3.20)$$

Ecuación definida en el intervalo de frecuencias normalizadas  $f \in (0, 1)$ .

El hecho de que no podemos contar con series de valores infinitamente largas para ser filtradas, equivale a decir que disponemos de una serie de muestras enventanada. Como el producto en el dominio del tiempo equivale a una convolución en el dominio de la frecuencia, podemos estudiar el efecto que este enventanado tiene sobre la respuesta frecuencial del filtro. Consideremos la ventana mas sencilla; la ventana rectangular. Supongamos que la aplicamos sobre una versión retardada de la respuesta ideal, su efecto en el dominio de la frecuencia será la convolución entre la respuesta de nuestro filtro ideal y la transformada esta ventana rectangular, es decir una función *sinc* de período  $1/N$  en donde  $N$  es la cantidad de muestras que entran en la ventana.

El efecto de enventanado o truncamiento de la respuesta es doble: por una parte, la anchura del lóbulo principal está relacionada con la aparición de una banda de transición en el filtro. Por otra, la presencia de lóbulos laterales (secundarios) lleva a la aparición de un ripple u oscilaciones en la respuesta en frecuencia, en ambas bandas, (más apreciable en la banda no pasante). La aparición de los lóbulos secundarios se debe a que la ventana rectangular presenta una discontinuidad abrupta que, al pasar al dominio de la frecuencia, conlleva un reparto de la energía por todo el espectro a causa del aliasing.

Una opción que se plantea es generalizar el concepto de ventana y emplear ventanas más suaves que la rectangular para realizar el truncamiento de la respuesta deseada, esta técnica es una de las formas de realizar un filtro FIR. Sin embargo, si analizamos la transformada de la ventana cuadrada vemos que presenta valores nulos cada  $1/N$ , que son los mismos lugares en donde aparecen las componentes espectrales de la DFT. Esto significa que los efectos de la ventana rectangular aparecen al convertir la respuesta de este filtro a tiempo continuo.

Otra opción sería diseñar un filtro analógico y transformar su respuesta a frecuencia discreta. Para esto contamos con fórmulas cerradas de diseño, por lo que podemos satisfacer cualquier especificación preestablecida. La utilización de esta técnica da como resultado un filtro IIR. Comparado con un FIR, un filtro IIR requiere un orden mucho menor para cumplir las especificaciones de diseño.

Aquí analizamos un sistema en el cual la respuesta es analizada en el dominio digital. Además, es necesario filtrar componentes espectrales de a una, lo que requiere una banda de transición muy estrecha, esto reduce el conjunto de filtros posibles. Por el lado del IIR probamos un filtro elíptico, este filtro presenta una banda de transición muy estrecha en sacrificio de un ripple que aparece tanto en la banda de paso como en la de rechazo. Por el lado del FIR probamos un filtro ideal con una ventana rectangular que abarca toda la serie de valores, en la sección 5.2 se detalla como fue implementado.

## Resultados

Para representar la dinámica en función del filtrado, se eligieron dos señales representativas (cuadrada y senoidal) y se les calcularon los cuantificadores descriptos en la sección 3.2 luego de ser filtrados por los filtros elegidos en la sección 3.2.6. Por otro lado, se calculan los mismos cuantificadores a una señal de ruido blanco gaussiano.

En la figura 3.21 se muestra el procedimiento utilizado. Primero se generó un vector de ruido blanco gaussiano de  $N = 50E3$  muestras, la desviación estándar  $\sigma$  es variable y se logra multiplicando al vector inicial de  $\sigma = 1$  por la desviación estándar elegida. Luego se genera la señal determinística de  $N = 50E3$  muestras, período  $T = 100$  muestras y amplitud unitaria, que se sumó el ruido para lograr la señal contaminada. La señal resultante se filtra para luego calcular cuantificadores. Como se explicó más arriba, para calcular la entropía de valores se genera el histograma de valores y se lo normaliza para calcular la Función Densidad de Probabilidad de valores  $PDF_{hist}$  a la que se le calcula la entropía de Shannon normalizada que da como resultado la entropía de valores normalizada  $H_{hist}$ . Para calcular la entropía de patrones de orden se utiliza el histograma de patrones de orden que cuando se normaliza se consigue la función densidad de probabilidad de patrones de orden  $PDF_{BP}$ , a la que se le calcula la entropía de Shannon normalizada para conseguir la entropía de patrones de orden  $H_{BP}$ .

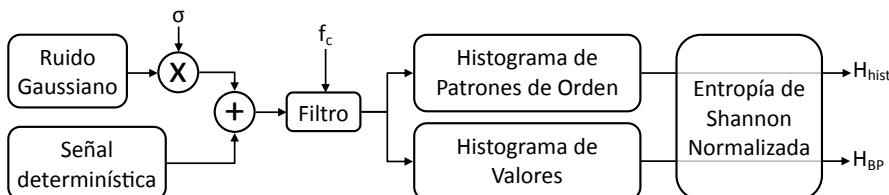


Figura 3.21: Diagrama de flujo del experimento.

Para evaluar la contribución de cada componente espectral a las entropías, se evaluaron dos filtros. Primero se aplicó un filtro elíptico de orden 10 con ripple pasabanda de  $0,5dB$ , ripple en la banda de rechazo de  $100dB$  y frecuencia de corte variable  $f_c$ , en la figura 3.22 se muestra su respuesta en ganancia (fig. 3.22b) y fase (fig. 3.22c) para el caso de  $f_c = 0,5$ . De esta forma se logra un filtrado lo suficientemente abrupto como para considerar que a medida que se barren distintas frecuencias de corte se eliminan componentes espectrales individualmente. Los resultados de este filtrado se compararon con los resultados de un filtro ideal (fig. 3.23), que consiste en una máscara aplicada a la transformada de Fourier de la señal a filtrar, de esta manera se consigue el espectro de la señal filtrada, el cual es antitransformado para recuperar la versión filtrada en las muestras. El diagrama de este filtro puede verse en la figura 3.23a. Este procedimiento equivale a un filtrado ideal sin retardo, por lo que el bode de amplitud es  $0dB$  en la banda de paso y  $-\infty dB$  en la banda de rechazo (fig. 3.23a); la fase  $\omega\tau = 0$  es lineal con pendiente nula (fig. 3.23c).

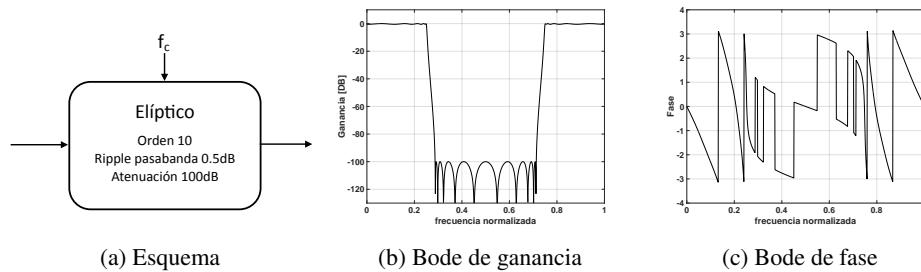


Figura 3.22: Filtro elíptico.

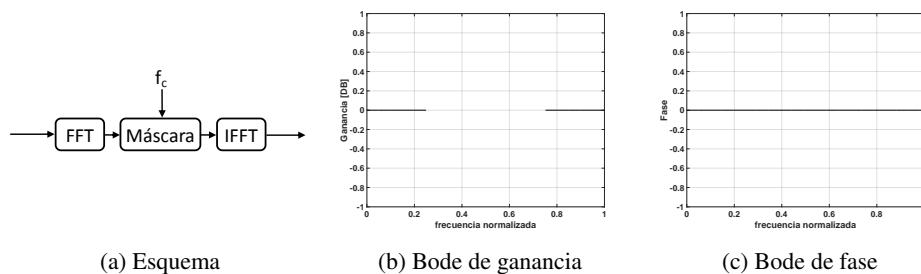
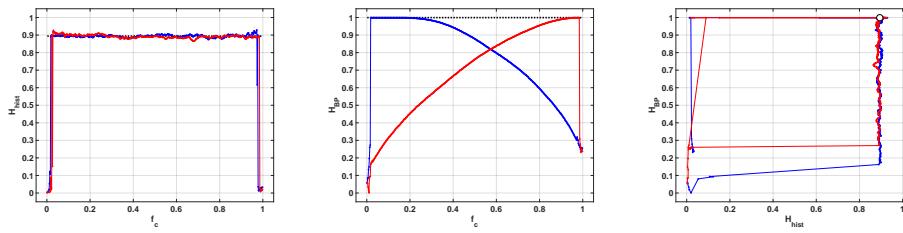


Figura 3.23: Filtro ideal.

Primero se aplicó una señal de ruido blanco gaussiano, es decir que la señal determinística es cero y la desviación estándar de la gaussiana unitaria. En la figura 3.24 se muestra el resultado de los cuantificadores a medida que se va barriendo la frecuencia de corte del filtro elíptico. En la figura 3.24a se muestra la entropía del histograma de valores  $H_{hist}$ , puede

verse que su valor se mantiene constante alrededor de 0,9 tanto para el filtro pasa-bajos (roja) como el pasa-altos (azul), este valor es el mismo que resulta de calcular la entropía del histograma de valores a la señal sin filtrar (resultado que se muestra con una línea punteada negra en el mismo plot). También puede verse que cuando la frecuencia de corte del filtro elíptico se acerca a los extremos el valor del cuantificador cae, en estas frecuencias el método numérico que calcula el vector filtrado diverge debido a la precisión finita. En la figura 3.24b se muestra la entropía de los patrones de orden,  $H_{BP}$  se mantiene en valores bajos cuando el filtro (pasa-altos en azul y pasa-bajos en rojo) deja pasar pocas componentes espectrales. Luego, a medida que la frecuencia de corte deja pasar más componentes espectrales, el cuantificador tiende a 1, que es justamente el valor que arroja cuando se ingresa con la señal sin filtrar (este valor se marca con una línea punteada negra). El cuantificador detecta los cambios en la forma de la señal a medida que es filtrada. Por último, en el plano  $H_{hist} - H_{BP}$  de la figura 3.24c se compacta la información de ambos cuantificadores, aunque se pierde la noción de la frecuencia de corte.

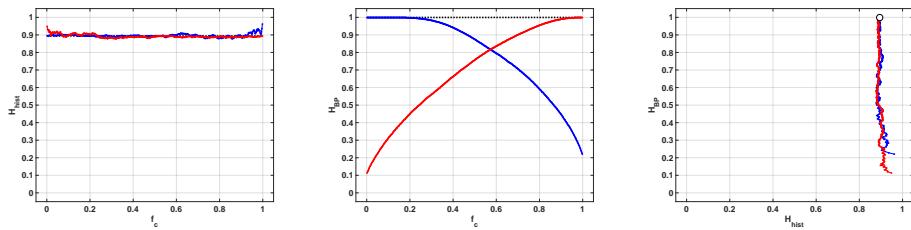


(a) Entropía de valores normalizada  
(b) Entropía de patrones de orden normalizada  
(c) Plano doble entropía

Figura 3.24: Cuantificadores calculados sobre la salida del filtro elíptico cuando se ingresa con ruido blanco gaussiano.

En la figura 3.25 se muestran los resultados del mismo procedimiento pero cuando se aplica un filtro ideal. El comportamiento de los cuantificadores es igual al del filtro elíptico en todos los casos con la diferencia que el método no diverge cuando  $f_c \rightarrow 1$  o  $f_c \rightarrow 0$ . Pueden verse por lo tanto los valores que arrojan los cuantificadores en los extremos de la frecuencia de corte. La entropía no causal de la figura 3.25a aumenta levemente en los extremos, en donde el histograma de valores deja de tener una distribución gaussiana y se aplana levemente. También puede verse en 3.25b que la entropía de valores  $H_{BP} \rightarrow 0,15$  cuando  $f_c \rightarrow 0$  para el pasa-bajos (rojo) y para el pasa-altos (azul)  $H_{BP} \rightarrow 0,22$  cuando  $f_c \rightarrow 1$ . En este caso es fácil comparar la sensibilidad al filtrado de ambos cuantificadores,

en el plano doble entropía de la figura 3.25c. El círculo blanco muestra la posición en este plano cuando ningún filtro es aplicado, podemos ver que el apartamiento en el eje vertical aumenta a medida que la serie es filtrada, mientras que no se aparta en el sentido horizontal. Esto muestra que la sensibilidad al filtrado de  $H_{BP}$  es mucho mayor que la de  $H_{hist}$ .



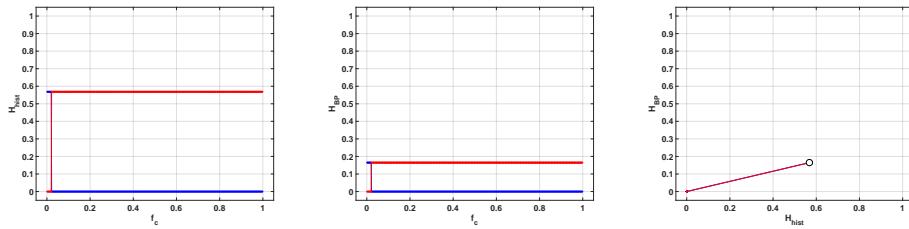
(a) Entropía de valores normalizados  
(b) Entropía de patrones de orden normalizada  
(c) Plano doble entropía

Figura 3.25: Cuantificadores calculados sobre la salida del filtro ideal cuando se ingresa con ruido blanco gaussiano.

Para el sistema planteado no se necesita volver al dominio continuo analógico, por lo que las dificultades mencionadas en la sección 3.2.6 respecto al filtrado ideal (como ripple en las bandas de paso y rechazo) no aplican a este caso. Por este motivo para esta serie de pruebas elegimos el filtro ideal, dado que presenta mejores resultados que el elíptico.

La primer señal determinística que se muestra es una senoidal de amplitud unitaria con período de 100 muestras, los resultados pueden verse en la figura 3.26. Mientras la única componente espectral no es filtrada, el valor de la entropía de valores es  $H_{hist} \approx 0,57$  en la figura 3.26a y la entropía de patrones de orden  $H_{BP} \approx 0,16$  en la figura 3.26b. Ambos cuantificadores caen a cero cuando la única componente espectral es filtrada, ya sea por el filtro pasa-bajos (azul) o por el pasa-altos (rojo). El plano doble entropía muestra un punto en  $(0,57; 0,16)$  para la senoidal sin filtrar y otro en  $(0; 0)$  cuando la única componente espectral es filtrada.

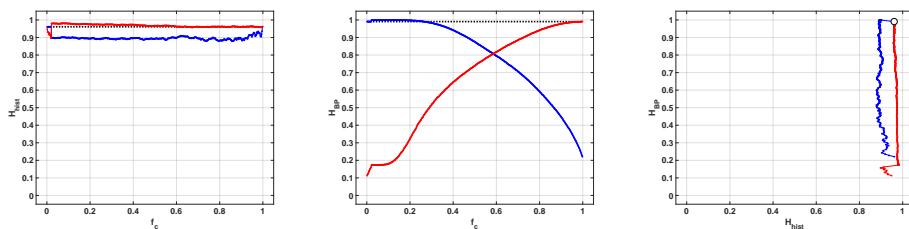
La salida de los cuantificadores cuando esta señal es contaminada con ruido gaussiano aditivo con  $\sigma = 0,2$  puede verse en la figura 3.27. Vemos en la figura 3.27a que la entropía de valores aumenta cuando el filtrado no elimina la componente espectral, dando valores incluso sobre el valor de la entropía de la gaussiana. Esto se debe a que la PDF de la senoidal es complementaria con la de la gaussiana, entonces la PDF de la resultante es más parecida a la del ruido uniforme. Para los patrones de orden de la figura 3.27b, el pasa-altos no deja ver un cambio significativo debido a que la componente espectral de la senoidal es eliminada



(a) Entropía de valores normalizada  
 (b) Entropía de patrones de orden normalizada  
 (c) Plano doble entropía

Figura 3.26: Cuantificadores calculados sobre la salida del filtro ideal cuando se ingresa con una senoidal limpia.

en la zona en la que su entropía es alta. El pasa-bajos en cambio muestra que mientras esta componente está presente el valor de la entropía es asintótico a  $H_{BP} \rightarrow 0,16$  a medida que la frecuencia de corte baja. Recordemos que  $H_{BP} \approx 0,16$  es el valor de la entropía de patrones de orden de la senoidal limpia. En el plano doble entropía (figura 3.27c) se ve que ambos cuantificadores son complementarios, en el sentido que la entropía de valores detecta la presencia o no de la señal determinística mientras que la entropía de patrones de orden detecta el filtrado sobre la señal de ruido.



(a) Entropía de valores normalizada  
 (b) Entropía de patrones de orden normalizada  
 (c) Plano doble entropía

Figura 3.27: Cuantificadores calculados sobre la salida del filtro ideal cuando se ingresa con una senoidal ruidosa.

En la figura 3.28 se muestran los resultados cuando la señal determinística es una cuadrada sin ruido de amplitud unitaria y período de 100 muestras. Tanto la entropía de valores  $H_{hist}$  como la entropía de patrones de orden  $H_{BP}$  presentan una forma escalonada, sus valores se mantienen constantes a medida que se barre la frecuencia de corte de los filtros hasta que la siguiente componente espectral es filtrada. También se ve que en ambos casos los valores resultantes se mantienen bastante lejos del valor sin filtrar, que se muestra con una línea negra punteada.

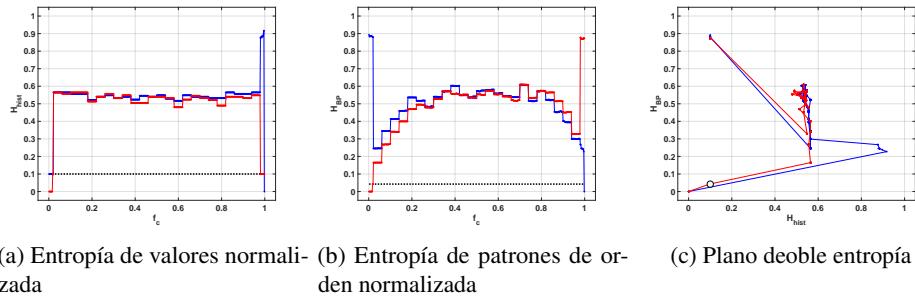


Figura 3.28: Cuantificadores calculados sobre la salida del filtro ideal cuando se ingresa con una cuadrada limpia.

El caso contaminado con ruido (figura 3.29) cambia respecto del caso sin contaminar. En la figura 3.29a se ve que para el pasabajos (rojo)  $H_{hist}$  se mantiene alrededor del valor sin filtrar (línea punteada), excepto con las tres frecuencias más bajas, en donde su valor aumenta un levemente por las mismas razones que aumentaba con la senoidal contaminada. Algo parecido sucede con  $H_{BP}$  en la figura 3.29b. Cuando la cuadrada se contamina con ruido su valor se mantiene cercano al del ruido gaussiano, esto es por que en las regiones en las que la cuadrada es plana su contribución al patrón de orden es nula. Para el pasa bajos se ve un escalonado en la posición de cada componente espectral que se hace más notorio para las frecuencias más bajas, en donde la contribución del ruido ya es bastante baja y a la vez se encuentran las componentes espectrales de mayor peso. Esto no es tan notorio en el pasa-altos, en este caso cuando la contribución del ruido es de baja amplitud también lo es la de la determinística, enmascarando este fenómeno.

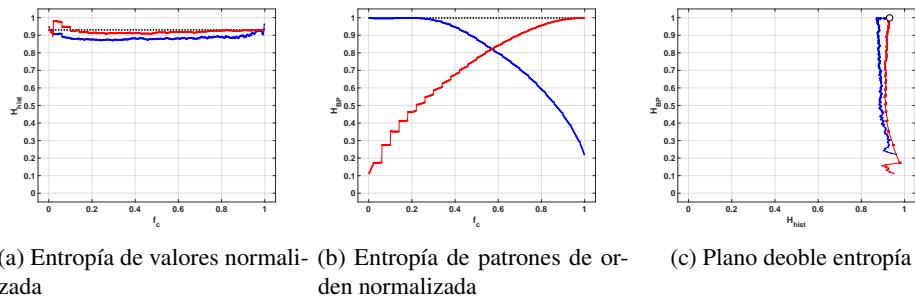


Figura 3.29: Cuantificadores calculados sobre la salida del filtro ideal cuando se ingresa con una cuadrada ruidosa.

Para caracterizar el comportamiento de los cuantificadores frente a la amplitud de ruido, se generaron cuadradas contaminadas con AWGN de dos amplitudes y se filtraron para

calcular cuantificadores. En la figura 3.30 se muestran ambos cuantificadores cuando se hace variar el ruido con valores de la desviación estándar  $\sigma = [0 \ 0,1 \ 1]$ . Cuando comparamos las figuras 3.30a, 3.30b y 3.30c vemos un cambio significativo cuando pasamos de la señal limpia de 3.30a a la contaminada con bajos niveles de ruido de la 3.30b, sin embargo cuando pasamos del bajo nivel de ruido de 3.30b al de la figura 3.30c el cambio es mucho más sutil. De modo similar, entre las figuras 3.30d y 3.30e hay muy poco parecido, mientras que las figuras 3.30e y 3.30f son bastante similares. En este segundo caso es más evidente la diferencia cuando cambia el nivel de ruido, con bajos niveles puede verse el escalonado que aparece cada vez que una frecuencia es filtrada, mientras que cuando la amplitud de ruido es mayor este escalonado aparece solo en el pasabajos para las tres primeras frecuencias, que resultan ser las de mayor peso.

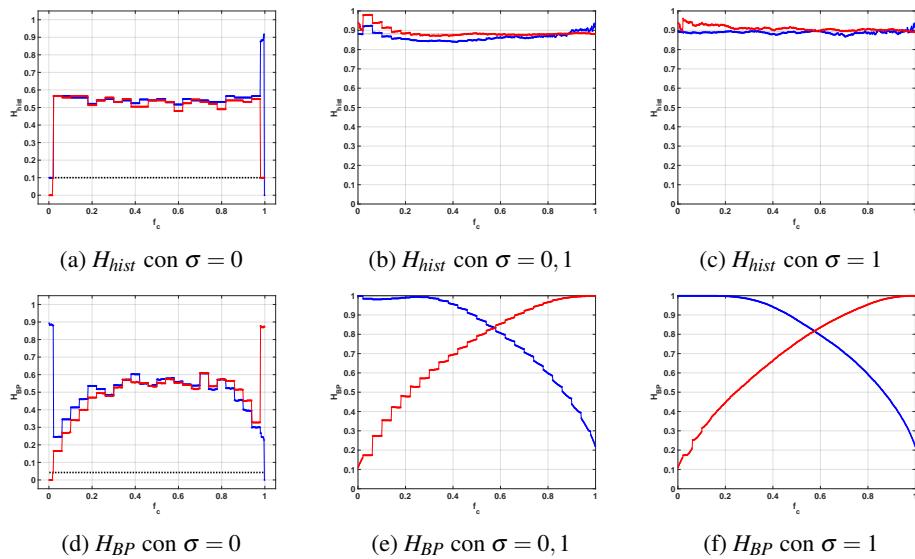


Figura 3.30: Cuantificadores calculados sobre la salida del filtro ideal cuando se ingresa con cuadradas contaminadas con AWGN de con amplitudes de ruido  $\sigma = [0 \ 0,1 \ 1]$ .

### 3.3. Conclusiones

En este capítulo presentamos las principales herramientas utilizadas para detectar caos y cuantificar la calidad estadística de los generadores de números aleatorios. Junto con la introducción tórica, se mostraron algunos avances en la implementación de dichas herramientas.

El algoritmo evolutivo desarrollado detecta con precisión el máximo *MLE* del sistema en cada región en el espacio de parámetros del conocido oscilador Logístico. El siguiente paso es reemplazar el oscilador logístico por el sistema de multiatractores caótico descrito en la sección ref caos. La búsqueda exhaustiva de *MLE* barriendo todos los valores de parámetros se vuelve muy complicada cuando aumenta el número de parámetros. Esta es la razón por la cual se empleó un algoritmo genético en este trabajo. Este algoritmo heurístico permite encontrar las áreas de interés, p.  $MLE > 0$ , de una manera más rápida y simple. Hoy en día, estamos trabajando para finalizar la implementación de hardware de todo el sistema. En la implementación de hardware del cálculo *MLE*, hemos explotado la naturaleza paralela de subrayado de las ecuaciones de cálculo *MLE* con el objetivo de optimizar el diseño de arquitectura propuesto, permitiendo su implementación concurrente basada en tecnología FPGA.

Se desarrolló e implementó un sistema que permite medir con buena precisión las entropías causal y no-causal de señales analógicas provenientes del exterior de la FPGA y también internas generadas por código. Se logró medir señales y realizar cálculos complejos con un microcontrolador modesto como el 8051 instanciado en la FPGA AFS1500 de ACTEL. Este primer prototipo cumple con las especificaciones de precisión y cantidad de recursos requeridos establecidas en el diseño, el próximo paso será optimizar el sistema en cuanto a frecuencia de operación e inmunidad al ruido. Se prevé que el sistema permita modificar, en tiempo de ejecución, la frecuencia de muestreo, de forma de que sea adaptable a la señal de entrada, con el límite superior de 500 Ks/s fijado por el ADC. Deberá agregarse también un umbral a partir del cual un valor es considerado distinto de otro, de esta forma se solucionaría el problema que presenta el ruido aditivo en el cálculo de  $H_{BP}$ . El código de este sistema ocupa el 15,4% del total de la memoria flash del micro instanciado, por lo que será posible agregar *software* para implementar otros cuantificadores y funcionalidades. En cuanto a los recursos disponibles en la FPGA se utilizaron 7349 celdas lógicas, quedando casi el 80% de los recursos de *hardware* disponibles para implementar los sistemas bajo prueba en forma concurrente.

También se exploraron las fuentes de error en un medidor de entropías implementado en FPGA. Para este primer análisis evaluamos que sucede aplicando un filtro abrupto, es por esto que elegimos para comparar un filtro elíptico y uno ideal. Las respuestas del filtro elíptico y del ideal fueron muy similares en el rango de frecuencias en los que el elíptico tiene un buen comportamiento, sin embargo cuando la frecuencia de corte del elíptico se

acerca a los extremos (es decir cuando  $f_c \rightarrow 0$  o  $f_c \rightarrow 1$ ) la salida del filtro diverge. El problema se debe a que el método numérico utilizado para calcular la salida del filtro diverge por la precisión finita utilizada. Como no necesitamos volver a la frecuencia continua nos quedamos con los resultados del ideal para hacer las pruebas, sin tener que preocuparnos por el ripple que aparece en las bandas de paso y rechazo cuando pasamos al mundo analógico. Cuando comparamos las respuestas de los cuantificadores con y sin ruido, vemos que las señales limpias tienen mesetas, es decir que se mantienen constantes hasta que el filtrado elimina la siguiente componente espectral. Sin embargo, cuando son contaminadas con ruido los cuantificadores cambian para parecerse más a los resultados que arroja el ruido blanco gaussiano sin ninguna señal determinística. En todos los casos se vio que estos cuantificadores son muy sensibles a la presencia de ruido, los que nos permite vincular a este hecho los errores en la medición. También vimos que los valores cambian a medida que se filtra la señal sin contaminar, lo que agrega una segunda fuente de error dada por el ancho de banda finito del sistema. Para continuar con este proyecto faltaría, por un lado caracterizar el sistema de medición en cuanto a su ancho de banda y su rechazo al ruido aditivo, y por otro lado probar con otros cuantificadores (como complejidad, desequilibrio, entropía diferencial, rate entropy, etc) o con variantes de los presentados aquí (Bandt & Pompe pesada, amplitud promedio en el emmbedding, etc).

## Capítulo 4

# Generadores de Números Aleatorios Usando Caos

En los últimos treinta años, los sistemas caóticos han producido una revolución en nuestra visión de la naturaleza ya que tienen dos características contrastantes: (1) son deterministas porque un modelo matemático determina su dinámica, pero (2) debido a su sensibilidad a las condiciones iniciales, se pierde la predicción a largo plazo y, en consecuencia, pueden incluirse en la clase de sistemas estocásticos que se estudian mediante herramientas estadísticas. Estos sistemas pueden generar señales estocásticas a partir de modelos simples subyacentes que son fáciles de implementar a través del software o hardware apropiado.

Esta *dualidad determinista-estocástica* hace que los sistemas caóticos sean especialmente interesantes para las aplicaciones de ingeniería, en la medida en que las señales generadas pueden usarse como ruidos controlados en una amplia gama de aplicaciones. Por lo general, se requiere una manipulación adecuada de las series de tiempo que generan estos modelos para mejorar sus propiedades estadísticas. Esto se debe a que las secuencias caóticas realmente presentan correlaciones internas no lineales, es necesario utilizar técnicas de aleatorización para mejorar la aleatoriedad de la serie [9]. La determinación del grado de estocasticidad tiene como objetivo proporcionar una metodología de diseño optimizada para la utilidad prevista dada al sistema caótico.

Así, por ejemplo, hay aplicaciones que requieren que el sistema caótico reemplace un sistema estocástico (criptografía [40], generadores de secuencia para difundir comunicacio-

nes de espectro [41, 42], generadores de números pseudoaleatorios [43, 44, 45], reducción de la interferencia electromagnética [46], etc.). Por otro lado, algunas aplicaciones requieren previsibilidad a largo plazo, por ejemplo para reproducir el sistema caótico de la manera más precisa posible, este es el caso de las comunicaciones analógicas que usan portadores de sincronización caóticos [47, 48].

Un problema es la determinación exacta del período de la secuencia pseudoaleatoria. Para generadores que se basan en operaciones lineales, el problema se ha estudiado en profundidad y existen criterios de diseño bien conocidos para obtener dispositivos de ciclo máximo. Ejemplos de algoritmos lineales son: el algoritmo Mersenne Twister que es un generador de números aleatorios muy rápido de período  $T = 2^{19937} - 1$  [49] y Multiply-With-Carry (MWC), un método inventado por George Marsaglia para la generación de secuencias de enteros aleatorios basados en un conjunto inicial de dos a muchos miles de valores de semilla elegidos al azar, presenta períodos inmensos, que van desde alrededor de  $2^{60}$  a  $2^{2000000}$  [50]. Sin embargo, desde el punto de vista criptográfico son débiles.

Cuando se trata de aplicaciones criptográficas, no se recomiendan métodos lineales para generar secuencias pseudoaleatorias (como LFSR, LCG o sus combinaciones adecuadas), ya que algoritmos eficientes para predecir la secuencia sobre la base de una secuencia de observación relativamente corta están a disposición [51, 52]. Por otro lado, para la mayoría de las familias de generadores no lineales, el problema parece ser intratable y, con pocas excepciones, no suele existir una evaluación analítica de sus períodos [53].

En realidad, si los sistemas caóticos pudieran implementarse con una precisión infinita, serían deterministas en sentido estricto. Sin embargo, solo disponemos de computadoras y dispositivos digitales, que pueden representar internamente las señales por un número finito de bits, esto significa que los valores se describen usando aritmética de precisión finita. Esta restricción es crítica para un sistema caótico ya que es extremadamente sensible a la aritmética empleada, estos dispositivos solo pueden generar atractores *pseudocaóticos*, en el mejor de los casos. Además, la discretización puede destruir el comportamiento *pseudocaótico* y, en consecuencia, es un proceso no trivial.

Otro de los problemas fundamentales, desde el punto de vista de la implementación en hardware, es la optimización de recursos. Contínuamente aparecen nuevos atractores, formas de implementar sistemas o de reducir área y potencia.

En este capítulo se resumen varios trabajos propios orientados a la implementación de sistemas caóticos en hardware. Primero, en la sección 4.1, se explora la la posibilidad

de implementar redes neuronales con comportamiento caótico. Este tipo de sistemas es interesante por presentar un comportamiento autónomo, que puede ser implementado de forma independiente al resto del circuito. Después, en la sección 4.2 se propone un nuevo esquema de codificación basado en los mapas cuadráticos bidimensionales presentados en la sección 2.3.1. Estos mapas presentan distintos atractores con propiedades muy diferentes según sus 12 parámetros, que pueden ser usados como llave, lo que permite mantener la estructura del circuito y generar salidas pseudoaleatorias muy distintas según sea la llave utilizada. Como se dijo más arriba, la precisión numérica es un factor que puede determinar la caoticidad y la estocasticidad de los generadores de números. En los capítulos 4.3 y 4.4 exploramos este tema. Primero, en 4.3 se estudia el comportamiento del sistema de Lorenz utilizando distintas estrategias de representación numérica. Se utilizan estrategias de aleatorización ya que, en este caso, el sistema está orientado a la generación de números pseudoaleatorios. En este caso se utilizaron herramientas estándar de uso libre para evaluar la estocasticidad del sistema resultante. Después en 4.4, se muestra un análisis exhaustivo de los atractores y regiones de atracción para los mapas presentados en la sección 2.3.1. Este estudio es necesario para desarrollar una estrategia de codificación robusta basada en el esquema de la sección 4.2.

## 4.1. Caos en redes neuronales

El problema del caos en las redes neuronales ha recibido mucha atención recientemente. Las actividades en este campo pueden ser divididas en tres categorías:

- Intentos por explicar experimentalmente el comportamiento aperiódico observado en una sola neurona perturbada o en un pequeño ensamble de neuronas.
- Intentos por explicar el comportamiento temporal complejo del cerebro y los posibles roles del caos en el procesamiento de la información.
- El estudio de las rutas al caos y las propiedades de los atractores caóticos en en modelos de redes neuronales.

Las redes neuronales artificiales proveen soluciones efectivas a problemas en diversos campos, en particular, pueden servir como generadores de señales caóticas. Las aplicaciones de señales caóticas son muy diversas, pero en este caso son especialmente atractivas ya que en los algoritmos de aprendizaje se utiliza una búsqueda aleatoria, en estos casos un

generador neuronal de caos puede ser una parte de la red neuronal determinística que se está entrenando.

#### 4.1.1. El modelo de Hopfield

Una de las piedras fundamentales para el reciente renacimiento en el campo de las redes neuronales fué el modelo asociativo propuesto por Hopfield en 1982. La aproximación de Hopfield es un enfoque teórico para pensar ensambles entre unidades de cómputo.

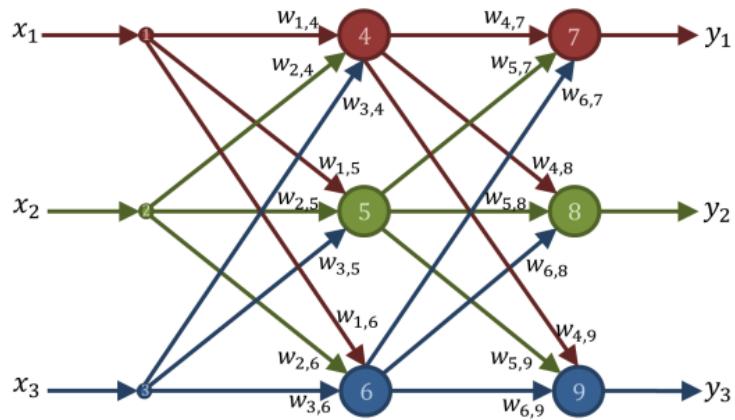
El perceptrón multicapa es una RNA formada por capas de neuronas. Las neuronas pueden pertenecer a la capa de entrada, capas ocultas o capa de salida. Estas neuronas no incorporan memoria por lo que su salida depende del estado de sus entradas en el instante actual (no tienen retardo), además, como el nombre de sus capas lo sugiere, las conexiones son hacia adelante. Es por esto que la matriz de pesos tiene solo algunos valores distintos de cero, no hay conexiones hacia atrás, ni en la misma capa, ni sobre la misma neurona, ni salteándose capas. En la figura 4.1 se ve un ejemplo para un perceptrón pequeño y su matriz de pesos.

Al contrario de los preceptrones multicapa ,los sistemas adaptativos y los mapas autoorganizados, las redes de Hopfield si tienen realimentación entre neuronas. Este tipo de arquitectura tiene como campo principal de aplicación la optimización de procesos. Se basa en el planteamiento de una memoria asociativa; se hace necesario entonces definir una una función de energía. Pone de manifiesto la analogía existente entre su modelo y la física estadística clásica, lo que permite usar sus bien conocidas herramientas matemáticas. Además, es muy interesante que se destaca la facilidad de implementación en FPGA y VLSI.

Esta red recurrente se basa en almacenar información en un sistema que presenta una configuración dinámica estable, es decir, se plantea como una memoria asociativa o memoria direccionable por contenido. Intuitivamente, la idea de Hopfield es localizar cada patrón que se requiere almacenar a la red en el fondo de un valle de la función de energía. Se parte de un determinado estado inicial (información de partida) tras lo cual se deja evolucionar el sistema hasta llegar a un estado estable. Este estado estable será el patrón que se corresponde con nuestro estado inicial (reconocimiento de patrones).

Hopfield, en su trabajo destaca tres diferencias con el preceptrón multicapa:

- Su modelo incluye realimentaciones, que son básicas en su modo de funcionamiento.



$0 \ 0 \ 0$	$w_{1,4} \ w_{1,5} \ w_{1,6}$	$0 \ 0 \ 0$	Vienen de la capa 1
$0 \ 0 \ 0$	$w_{2,4} \ w_{2,5} \ w_{2,6}$	$0 \ 0 \ 0$	
$0 \ 0 \ 0$	$w_{3,4} \ w_{3,5} \ w_{3,6}$	$0 \ 0 \ 0$	
$0 \ 0 \ 0$	$0 \ 0 \ 0$	$w_{4,7} \ w_{4,8} \ w_{4,9}$	Vienen de la capa 2
$0 \ 0 \ 0$	$0 \ 0 \ 0$	$w_{5,7} \ w_{5,8} \ w_{5,9}$	
$0 \ 0 \ 0$	$0 \ 0 \ 0$	$w_{6,7} \ w_{6,8} \ w_{6,9}$	
$0 \ 0 \ 0$	$0 \ 0 \ 0$	$0 \ 0 \ 0$	Vienen de la capa 3
$0 \ 0 \ 0$	$0 \ 0 \ 0$	$0 \ 0 \ 0$	
Llegan a la capa 1	Llegan a la capa 2	Llegan a la capa 3	

Figura 4.1: Perceptrón multicapa y matriz de pesos asociada. Puede verse que la topología de la red y la configuración de la matriz de pesos son biunívocas.

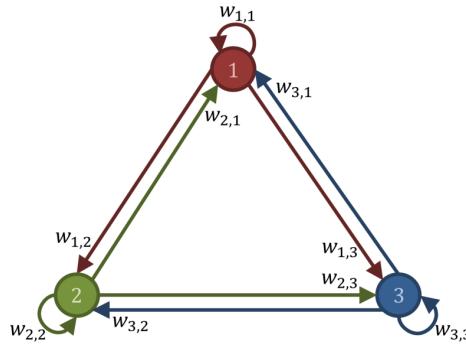


Figura 4.2: Red de Hopfield. Ahora, la matriz de pesos tiene todos sus valores permitidos.

- La elección de la arquitectura del perceptrón multicapa se realiza en forma arbitraria.
- El perceptrón multicapa funciona de manera síncrona, es decir, todas las neuronas cambian al mismo tiempo. La red de Hopfield permite un funcionamiento tanto síncrono como asíncrono, aunque el funcionamiento asíncrono es el más habitual en las neuronas biológicas.

El grafo de la red cambia con respecto al perceptrón multicapa, la representación no es la de un grafo separable por capas con conexiones hacia adelante, sino la de un grafo completo como se ve en la figura 4.2.

#### 4.1.2. Estudio de la RNA en función de un parámetro

La red neuronal usada tiene el modelo de tiempo contínuo

$$\dot{u} = -u + W \cdot f(u); u \in \mathbb{R}^3 \quad (4.1)$$

en donde  $u$  es un vector de tres dimensiones,  $W$  es la matriz de pesos y  $f$  es la función de activación

$$u = \begin{pmatrix} x \\ y \\ z \end{pmatrix}; W = \begin{pmatrix} w_{1,1} & w_{1,2} & w_{1,3} \\ w_{2,1} & w_{2,2} & w_{2,3} \\ w_{3,1} & w_{3,2} & w_{3,3} \end{pmatrix}; f = \begin{pmatrix} \arctan x \\ \arctan y \\ \arctan z \end{pmatrix} \quad (4.2)$$

Ecuaciones que se corresponden con el diagrama de la figura 4.2. Vemos de la ecuación que se corresponde con una red de Hopfield de memoria diferencial. No disponemos de computadoras analógicas, por lo que el sistema debe ser convertido a tiempo discreto.

Aunque el paquete de programas Matlab incluye rutinas para el cálculo de ecuaciones diferenciales, perdemos el control de paso de tiempo necesario para calcular el exponente de Lyapunov con el método descripto en la sección ??, además lo necesitamos para una futura implementación en hardware. Usamos para esto una aproximación de Euler de primer orden, en donde la derivada se aproxima con un trapecio de base  $\Delta t$ .

$$\begin{aligned} \frac{u_{n+1} - u_n}{\Delta t} \approx \dot{u}_n &= -u + W \cdot f(u_n) \Rightarrow \\ \Rightarrow u_{n+1} &= (1 - \Delta t)u_n + \Delta t W \cdot f(u_n) \\ &= Gu_n + \Omega f(u_n) \end{aligned} \quad (4.3)$$

En la figura 4.3 se muestra nuestra nueva red neuronal en tiempo discreto. Sus coeficientes dependen del paso de tiempo. Este sistema se aproxima al de tiempo continuo en el límite  $\Delta t \rightarrow 0$ , en nuestro caso se verificó que el sistema converge al planteado. Pudo verse que con  $\Delta t = 1$  y  $\Delta t = 0,1$  las soluciones en el espacio de fases fueron las mismas, para hacer los cálculos utilizamos  $\Delta t = 0,01$ .

Se barrió un parámetro (peso de un axón) para identificar la existencia de caos en función de éste. Siguiendo a [?] en donde se reporta una transición al caos en torno a un juego de parámetros, utilizamos la siguiente matriz de pesos:

$$W = \begin{pmatrix} 2 & -1,2 & 0 \\ 1,9 + p & 1,71 & 1,15 \\ -4,75 & 0 & 1,1 \end{pmatrix} \quad (4.4)$$

en donde  $p$  es el parámetro a barrer entre  $-0,35$  y  $0,55$  en pasos de  $9 \times 10^{-5}$ .

Para cada valor del parámetro se le da condiciones iniciales al sistema  $[1,68; -0,292; -3,47]$  y se lo deja evolucionar 800s, esto es 200s más que el transitorio más largo reportado en [?], con esto nos aseguramos de descartar el transitorio y que el sistema se encuentra en régimen permanente. Se calcula el MLE para  $t \in (800; 1000]$ .

De esta forma se genera la figura 4.4 en donde se muestra el MLE en función del parámetro. Como es usual, el MLE no es una función suave, sinó que es una función discontinua que presenta saltos abruptos en todo el dominio, sin embargo, se encontraron zonas de caos robusto frente al parámetro  $p$  en algunos intervalos, especialmente en  $p \in (0,0223; 0,0791)$ , esto significa que el caos persiste con una variación no infinitesimal del parámetro, esta zona es muy buscada para implementaciones prácticas.

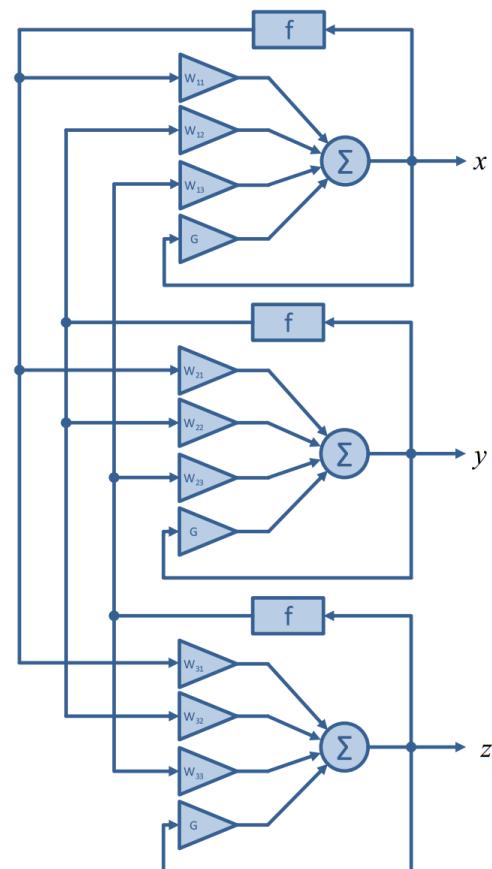


Figura 4.3: Red utilizada. Se trata de una red de Hopfield tridimensional de memoria diferencial, el diseño está orientado a una posterior implementación en FPGA.

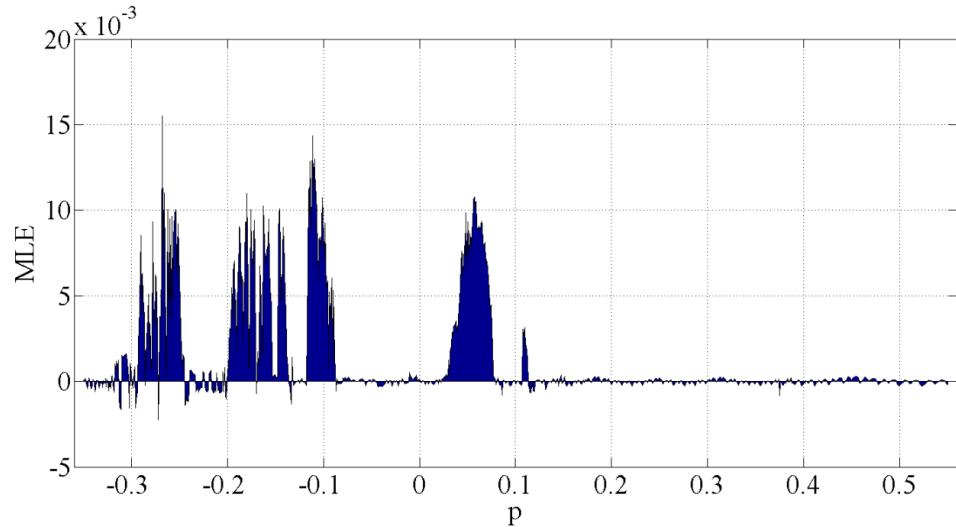


Figura 4.4: Exponente de Lyapunov en función del parámetro  $p$ . Existe caos en toda la zona en la que es positiva.

Para mostrar la transición al caos y la relación entre el MLE y el espacio de fases, se eligieron dos parámetros  $p_1 = -0,2725$  y  $p_2 = 0,268$ , para  $p_1$  el  $MLE = -2,2 \times 10^{-3}$ , para  $p_2$  el  $MLE = 1,55 \times 10^{-2}$ . Se muestra la trayectoria resultante para cada uno en la figura 4.5.

Para el atractor caótico, dos trayectorias generadas a partir de condiciones iniciales muy cercanas deben, al cabo de un tiempo, separarse y oscilar en trayectorias distintas. En la figura 4.6 puede verse este efecto.

## 4.2. Cripto-codificación caótica variante en el tiempo

En esta sección se presenta una nueva técnica para la criptocodificación de datos mediante una familia de mapas caóticos. El diseño se basa en los mapas cuadráticos bidimensionales presentados en la sección 2.3.1, aprovechando su característica de modificar su atractor según los valores que tomen sus 12 coeficientes reales. Para la implementación se utilizó aritmética de punto fijo con 19 bits. Se realizaron simulaciones y el diseño en VHDL mediante el programa Quartus II v8.0 de ALTERA, para su posterior implementación en FPGA.

En los sistemas de comunicaciones y particularmente en los dedicados a la codificación para el control de error y encriptamiento de datos se usan técnicas derivadas de la teoría

76 CAPÍTULO 4. GENERADORES DE NÚMEROS ALEATORIOS USANDO CAOS

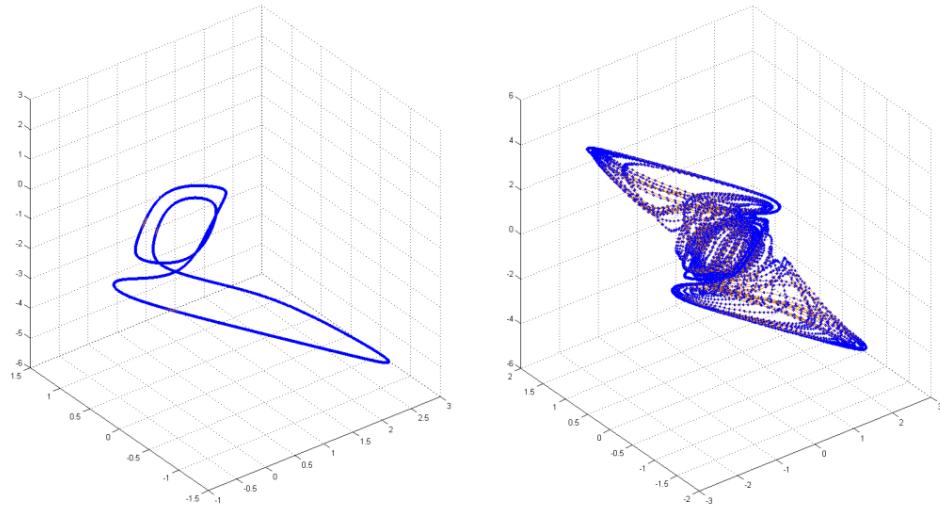


Figura 4.5: Dos trayectorias características del sistema en el espacio de fases. La trayectoria de la izquierda se corresponde con un  $MLE < 0$  y la positiva con un  $MLE > 0$ .

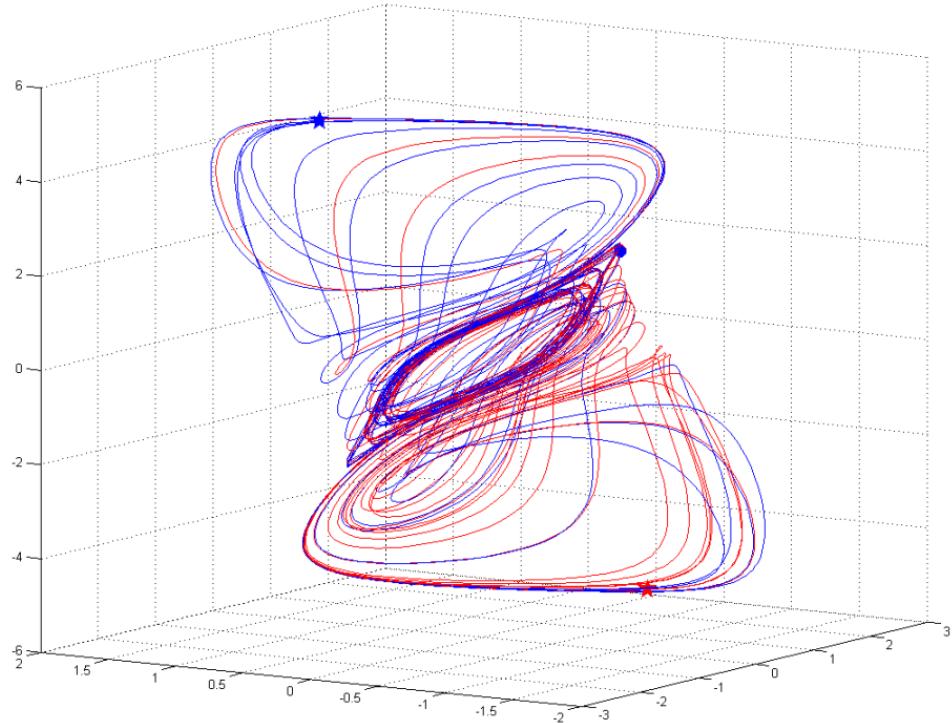


Figura 4.6: Dos trayectorias de la red de Hopfield para condiciones iniciales próximas. Las condiciones iniciales están marcadas con dos puntos grandes cerca del centro del atractor y los valores después de  $\Delta t = 3s$  con estrellas en ambos extremos de la figura.

de señales. Estas técnicas se aplican típicamente en la forma lineal debido a la simplicidad que ésto trae aparejado. Además cada una se implementa algorítmicamente o físicamente como una entidad independiente. Para cada sistema en particular se las elige con criterios de conveniencia práctica, y se las aplica en forma consecutiva o encadenada. La teoría de los sistemas no lineales [?, 54] aparece como un marco de trabajo ideal para ser utilizado en el contexto anteriormente mencionado. La existencia de los sistemas caóticos, y la relación de estos con la aleatoriedad, o pseudo aleatoriedad, otorga una plataforma de diseño que hasta hoy se encuentra poco explotada.

En los últimos veinte años se han presentado diversos trabajos que emplean caos en los sistemas de comunicaciones, como por ejemplo el empleo de portadoras caóticas sincronizadas en las transmisiones analógicas [47, 48]. Si nos centramos en la representación discreta un referente muy importante es el excelente trabajo de Kozic et als. [?, ?] en el que se presenta una técnica de modulación empleando mapas caóticos unidimensionales lineales por tramos, la técnica consiste en la introducción del mensaje a codificar en el bit menos significativo de la secuencia generada. Así, se obtiene una secuencia levemente alterada lo que impide que el sistema entre en ciclos periódicos.

En este trabajo se propone un grupo de atractores como generadores de señales pseudoaleatorias para realizar el proceso de codificación y encriptamiento. El esquema de codificación se basa en la familia de mapas cuadráticos bidimensionales, cuyas salidas presentan comportamiento caótico, con distintos atractores conforme a los coeficientes que se empleen. La idea es que cada palabra a codificar sea unívoca con un juego de coeficientes que serán parámetros de un mapa cuadrático bidimensional. Como resultado de este procedimiento, la señal de salida son puntos pertenecientes a distintos atractores elegidos por la información a transmitir.

La ventaja de este método reside en que la estructura de toda la familia de mapas es única y común. Modificándose solamente los coeficientes se consiguen atractores distintos. Esta propiedad reduce y facilita la implementación en hardware. Resultados preliminares obtenidos mediante simulaciones muestran que el sistema presenta una performance comparable a la obtenida en sistemas clásicos de encriptamiento, en cuanto a probabilidad de error y distancia mínima.

### 4.2.1. Implementación

Desde el punto de vista del esquema de codificación propuesto, estos mapas son muy atractivos por el hecho de contar con 12 coeficientes para generar cada atractor. Por lo tanto, las combinaciones posibles serán  $N^{12}$ , en donde  $N$  es la cantidad de símbolos posibles según la aritmética utilizada. En nuestro caso empleamos una aritmética de 19 bits expresados en complemento a 2 con aritmética de punto fijo, con 1 bit de signo, 3 bits de parte entera y 15 bits de parte decimal. Esta aritmética limita y discretiza el plano  $xy$  que queda delimitado por  $\Delta x = 4, -\Delta x = -4, \Delta y = 4, -\Delta y = -4$ , como puede verse en la figura ???. Estas limitaciones al plano de atracción tienen como consecuencia dos cuestiones a tener en cuenta:

- Debido a que los coeficientes se generan con la misma aritmética que las variables, nos encontramos con  $N = 2^{19}$  valores posibles para cada coeficiente, lo que arroja  $(2^{19})^{12} \cong 4,3^{68}$  combinaciones posibles de coeficientes para generar distintos atractores.
- En cuanto a las trayectorias de los atractores sobre el plano discretizado, éstas se tornan periódicas debido a la discretización.

No todos los juegos de coeficientes generan atractores caóticos contenidos en el plano dado por la aritmética utilizada. Aunque esto no sería problema para la codificación/decodificación, se eligieron los coeficientes de modo que se generen atractores contenidos en el plano a modo de validación visual.

Dada la naturaleza de los mapas caóticos, un punto muy lejano a la zona de atracción puede hacer que el punto calculado para la próxima iteración diverja, por lo tanto las condiciones iniciales deben ser normalizadas antes de cambiar al mapa siguiente. Para solucionar este problema se utiliza la siguiente estrategia:

- Primero se define el plano mínimo que contiene al atractor. Para identificarlo se simularon los mapas mediante Quartus generando secuencias de salida lo suficientemente largas como para verificar la periodicidad. Luego se analizó este vector de datos con Matlab buscando los valores extremos en cada una de las variables:  $X_{1\max}, X_{1\min}, Y_{1\max}, Y_{1\min}$ . Estos límites delimitan al plano mínimo que contiene al atractor. La normalización dada por la ecuación 4.5 se aplica a la salida  $(x,y)$  para mapear este plano mínimo a todo el plano delimitado por la aritmética utilizada de dimensiones  $\Delta x, -\Delta x, \Delta y, -\Delta y$ .

- Segundo, se halla el plano máximo que contiene las condiciones iniciales que hacen que no diverja la solución sino que genere el atractor. Para esto se realizó un programa en Matlab que genera los atractores desde todas las condiciones iniciales del plano delimitado y discretizado por la aritmética utilizada, a continuación se marcan todos los puntos que generan trayectorias divergentes o bien convergentes a un punto fijo. Este proceso genera la zona de condiciones iniciales factible para generar atractores, nuevamente se identificaron los valores máximos y mínimos del área rectangular máxima que contenga todos sus puntos como condiciones iniciales factibles  $X2_{max}$ ,  $X2_{min}$ ,  $Y2_{max}$ ,  $Y2_{min}$ . La normalización dada por la ecuación 4.6 se aplica a la entrada de condiciones iniciales  $(x_{n-1}, y_{n-1})$  para mapear todo el plano de dimensiones  $\Delta x$ ,  $-\Delta x$ ,  $\Delta y$  y  $-\Delta y$  al de condiciones iniciales factibles.

$$\begin{aligned}
 x_{1norm} &= a_{1x}x + b_{1x} \\
 y_{1norm} &= a_{1y}y + b_{1x} \\
 a_{1x} &= \frac{2\Delta x}{x_{1max} - x_{1min}} \\
 a_{1y} &= \frac{2\Delta y}{y_{1max} - y_{1min}} \\
 b_{1x} &= -\frac{x_{1max} - x_{1min}}{2} \\
 b_{1x} &= -\frac{y_{1max} - y_{1min}}{2}
 \end{aligned} \tag{4.5}$$

$$\begin{aligned}
 x_{1norm} &= a_{2x}x + b_{2x} \\
 y_{1norm} &= a_{2y}y + b_{2x} \\
 a_{2x} &= \frac{x_{2max} - x_{2min}}{2\Delta x} \\
 a_{2y} &= \frac{y_{2max} - y_{2min}}{2\Delta y} \\
 b_{2x} &= \frac{x_{2max} - x_{2min}}{2} \\
 b_{2x} &= \frac{y_{2max} - y_{2min}}{2}
 \end{aligned} \tag{4.6}$$

El problema de la existencia de puntos fijos para cierto conjunto de coeficientes y condiciones iniciales queda salvado al perturbar continuamente al atractor actual con valores afectados por la información.

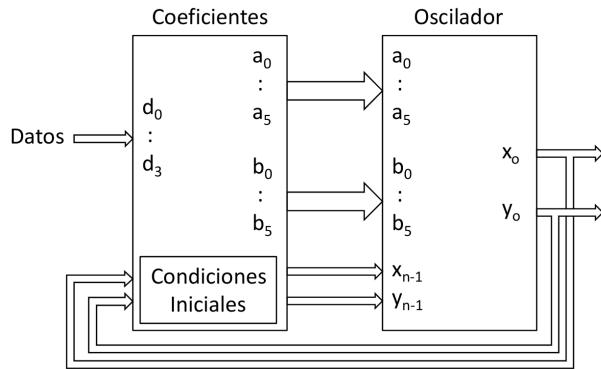


Figura 4.7: Generador de atractores.

Se generó un circuito en VHDL con un total de 16 juegos de parámetros seleccionables con la palabra de entrada de 4 bits que se desea encriptar. Esta palabra multiplexa estos coeficientes y alimenta un oscilador que calcula la próxima iteración de datos, además, este circuito almacena la salida del oscilador y la realimenta como "condición inicial" para calcular la iteración siguiente (Fig. 4.7). Como resultado de este proceso, la salida encriptada resulta ser el oscilador actual seleccionado por la palabra de entrada perturbado por la historia de los mapas seleccionados por las entradas anteriores. Este circuito de dos bloques se encarga de generar los atractores, por lo que se lo llama "generador de atractores".

Para la primer iteración, las condiciones iniciales son  $(x; y) = (0,1; 0,1)$  para cualquiera de los atractores.

### Codificador

El bloque del Codificador consiste en circuito generador y acondicionamiento de la salida. Para codificar una palabra de cuatro bits de entrada se generan los valores de  $x$  e  $y$  con el circuito generador correspondiente a esta palabra y se los concatena en un circuito posterior formando un vector  $[x : y]$  (Fig. 4.8). De esta forma cada palabra de información a ser enviada será representada por la salida  $xy$  del oscilador del atractor correspondiente, por lo tanto una palabra a codificar no se corresponderá con una palabra codificada, dos palabras iguales generarán dos salidas distintas.

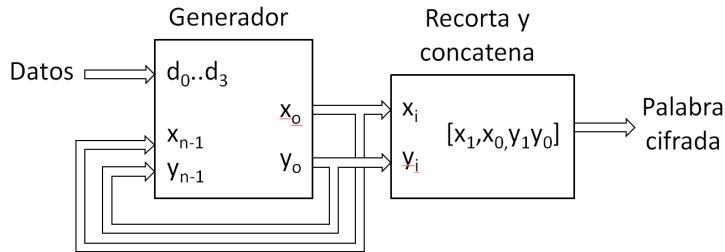


Figura 4.8: Codificador.

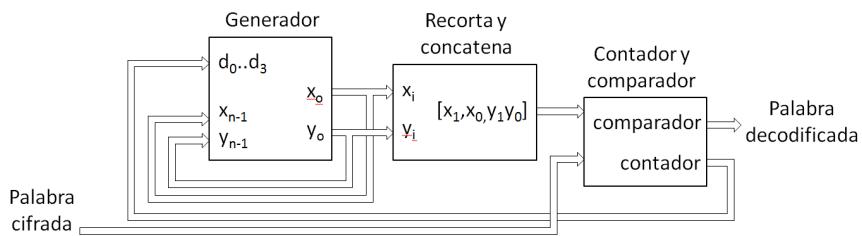


Figura 4.9: Decodificador.

### Decodificador

Un segundo circuito generador de atractores funciona en el decodificador generando las 16 palabras posibles para la próxima iteración. Luego, se ingresan todas estas posibles palabras cifradas junto con la que se desea decodificar a un comparador que aplica una XOR a la palabra ingresada contra todas las palabras posibles generadas localmente para decodificarla. La salida de este circuito es la palabra decodificada (Fig. 4.9).

#### 4.2.2. Resultados

Se realizó un primer esquema del diseño mediante la herramienta Quartus II v8.0 de ALTERA, para implementar el sistema en una FPGA *Altera Cyclone III EP3C120*.

Se obtuvieron resultados preliminares de simulaciones realizadas mediante el programa Matlab y mediante simulaciones con el programa Quartus de Altera, estas últimas tienen en cuenta el empleo de la precisión finita elegida para representar los valores.

En la Fig. 4.10 se pueden ver las salidas del bloque generador para una transmisión de los datos [1,2,3,2,3,3,1,3,1,3,1]. En este caso se mantiene el dato a enviar durante 100 ciclos con el objetivo de que sea visible en la figura, en el sistema real cada oscilador codifica una

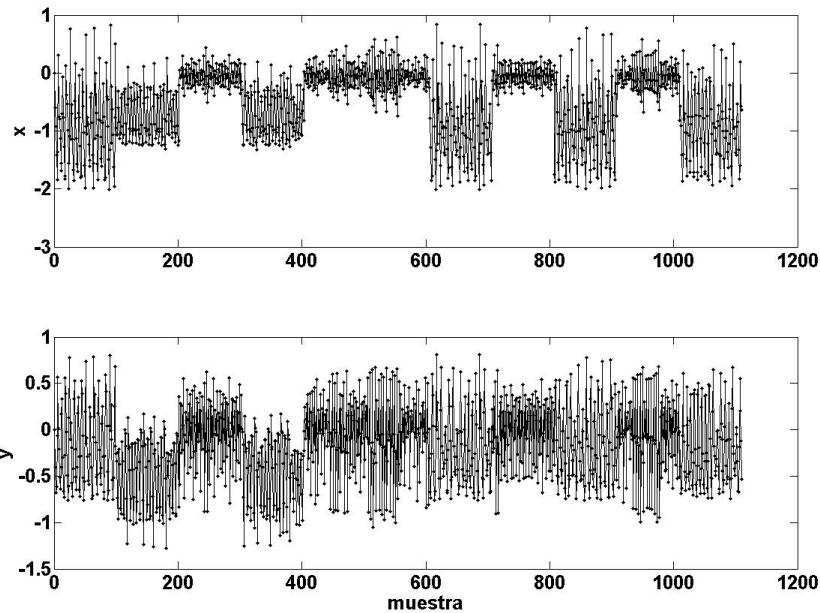


Figura 4.10: Señales a transmitir.

palabra de información en cada iteración. Aquí puede observarse que el sistema cambia el atractor generado según los coeficientes que dependen de la entrada de información a transmitir.

### 4.3. Implementación de atractor Determinístico - Estocástico

En aplicaciones digitales, el tiempo y la variable de estado tienen valores discretos. La discretización de tiempo impone el uso de un algoritmo para aproximar las ecuaciones diferenciales de tiempo continuo que modelan el sistema. El algoritmo más simple es el método de Euler de primer orden en el que los diferenciales se reemplazan directamente por incrementos finitos. Los algoritmos más elaborados, como los algoritmos de paso variable Runge-Kutta de cuarto orden (o superior), hacen que el sistema discreto evolucione más cerca del sistema continuo, pero con mayores requisitos de recursos de hardware y tiempos de cálculo. En consecuencia, deben usarse solo si la exactitud es un requisito de la aplicación específica. Este no es el caso en PRNG, donde la aleatoriedad es la característica principal

que debe garantizarse.

Se han propuesto varias estrategias para una selección correcta del número óptimo de bits en las implementaciones en hardware. Sin embargo, la mayoría de estos procedimientos están limitados a sistemas lineales [55, 56]. En los sistemas digitales caóticos, se puede obtener un comportamiento completamente diferente al variar la precisión. Este problema ha ganado interés recientemente, y se han propuesto varios esquemas nuevos [?, 57, 58].

En resumen, a pesar de la aritmética utilizada, ya sea de punto fijo o punto flotante, el conjunto de números que se pueden representar es limitado. Incluso utilizando una precisión extremadamente alta como lo hacen Liao y Wang [?], las secuencias generadas por un sistema caótico que usa hardware digital siempre serán periódicas.

En esta sección, implementamos un oscilador discreto de Lorenz obtenido mediante el uso del algoritmo de primer orden de Euler y tres estándares de representación diferentes. Además aplicamos técnicas de aleatorización a las variables de estado para obtener un PRNG en tiempo real. El objetivo de este trabajo es estudiar la influencia del procedimiento de discretización en la dinámica del sistema. En [59] se estudió el grado de estocasticidad de un sistema caótico determinista mediante su implementación en coma flotante de precisión simple (32 bits).

Elegimos el sistema caótico de Lorenz porque es un sistema ampliamente estudiado y también ha sido implementado por otros autores con diferentes metodologías [57, 58, 60]. Por ejemplo, en [57], se implementó un oscilador caótico Lorenz mediante una toolbox del Generador de Sistemas Xilinx que funciona bajo *MATLAB-Simulink*<sup>©</sup>. Esta toolbox convierte el modelo MATLAB-Simulink en el modelo de Xilinx System Generator y luego se obtiene el código VHDL. Como es una operación automática, no permite ciertos cambios específicos y presenta algunas limitaciones. La operación de integración se aproximó con el algoritmo de Euler, utilizando bloques de suma y retardo. La implementación propuesta en [58] y [60] usa *RK4* en una arquitectura de punto fijo de 32 bits.

Se utilizó el software *QuartusII*<sup>©</sup> 7.2 para generar el lenguaje de descripción de hardware VHDL y la implementación física se realiza en la placa de desarrollo *Altera*<sup>©</sup> *Cyclone III EP3C12*. Tres representaciones numéricas son estudiadas: 1) punto flotante IEEE 754 estándar, 2) punto fijo decimal, y 3) aritmética entera [61]. Cada representación implica una cantidad diferente de bits. Consideraremos dos representaciones de coma flotante para los estándares simple o doble, con 32 y 64 bits respectivamente para representar el signo, el exponente y la mantisa; La aritmética decimal de punto fijo usa  $p$  bits para representar la

parte entera y  $m$  bits para representar la parte fraccional. Consideramos representaciones de punto fijo de 32 y 64 bits con 9 bits para la parte entera y 1 bit para el signo y los 22 o 54 bits restantes para la parte fraccionaria. En aritmética de enteros  $k$  bits el alfabeto tiene  $2^k$  símbolos. Consideramos  $k = 54$ .

Para cuantificar la aleatoriedad del sistema, se utiliza el conjunto de pruebas DIEHARD de Marsaglia. Estas pruebas han sido ampliamente utilizadas en la literatura abierta y son muy efectivas para clasificar sistemas determinísticos y estocásticos.

### 4.3.1. Discretización temporal del oscilador de Lorenz

El sistema de Lorenz se define mediante el siguiente conjunto de ecuaciones diferenciales ordinarias acopladas:

$$\begin{aligned}\frac{dx}{dt} &= -\delta(x-y), \\ \frac{dy}{dt} &= \Gamma x - y - xz, \\ \frac{dz}{dt} &= -bz + xy,\end{aligned}\tag{4.7}$$

donde  $\delta$ ,  $\Gamma$  y  $b$  son parámetros constructivos del sistema. Para ciertos valores de estos parámetros, el sistema tiene un comportamiento caótico. Siempre se requiere un algoritmo para convertir un sistema dinámico continuo en un sistema dinámico de tiempo discreto. El algoritmo más simple fue propuesto por Euler y, para las Ecs. 4.7 surge el siguiente modelo discreto:

$$\begin{aligned}\tilde{X}_{t+\Delta t} &= \tilde{X}_t + \Delta t \left[ -\delta(\tilde{X}_t - \tilde{Y}_t) \right], \\ \tilde{Y}_{t+\Delta t} &= \tilde{Y}_t + \Delta t \left[ -\tilde{X}_t \tilde{Z}_t + \Gamma \tilde{X}_t - \tilde{Y}_t \right], \\ \tilde{Z}_{t+\Delta t} &= \tilde{Z}_t + \Delta t \left[ \tilde{X}_t \tilde{Y}_t - b \tilde{Z}_t \right],\end{aligned}\tag{4.8}$$

donde  $\Delta t$  es el tamaño de paso de tiempo y  $\tilde{X}$ ,  $\tilde{Y}$  y  $\tilde{Z}$  son variables de estado de tiempo discreto (reales).

El algoritmo de Euler es un algoritmo de un solo paso porque para calcular las variables en el momento  $t + \Delta t$ , solo es necesario conocer los valores en el instante anterior. Calculando iterativamente con un paso apropiado  $\Delta t$ , es posible obtener la evolución del sistema discreto. Es razonable esperar que cuanto menor sea el valor de  $\Delta t$ , más exactos serán los valores

obtenidos. Aunque, al reducir el valor de  $\Delta t$  se incrementa la cantidad de cálculos y esto genera más errores de redondeo.

En aplicaciones que requieren una reproducción exacta de la dinámica del sistema continuo, los algoritmos más exactos son obligatorios, pero en el caso de los PRNG, solo las propiedades estadísticas y la aleatoriedad de las series temporales son importantes y, por consiguiente, el algoritmo de Euler es lo suficientemente bueno.

### 4.3.2. Discretización de las variables de estado

Como se señaló en la introducción, se utilizan tres representaciones numéricas diferentes en este documento. Cada una se describe en las siguientes subsecciones.

#### Estándar IEEE 754

La representación en punto flotante es uno de los métodos para representar números reales con precisión finita. La ventaja de la representación de punto flotante sobre las representaciones de punto fijo y entero es que puede admitir un rango de valores mucho más amplio porque escala automáticamente cada número para usar la longitud de palabra completa para la mantisa; esto se hace moviendo el punto decimal (este procedimiento implica un cambio en el valor del exponente) hacia la posición del bit más significativo. En consecuencia, la precisión total se conserva incluso para números pequeños. La aritmética de punto flotante binaria es más adecuada para trabajar con cantidades del mundo real en una amplia gama de escalas. Se debe tener especial cuidado debido a algunos problemas de precisión.

El estándar de precisión simple IEEE 754 asigna 23 bits a la mantisa (bit 0 a 22), el exponente ocupa los siguientes 8 bits (23 a 30) y el bit 31 está asignado al signo. El estándar de precisión doble IEEE 754 asigna 52 bits a la mantisa (bit 0 a 51), el exponente ocupa los siguientes 11 bits (52 a 62) y el bit 63 está asignado al signo.

Las operaciones aritméticas de punto flotante son más complicadas que las de punto fijo. Su ejecución requiere más tiempo y hardware complejo. Sin embargo, gracias al avance tecnológico y al desarrollo de nuevos materiales, hoy en día existen FPGAs con más memoria y recursos, capaces de trabajar a altas frecuencias en estos estándares.

### Implementación en punto fijo

Cuando todos los números se encuentran dentro de un rango conocido, es posible lograr una mayor precisión utilizando la denominada representación de punto fijo en lugar de la representación de punto flotante. El hardware requerido para manipular estas representaciones es el mismo comúnmente utilizado para realizar operaciones enteras y es menos costoso que el requerido para el caso de punto flotante.

Para evitar el desbordamiento, es necesario realizar inicialmente un análisis para determinar el mayor valor involucrado en el cálculo, incluidas las operaciones intermedias. Con esta información, se determina el número mínimo de bits que se emplearán. Una vez establecido el número de bits necesarios para representar la parte entera, se usa un bit adicional para representar números negativos basados en complemento a 2 (CA2). Los bits restantes se utilizan para mejorar la precisión ya que representan la parte decimal.

Las operaciones de suma, resta y multiplicación se implementan de la misma manera que en la aritmética de enteros. Solo es necesario cuidar la posición del punto de base.

En este documento consideramos dos casos, 32 y 64 bits por cada número entero. En ambos casos usamos 9 bits para la parte entera, más 1 bit para el signo, dejando los bits restantes, 22 o 54 respectivamente, para la parte decimal.

### Impelmentación en aritmética entera

En aritmética de enteros, los circuitos se pueden reducir significativamente si se adoptan divisores con una potencia de 2. Para obtener la versión entera para el sistema Lorenz, se realizaron las siguientes transformaciones de polarización y escalado: [61]:

$$\begin{aligned} X_t &= (\tilde{X}_t + B) S, \\ Y_t &= (\tilde{Y}_t + B) S, \\ Z_t &= (\tilde{Z}_t + B) S, \end{aligned} \tag{4.9}$$

donde  $B$  y  $S$  son los parámetros de polarización y escala, respectivamente. Reemplazando la eq. 4.9 en 4.8 se obtiene:

$$\begin{aligned} X_{t+\Delta t} &= X_t + \Delta t \delta (Y_t - X_t) , \\ Y_{t+\Delta t} &= (1 - \Delta t) Y_t + \Delta t (B + \Gamma) X_t + \Delta t B Z_t \\ &\quad - \frac{\Delta t}{S} X_t Z_t + \Delta t B S (1 - \Gamma - B) , \\ Z_{t+\Delta t} &= (1 - \Delta t b) Z_t - \Delta t B (X_t + Y_t) \\ &\quad + \frac{\Delta t}{S} X_t Y_t + \Delta t B S (B - b) . \end{aligned} \quad (4.10)$$

En este caso, fue adoptado:  $\delta = 8$ ,  $\Gamma = 24$ ,  $b = 2$ ,  $\Delta t = 2^{-n}$ ,  $B = 40$ ,  $S = 512$ .

Debe tenerse cuidado cuando se elijen los parámetros del sistema, en este caso se seleccionaron coeficientes enteros y se realizó un análisis de estabilidad para garantizar que el sistema no converja a un punto fijo o a una órbita de período bajo.

El sistema final es:

$$\begin{aligned} X_{t+\Delta t} &= X_t + \text{floor} \left[ \frac{Y_t}{2^{n-3}} \right] - \text{floor} \left[ \frac{X_t}{2^{n-3}} \right] , \\ Y_{t+\Delta t} &= Y_t - \text{floor} \left[ \frac{Y_t}{2^n} \right] + \text{floor} \left[ \frac{X_t}{2^{n-6}} \right] \\ &\quad + \text{floor} \left[ \frac{Z_t}{2^{n-3}} \right] + \text{floor} \left[ \frac{Z_t}{2^{n-5}} \right] \\ &\quad - \text{floor} \left[ \frac{X_t}{2^{(22+\text{floor}[\frac{n}{2}+1])}} \right] \\ &\quad \text{floor} \left[ \frac{Z_t}{2^{(22+\text{floor}[\frac{n}{2}])}} \right] - 2^{(44-n)} 2520 , \\ Z_{t+\Delta t} &= Z_t - \text{floor} \left[ \frac{Z_t}{2^{n-1}} \right] - \text{floor} \left[ \frac{(X_t + Y_t)}{2^{n-3}} \right] \\ &\quad - \text{floor} \left[ \frac{(X_t + Y_t)}{2^{n-5}} \right] + \text{floor} \left[ \frac{X_t}{2^{(22+\text{floor}[\frac{n}{2}+1])}} \right] \\ &\quad \text{floor} \left[ \frac{Y_t}{2^{(22+\text{floor}[\frac{n}{2}])}} \right] + 2^{44-n} 1680 . \end{aligned} \quad (4.11)$$

Este sistema discreto tiene un comportamiento caótico (de hecho pseudocaótico) y todos los divisores tienen un poder de 2. Todo el procedimiento de preprocesamiento de las ecuaciones minimiza los recursos de hardware necesarios (como se mostrará más adelante).

### 4.3.3. Resultados

Para eliminar o mitigar las estructuras de correlación internas que no son deseables aquí, se analizan dos soluciones, que no requieren un hardware más grande:

1. *descartar*: se forma una nueva secuencia cuyos elementos son números enteros formados por los 32 bits menos significativos de cada elemento de datos (llamado  $x_{disc}$ ,  $y_{disc}$  y  $z_{disc}$  respectivamente);
2. *concatenar*: se forman nuevos enteros de 32 bits al concatenar los bits menos significativos de cada variable (11 bits de  $z$ , 10 bits de  $y$  y 10 bits de  $x$ , se debe tener en cuenta esta es una de las muchas posibilidades), llamado  $zyx$ .

Estos procedimientos se aplicaron a las secuencias de salida generadas por todas las implementaciones descritas en las secciones anteriores. Además, variamos  $\Delta t$  para encontrar su valor óptimo.

Hay varias propiedades básicas que debe tener un buen PRNG: longitud de ciclo larga, aleatoriedad, velocidad, reproducibilidad y portabilidad. Varias suites de prueba [62] están disponibles para los investigadores académicos y la industria que deseen analizar su PRNG recientemente desarrollado. Algunas suites de pruebas de propósito general son DIEHARD de George Marsaglia [63], Crypt-XS de Helen Gustafson de la Universidad Tecnológica de Queensland [64], la suite de pruebas estadísticas del Instituto Nacional de Estándares y Tecnología (NIST) [65], el Test U01 por L'Ecuyer y R. Simard [66] y DIEHARDER [67]. En este documento usamos las 15 pruebas más estrictas de DIEHARD [63] para medir la estocasticidad de cada implementación, pero si la aplicación específica es un PRNG, se recomienda el uso de todas las pruebas mencionadas anteriormente, especialmente NIST 800/22 y Prueba U01.

Para cada PRNG se requiere un archivo con más de  $80 \times 10^6$  bits. Cada ejecución de cada prueba en DIEHARD devuelve un valor  $p$ , que debe ser uniforme en  $[0, 1)$  si el archivo de entrada contiene bits aleatorios verdaderamente independientes.<sup>31</sup> Esos valores  $p$  deben ser  $p < 0,025$  o  $p > 0,975$  para que consideremos que la prueba ha sido aprobada. Cada prueba se ejecuta varias veces dando un valor  $p$  por cada ejecución. Combinando todos estos  $p$ -valores (229 por cada PRNG) obtuvimos un valor general de  $p$  por medio de KStest. Solo si todos los  $p$  individuales y también los  $p$  globales están en el rango apuntado arriba, colocamos “si” en la tabla ??.

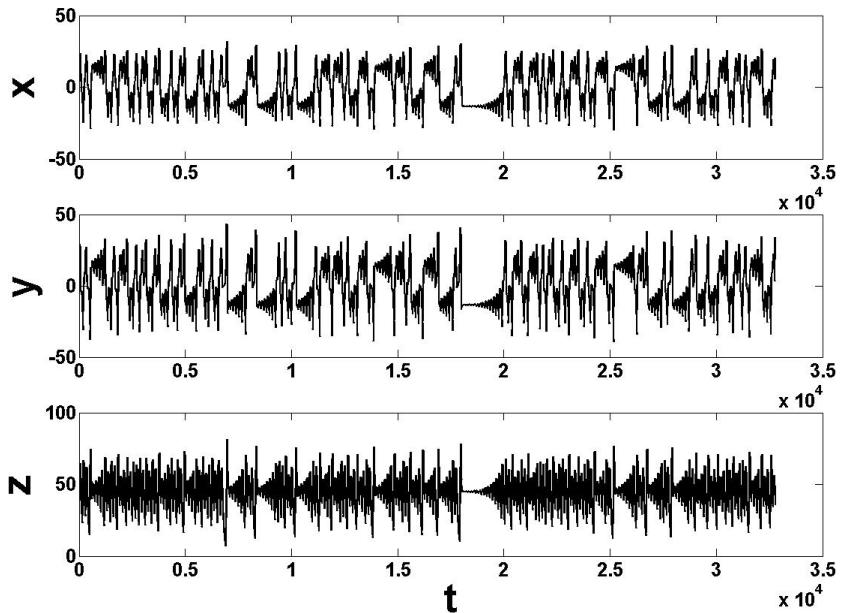


Figura 4.11: Lorenz time series.

Las implementaciones presentadas aquí se desarrollaron completamente con el software *Quartus II 7.2* <sup>©</sup>. Las implementaciones físicas se realizaron en el kit de desarrollo *Altera* <sup>© Cyclone III EP3C120</sup>.

Se utilizó *SignalTap II Embedded Logic Analyzer* para realizar la evaluación de hardware para cada diseño. Esta es una herramienta de depuración a nivel de sistema, proporcionada por *Altera*, que captura y muestra el comportamiento de la señal en tiempo real. Le permite a uno observar las interacciones entre el hardware y el software en los diseños del sistema. Después de capturar los datos y guardarlos en un archivo *SignalTap II*, se pueden analizar y visualizar como una forma de onda [68].

Las figuras 4.11 y 4.12 muestran respectivamente la serie temporal y el atractor, obtenidos por la implementación del hardware con  $\Delta t = 0,0045$  y precisión simple de coma flotante (las cifras con la otra representación numérica son muy similares).

El hardware requerido se muestra en la tabla ???. Aquí se muestra una comparación entre los resultados de la compilación en las tres representaciones numéricas estudiadas:

- *aritmética de punto flotante*: los dos casos, precisión simple y doble (Flotante(32bits) y Flotante(64bits) respectivamente),

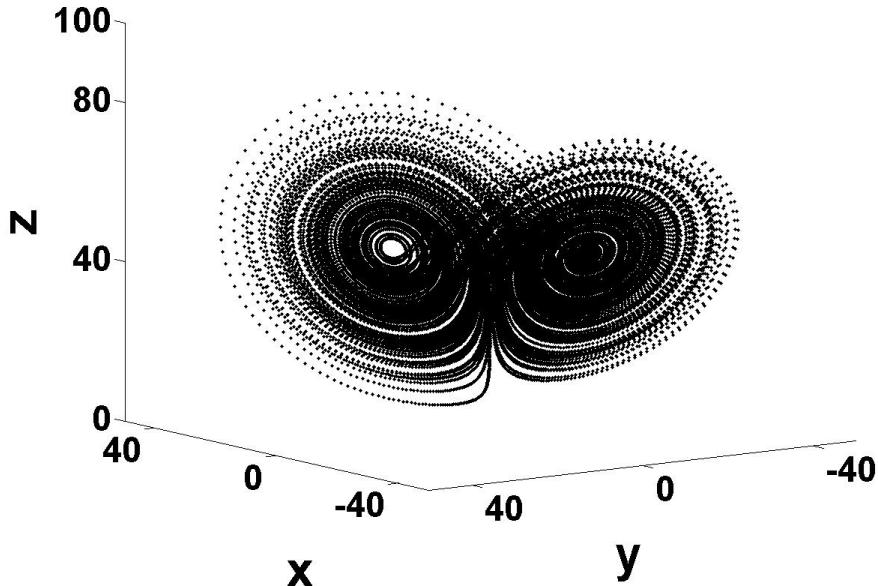


Figura 4.12: Lorenz attractor.

- aritmética entera (Enteros(54bits)) y
- aritmética de punto fijo: los dos casos, ambos con 9 bits de parte entera más 1 bit de signo más los bits para la parte decimal, 22 bits para Punto fijo(32bits) o 54 bits para Punto fijo(64bits) respectivamente.

La implementación aritmética de enteros es la que emplea recursos mínimos y admite un  $f_{max}$  más alto, la razón de esto es que las ecuaciones implementadas fueron optimizadas previamente para esta aplicación en particular. En el caso de la representación de punto flotante, la optimización se realizó para disminuir el área, pero se pueden aplicar otras

Cuadro 4.1: Resultados de compilación en CYCLONE III EP3C120F780C7.

	Punto fijo (32bits)	Punto fijo (64bits)	Flotante (32bits)	Flotante (64bits)	Enteros (54bits)
Elementos lógicos [Total]	2,392	6,104	8,176	17,532	1,297
Elementos lógicos [%]	2,00	5,12	6,86	14,72	1,08
Total de registros	1,658	1,754	4,753	8,532	159
Reloj $f_{max}$ [MHz]	37,82	20,51	7,48	5,42	55,38
Throughput [Mbs]	1,210,24	656,32	14,96	173,44	1,772,16

Cuadro 4.2: Resultados del test DIEHARD.  $\Delta t = 2^{-n}$ .

	$n$	6	7	8	9	10
Flotante (64 bits)	$x_{disc}$	no	no	si	si	no
	$y_{disc}$	no	no	si	si	no
	$z_{disc}$	si	si	si	no	no
	$zyx$	no	no	no	no	si
Punto fijo (64 bits)	$x_{disc}$	si	si	no	no	no
	$y_{disc}$	si	si	no	no	no
	$z_{disc}$	si	si	no	no	no
	$zyx$	si	si	si	no	no
Enteros (54 bits)	$x_{disc}$	si	si	no	no	no
	$y_{disc}$	si	si	no	no	no
	$z_{disc}$	si	si	no	no	no
	$zyx$	si	si	si	si	si

técnicas de optimización para mejorar la frecuencia o el consumo de energía [69, 70].

Para utilizar este sistema como PRNG, los datos de salida se procesan con las técnicas *descarte* y *concatenado*. Ambas técnicas mantienen los bits menos significativos porque presentan el comportamiento más variable. En el caso de la técnica de *concatenado*, la parte más ruidosa de cada variable de estado se mantiene y se recomienda, y se obtiene una salida de secuencia de 32-bits en cada iteración.

Se generaron archivos de datos de análisis estocástico con 3,000,000 palabras de 32-bits cada uno, para  $\Delta t = 2^{-n}$ , con  $n = 6, 7, 8, 9$  y  $10$ . Se calcularon las pruebas DIEHARD para todos los archivos generados. En la tabla ?? se informan algunos de los resultados más relevantes. Definimos los valores  $x_{disc}$ , ( $y_{disc}, z_{disc}$ ) como la serie temporal  $x$  ( $y, z$ ) después de aplicar la técnica de randomización por *descarte*. La variable  $xyz$  es la serie de tiempo obtenida mediante la técnica de aleatorización de *concatenado*.

Esta tabla muestra que en los casos de implementaciones de enteros y punto fijo la técnica de aleatorización de *descarte* funciona mejor a medida que  $\Delta t$  aumenta porque, para elementos  $\Delta t$  inferiores, las series temporales son más correlacionadas y esta técnica de aleatorización no los mezcla lo suficiente. Para utilizar valores de  $\Delta t$  más bajos, más bits deben descartarse para obtener buenos PRNG. Por otro lado, la técnica de aleatorización de *concatenación* funciona bien independientemente del valor de  $\Delta t$  (dentro del rango analizado).

#### 4.4. Mapas cuadráticos 2-D implementados en punto fijo

Al iterar mapas caóticos en  $\mathbb{R}^2$ , después de un transitorio que depende del parámetro de mezcla ( $r_{mix}$ ), la secuencia generada limita en un punto o colección de puntos llamado atractor. Un mapa caótico puede tener uno o más atractores. Dominio de atracción se llama a todas las condiciones iniciales (IC) que convergen a cada atractor. Las secuencias ergódicas de los atractores, generadas por el mapa, tienen una distribución determinada llamada Función de densidad de probabilidad invariable (IPDF). Las principales características de los mapas caóticos, IPDF y  $r_{mix}$ , pueden obtenerse calculando el operador Perron-Frobenius (PFO), que depende de la estructura del mapa. Los puntos fijos de su espectro son las densidades invariables y corresponden a los vectores propios con valor propio igual a uno, la constante de mezcla corresponde al segundo mayor valor propio del PFO, [54, 71].

Cuando se utiliza precisión finita, este análisis no es válido, todos los atractores toman la forma de puntos fijos u órbitas periódicas. El PFO del mapa ya no describe las características de las secuencias. Con respecto al dominio de atracción, también cambiará cuando se digitalice, cada valor inicial será parte de, o convergerá a, un cierto punto fijo u órbita periódica. En general, aparecen muchas nuevas órbitas periódicas y cambian cuando varía el número de bits empleados.

Con el propósito de utilizar estos sistemas en aplicaciones electrónicas, se hace necesario comprender cómo evoluciona el dominio de atracción con la variación de bits empleados. Principalmente es importante saber cuál es la duración del período y el *grado de aleatoriedad* del ciclo en el que converge cada semilla. Por esta razón, hemos incluido cuantificadores de aleatoriedad que estiman indirectamente el  $r_{mix}$  e IPDF del sistema digitalizado.

En esta sección hemos emulado el comportamiento de una implementación en hardware digital, como FPGA, Dispositivo lógico programable complejo (CLPD) o Circuito integrado de aplicaciones específicas (ASIC), para replicar exactamente el funcionamiento del dispositivo. Nuestro interés es medir cómo los dominios de atracción se degradan con un cambio en el número de bits  $n$  empleados, así como también encontrar el valor umbral  $n_{min}$ .

El trabajo de Grebogi [72] mostró que la longitud promedio de las órbitas periódicas  $T$  de un sistema dinámico implementado en una computadora, escala en función de la precisión de la computadora  $\xi$  y la dimensión de correlación  $D$  del atractor caótico, como  $T \sim \xi^{-D/2}$ . El objetivo es investigar las características de cada precisión para que el diseñador tenga una visión general completa de las opciones que se utilizarán en su implementación. De esta

manera, que los diseñadores pueden decidir qué propiedades rescindir según los recursos y requisitos disponibles.

Una cosa importante a tener en cuenta es que además de analizar los cambios en las duraciones de los períodos, las propiedades estadísticas de las secuencias serán diferentes de las del sistema real, por lo que también deberían analizarse. En [?] se desarrolló un excelente trabajo sobre las consecuencias que la precisión finita tiene sobre la periodicidad de un PRNG basado en el mapa logístico. Allí, se determinaron el número, retardo y período de las órbitas del mapa logístico con diversos grados de precisión, sin embargo, carecían de un análisis estadístico. Nuestra investigación complementa su trabajo al agregar cuantificadores estadísticos. Lo que es más, analizaron la arquitectura de coma flotante del mapa, mientras que aquí se eligió la arquitectura de punto fijo ya que es la arquitectura óptima para las implementaciones en hardware. Desde el punto de vista de la ingeniería, la aritmética de punto fijo es más eficiente que la de punto flotante, consume menos recursos y sus operaciones requieren un menor número de ciclos de reloj. Como consecuencia, el consumo de energía también se ve disminuido.

Entre muchos sistemas caóticos disponibles en la literatura, estamos interesados en una familia de mapas 2D propuestos por Sprott [73]. La principal característica de este sistema es que presenta múltiples atractores caóticos dependiendo del punto seleccionado en el espacio de los parámetros, esta característica es muy atractiva para ser utilizada en aplicaciones electrónicas. Solo los resultados para la representación analítica de los mapas en [73] han sido publicados en la literatura abierta.

El objetivo en esta sección es ampliar el análisis a la versión digital para posibilitar la implementación del hardware en aritmética de punto fijo. Para lo cual es imprescindible conocer las dos características, la duración del período y el grado de aleatoriedad de las secuencias. Desarrollamos un análisis detallado de la *degradación* del sistema caótico multiatractor a medida que se utiliza una implementación de punto fijo. Por *degradación* queremos decir: (a) la aparición de puntos fijos estables y órbitas periódicas estables con períodos cortos, dentro de un dominio de atracción de coma flotante sin órbitas estables; (b) el atractor mismo se vuelve periódico y sus características estadísticas cambian, lo que hace que el sistema sea más determinista.

Las principales contribuciones de esta sección son:

- el análisis de los dominios de atracción de los atractores caóticos para un conjunto dado de parámetros a medida que aumenta el número de bits; en términos de la

duración del período y la aparición de puntos fijos estables y órbitas periódicas con períodos cortos se consideran especialmente;

- la determinación del consecuente umbral para el ancho del bus, para hacer que las propiedades estadísticas de la implementación digital sean cercanas a las de la implementación de coma flotante;
- Dos funciones de distribución de probabilidad diferentes (PDF) se asignan para evaluar la estocasticidad de la serie temporal para diferentes anchos de bus. Cada PDF  $P$  se mide por la correspondiente entropía de Shannon normalizada  $H(P)$ . Estas entropías tienen cambios abruptos en anchos de bus específicos. Las duraciones de los períodos y el *MLE* también se evalúan y los resultados se comparan con las  $H_s$ .

#### 4.4.1. Resultados

Un código ANSI C que simula un sistema no lineal iterando (el mapa cuadrático) en cualquier dispositivo electrónico digital fue desarrollado con el fin de generar secuencias que luego fueron analizadas.

Este código itera el mapa cuaratónico  $2D$   $10^5$  veces, en este caso los coeficientes  $a_0$  a  $a_{11}$  tienen los valores:  $\{a_i\} = \{-1,0, 0,9, 0,4, -0,2, -0,6, -0,5, 0,4, 0,7, 0,3, -0,5, 0,7, -0,8\}$ . El sistema fue diseñado para trabajar en arquitectura fraccionaria de punto fijo con  $n$  bits, donde  $n = n_i + n_f$ , en representación de complemento a 2 ( $Ca_2$ ). En este caso, empleamos  $n_i = 4$  bits para representar la parte entera, y el código varía automáticamente la cantidad de bits que representan la parte fraccionaria del número,  $n_f$ , para analizar cómo reacciona el sistema cuando cambia la precisión. El código se ejecuta a partir de todas las condiciones iniciales (ICs) dentro del intervalo  $[-2, 2]$  en pasos determinados por el  $n_f$  actual, por lo tanto, la grilla tendrá un paso de:

$$step\_grid = \frac{1}{n_f, 2^{n_f}}. \quad (4.12)$$

En cada caso se determinó si los sistemas evolucionan a un punto fijo, divergen o van hacia un ciclo periódico, también se generaron secuencias para esa misma IC usando diferentes  $n_f$  bits de precisión. Estos datos fueron luego evaluados utilizando los cuantificadores de aleatoriedad previamente introducidos en la sección 3.

La figura 4.13 muestra los dominios de atracción obtenidos para  $n_i = 4$  y algunos

valores de  $n_f$ . Los ejes de abscisas y ordenadas corresponden a valores iniciales de  $x$  e  $y$  respectivamente. Cada punto representa una IC y el color está asociado a su estado final, mientras más oscuro es el tono de gris, más corto es el ciclo al que converge, los puntos fijos están en negro y los puntos divergentes en blanco. Entonces, se pueden ver aquí los diferentes dominios de atracción (incluyendo los atractores) que coexisten en el sistema.

Con el fin de poder distinguir las diferentes áreas coexistentes, se ha utilizado una amplia gama de tonos grises en cada figura. Se debe tener en cuenta que cada figura tiene su propio rango de grises, esto significa que, por ejemplo, un área casi blanca cuando  $n_f = 5$  (Fig. 4.13.a) corresponde a un período de 6, mientras que un área más oscura en una figura con mayor  $n_f$  puede corresponder a un período superior a mil (Fig. 4.13.e). Estas cifras permiten reflejar los complejos dominios de atracción que aparecen al digitalizar.

Se puede ver en la Fig. 4.13 cuánto menor es el valor de  $n_f$ , mayor es el área de ICs que tiende a divergir y converger a puntos fijos. A medida que  $n_f$  aumenta, el área de puntos divergentes y fijos disminuye. Estas figuras junto con la tabla 4.3 permiten interpretar fácilmente el comportamiento del sistema. En la tabla 4.3 las longitudes de las secuencias que aparecen en el dominio de atracción para cada  $n_f$  se ordenan por el número de circuitos integrados menos numerosos que convergen en ese ciclo. Se puede ver la tasa de ocurrencia. De hecho, las figuras con valores más bajos de  $n_f$  presentan superficies irregulares o rugosas, señalando que los ciclos de diferentes longitudes coexisten allí. Por ejemplo, para  $n_f = 5$  hay una prevalencia de ciclos de períodos cortos. En ese caso, existen solo dos ciclos límite, la zona gris más clara corresponde al dominio de atracción de los ciclos límite de longitud seis, que es el ciclo menos numeroso, de acuerdo con la Tabla 4.3, y la zona más oscura corresponde al dominio de atracción de longitud de ciclo dos.

Aunque para  $n_f \geq 13$  (Figuras 4.13.i a 4.13.l), el dominio de atracción parece ser suave y uniforme, todavía hay ciclos con diferentes períodos que coexisten en el atractor por  $n_f = 14, 17$  y  $18$ . Esto se puede ver si ampliamos una sección de las figuras (Fig. 4.14).

Sin embargo, cuando queremos hacer una comparación general de lo que ocurre con los períodos en los que las precisiones son variadas, se requiere una escala de colores, ver Fig. 4.15.

La figura 4.15 muestra que a medida que aumenta el valor de  $n_f$  el color del área se vuelve más uniforme y claro, lo que indica que las ICs convergen a ciclos de períodos más altos. Esto también se puede ver en la tabla 4.3, donde a medida que  $n_f$  aumenta, la longitud del ciclo límite predominante también aumenta.

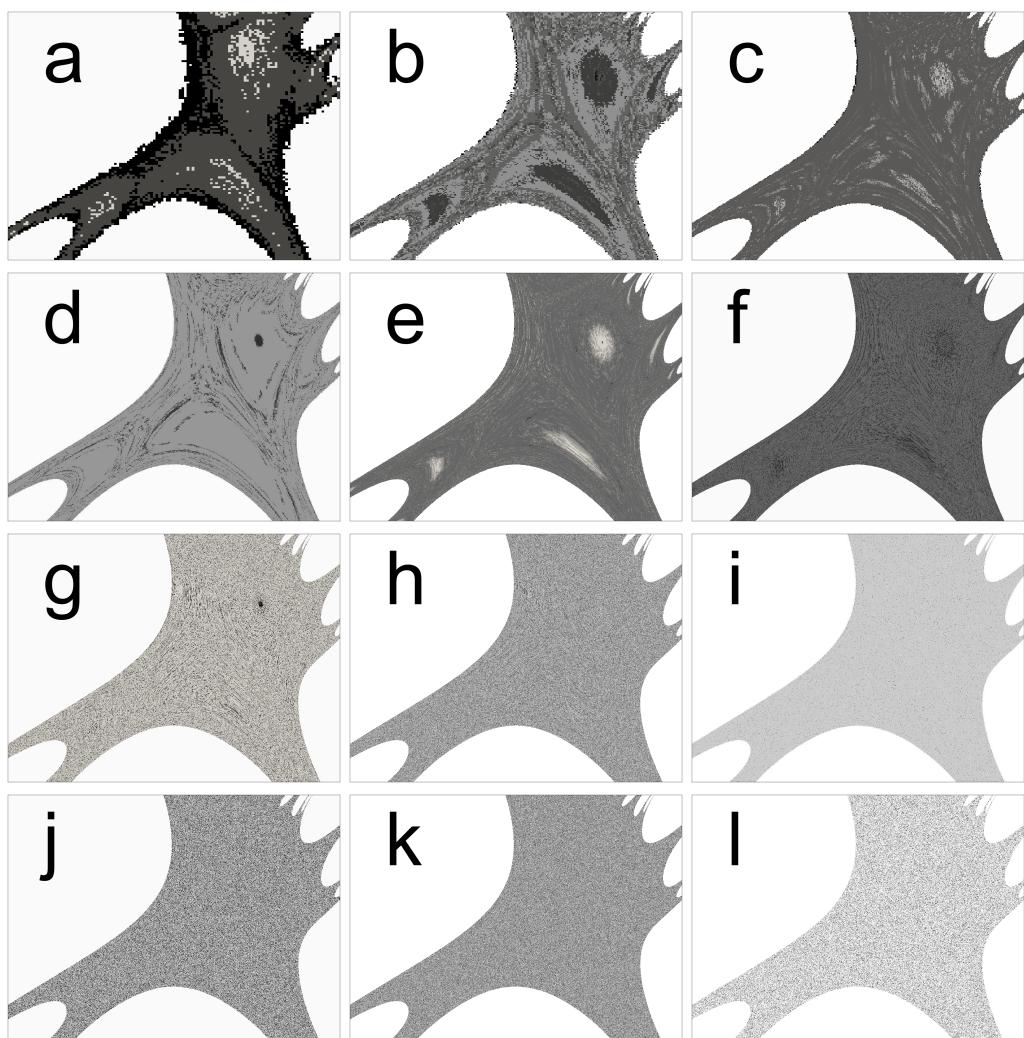
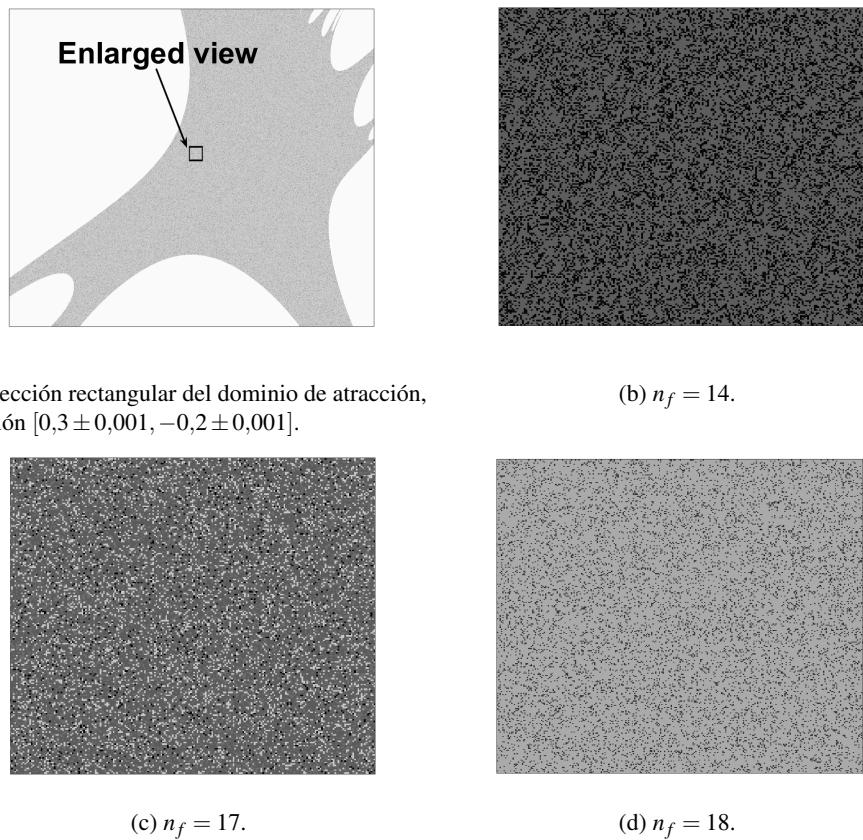


Figura 4.13: Áreas coexistentes en el dominio de atracción para: (a)  $n_f = 5$ , (b)  $n_f = 6$ , (c)  $n_f = 7$ , (d)  $n_f = 8$ , (e)  $n_f = 9$ , (f)  $n_f = 10$ , (g)  $n_f = 11$ , (h)  $n_f = 12$ , (i)  $n_f = 13$ , (j)  $n_f = 14$ , (k)  $n_f = 17$ , (l)  $n_f = 18$ .



(a) Sección rectangular del dominio de atracción,  
sección  $[0,3 \pm 0,001, -0,2 \pm 0,001]$ .

(b)  $n_f = 14$ .

(c)  $n_f = 17$ .

(d)  $n_f = 18$ .

Figura 4.14: Vistas ampliadas del dominio de atracción para distintos valores de  $n_f$ .

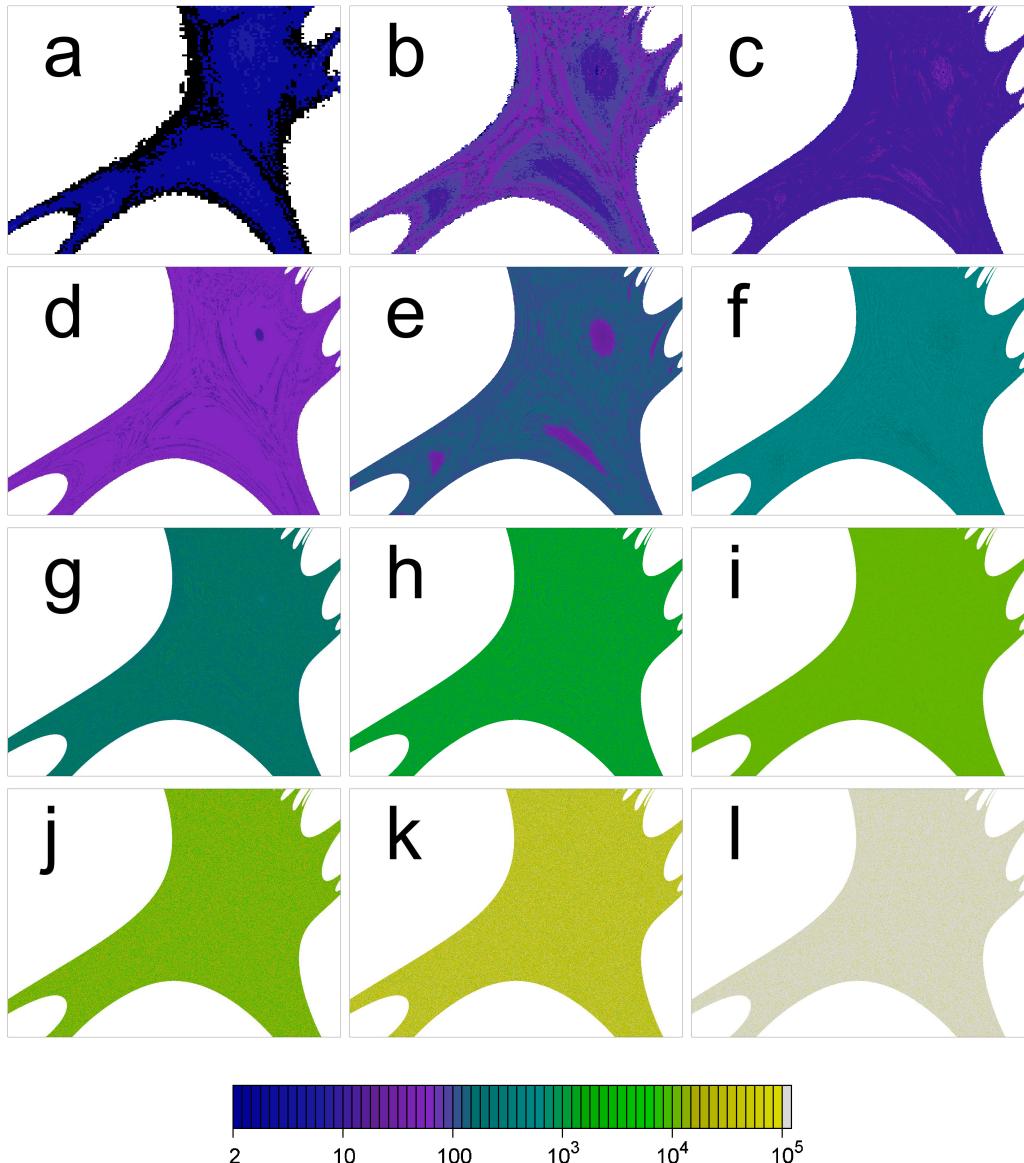


Figura 4.15: Evolución de las longitudes de período de los dominios de atracción para: (a)  $n_f = 5$ , (b)  $n_f = 6$ , (c)  $n_f = 7$ , (d)  $n_f = 8$ , (e)  $n_f = 9$ , (f)  $n_f = 10$ , (g)  $n_f = 11$ , (h)  $n_f = 12$ , (i)  $n_f = 13$ , (j)  $n_f = 14$ , (k)  $n_f = 17$ , (l)  $n_f = 18$ .

Cuadro 4.3: Lengths of the periods within the attractor domain  $x$  and  $y \in [-2, 2]$ .

$n_f$	$T$ (Percentage of ICs that converge to this period's length cycle)
5	2 (92,7%); 6 (7,3%)
6	88 (41,6%); 44 (36,7%); 12 (13,8%); 16 (6,2%); 2 (0,8%); 24 (0,6%); 26 (0,2%)
7	12 (83,5%); 14 (8,9%); 24 (5,2%); 34 (1,8%); 2 (0,6%)
8	68 (91,7%); 14 (6,2%); 12 (1,8%); 17 (0,2%); 15 (0,1%)
9	140 (54,5%); 123 (25,4%); 34 (8,6%); 44 (4,3%); 38 (3,9%); 22 (2,9%); 48; 2; 12; 4 (< 0,1%)
10	655 (78,2%); 212 (21,1%); 143 (0,5%); 12 (0,1%); 2; 36; 13; 20; 10; 4 (< 0,1%)
11	153 (78,1%); 461 (10,8%); 1381 (8,7%); 434 (2,3%); 18; 30; 53; 32; 34; 10; 2 (< 0,1%)
12	2,278 (64,4%); 438 (22,4%); 598 (7,6%); 886 (4,7%); 12 (0,7%); 87; 2; 42; 23; 32; 10 (< 0,1%)
13	11,510 (98,9%); 1052 (1%) ; 12; 26; 2; 10 (< 0,1%)
14	21,333 (69,2%); 5,804 (16,5%); 4,795 (7,9%); 1,264 (5,8%); 2,429 (0,5%) 46; 23; 21; 10; 12; 17 (< 0,1%)
15	10,099 (58,6%); 1,762 (19,4%); 14,887 (18,3%); 1,598 (3,4%); 750; 105; 23; 14; 2; 10 (< 0,1%)
16	54,718 (87,5%); 5,017 (4,7%); > $10^5$ (3,7%); 5,367 (2,5%); 703 (0,9%) 1,159; 1,802 (0,2%); 377; 75; 10 (< 0,1%)
17	37,812 (53,1%); 38,456 (24,1%); > $10^5$ (16,0%); 34,749 (3,0%); 3,362; 718 (1,5%) 3,006,5,222 (0,1%); 15 (< 0,1%)
18	> $10^5$ (87,4%); 52,069 (12,5%); 2,471 (0,1%); 146; 51 (< 0,1%)
float	> $10^5$ (100 %)

Para comparar los valores obtenidos con las secuencias reales, iteramos los atractores en punto flotante con mantisa de 236 bits (IEEE754 de punto flotante binario de precisión de octuple) lo que llamamos aquí *punto flotante* o simplemente *flotante*, es la aritmética más cercana a los números reales a la que podemos acceder con tiempos de cómputo razonables. Luego, utilizando esa precisión en flotantes, todos los ciclos límite son superiores a  $10^5$ , convergen al atractor caótico que se ve en la figura 2.17.d.

En relación con los cuantificadores de la aleatoriedad, nos dimos cuenta de que el análisis realizado hasta este punto no era suficiente para describir completamente los cambios en la dinámica de un sistema caótico digitalizado. Alcanzar períodos largos no garantiza que los sistemas exhiban buenas propiedades con respecto a la aleatoriedad. Así que decidimos estudiar más a fondo los datos obtenidos mediante el empleo de cuantificadores estadísticos.

Como se dijo, en la Fig. 4.13.a las dos zonas grises corresponden a las condiciones iniciales que convergen a los dos ciclos coexistentes de período dos y seis, respectivamente. Entonces, estos dos ciclos tendrán un valor determinado de  $H_{BP}$ ,  $H_{hist}|_{T=2} = 0,0625$ ,  $H_{hist}|_{T=6} = 0,1199$ ,  $H_{BP}|_{T=2} = 0,1053$  y  $H_{BP}|_{T=6} = 0,2723$ . Sin embargo, el valor reportado de estos cuantificadores no puede ser el promedio de ambos, ya que la tasa de ocurrencia del ciclo dos es mucho mayor que la del ciclo seis (el período dos aparece 92,7 % veces mientras que el período seis solo 7,3 %, ver Tabla 4.3). Por lo tanto, hemos calculado los

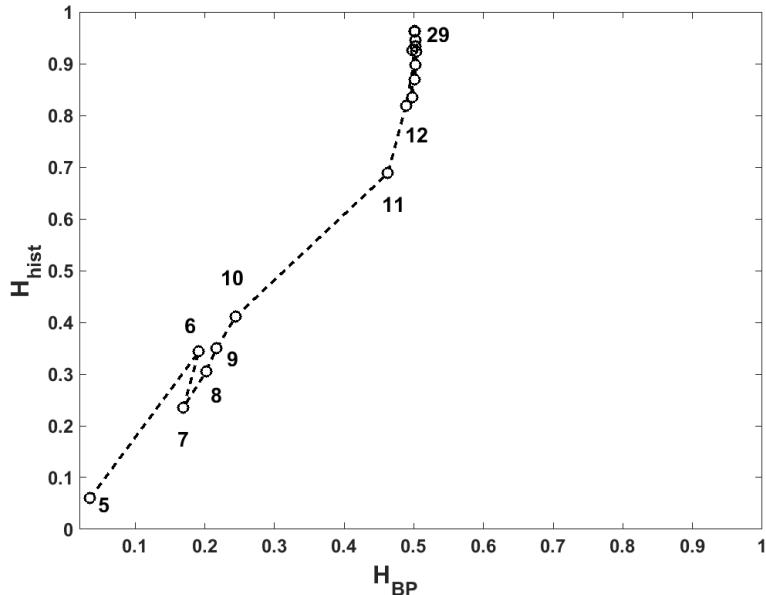


Figura 4.16: Plano  $H_{hist}$  -  $H_{BP}$  para diferentes números de bits.

cuantificadores promedios ponderando cada cuantificador por su tasa de ocurrencia.

El plano  $H_{hist}$  vs  $H_{BP}$ , que se muestra en la Fig. 4.16, permite una visualización rápida del comportamiento en términos de aleatoriedad del sistema, en este plano el punto “ideal”, desde el punto de vista estadístico, es  $(1, 1)$ . Aquí, el sistema parece estabilizarse para  $n_f$  superior a 12. Se puede observar que mientras  $H_{hist}$  se estabiliza cerca del valor máximo ( $H_{hist} = 1$ ), el  $H_{BP}$  tiende a estabilizarse a 0,5. Este valor de  $H_{BP}$  es característico de los sistemas caóticos y se debe a las estructuras internas de sus atractores.

Un resumen del análisis observado de estos resultados se puede ver en la Fig. 4.17. La Fig. 4.17.a y 4.17.b muestran el número de puntos que divergen y convergen en puntos fijos respectivamente a medida que aumenta el valor de  $n_f$ , en ambos casos, el valor final tiende al que se obtiene en implementación en punto flotante. De estas figuras se desprende que para  $n_f \sim 12$  el sistema parece haberse estabilizado. La figura 4.17.c muestra que el período promediado aumenta a una velocidad logarítmica. Finalmente, la Fig. 4.17.d muestra el número de condiciones iniciales que presentan períodos  $T$  más altos y más bajos que 1,000. De nuevo, un valor de 12 para  $n_f$  parece ser el límite para obtener una buena aproximación del sistema.

La figura 4.18 muestra el promedio ponderado de los cuantificadores  $H_{hist}$ ,  $H_{BP}$  y  $MLE$ . En la figura se puede ver que los tres cuantificadores tienden al valor calculado

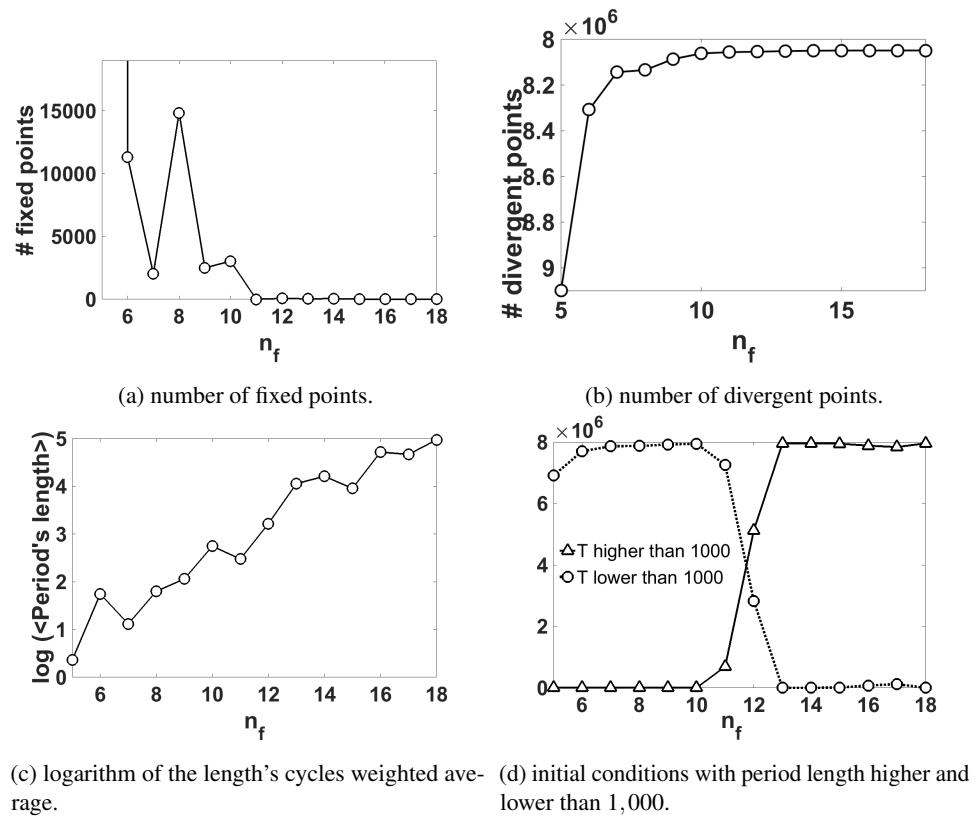


Figura 4.17: Summary of initial conditions' behavior.

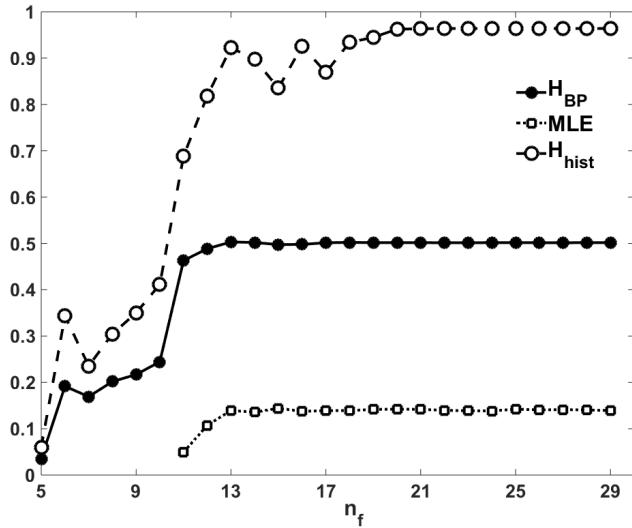


Figura 4.18: Weighted average of quantifiers  $H_{BP}$ ,  $H_{hist}$  and  $MLE$  as functions of the number of bits.

usando aritmética de punto flotante. Mientras  $H_{BP}$  y  $MLE$  se estabilizan para  $n_f \sim 12$  o  $13$ ,  $H_{hist}$  alcanza el valor en coma flotante de  $n_f \sim 19$ , mostrando que hay propiedades de las secuencias de salida que solo este cuantificador puede detectar. Esto confirma la necesidad de usar ambos cuantificadores para caracterizar la aleatoriedad de las secuencias. Como puede verse en el análisis anterior, el número mínimo de bits está determinado por  $H_{hist}$  y los resultados son  $n_f = 19$  más la cantidad de bits utilizados para representar la parte entera  $n_i = 4$ , por lo tanto  $n_{min}$  resulta ser igual a 23.

## 4.5. Conclusiones

En este capítulo se resumen los resultados de cuatro trabajos orientados a la implementación de sistemas caóticos. Se propusieron y analizaron distintos sistemas y aplicaciones desde el punto de vista estadístico, siempre contemplando la implementación orientada a la ingeniería.

!!!!!!!!!!!!!!FALTA PONER ALGO DE RNA!!!!!!!!!!!!!!

Se desarrolló un nuevo método para el diseño de sistemas de criptocodificación mediante el empleo de mapas caóticos cuadráticos acoplados. Se obtuvieron resultados muy prometedores hasta el momento mediante las simulaciones realizadas. También se obtuvieron buenos resultados en la implementación en VHDL del sistema codificador, en la que se

verificó que la salida generada por el sistema no cayera en ciclos periódicos debido a la utilización de presición finita. En cuanto al análisis de performance que presenta el sistema se deben tener en cuenta dos aspectos:

- La distancia mínima de la modulación codificada resultante. Esta es usualmente empleada para proveer un límite de error en la región de piso.
- Una descripción precisa de la tasa binaria de error del sistema o BER (en inglés, Bit Error Rate) también es un parámetro muy importante, ya que da una estimación del comportamiento que presentara el código.

A partir de los resultados presentados para PRNGs determinístico-estocásticos, es posible concluir que para obtener un PRNG, los mejores corresponden a la representación de aritmética entera tanto en hardware (recursos y frecuencia) como en propiedades estadísticas. La técnica de aleatorización de *concatenado* hace que la calidad sea independiente de  $\Delta t$  para esta representación numérica. Para la técnica de aleatorización de *descarte* se obtienen buenos resultados solo para valores grandes de  $\Delta t$ . Lo mismo ocurre con las implementaciones de punto fijo con ambas técnicas de aleatorización. En términos de uso de recursos y limitaciones de frecuencia, el rendimiento en aritmética de enteros es considerablemente mejor que en punto flotante y punto fijo. Observemos que para minimizar los recursos, se requiere un preprocesamiento del sistema caótico (escalado y polarización) para obtener divisores con una potencia de 2, tal como se explica en la subsección 4.3.2. Por otro lado, para el caso de la aritmética de punto flotante, el exponente se descarta en todas las técnicas de aleatorización utilizadas y, en consecuencia, la dinámica se ve muy perturbada por el proceso de aleatorización. Entonces, como se muestra en la Tabla ??,  $\Delta t$  no es la variable relevante para predecir si un PRNG será bueno o malo.

Finalmente, hemos desarrollado un análisis detallado de los cambios en el comportamiento de una implementación en punto fijo de un mapa cuadrático bidimensional. El objetivo fue reportar la tasa de degradación de la propiedad de cada sistema, para que los autores la utilicen al momento de diseñar sus aplicaciones particulares. Los resultados muestran que es posible determinar un umbral para el número de bits empleados en la representación de punto fijo del sistema, mientras que el dominio de atracción conserva su integridad y se mantienen las características de las secuencias generadas. Con la ayuda de los cuantificadores de aleatoriedad introducidos fue posible determinar ese límite, en el caso del estudio fue de 23 bits. El mismo procedimiento debe repetirse para cualquier otro

104 CAPÍTULO 4. GENERADORES DE NÚMEROS ALEATORIOS USANDO CAOS

sistema si se desea utilizarlo en una aplicación electrónica digital, como generadores de ruido controlados o para desarrollar nuevos sistemas de encriptación.

## **Capítulo 5**

# **Mapas conmutados en precisión finita**

### **5.1. Introduction**

En los últimos años, los sistemas digitales se convirtieron en el estándar en todas las ciencias experimentales. Mediante el uso de nuevos dispositivos electrónicos programables como DSP y electrónica reconfigurable como FPGA o ASIC, los experimentadores pueden diseñar y modificar sus propios generadores de señales, sistemas de medición, modelos de simulación, etc.

Cuando se implementa un sistema caótico en computadoras o cualquier dispositivo digital, el atractor caótico se vuelve periódico por el efecto de la precisión finita, entonces solo se pueden generar atractores pseudocaóticos [?, 74]. La discretización puede incluso destruir el comportamiento pseudocaótico y, en consecuencia, es un proceso no trivial [?, ?, ?].

En estos nuevos dispositivos, el punto flotante y el punto fijo son las aritméticas más comunes. El punto flotante es la solución más precisa, pero no siempre se recomienda cuando se requieren velocidad, baja potencia y/o área de circuito pequeño, una solución de punto fijo es mejor en estos casos.

El efecto de la discretización numérica sobre un mapa caótico fue abordado recientemente en [?] y [?]. En [?], el autor caracteriza las interfaces de Moire en el sistema Mandelbrot. Estas interfaces son consecuencia del tipo de precisión de los datos y no aparecen en el

sistema ideal con números reales. En [?], los autores exploran la degradación estadística del espacio de fases para una familia de mapas cuadráticos 2D. Estos mapas presentan una dinámica multiatractor que los hace muy atractivos como generadores de números aleatorios en campos como criptografía, codificación, etc. En [?] y [?], los autores propusieron usar el valor de la entropía para elegir el número de bits en la parte fraccionaria, cuando se implementan mapas en aritmética entera.

Grebogi y colaboradores [72] estudiaron este tema y vieron que el período  $T$  escala con el redondeo  $\epsilon$  como  $T \sim \epsilon^{-d/2}$  donde  $d$  es la dimensión de correlación del atractor caótico. Conseguir un período grande  $T$  es una propiedad importante de los mapas caóticos, en [75] Nagaraj *et. al* se estudió el efecto de cambiar las longitudes de período promedio de los mapas caóticos en precisión finita. Vieron que el período  $T$  del mapa compuesto obtenido al conmutar entre dos mapas caóticos es más alto que el período de cada mapa. Liu *et. al* [76] estudió diferentes reglas de conmutación aplicadas a sistemas lineales para generar caos. El problema de la conmutación también se trató en [77], el autor consideró algunos aspectos matemáticos, físicos y de ingeniería relacionados con sistemas singulares, principalmente de conmutación. Los sistemas conmutados surgen naturalmente en la electrónica de potencia y en muchas otras áreas de la electrónica digital.

La estocasticidad y la mezcla también son relevantes para caracterizar un comportamiento caótico. Para investigar estas propiedades, se estudiaron varios cuantificadores [45]. La entropía y la complejidad de la teoría de la información se aplicaron para dar una medida de la entropía causal y no causal y la complejidad causal.

Una cuestión fundamental es el criterio para seleccionar la función de distribución de probabilidad (PDF) asignada a las series de tiempo, son posibles las opciones causales y no causales. Aquí consideramos la PDF tradicional no causal obtenido al normalizar el histograma de la serie temporal. Su cuantificador estadístico es la entropía normalizada  $H_{hist}$  que es una medida de equiprobabilidad entre todos los valores permitidos. También consideramos una PDF causal que se obtiene asignando patrones de orden a segmentos de trayectoria de longitud  $D$ . Este PDF primero fue propuesto por Bandt & Pompe en [?]. La entropía correspondiente  $H_{BP}$  también fue propuesta como un cuantificador por Bandt & Pompe, en [?] los autores aplicaron la complejidad causal  $C_{BP}$  para detectar el caos. Entre ellos, merece una consideración especial el uso de una representación planar de complejidad y entropía (plano  $H_{hist} \times C_{BP}$ ) y el plano entropía causal vs. no causal (plano  $H_{BP} \times H_{hist}$ ) [45, ?, ?, 9, ?, ?, ?].

Recientemente, la información de amplitud se introdujo en [?] para agregar cierta inmunidad al ruido débil en un PDF causal. El nuevo esquema rastrea mejor los cambios abruptos en la señal y asigna menos complejidad a los segmentos que exhiben regularidad o están sujetos a efectos de ruido. Luego, definimos la entropía causal con contribuciones de amplitud  $H_{BPW}$  y la complejidad causal con contribuciones de amplitud  $C_{BPW}$ . Además, presentamos los planos modificados  $H_{hist} \times C_{BP}$  y  $H_{BP} \times H_{hist}$ . fied planes  $H_{hist} \times C_{BP}$  and  $H_{BP} \times H_{hist}$ .

Amigó y colaboradores propusieron el número de patrones prohibidos como un cuantificador de caos [?]. Básicamente, informan la presencia de patrones prohibidos como un indicador del caos. Recientemente se demostró que el nombre de patrones prohibidos no es conveniente y fue reemplazado por patrones faltantes (MP) [27], en este trabajo los autores muestran que existen sistemas caóticos que presentan MP a partir de una cierta longitud mínima de patrones. Nuestro principal interés en MP es porque da un límite superior para los cuantificadores causales.

Siguiendo [75], en este trabajo estudiamos las características estadísticas de cinco mapas, dos mapas bien conocidos: (1) los mapas tent (TENT) y (2) logístico (LOG), y tres mapas adicionales generados a partir de ellos: (3) SWITCH, generado al comutar entre TENT y LOG; (4) EVEN, generado al omitir todos los elementos en posiciones impares de la serie temporal SWITCH y (5) ODD, generados descartando todos los elementos en posiciones pares en la serie de tiempo SWITCH. Se usan números binarios flotantes y de punto fijo, estos sistemas numéricos específicos pueden implementarse en modernos dispositivos lógicos programables.

## 5.2. Resultados

Se estudiaron cinco mapas pseudocaóticos: dos mapas simples y tres combinaciones de ellos. Para cada uno hemos usado números representados por coma flotante (80 bits de mantisa) y números de punto fijo con  $1 \leq B \leq 53$ , donde  $B$  es el número de bits que representa la parte fraccionaria. Las series de tiempo se generaron usando 100 condiciones iniciales elegidas al azar dentro de su dominio de atracción (intervalo  $[0, 1]$ ), para cada una de estas 54 precisiones numéricas.

Los mapas estudiados son: logístico (LOG), tent (TENT), comutación secuencial entre TENT y LOG (SWITCH) y skipping descartando los valores en las posiciones impares

(EVEN) o los valores en las posiciones pares (ODD), respectivamente.

El mapa logístico es interesante porque es representativo de la gran familia de mapas cuadráticos. Su expresión es:

$$x_{n+1} = 4x_n(1 - x_n) \quad (5.1)$$

con  $x_n \in \mathbb{R}$ .

Efectivamente, para trabajar en una representación dada, es necesario cambiar la expresión del mapa para realizar todas las operaciones en los números de representación elegidos. Por ejemplo, en el caso de LOG, la expresión en números binarios de punto fijo es:

$$x_{n+1} = 4\epsilon \text{ floor} \left\{ \frac{x_n(1 - x_n)}{\epsilon} \right\} \quad (5.2)$$

con  $\epsilon = 2^{-B}$  donde  $B$  es la cantidad de bits que representa la parte fraccionaria.

Ésta técnica de redondeo es la misma que la utilizada en [78, 72, 75] y tiene algunas ventajas, ya que es algorítmicamente fácil de implementar y es independiente de la plataforma en donde es utilizada, siempre y cuando  $B$  sea menor que la mantisa de la unidad aritmética lógica de la máquina local. En nuestro caso, los resultados fueron obtenidos con una PC Intel i7, que cuenta con una ALU con estándar IEEE-754 de punto fijo de doble precisión, lo cual limita el método a  $B \leq 53$  bits.

El mapa TENT ha sido ampliamente estudiado en la literatura porque teóricamente tiene buenas propiedades estadísticas que pueden obtenerse analíticamente. Por ejemplo, es fácil probar que tiene un histograma uniforme y, en consecuencia, un  $H_{hist} = 1$  ideal. El operador Perron-Frobenius y sus autovalores y autofunciones correspondientes se pueden obtener analíticamente para este mapa [54].

El mapa tent se representa con la ecuación:

$$x_{n+1} = \begin{cases} u x_n & , \text{if } 0 \leq x_n \leq 1/u \\ \frac{u}{1-u} (1 - x_n) & , \text{if } 1/u < x_n \leq 1 \end{cases} \quad (5.3)$$

con  $x_n$  and  $u \in \mathbb{R}$ .

En el redondeo de números fraccionarios base-2, la ecuación (5.3) se convierte en:

$$x_{n+1} = \begin{cases} \epsilon \text{ floor} \left\{ \frac{1}{\epsilon} \mu (x_n) \right\} & , \text{if } 0 \leq x_n \leq \mu^- \\ \epsilon \text{ floor} \left\{ \frac{1}{\epsilon} \rho (1 - x_n) \right\} & , \text{if } \mu^- < x_n \leq 1 \end{cases} \quad (5.4)$$

con  $\varepsilon = 2^{-B}$ ,  $\mu = \varepsilon \text{ floor}\{\frac{1}{\varepsilon}u\}$ ,  $\mu^- = \varepsilon \text{ floor}\{\frac{1}{\varepsilon}(1/\mu)\}$  y  $\rho = \varepsilon \text{ floor}\{\frac{1}{\varepsilon}(\mu/(1-\mu))\}$ .

En [?], los autores mostraron la evolución de la entropía de valores  $H_{hist}$  con respecto a la precisión binaria. Ellos caracterizaron la evolución del mapa TENT como función de la precisión binaria en aritmética de punto fijo. En su esquema de generación de números aleatorios usaron dos etapas de postprocesamiento, primero binarizaron los datos detectando el cruce por un umbral y luego estos datos fueron procesados por una compuerta XOR. En nuestro caso, utilizamos la salida de los mapas caóticos sin ningún proceso de randomización, sin embargo sus resultados son muy interesantes para hacerse de un criterio acerca de cuales parámetros son útiles para implementar. En este trabajo se utilizan dos valores de  $u$  por dos distintas razones, siguiendo a [?] un valor interesante es  $u = 1,96$  o el valor más cercano en la aritmética utilizada, por otro lado, el valor  $u = 2$  es muy atractivo dado su extremadamente bajo costo de implementación.

En la figura 5.1 se muestran los procedimientos de conmutación, skipping par y skipping impar.

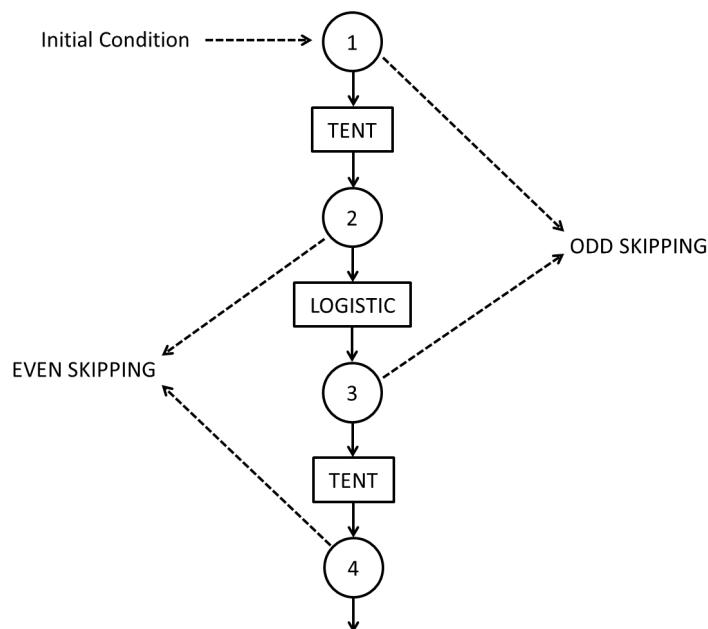


Figura 5.1: Comutación secuencial entre TENT y LOG. En la figura también se muestran las estrategias de skipping par e impar.

El mapa SWITCH se expresa como:

$$\begin{cases} x_{n+1} = \begin{cases} u x_n & , \text{if } 0 \leq x_n \leq 1/u \\ \frac{u}{1-u} (1 - x_n) & , \text{if } 1/u < x_n \leq 1 \end{cases} \\ x_{n+2} = 4 x_{n+1} (1 - x_{n+1}) \end{cases} \quad (5.5)$$

con  $x_n \in \mathbb{R}$  y  $n$  un número par.

Sin embargo, como en el resto de los casos, se utiliza su contraparte pseudocaótica, que puede ser expresada como:

$$\begin{cases} x_{n+1} = \begin{cases} \varepsilon \text{ floor}\left\{\frac{1}{\varepsilon} \mu(x_n)\right\} & , \text{if } 0 \leq x_n \leq \mu^- \\ \varepsilon \text{ floor}\left\{\frac{1}{\varepsilon} \rho(1 - x_n)\right\} & , \text{if } \mu^- < x_n \leq 1 \end{cases} \\ x_{n+2} = 4 \varepsilon \text{ floor}\left\{\frac{x_n(1-x_n)}{\varepsilon}\right\} \end{cases} \quad (5.6)$$

El skipping es una técnica habitual de aleatorización que solo aumenta la calidad de mezcla de un mapa y, por consiguiente, aumenta el valor de  $H_{BP}$  y disminuye  $C_{BP}$  de la serie temporal. El skipping no cambia los valores de  $H_{hist}$  para los mapas ergódicos porque se evalúan utilizando el PDF no causal (histograma de valores normalizado) [9].

En el caso bajo consideración, estudiamos saltos pares e impares de la commutación secuencial de los mapas de tent y de logístico:

1. Skipping par de la commutación secuencial de mapas Tent y Logístico (EVEN).

Si  $\{x_n; n = 1, \dots, \infty\}$  es la serie de tiempo generada por la eq. 5.5, descarta todos los valores en posiciones impares y conserva los valores en posiciones pares.

2. Skipping impar de la commutación secuencial de mapas Tent y Logístico. Si  $\{x_n; n = 1, \dots, \infty\}$  es la serie de tiempo generada por la eq. 5.5, descarta todos los valores en posiciones pares y conserva todos los valores en posiciones impares.

El skipping par se puede expresar como la función de composición TENT  $\circ$  LOG mientras que el skipping impar se puede expresar como LOG  $\circ$  TENT. La evolución del período como función de la precisión para estos mapas se informó en [75].

Los resultados para cada uno de estos mapas son los siguientes.

### 5.2.1. Período $T$ en función de $B$

Grebogi y colaboradores [72] han estudiado cómo el período  $T$  se relaciona con la precisión. Allí vieron que el período  $T$  escala con el redondeo  $\varepsilon$  como  $T \sim \varepsilon^{-d/2}$  donde  $d$  es la dimensión de correlación del atractor caótico.

Nagaraj *et al.* [75] estudió el caso de la commutación entre dos mapas. Vieron que el período  $T$  del mapa compuesto obtenido al comutar entre dos mapas caóticos es más alto que el período de cada mapa y encontraron que una commutación aleatoria mejora los resultados. Aquí hemos considerado el solo la commutación secuencial para evitar el uso de otra variable aleatoria, ya que esta puede introducir sus propias propiedades estadísticas en la serie temporal.

La Fig. 5.2 muestra  $T$  vs.  $B$  en escala semi logarítmica para el mapa logístico. Para cada presición, se generaron 100 surrogados diferentes, cada uno con una condición inicial generada aleatoriamente. La figura muestra 100 puntos rojos por cada precisión de punto fijo ( $1 \geq B \geq 53$ ) y los resultados promediados (puntos negros conectados con líneas enrte cortadas negras). Los puntos promediados experimentales se pueden ajustar por una línea recta expresada como  $\log_2 T = mB + b$  donde  $m$  es la pendiente y  $b$  es la ordenada al origen.

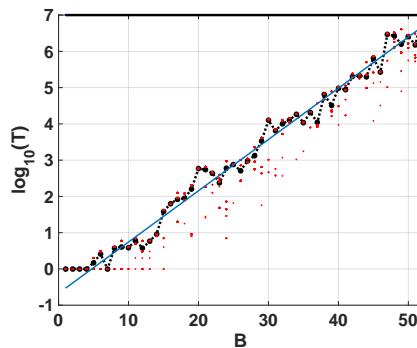


Figura 5.2: Período  $T$  en función de la preceisión  $B$  en números binarios para el mapa LOG.

Los resultados para todos los mapas considerados se resumen en la tabla 5.1. Pudimos detectar que el período promediado fué el mismo usando  $u = 2$  y  $u = 1,96$  cuando se ustiliza la estrategia de switching. Por lo tanto para calcular los resultados mostrados en la tabla para SWITCH, EVEN y ODD se iteró con  $u = 2$ .

Los resultados son compatibles con los obtenidos en [75]. La commutación entre mapas aumenta el período  $T$  pero el procedimiento de skipping lo disminuye casi a la mitad.

Cuadro 5.1: Período  $T$  en función de la precesión  $B$  para todos los mapas considerados. SWITCH, EVEN y ODD fueron calculados con  $u = 2$ .

map	m	b
TENT $u = 2$	0	0
TENT $u = 1,96$	0.1487	-0.01177
LOG	0.139	-0.6188
SWITCH	0.1462	-0.5115
EVEN	0.1447	-0.7783
ODD	0.1444	-0.7683

Además, los resultados para el mapa TENT con  $u = 1,96$  exhibe los mejores resultados.

### 5.2.2. Cuantificadores de mapas simples

Aquí informamos nuestros resultados para mapas simples, LOG y TENT

#### LOG

Las Figs. 5.3a a 5.3f muestran las propiedades estadísticas del mapa LOG en representación de coma flotante y punto fijo. Todas estas figuras muestran: 100 puntos rojos (surrogados) por cada precisión de punto fijo ( $1 \geq B \geq 53$ ) y en negro su promedio (línea negra discontinua que conecta puntos negros), 100 líneas discontinuas horizontales azules que son el resultado de cada surrogado en punto flotante y una línea continua negra en su promedio. Tenga en cuenta que estas líneas son independientes del eje x. En este caso, todas las líneas del punto flotante se superponen.

Según  $B$  crece, las propiedades estadísticas varían hasta que se estabilizan. Para  $B \geq 30$ , el valor de  $H_{hist}$  permanece casi idéntico al valor de la representación en coma flotante, mientras que  $H_{BP}$  y  $C_{BP}$  se estabilizan a  $B > 21$ . Sus valores son:  $\langle H_{hist} \rangle = 0,9669$ ;  $\langle H_{BP} \rangle = 0,6269$ ;  $\langle C_{BP} \rangle = 0,4843$ . Tenga en cuenta que el valor estable de los patrones faltantes  $MP = 645$  hace que el valor óptimo sea  $H_{BP} \leq \ln(75)/\ln(720) \simeq 0,65$ . Entonces,  $B = 30$  es la opción más conveniente para la implementación en hardware porque un aumento en el número de dígitos fraccionarios no mejora las propiedades estadísticas.

Se pueden sacar algunas conclusiones con comparando los cuantificadores de BP y BPW. Para  $B = 1,2,3$  y 4, los cuantificadores de BP promediados son casi 0 mientras que los cuantificadores de BPW promediados no se pueden calcular (ver en las figuras 5.3c y 5.3e la línea punteada negra faltante). Esto se debe a que para esas secuencias la condición inicial

era 0, todas las iteraciones resultan ser una secuencia de ceros (el punto fijo del mapa), esto es más probable que ocurra cuando se usan pequeñas precisiones debido al redondeo.

Cuando  $B$  aumenta las condiciones iniciales se redondean a cero con menos frecuencia, esto se puede ver para  $B > 6$ . En este caso, las secuencias generadas que comienzan desde un valor no nulo caen a cero después de un transitorio cortomuy frecuentemente. Un tema interesante en las Figs. 5.3c y 5.3e, es que los cuantificadores de BPW muestran una alta dispersión a diferencia de los cuantificadores de BP. Esto se debe a que el procedimiento BPW tiene en cuenta transitorios y descarta los puntos fijos, a diferencia del procedimiento BP, que considera todos los valores de la secuencia. Podemos ver en las Figs. 5.3c y 5.3e para  $1 < B < 10$  líneas horizontales de puntos rojos que no aparecen en las Figs. 5.3b y 5.3d, esto evidencia que las diferentes condiciones iniciales caen en las mismas órbitas, incluso para las precisiones adyacentes.

Los mismos resultados se muestran en planos de doble entropía con la precisión como parámetro (Fig. 5.4a sin contribuciones de amplitud y Fig. 5.4b con contribuciones de amplitud). Estas figuras muestran: 100 puntos rojos por cada precisión de punto fijo ( $B$ ) y su promedio en negro (línea negra discontinua que conecta puntos negros), 100 puntos azules que son los resultados de cada surrogado en coma flotante y la estrella negra es su promedio. Aquí, los 100 puntos azules y su promedio se superponen.

Como se esperaba, la implementación de la arquitectura de punto fijo converge al valor de coma flotante a medida que aumenta  $B$ . Para ambos planos,  $H_{hist} \times H_{BP}$  y  $H_{hist} \times H_{BPW}$ , desde  $B = 20$ ,  $H_{hist}$  aumenta pero  $H_{BP}$  y  $H_{BPW}$  permanecen constantes. Se puede ver que la entropía de distribución de valores es alta ( $\langle H_{hist} \rangle = 0,9669$ ) pero su mezcla es pobre ( $\langle H_{BP} \rangle = 0,6269$ ).

En la Fig. 5.5a y 5.5b, mostramos los planos entropía - complejidad. Las líneas grises punteadas son los márgenes superior e inferior, se espera que un sistema caótico permanezca cerca del margen superior. Estos resultados caracterizan un comportamiento caótico, en el plano  $H_{BP} \times C_{BP}$  podemos ver una baja entropía y alta complejidad.

## TENT

La ecuación que representa la implementación para  $u = 2$  es:

$$x_{n+1} = \begin{cases} 2 x_n & , \text{if } 0 \leq x_n \leq 0,5 \\ \varepsilon \text{ floor}\{\frac{1}{\varepsilon}2(1-x_n)\} & , \text{if } 0,5 < x_n \leq 1 \end{cases} \quad (5.7)$$

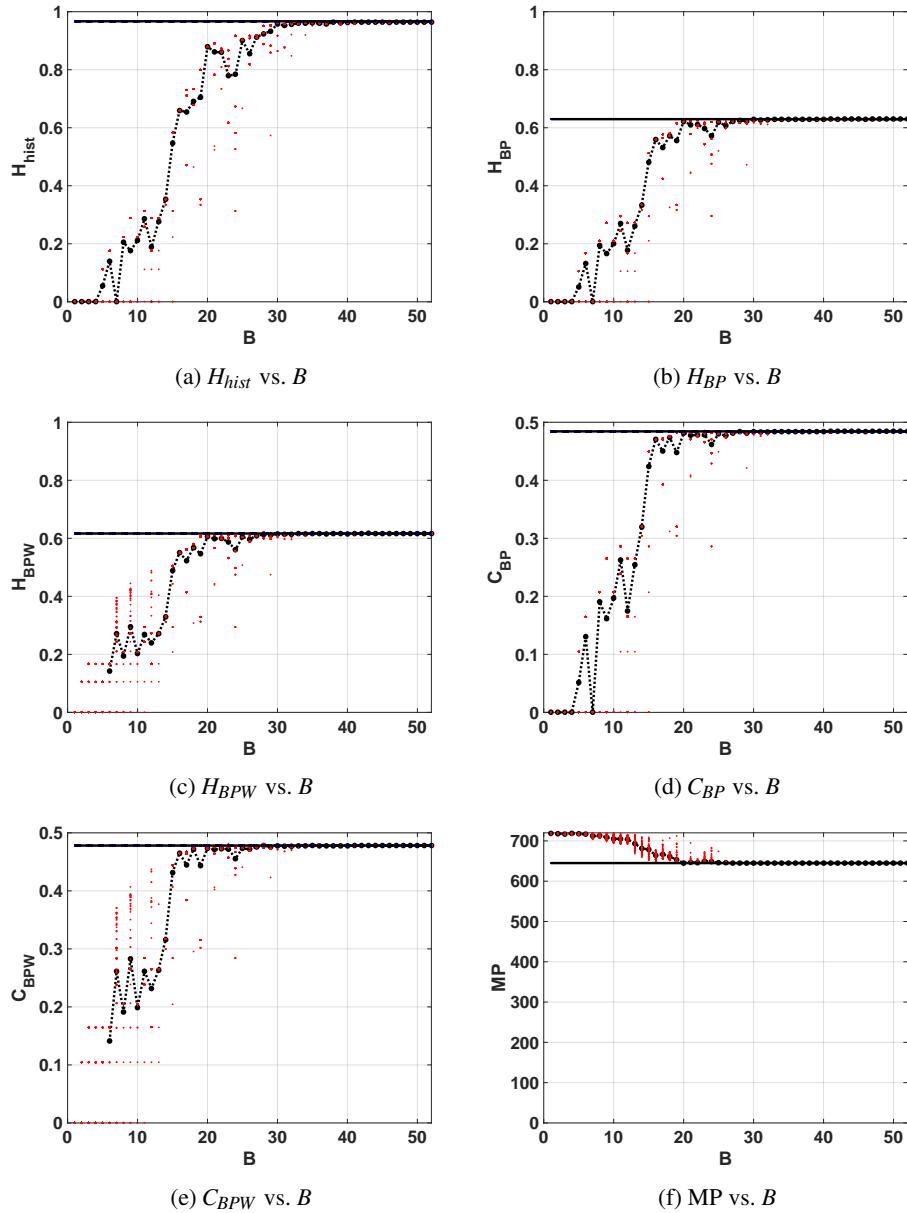


Figura 5.3: Propiedades estadísticas para el mapa LOG en función de  $B$ .

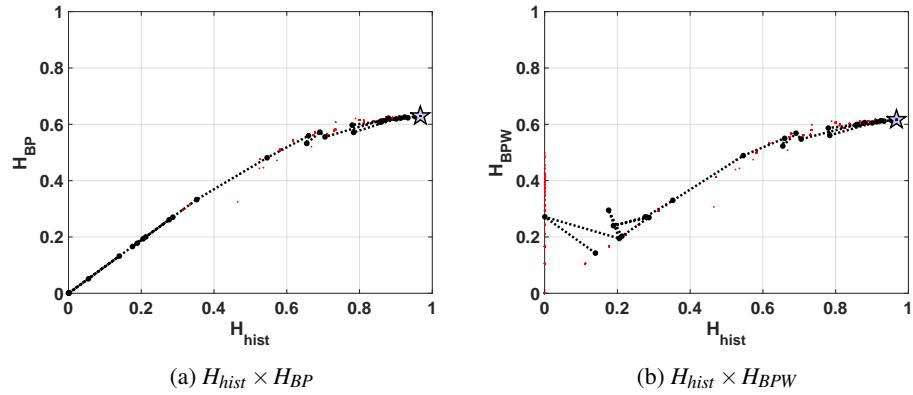


Figura 5.4: evolución de las propiedades estadísticas en el plano de doble entropía para el mapa LOG.

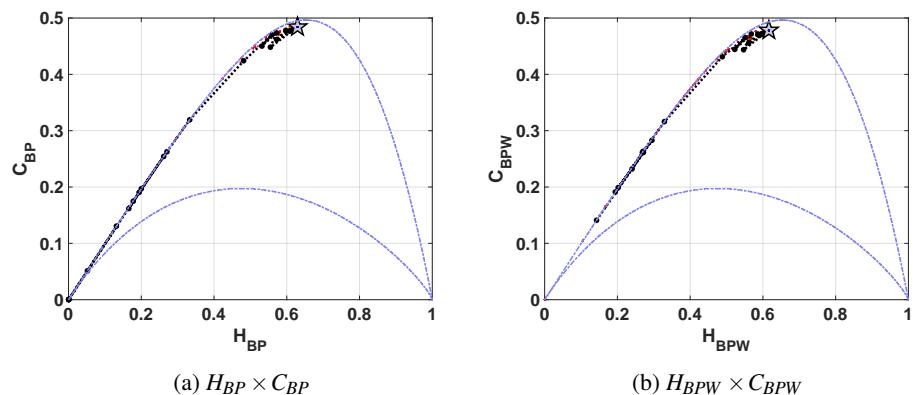


Figura 5.5: Evolution of statistical properties in causal entropy-complexity plane for LOG map

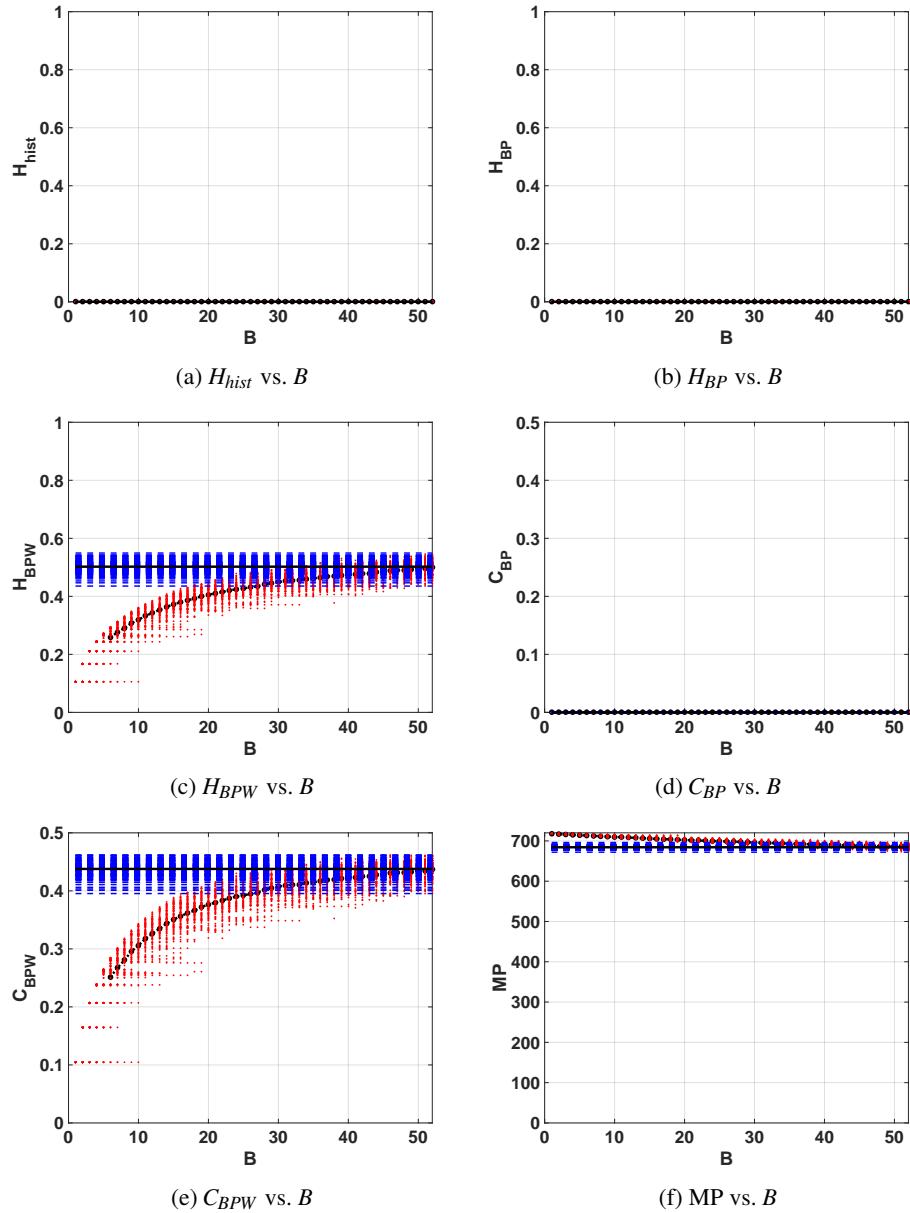
En este caso el redondeo es necesario solo en la segunda multiplicación por que la multiplicación por dos es equivalente a un acarreo hacia la izquierda.

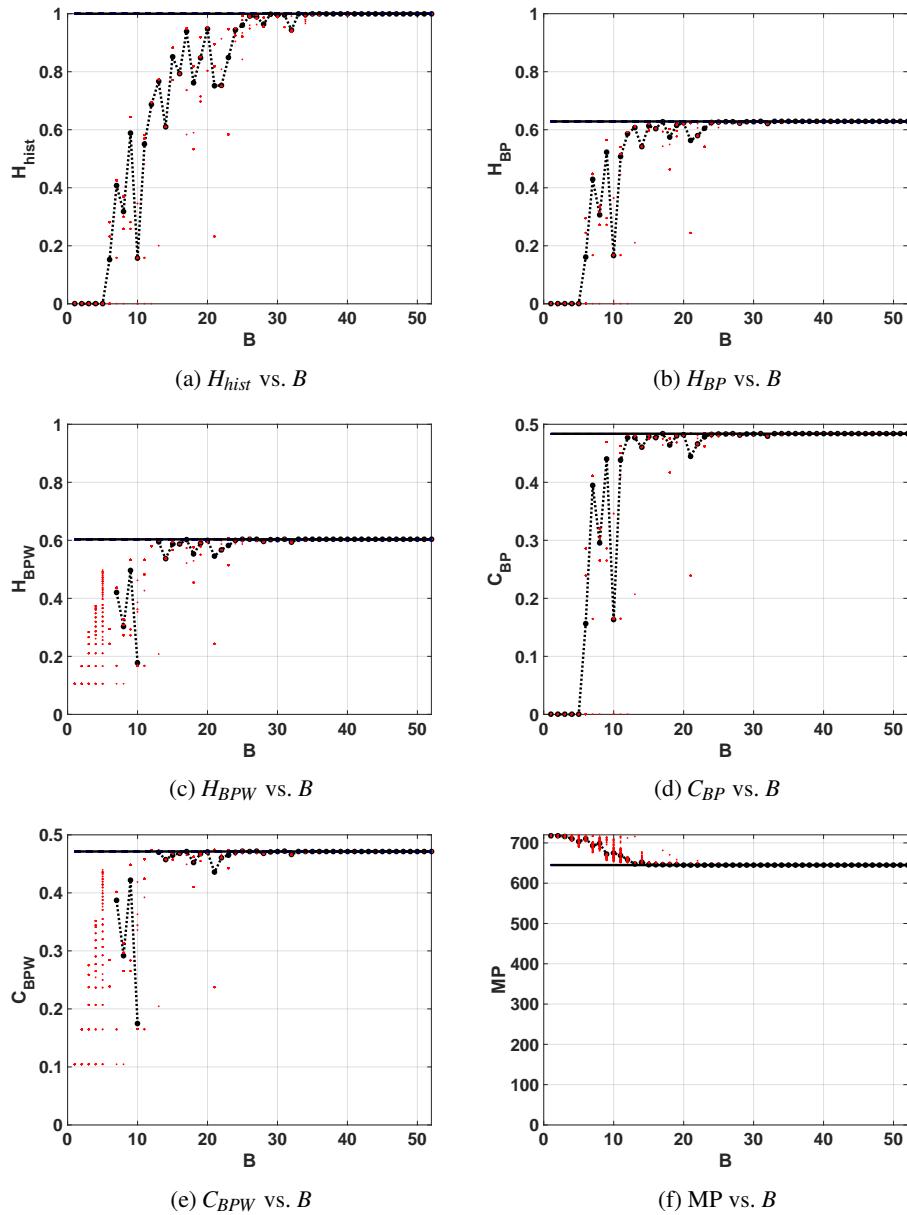
Cuando este mapa se implementa con  $u = 2$  en una computadora que utiliza cualquier sistema de representación numérica binaria (¡incluso punto flotante!), los errores de truncamiento aumentan rápidamente y hacen que el punto fijo inestable en  $x^* = 0$  se estabilice. Las secuencias dentro del dominio de atracción de este punto fijo tendrán un corto transitorio de longitud entre 0 y  $B$  seguido de un número infinito de 0s [?, ?]. Este problema se explica de forma muy sencilla en [?], el problema aparece porque todas las iteraciones tienen una operación de desplazamiento a la izquierda que arrastra los 0s del lado derecho del número a las posiciones más significativas.

Las Figs. 5.6a a 5.6f muestran los cuantificadores para representaciones numéricas de coma flotante y fija. Los cuantificadores  $H_{hist}$ ,  $H_{BP}$  y  $C_{BP}$  son iguales a cero para todas las precisiones, esto refleja que las series convergen rápidamente hacia un punto fijo para cada condición inicial. En el caso de  $H_{BPW}$  y  $C_{BPW}$  los cuantificadores son diferentes a cero porque el procedimiento BPW descarta los elementos una vez que se alcanza el punto fijo. Las altas dispersiones en  $H_{BPW}$ ,  $C_{BPW}$  y MP están relacionadas con la corta duración del transitorio de la serie. Estos transitorios que convergen en un punto fijo tienen una longitud máxima de  $B$  elementos (iteraciones) para aritmética de punto fijo y 80 para punto flotante (precisión long-double). Resumiendo, a pesar de usar un alto número de bits (con cualquier representación numérica en base 2) para representar el mapa TENT digitalizado, siempre converge rápidamente al punto fijo en  $(x_n, x_{n+1}) = (0, 0)$ .

Cuando este mapa se calcula con un valor distinto de  $u$  los resultados son completamente distintos, como se muestra en las figuras 5.7, en donde se muestran los resultados tomando  $u = 1,96$ . Los resultados son similares a los del mapa LOG, en cuanto a que el valor promediado de los cuantificadores tiende no monótonamente al valor encontrado en punto flotante y se estabiliza a partir de cierto valor de  $B$ . Sin embargo, fueron necesarios más bits de precisión para alcanzar estas asíntotas. Por otro lado, se puede ver que el valor de  $H_{hist}$  es mejor que el encontrado para LOG y que  $H_{BP}$  es similar. Mediante los cuantificadores  $H_{BPW}$  y  $C_{BPW}$  se puede detectar que con una precisión por debajo de 13 bits, algunas condiciones iniciales convergen a puntos fijos o divergen, por lo que no es posible utilizar este mapa con  $B < 13$ .

Las posiciones en los planos doble entropía (Figura 5.8) y entropía-complejidad (Figura 5.8) son marginalmente mejores que los que se obtienen para el mapa LOG y son

Figura 5.6: Propiedades estadísticas del mapa TENT con  $u = 2$ .

Figura 5.7: Propiedades estadísticas del mapa TENT con  $u = 1.96$ .

característicos de los mapas pseudocaóticos.

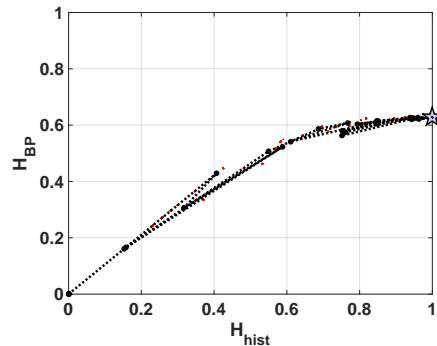


Figura 5.8: Evolution of statistical properties in double entropy plane for TENT map with  $u = 1,96$ .

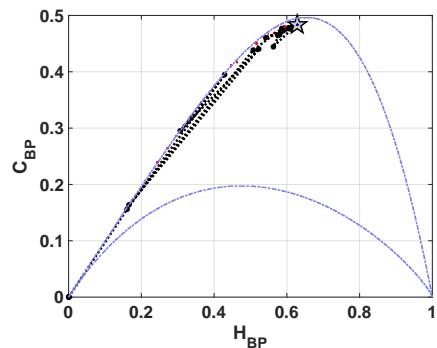


Figura 5.9:  $H_{BP} \times C_{BP}$

Figura 5.10: Evolution of statistical properties in causal entropy-complexity plane for TENT map with  $u = 1,96$ .

### 5.2.3. Cuantificadores de mapas combinados

Aquí presentamos nuestros resultados para las tres combinaciones de mapas simples, SWITCH, EVEN y ODD.

#### SWITCH

Entre los dos parámetros analizados para el mapa TENT, encontramos que, cuando se utilizan dentro del esquema switcheado, la mezcla y la estocasticidad convergen a los mismos valores ya sea con  $u = 2$  como con  $u = 1,96$ . Entonces, elegimos  $u = 2$  dada su

simplicidad para ser utilizado tanto en simulaciones de software como en la implementación en hardware.

Los resultados con conmutación secuencial se muestran en las Figs. 5.11a a 5.11f. El valor de entropía calculado para la implementación en punto flotante es  $\langle H_{hist} \rangle = 0,9722$ , este valor es ligeramente más alto que el obtenido para el mapa LOG. Para la aritmética de punto fijo, este valor se alcanza en  $B = 24$ , pero se estabiliza desde  $B = 28$ . En cuanto a los patrones perdidos, el número de MP disminuye a 586, este valor es menor que el obtenido para el mapa LOG. Significa que la entropía  $H_{BP}$  puede aumentar hasta  $\ln(134)/\ln(720) \simeq 0,74$ . Los cuantificadores BP y BPW alcanzan su máximo de  $\langle H_{BP} \rangle = 0,6546$  y  $\langle H_{BPW} \rangle = 0,6313$  a  $B = 16$ , pero se estabilizan desde  $B = 24$ . Las complejidades son menores que para LOG,  $\langle C_{BP} \rangle = 0,4580$  y  $\langle C_{BPW} \rangle = 0,4578$ , estos valores se alcanzan para  $B \geq 15$  pero se estabilizan en  $B \geq 23$ . Comparado con LOG, las propiedades estadísticas son mejores con menos cantidad de bits, para  $B \geq 24$  este mapa alcanza mejores características en el sentido de generador aleatorio.

Además, encontramos una condición inicial con un comportamiento anómalo en doble precisión de coma flotante. Las Figs. 5.11a, 5.11b y 5.11d muestran una línea discontinua azul horizontal que está lejos del valor promedio, esto no es detectado por los cuantificadores basados en el procedimiento con contribuciones de amplitud BPW de las Figs. 5.11c y 5.11e. Sin embargo, al comparar ambos procedimientos (BP y BPW) pudimos detectar una caída a un punto fijo después de un transitorio largo, el procedimiento BPW descarta los valores constantes (que corresponden a un punto fijo) y calcula solo sobre los valores transitorios.

El plano de doble entropía  $H_{hist} \times H_{BP}$  se muestra en la Fig. 5.12. El punto alcanzado en este plano para el mapa SWITCH es similar al alcanzado para el mapa LOG, y se indica con una estrella en la figura. La mezcla es levemente mejor en este caso.

El plano de entropía - complejidad  $H_{BP} \times C_{BP}$  se muestra en la Fig. 5.13. Si comparamos con el mismo plano en el caso de LOG (Fig. 5.5a),  $C_{BP}$  es menor para SWITCH, este hecho muestra un comportamiento más aleatorio.

## EVEN y ODD

En las Figs. 5.14a y 5.15a podemos ver que los cuantificadores relacionados con el histograma de valores normalizado se degradan ligeramente con el procedimiento skipping. Por ejemplo,  $\langle H_{hist} \rangle$  reduce de 0,9722 sin saltarse a 0,9459 para EVEN y 0,9706 para ODD.

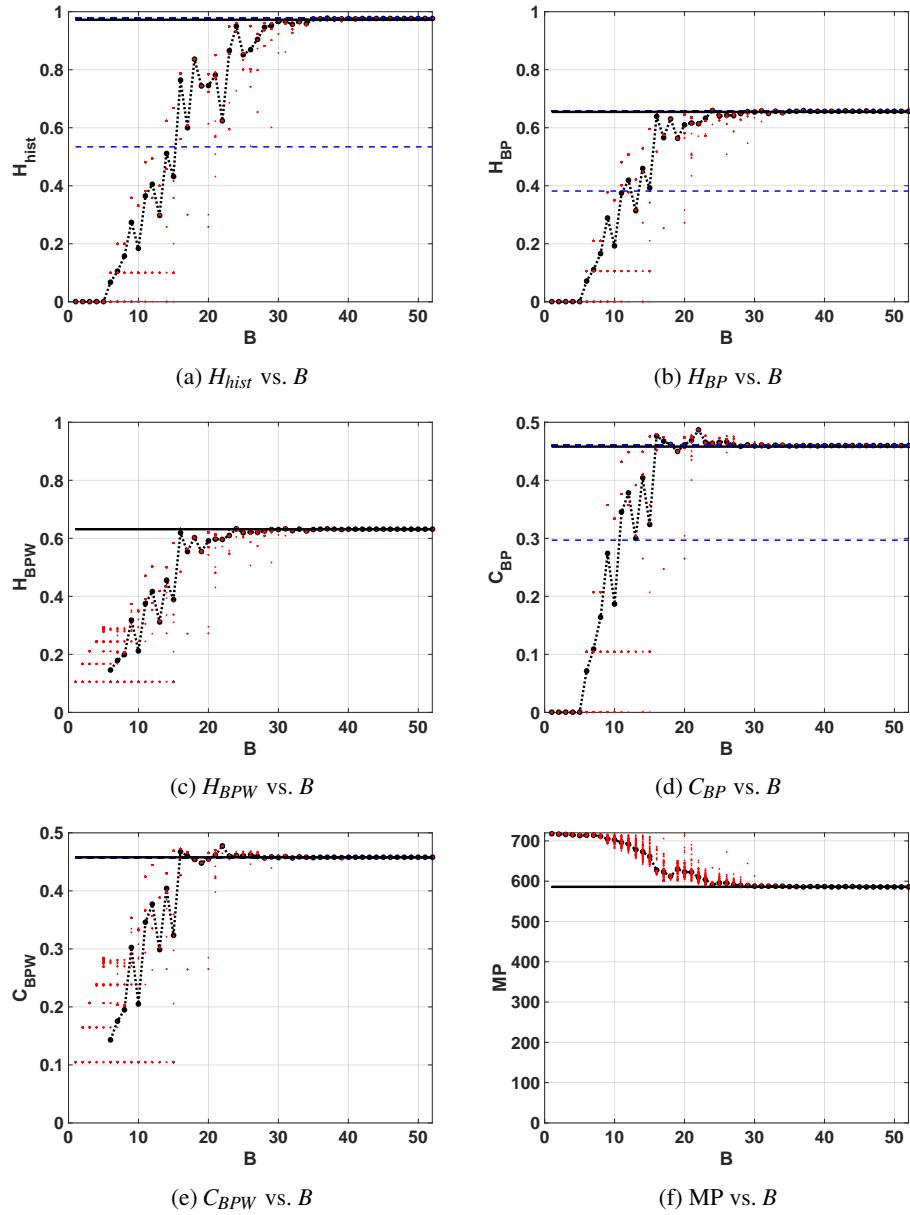


Figura 5.11: Propiedades estadísticas del mapa SWITCH

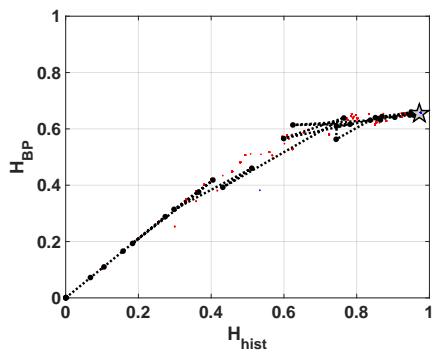


Figura 5.12: Evolución de las propiedades estadísticas en el plano doble entropía para el mapa SWITCH  $H_{hist} \times H_{BP}$ .

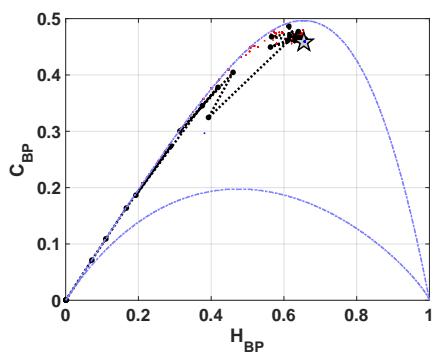


Figura 5.13: Evolución de las propiedades estadísticas en el plano entropía - complejidad para el mapa SWITCH  $H_{BP} \times C_{BP}$ .

Esta diferencia entre EVEN y ODD en coma flotante se debe a que se obtuvo una alta dispersión para  $H_{hist}$ ,  $H_{BP}$  y  $C_{BP}$  pero no para  $H_{BPW}$  o  $C_{BPW}$ .

Las figuras 5.14b a 5.14f y las Figs. 5.15b a 5.15f muestran los resultados de los cuantificadores BP y BPW para EVEN y ODD, respectivamente. Se requiere una mayor precisión para lograr una complejidad menor, a diferencia de los casos sin skipping que convergen a valores altos. Desde el punto de vista de MP, se obtiene una gran mejora utilizando cualquiera de las estrategias de omisión, pero el ODD es ligeramente mejor que EVEN. Los patrones faltantes se reducen a  $MP = 118$  para EVEN y ODD, lo que aumenta la entropía Bandt & Pompe máxima permitida que alcanza el valor medio  $\langle H_{BP} \rangle = 0,8381$  para EVEN, y  $\langle H_{BP} \rangle = 0,9094$ . La complejidad se reduce a  $\langle C_{BP} \rangle = 0,224$  para EVEN y  $\langle C_{BP} \rangle = 0,282$  para ODD. El número mínimo de bits para converger a este valor es de  $B > 40$  para los mapas EVEN y ODD.

La mejora mostrada en las figuras 5.14 y 5.15 se refleja en la posición del punto asintótico en los planos 5.16, y 5.17. En ambos casos, esta posición es la más cercana al punto ideal  $(H_{hist}, H_{BP}) = (1, 1)$ , porque los vectores resultantes presentan una mejor mezcla.

Los resultados que se muestran en las Figs. 5.18 y 5.19 son compatibles, la posición del punto asintótico es más cercana al punto ideal  $(H_{hist}, H_{BP}) = (1, 0)$ . Este resultado refleja que la mezcla es mejor porque la complejidad del sistema resultante es menor. Este plano detecta que en los vectores generados por skipping, la mezcla de ODD es levemente mejor que EVEN.

### 5.3. Conclusiones

Exploramos la degradación estadística debido al error inherente de los sistemas en base 2 para de mapas caóticos simples, comutados y con skipping. Evaluamos las distribuciones de mezcla y amplitud desde un punto de vista estadístico.

Este trabajo complementa los resultados anteriores dados en [75], donde se investigaron las duraciones de los períodos. En ese sentido, nuestros resultados fueron compatibles. Podemos ver que la conmutación entre dos mapas aumenta la dependencia del período en función de la precisión, esto se debe a que la longitud de correlación también se incrementa. Sin embargo, el procedimiento estándar de skipping reduce la duración del período en casi la mitad.

Todas las estadísticas de los mapas representados en punto fijo producen una evolución

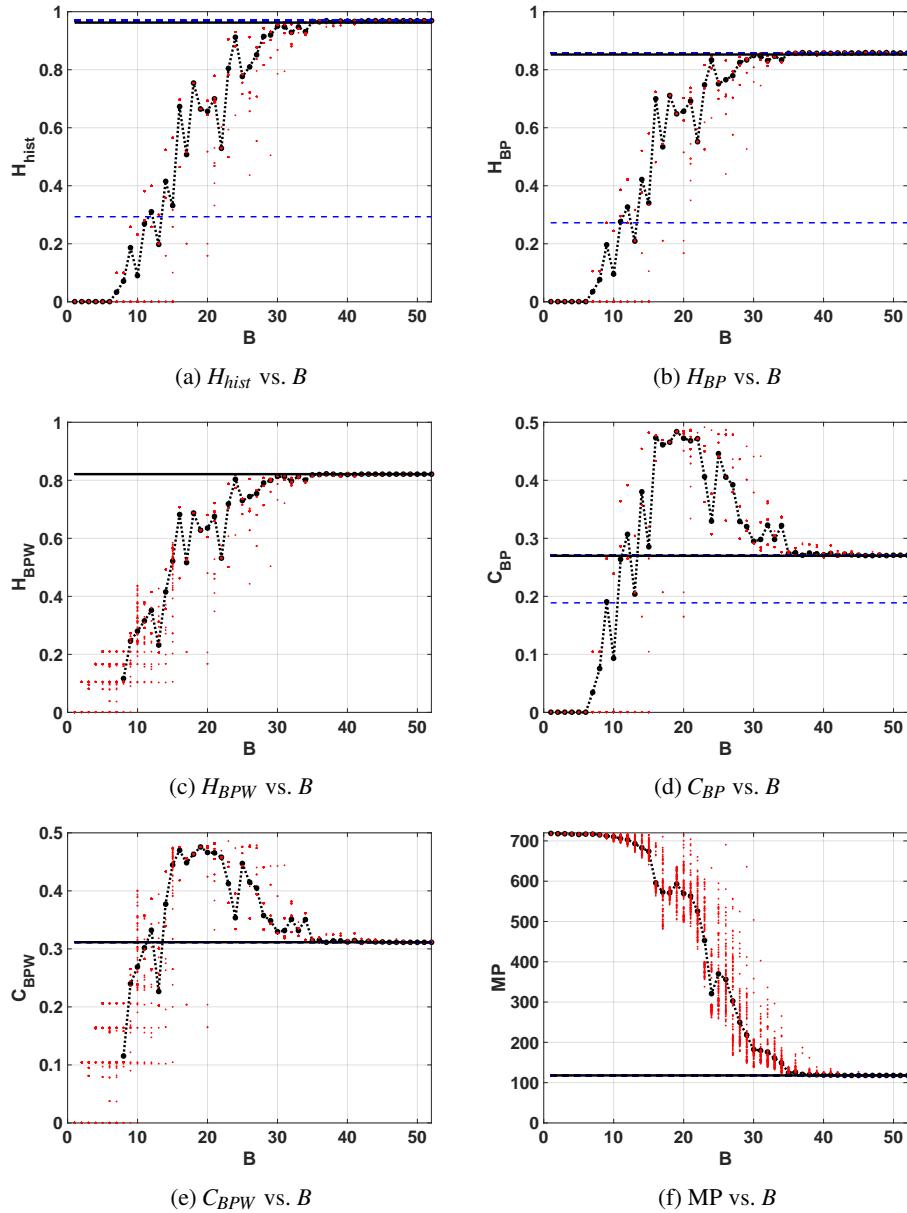


Figura 5.14: Propiedades estadísticas para el mapa EVEN

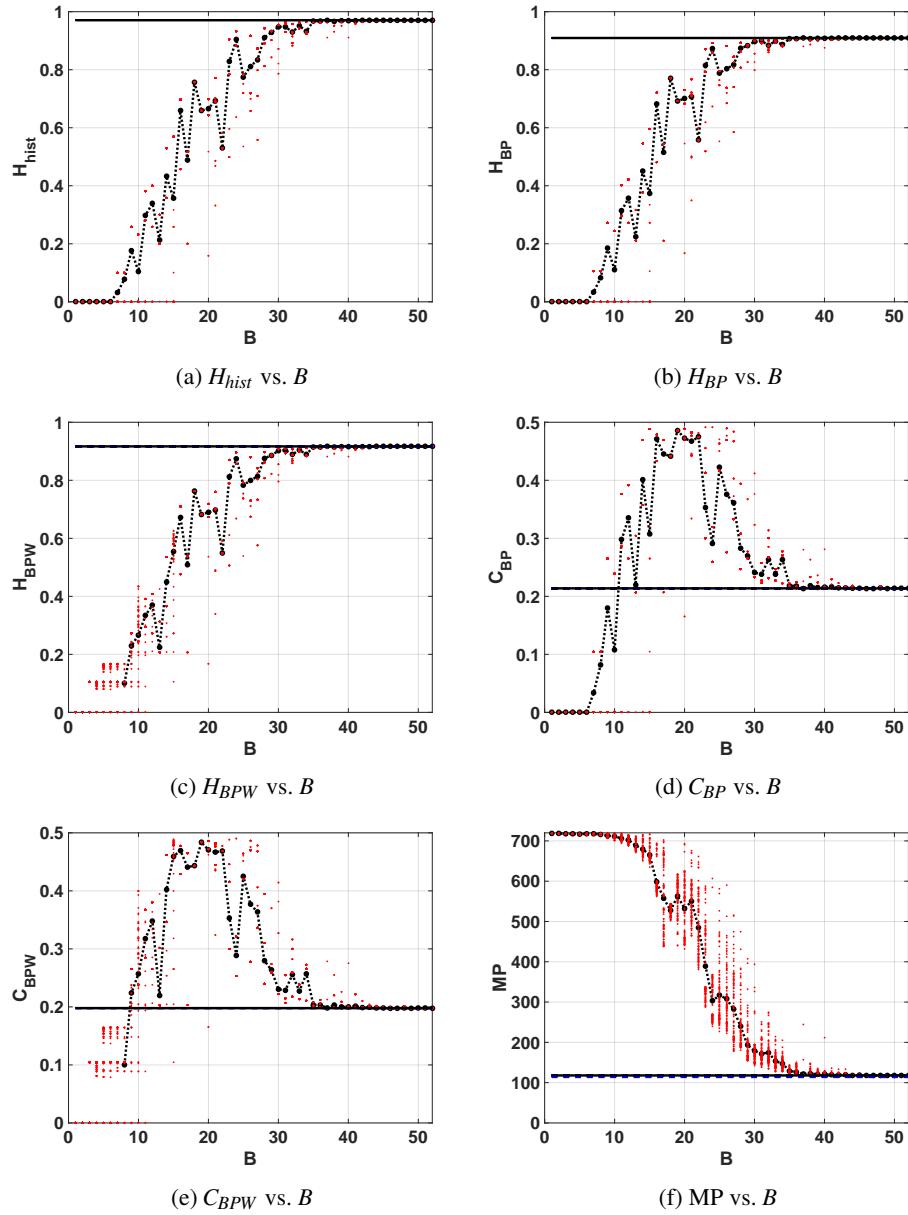


Figura 5.15: Propiedades estadísticas para el mapa ODD

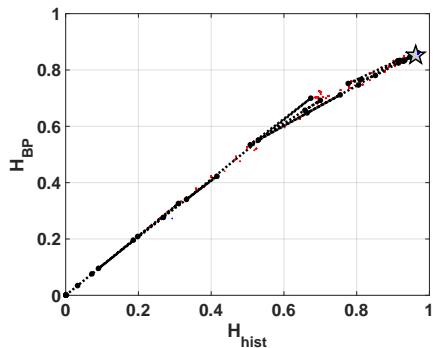


Figura 5.16: Evolución de las propiedades estadísticas en el plano doble entropía para el mapa EVEN  $H_{hist} \times H_{BP}$ .

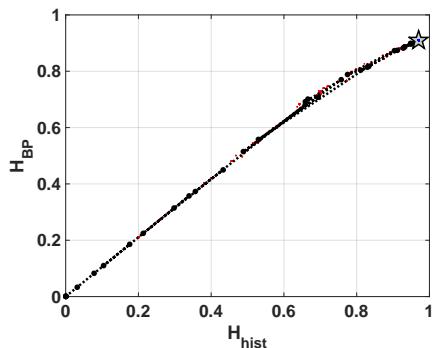


Figura 5.17: Evolución de las propiedades estadísticas en el plano doble entropía para el mapa ODD  $H_{hist} \times H_{BP}$ .

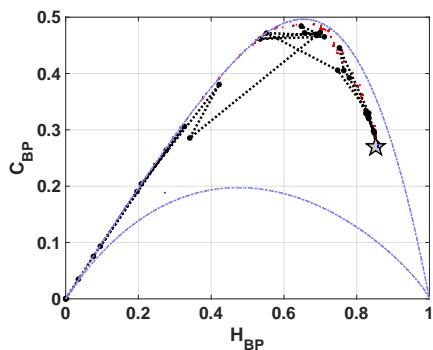


Figura 5.18: Evolución de las propiedades estadísticas en el plano entropía - complejidad para el mapa EVEN  $H_{BP} \times C_{BP}$ .

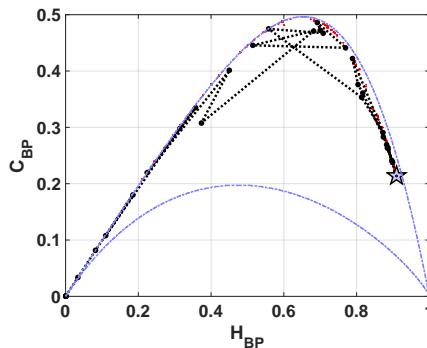


Figura 5.19: Evolución de las propiedades estadísticas en el plano entropía - complejidad para el mapa ODD  $H_{BP} \times C_{BP}$ .

no monótona hacia los resultados de coma flotante. Este resultado es relevante porque muestra que no siempre se recomienda aumentar la precisión.

Es especialmente interesante observar que algunos sistemas (TENT) con muy buenas propiedades estadísticas en el mundo de los números reales, se vuelven “patológicos” cuando se usan representaciones numéricas binarias. Como regla general, si un mapa se genera solo por operaciones de shifteo (esto depende de la base de la unidad lógica aritmética y del mapa en sí), todas las condiciones iniciales convergerán a un punto fijo con un transitorio no mayor que la longitud de la mantisa que está siendo utilizada.

Al comparar los cuantificadores BP y BPW, pudimos detectar caídas a puntos fijos y pudimos estimar la longitud relativa de sus transitorios. Esto puede verse en todas las implementaciones de TENT, en una condición inicial de SWITCH y EVEN para la implementación en coma flotante.

En relación con el comportamiento estadístico, nuestros resultados muestran que SWITCH tiene una mejora marginal en la mezcla con respecto a LOG (y TENT, por supuesto). Sin embargo, la mayor mejora se produce cuando se aplica el skipping, podemos ver que las entropías de BP y BPW crecen y las complejidades de BP y BPW disminuyen, para una dada representación numérica. Este resultado es relevante porque evidencia de que un período largo no es sinónimo de buenas estadísticas, los mapas con skipping EVEN y ODD tienen longitudes de período de la mitad que los de SWITCH, pero su mezcla es mejor y sus distribuciones de amplitud se mantienen casi iguales. Como contrapartida, se necesita más precisión para alcanzar las mejores asíntotas que ofrecen el método de skipping.

Resultó muy interesante el hecho de que el mapa TENT con  $u = 2$  (el cual produce

salidas que convergen rápidamente a cero) y  $u = 1,96$  (con propiedades estadísticas mejores que LOG) produzcan salidas con los mismos resultados en el esquema switcheado.

## Capítulo 6

# Generadores de TRNG usando ROs en FPGA

### 6.1. Introduction

El *Jitter* es cualquier desviación leve del período medio de una señal presuntamente periódica. Hay muchos ejemplos físicos donde esta inestabilidad es relevante. Algunos ejemplos de diferentes áreas son: (a) Stalberg *et. al* [?] encontraron que el intervalo de tiempo entre los dos potenciales de acción de las fibras de dos fibras musculares, que pertenecen a la misma unidad motora en los músculos humanos normales, muestra una variabilidad o inestabilidad; (b) Mecozzi *et. al* [?] detectaron jitter de temporal y variaciones de amplitud en enlaces ópticos utilizando transmisión de pulso altamente disperso; (c) Derickson *et. al* [?] realizó una comparación completa de la fluctuación de tiempo en el caso de los láseres semiconductores en modo bloqueado; (d) el California y Carnegie Planet Search en el Observatorio Keck [?] informó la inestabilidad de las estrellas en las velocidades radiales; (e) Roberts & Guillemin estudiaron los retardos debidos a las colas en etapas de *upstream multiplexing*, en una red de Modo de transferencia asíncrono (ATM); (f) Baron et al [?] consideró la calidad de la señal del *bunch clock* del *Large Hadron Collider* (LHC), en términos de inestabilidad, un problema fundamental porque sincroniza todos los sistemas electrónicos en el detector; (g) Marsalek *et. al* analizaron la relación entre la entrada sináptica y la fluctuación de fase de salida pico en neuronas individuales [?], etc.

Además, los instrumentos digitales se utilizan en cualquier experimento moderno y la

inestabilidad inevitable en los sistemas de adquisición de datos produce incertidumbres en el tiempo y, por consiguiente, en cualquier determinación del espectro.

Este capítulo está dedicado a los osciladores de anillos (*RO*). Recalcemos que en esta aplicación particular, el *jitter* no siempre es indeseable. El *jitter* no es deseado en aplicaciones que usan un *RO* como generador de reloj [?, ?, ?, ?, ?]. Por el contrario, los generadores de números aleatorios *RNG* basados en *RO*'s, usan *jitter* como fuente de aleatoriedad, [?, ?]. El *jitter* también mejora la compatibilidad electromagnética para distribuir la frecuencia del reloj sobre una banda, mejorando la Compatibilidad Electromagnética (EMC) [?].

La determinación del *jitter* de fase en *RO* se ha estudiado en varios artículos: en [?] se presentó el estudio de tres medidas relevantes del *jitter* en el dominio del tiempo. En [?] se propuso un modelo para la generación y distribución del *jitter* en *RO*. En este artículo, los autores separan las fuentes de inestabilidad en deterministas y aleatorias (gaussianas); además, cada fuente se clasifica adicionalmente en local o global. Demuestran que las contribuciones más importantes son la inestabilidad gaussiana local y la inestabilidad determinística global y solo la primera debe usarse como una fuente de aleatoriedad de generadores de números aleatorios verdaderos (*TRNG*). El mismo enfoque se usó en [?, ?, ?, ?]. En Lubicz *et. al* se describe un método práctico y eficiente para estimar la tasa de entropía de un *TRNG* basado en osciladores libres; enfatizaron que su método no requiere extraer las señales del dispositivo y analizarlas con equipos externos [?] (una metodología que introduce fluctuación y distorsión extra en la señal medida debido a la cadena de adquisición de datos).

Por lo general, *jitter determinista* es el nombre que se le da a cualquier *jitter no gaussiano*. Está limitado y se caracteriza por su valor máximo de  $\Delta_{pp}$ . *Jitter aleatorio* es el nombre utilizado para la *jitter gaussiano* y se caracteriza por su valor RMS. A veces aparece *jitter* periódico determinístico. Tiene un *periodo* que es el intervalo entre dos tiempos el efecto máximo (mínimo); el inverso del período de tiempo es la *frecuencia del jitter*. El *jitter* periódico con una frecuencia de fluctuación inferior a  $10Hz$  usualmente se denomina *wander* y el nombre *jitter* está reservada solo a la fluctuación periódica con frecuencias en o por encima de  $10Hz$ . En comunicaciones, *jitter total* es  $T = \Delta_{pp} + 2nR_{rms}$  donde  $n$  es un número entre 6 y 8 relacionado con la tasa de error de bit (*BER*).

Los *ROs* son uno de los principales componentes de los circuitos integrados analógicos y digitales y se han utilizado ampliamente como osciladores *on-chip* para generar relojes en circuitos de alta velocidad. Además, los *ROs* se pueden implementar fácilmente en circuitos

digitales programables como *FPGAs*. Las principales ventajas de los osciladores integrados *RO* sobre los *LC* son su área de chip más pequeña, su rango de funcionamiento más amplio (que puede ser sintonizado eléctricamente) y su menor consumo de energía.

Ya sea que se quiera usar o eliminarlo, el *jitter* en *ROs* debe medirse, lo que no es una tarea simple. La principal contribución de este trabajo es proporcionar una técnica de medición del *jitter* basada en cuantificadores de la teoría de la información (*ITQ*). Utilizamos un modelo estocástico cuya aleatoriedad está relacionada con la amplitud de la inestabilidad. Cada *ITQ* propuesto utilizado en este trabajo se basa en una entropía, es decir, una función de Shannon de la función de distribución de probabilidad (*PDF*) asignada a la serie de tiempo del proceso estocástico. También se pueden usar desequilibrios y complejidades [31, ?], pero no representan una mejora en nuestro caso. En trabajos anteriores [9, 45] mostramos que muchas *PDFs* diferentes pueden asignarse a la misma cadena de datos. La mejor opción depende de la aplicación específica. En este caso utilizamos dos opciones para *PDF*: el *histograma normalizado* y el *histograma de patrones de orden*. Se usa un plano de representación para comparar diferentes situaciones. Una vez que se elige la *PDF*, la Entropía de Shannon es la función básica que cuantifica la uniformidad de la *PDF*. Las *entropías normalizadas*, *entropías diferenciales* y *tasa entropía* son las otras *ITQs* evaluadas. En nuestro caso las *entropías diferenciales* obtienen los mejores resultados y se utiliza un *plano de entropías diferenciales* para comparar su sensibilidad como medida de *jitter*.

## 6.2. Determinación del jitter en *RO's*

Hay dos situaciones diferentes en lo que concierne al *jitter* en *ROs*: (a) en algunas aplicaciones es suficiente con asegurar que el *jitter* no perturba a la señal por encima de un límite aceptable. En este caso la señal se observa en un osciloscopio con un amáscara sobre la pantalla, lo que es suficiente para verificar que la señal se mantiene dentro de los márgenes de tolerancia; (b) en otros casos se precisa una determinación exacta del *jitter*. Entre esos casos está la caracterización de *ROs* considerada en este trabajo.

Los *ROs* ideales están compuestos por un número impar de inversores. Cada inversor tiene un tiempo de propagación y por lo tanto los flancos de subida y bajada separados por medio período viajan a través de los inversores. Si todos los tiempos de propagación son constantes, la salida de este *RO* ideal es una señal cuadrada con un espectro de frecuencia discreto. Pero los tiempos de propagación no son constantes, por lo tanto hay *jitter*. El

*jitter* distorsiona el espectro de potencia ensanchando cada delta en un máximo con cierta anchura.

Supongamos que  $T/2$  es el medio período de un *RO* ideal. Entonces está dado por:

$$\frac{T}{2} = k \sum_{i=1}^k d_i \quad (6.1)$$

En donde  $k$  es el número de inversores y  $d_i$  es el tiempo de propagación a través del  $i$ -ésimo inversor. Cuando hay *jitter*,  $d_i$  es una variable aleatoria que modelamos como:

$$d_i = D_i + \Delta d_i \quad (6.2)$$

donde  $D_i$  es el valor medio de  $d_i$  con el nivel nominal de voltaje de fuente y la temperatura normal, y  $\Delta d_i$  es la variación del retardo producida por los eventos físicos locales y los cambios globales en las condiciones de trabajo del dispositivo (como  $V_{CC}$ , temperatura, etc.). Entonces, el *jitter* en *ROs* se evidencia por el desplazamiento aleatorio de la ubicación de los flancos ascendentes (descendentes), con respecto a la ubicación perfectamente periódica. La medición directa de este desplazamiento tiene dos problemas principales: (a) requiere un instrumento de muy alta frecuencia, porque la resolución del tiempo está limitada por el período de muestreo  $T_s$ ; (b) esta técnica introduce fluctuaciones y distorsiones adicionales en la señal medida proveniente de la cadena de adquisición de datos. Entonces es más conveniente usar *medidas indirectas*, por medio de variables aleatorias auxiliares relacionadas con las propiedades estadísticas relacionadas con el *jitter* para medir la fluctuación de fase con una perturbación mínima [?]. El procedimiento general es el siguiente:

1. Se muestrea la salida con el período de muestreo  $T_s$  para obtener una serie de tiempo binaria. En el caso ideal de *no-jitter*, la salida es una *onda cuadrada continua y perfectamente periódica* con un período  $T$ . Entonces es posible ajustar  $T_s$  para hacer  $T/2 = mT_s$  con  $m \in N^+$ . La serie de tiempo binaria será periódica con  $m$  unos seguidos de  $m$  ceros. Cuando el *jitter* está presente, la serie binaria no es periódica sino estocástica. Este modelo estocástico se conoce como *proceso de renovación alterna*.
2. Se pueden usar muchos cuantificadores de aleatoriedad diferentes para caracterizar el modelo estocástico asociado con el *jitter* medido. En este trabajo utilizamos cuantificadores de la teoría de la información.

Tengamos en cuenta que el *jitter* es acumulativo y surgen dos situaciones básicas: (a) si

se supone que el *jitter* introducido por cada etapa es totalmente independiente del *jitter* introducido por otras etapas, significa que  $\sigma_T^2 = m * \sigma_s^2$ , en donde  $\sigma_s$  es el *jitter* de cada muestra, y se supone que todas las muestras tienen fluctuaciones con la misma distribución normal; (b) si las fuentes de *jitter* están totalmente correlacionadas entre sí, entonces  $\sigma_T = m * \sigma_s$ .

### 6.2.1. Resultados

Se simuló con Matlab<sup>®</sup> una salida de un *RO* muestreada uniformemente sin *jitter* y se generó un archivo de salida con una longitud de  $N_b = 7,000,000$  de bits. Se exploró un conjunto de cien valores de relación de muestreo  $r = T_s/T \in [6,5; 9,5]$  (donde  $T_s$  es el período de muestreo y  $T$  es el período de salida *RO*). *Jitter* con una distribución normal con un conjunto de diferentes valores de varianza  $\sigma_s$  (ver a continuación) se agregaron y se generaron nuevos archivos de la misma longitud. Nuestro método emula el verdadero proceso de muestreo de la salida ruidosa de un *RO* real; el código detallado se publicó en Mathworks [79].

Por cada valor de  $\sigma_s$ , ten surrogates (each one with a different random initial condition) were generated and new files with  $N_b$  bits each were stored. It was assumed that jitter of individual samples is independent, normal distributed random variables, with zero mean value and variance  $\sigma_i = \sigma_s$ . Consequently, the variance of the accumulated jitter over one period  $T$  is given by  $\sigma_T^2 = r\sigma_s^2$  [?]. The values considered are  $\sigma_T = \{0, 0,001, 0,002, 0,003, 0,004, 0,005, 0,007, 0,01, 0,02, 0,02, 0,04, 0,05, 0,07, 0,1\}$ .

Para cada valor de  $\sigma_s$ , se generaron diez surrogados (cada uno con una condición inicial aleatoria diferente) y se almacenaron nuevos archivos con  $N_b$  bits cada uno. Se asumió que el *jitter* de las muestras individuales es independiente, con variables aleatorias distribuidas normales y un valor medio cero y varianza  $\sigma_i = \sigma_s$ . En consecuencia, la varianza del *jitter* acumulada durante un período de  $T$  está dada por  $\sigma_T^2 = r\sigma_s^2$  [?]. Los valores considerados son  $\sigma_T = \{0, 0,001, 0,002, 0,003, 0,004, 0,005, 0,007, 0,01, 0,02, 0,02, 0,04, 0,05, 0,07, 0,1\}$ .

Por cada archivo se evaluaron todos los cuantificadores definidos en la sección ?? para  $D \in [2, 10]$  y  $W \in [1, 26]$ . Los detalles sobre la evaluación, las ventajas y los inconvenientes de cada cuantificador se informan en la sección 3: ellos son  $S_W$ ,  $S_{BP}^{(D)}$ ,  $H_W$ ,  $H_{BP}^{(D)}$ ,  $h$  and  $h^*$ . Aquí mostraremos solo los resultados más relevantes para mostrar la razón por la cual los dos últimos cuantificadores ( $h$  y  $h^*$ ) resultan los más adecuados para este problema.

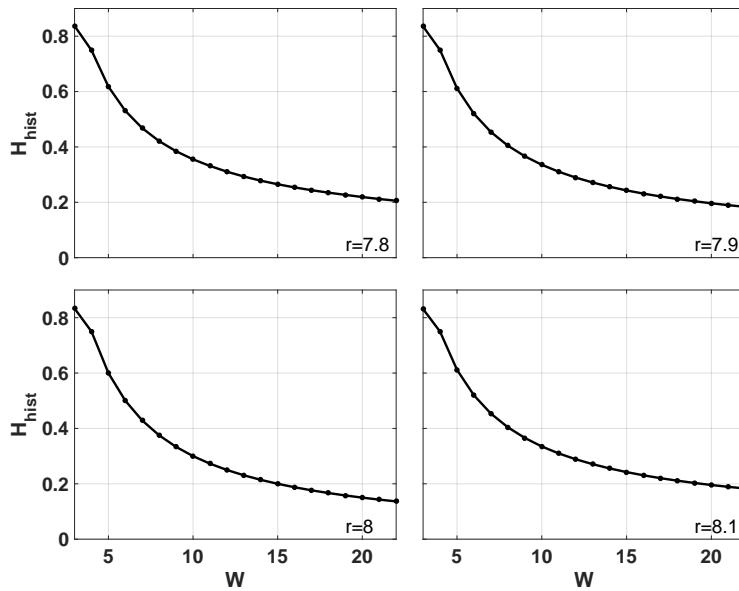


Figura 6.1: Entropía normalizada  $H_W$  en función de  $W$  para un *RO* sin *jitter* muestreado con diferentes valores de  $r$ .

- En el caso de entropía normalizada  $H_W$ , depende en gran medida de  $W$ . Además, el análisis de  $H_W$  en función de  $r$  muestra que no permite determinar un valor óptimo de la relación de muestreo  $r$  (ver Fig. 6.1). Este es un problema importante si los cuantificadores se van a usar para configuraciones experimentales.
- En el caso de la entropía de Bandt & Pompe normalizada  $H_{BP}^{(D)}$ , también está presente una fuerte dependencia con la dimensión de embedding  $D$ . Nuevamente, no es fácil determinar el valor óptimo de  $r$  del análisis de este parámetro en función de  $r$  (ver Fig. 6.2).
- Un comportamiento similar aparece en todos los otros funcionales relacionados con estas dos entropías. En resumen, nuestros resultados muestran que tanto  $h$  y  $h^*$  son independientes de cualquier parámetro arbitrario utilizado en su determinación estadística. Estos dos cuantificadores también se han considerado en dos excelentes artículos [28, 23].

Estos resultados muestran que los dos cuantificadores,  $h$  y  $h^*$ , son apropiados para ser usados como medidores de *jitter* debido a que:

- (a) Para  $\sigma_T = 0$  (salida sin *jitter*) se acercan rápidamente a un valor límite constante

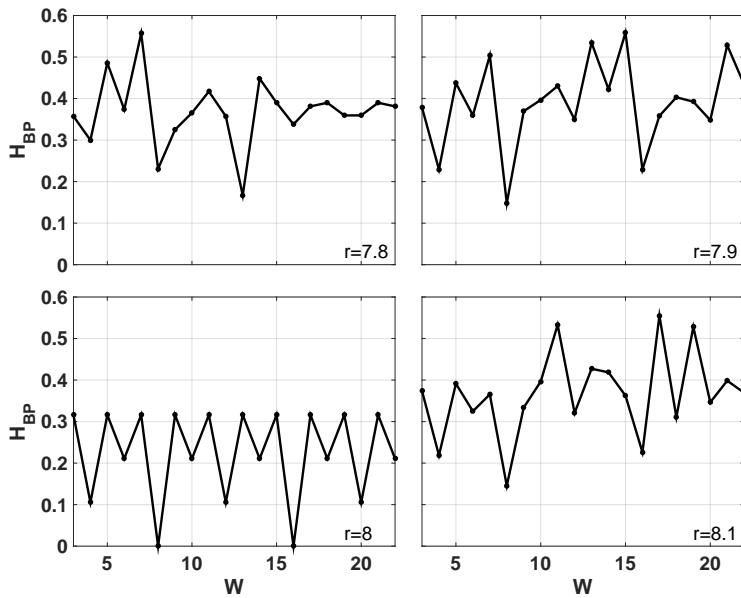


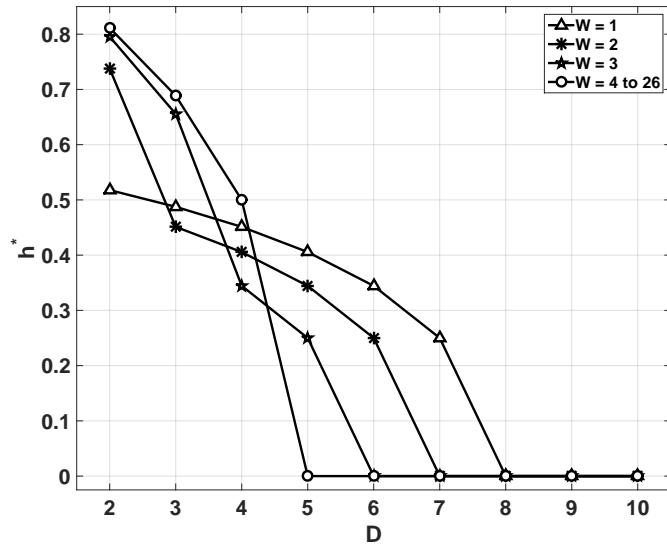
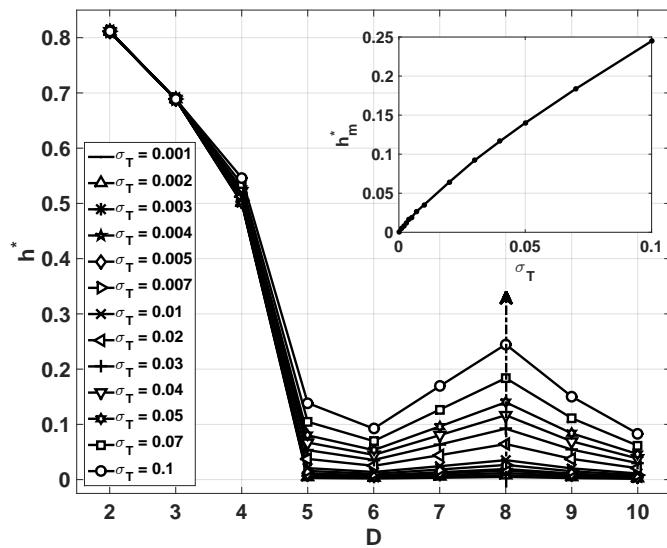
Figura 6.2:  $H_{BP}^{(D)}$  en función de  $W$  para un *RO* sin *jitter* muestreado con diferentes valores de  $r$ . Los cálculos fueron hechos con superposición de palabras

ya que tanto  $D$  como  $W$  tienden a  $\infty$  y este valor es independiente de  $D$  y  $W$ ;

- (b) Son funciones monótonas y proporcionales de  $\sigma_T$ .
- (c) A partir de su análisis, es posible detectar el valor óptimo de la relación de muestreo  $r$ . En las siguientes figuras mostraremos estas afirmaciones que son representativas de todos nuestros resultados.

La figura 6.3 muestra la entropía diferencial de Bandt & Pompe  $h^*$ , como función de  $D$ , con  $W$  como parámetro, para un *RO* sin *jitter*. Se puede ver que existe un valor umbral  $W = 4$  sobre el cual todas las curvas colapsan en una sin importar el valor de  $D$ . Además, la Fig. 6.3 también muestra que para  $D \geq 8$  todas las curvas colapsan en una, independientemente del valor de  $W$ . En conclusión, si  $D \geq 8$  y  $W \geq 4$  obtenemos un cuantificador independiente de  $D$  y  $W$ .

La influencia del *jitter* en este cuantificador se muestra en la figura 6.4, donde  $h^*$  se representa como una función de  $D$  con  $\sigma_T$  como parámetro. Los valores considerados son  $\sigma_T = \{0(\sin jitter), 0,001, 0,002, 0,003, 0,004, 0,005, 0,007, 0,01, 0,02, 0,02, 0,04, 0,05, 0,07, 0,1\}$ . El recuadro de la Fig. 6.4 muestra  $h^*$  como una función de  $\sigma_T$  para  $D = 8$ . Este recuadro muestra que este cuantificador es una función monótona creciente de  $\sigma_T$ .

Figura 6.3:  $h^*$  en función de  $D$  para un  $RO$  sin *jitter* muestreado con  $r = 8$ .Figura 6.4:  $h^*$  en función de  $D$  para un  $RO$  muestreado con  $r = 8$  con longitud de palabra  $W = 6$  para *jitter* con diferentes varianzas. El recuadro muestra  $h^*$  en función de  $\sigma_T$  para  $r = 8$ ,  $W = 6$  y  $D = 8$ .

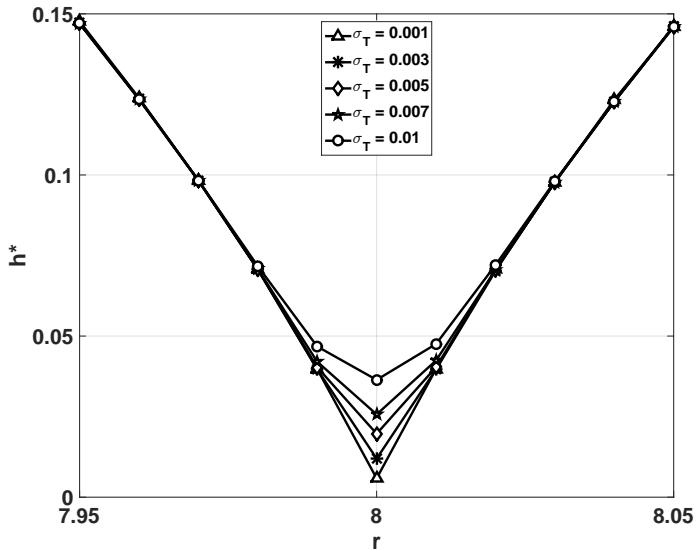


Figura 6.5:  $h^*$  en función de  $r$  para  $r \in [7.95, 8.05]$ , con algunos  $\sigma_T$ ,  $W = 6$  y  $D = 8$ . La curva tiene un mínimo en el valor correcto de  $r = 8$ .

Finalmente, la Fig.6.5 muestra  $h^*$  como una función de la relación de muestreo  $r$ . En esta figura, se muestra que hay un mínimo para el  $r$  correcto (en este caso  $r = 8$ ). Además, la sensibilidad de  $h^*$  en función del jitter es máxima para este mismo valor ideal de  $r$ .

Analicemos ahora el segundo cuantificador,  $h$ . Este cuantificador solo depende de  $W$  porque  $D$  no se usa para definir la PDF asignada a la serie de datos. La Fig. 6.6 muestra un caso sin jitter,  $h$  es independiente de  $W$  para  $W \geq 4$ . Para lo siguiente adoptamos  $W = 6$ .

La figura 6.7 muestra la influencia del jitter sobre este cuantificador. Queda claro en el recuadro de esta figura que, para el valor seleccionado  $W = 6$ ,  $h$  es una función monótona creciente de la varianza del jitter  $\sigma_T$ .

La Fig. 6.8 muestra que  $h$  tiene un mínimo cuando  $r$  toma su valor óptimo ( $r = 8$ ). Note que este mínimo es robusto también en presencia de jitter.

Se debe realizar un análisis adicional para asegurar que los valores seleccionados  $W = 6$  y  $D = 8$  produzcan archivos simbólicos con una buena estadística. Para un alfabeto dado  $\mathcal{A}$  con  $m$  elementos, y un archivo simbólico dado de longitud  $n$ , el parámetro de calidad  $\alpha = n/m$ , vea 3. La calidad es mejor a medida que  $\alpha$  aumenta y se acepta un valor mínimo  $\alpha = 10$ . De acuerdo con la sección 3 los valores seleccionados  $W = 6$  y  $D = 8$  proporcionan  $\alpha_h \simeq 10^5$ ,  $\alpha_{h^*} \simeq 175$  con superposición y 29 sin superposición. Todos los casos dan  $\alpha > 10$  como es requerido.

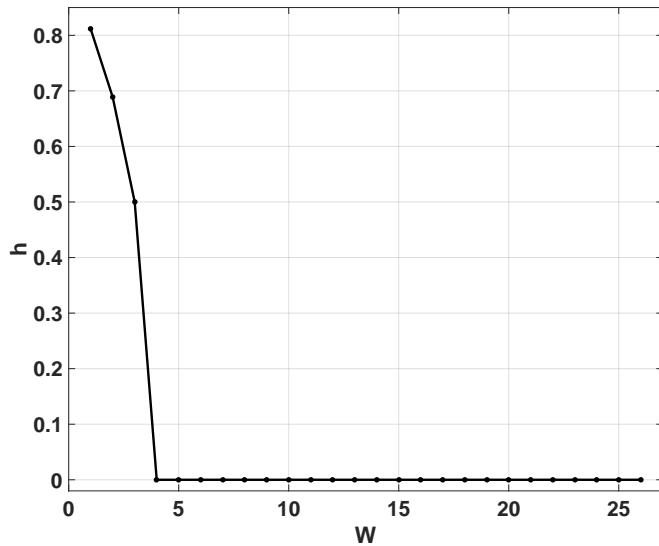


Figura 6.6:  $h$  en función de  $W$  para un  $RO$  sin *jitter* muestreado con  $r = 8$ .

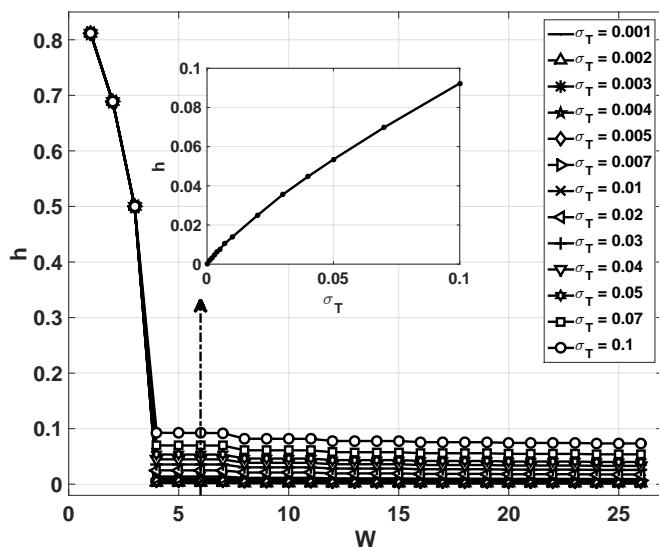


Figura 6.7:  $h$  en función de  $W$  para un  $RO$  muestreado con  $r = 8$ , con *jitter* con distintas varianzas. El recuadro muestra  $h$  en función de  $\sigma_T$  con  $r = 8$  y  $W = 6$ .

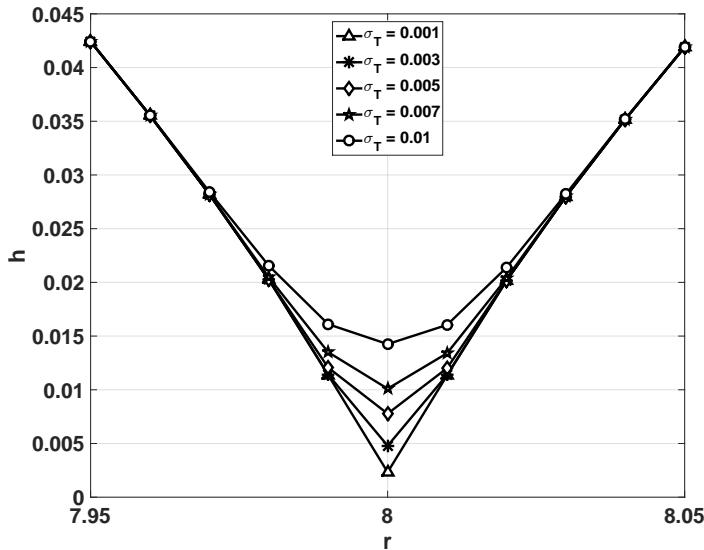


Figura 6.8:  $h$  en función de  $r$  con  $r \in [7.95, 8.05]$ , para distintos  $\sigma_T$  y  $W = 6$ . La curva tiene un mínimo en  $r = 8$ .

|||||||||||||EN LA SECCIÓN CUANTI TENGO QUE PONER COMO SE CALCULA ALFA!!!!!!!!!!!!!!

La figura 6.9 muestra el plano  $h_m^* \times h$ . Los cuantificadores se calcularon barriendo los valores de  $D$  de 2 a 11 y  $W$  de 2 a 26 (barrimos ambos para  $h^*$  y solo  $W$  en el caso de  $h_{hist}$ ). Se obtiene una mejor diferenciación para valores más altos de los parámetros, esto es porque ambos cuantificadores tienden a cuantificar la entropía de la fuente cuando  $D$  y  $W$  tienden a infinito. Sin embargo esto es imposible en la práctica real, la cantidad de datos disponibles limita los valores de los parámetros para lograr buenas estadísticas. Por lo tanto, buscamos los valores mínimos (valor umbral) de los parámetros que distinguen el jitter lo suficientemente bien.

En la figura ?? se puede ver que para valores de  $W$  iguales o menores a 3, el cuantificador  $h_{hist}$  no es sensible a las variaciones del jitter. Por lo tanto,  $W$  debe ser o superior, este resultado está en concordancia con el umbral determinado en las Figuras ???. En el caso de  $h^*$  el valor de  $W$  debe ser igual o superior a 4 y el valor de  $D$  superior a 7, nuevamente este resultado está en concordancia con los derivados de las Figuras ?? y ???. El área inferior izquierda del plano es la que tiene un mejor rendimiento de ambos cuantificadores, sin embargo es la que precisa un mayor esfuerzo de cómputo y una mejor estadística.

|||||||||TENGO QUE PONER EL PLANO EN LAS FIGURAS!!!!!!!!!!!!!!

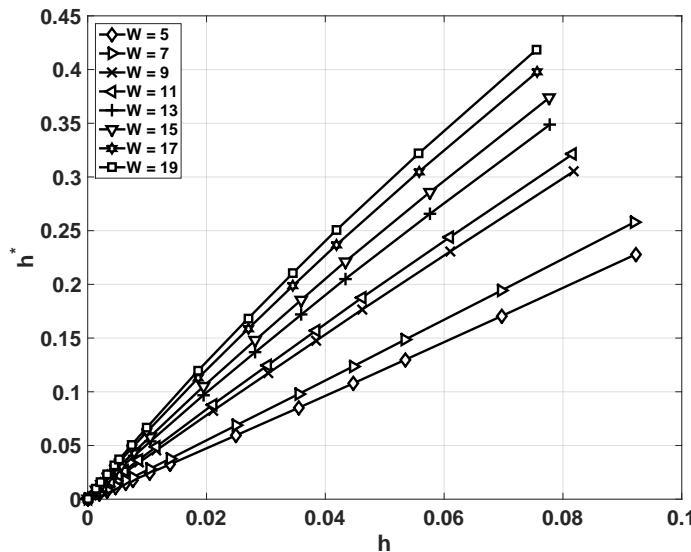


Figura 6.9:  $h^*$  como función de  $h$  para  $r = 8$ ,  $D = 8$  y diferentes valores de  $W$ .

Una comparación entre ambos cuantificadores se muestra en la figura 6.9. Los marcadores corresponden a varianzas  $\sigma_T = \{0, 0,001, 0,002, 0,003, 0,004, 0,005, 0,007, 0,01, 0,02, 0,03, 0,04, 0,05, 0,07, 0,1\}$ . Hay que tener en cuenta que la pendiente de cualquiera de estas curvas es  $dh^*/dh$  y es igual al cociente entre pendientes de curvas en las inserciones de las Figs. 6.4, y 6.7. Si  $dh^*/dh \rightarrow 1$ ,  $h^*$  es más sensible que  $h$  para medir el jitter. La pendiente aumenta levemente de  $\sim 2,47$  para  $W = 5$  a  $\sim 5,54$  para  $W = 19$ , esto muestra que  $h^*$  se vuelve más sensible a medida que aumenta  $W$ .

También evaluamos  $h^*$  sin la superposición de bits entre números naturales consecutivos pero manteniendo la superposición de los  $D - 1$  números naturales entre patrones de orden (en todos los casos  $h$  se evaluó con la superposición de  $W - 1$  bits consecutivos). Los resultados se representan en la Fig. 6.10 donde se muestra que al eliminar la superposición aumenta la sensibilidad de este cuantificador. Por supuesto, obtenemos una cantidad menor de  $W$  bits en números naturales del archivo original de siete millones de binarios, y en consecuencia, la calidad estadística es menor que la del cálculo original con superposición. Para aumentar  $\alpha$  hasta su valor anterior, se requieren archivos binarios más largos.

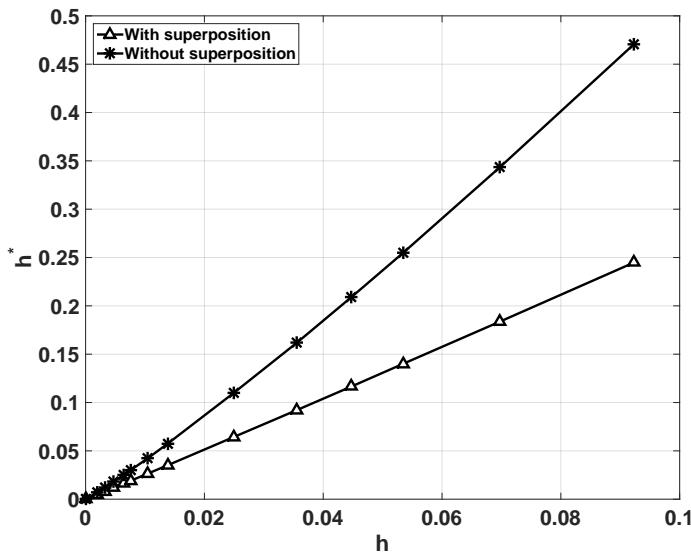


Figura 6.10:  $h^*$  en función de  $h$  para  $r = 8$ ,  $W = 6$  y  $D = 8$ . Son considerados los dos procedimientos para obtener números naturales de  $W$ -bits: con y sin superposición (see text).

### 6.2.2. Conclusiones

Dada su utilidad como *PRNG* y generadores de reloj, los *ROs* se están convirtiendo en uno de los principales componentes básicos de los circuitos digitales. El jitter es inevitable en *ROs*, y en consecuencia, necesita ser caracterizado. La mezcla y la distribución de valores son las principales propiedades a considerar. Varios *ITQ* fueron evaluados aquí.  $S_W$ ,  $S_{BP}^{(D)}$ ,  $H_W$  y  $H_{BP}^{(D)}$  resultan dependientes de los parámetros  $W$  y  $D$ . Esto es un inconveniente si los usamos como medidas de inestabilidad. Por otro lado, no es posible calcular *rate entropies*,  $h_0^*$  y  $h_0$ , ya que se necesita una cantidad infinita de datos para su cálculo. Las dos *entropías diferenciales*,  $h^*$  y  $h$ , en cambio, son independientes de los parámetros utilizados para su determinación y son estimadores de la *rate entropy*. Hemos mostrado en la sección 6.2.1 que en el caso de *ROs* muestreados, presentan un mínimo para la tasa de muestreo correcta, lo que los convierte en una buena medida de la calidad tanto de los *ROs* como de los *PRNGs* derivados de ellos.

El plano de entropía dual determinado por estos cuantificadores ha demostrado discernir satisfactoriamente entre las dos principales propiedades deseadas de *PRNG*, la equiprobabilidad entre todos los valores posibles y la independencia estadística entre valores consecutivos. Por lo tanto, permite ver claramente lo que debe mejorarse en una secuencia determinada.

Los ejemplos presentados aquí han demostrado la necesidad de utilizar ambos histogramas para caracterizar secuencias.

## 6.3. Implementación y análisis estadístico de *TRNG* basado en *ROs*

### 6.3.1. Resumen

Este capítulo sobre el uso de los osciladores en anillo (*ROs*) como generadores de números aleatorios (*TRNG*). Se explica el diseño, hecho para *ALTERA Cyclone III* <sup>®</sup>, usando primitivas de bajo nivel. Se consideran dos características relevantes de un *PRNG* para validar el diseño: 1) el equiprobabilidad de todos los resultados posibles y 2) la estadística independencia de valores consecutivos. En este trabajo, estas propiedades se miden a través de Cuantificadores de teoría de la información. Un plano de doble entropía se usa para representar las series de tiempo y visualizar fácilmente los resultados obtenidos con diferentes configuraciones. La calidad también se compara con otros *RNG* disponibles por medio del plano de entropía dual. Nuestro método constituye una reducción efectiva del análisis completo realizado con la prueba suites como *DIEHARD* o *NIST*.

### 6.3.2. Introducción

El jitter y los ruidos de fase presentes en los osciladores en anillo no son convenientes en varias aplicaciones de *ROs*, por ejemplo en la implementación de *osciladores en el chip* para generar relojes en circuitos de alta velocidad [?, ?, ?]. Sin embargo, son la fuente de aleatoriedad para un *TRNG* basado en *ROs* [?, ?]. Además, un *RO* se puede implementar en un circuito totalmente digital como arreglos de compuertas programables por campo (*FPGAs*) ya que básicamente son solo una serie de inversores.

En [?], Sunar et al. presentó un *PRNG* usando jitter estocástico combinando varios *ROs*. Ellos requerían un procesamiento posterior del flujo de bits basado en funciones resilientes, para enmascarar imperfecciones en la fuente de entropía y para aumentar inmunidad contra los cambios en las condiciones ambientales. En ese trabajo se utilizó la entropía del flujo de bits para validar los resultados en.

Wold et al. [?] propuso una versión mejorada con mejores características aleatorias y sin un procesamiento posterior. Ellos solo agregaron un flip-flop D adicional en cada salida de

### 6.3. IMPLEMENTACIÓN Y ANÁLISIS ESTADÍSTICO DE TRNG BASADO EN ROS143

anillo. La efectividad de su propuesta fue probada por medio de suites de prueba disponibles en la literatura abierta [?, ?, ?].

En este capítulo se realiza una descripción detallada de una implementación de hardware muy compacta de *TRNGs* basados en *ROs* propuesto en [?]. Para validar la aleatoriedad de las secuencias de ruido generadas, se usan dos cuantificadores derivados de la teoría de la información y el plano de doble entropía  $H_{BP} \times H_{hist}$  propuestos en la sección 3. Según lo explicado arriba,  $H_{hist}$  es una medida de la equiprobabilidad entre todos los valores posibles y  $H_{BP}$  es una medida de la independencia entre valores consecutivos.

A continuación se muestra la implementación de hardware del *ROs* mapeado en *FPGA* *Cyclone III* y los resultados obtenidos para diferentes configuraciones, comparando estos resultados con los arrojados por otros generadores.

#### 6.3.3. Implementación en Hardware

Los *TRNG* implementados consisten en varios *ROs* con sus salidas XOR juntas y muestreadas por un flip flop *D*. El flip flop latches la salida a una frecuencia seleccionada (aquí 100 MHz) [?]. La implementación física se realiza en el kit de desarrollo con *EP3C120F780C7N* *FPGA* cuyo dispositivo principal es una *ALTERA* © *Cyclone III EP3C120*. El diseño está hecho con el software *Quartus* © II 13.1.

#### Reseña del Chip

Las *FPGAs* consisten en una gran cantidad de bloques de matriz lógica (*LAB s*), con grupos de elementos lógicos (*LE s*) para implementar circuitos tanto secuenciales como combinatorios. En la arquitectura de la familia *Cyclone III* cada *LAB* contiene 16 *LEs*. Básicamente, cada *LE* es un Flip Flop (*FF*) con una (*LUT*) de cuatro entradas(ver Fig. 6.11). Cada *LUT* puede implementar cualquier función de veinticuatro variables. El *FF* y el *LUT* se pueden usar juntos o independientemente, [80].

Por lo general, el software de síntesis asigna recursos sin la intervención del diseñador. Pero en el diseño de *PRNGs* basados en *ROs* es necesario controlar la ubicación exacta de cada componente individual para evitar la simplificación de los inversores realizada por la herramienta de síntesis. En *Altera* el uso de primitivas de bajo nivel permite controlar la implementación. Por consiguiente, estas primitivas y asignaciones de bajo nivel se emplean dentro del código *HDL* empleado en nuestro diseño. Además, se debe configurar

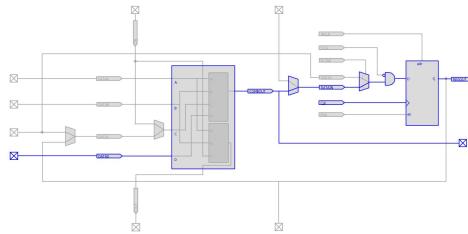


Figura 6.11: Imagen del Chip Planner que muestra la implementación de un inversor y un Flip Flop.

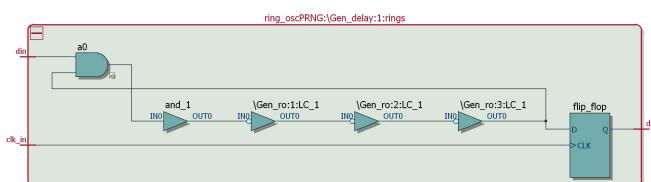


Figura 6.12: Vista RTL de un ring con 3 inversores.

la herramienta de síntesis para evitar que la herramienta de síntesis elimine los búferes redundantes.

Las cadenas de *ROs* se pueden programar en el chip instanciando los *LUTs* como inversores. Es necesario evitar que el motor de síntesis *Quartus II* fusione dos compuertas *NOT* en serie, utilizando una primitiva llamada *LCELL*. Una *LCELL* siempre consume una celda lógica y no es eliminada del proyecto durante la síntesis lógica. Para crear un *RO*, se programan *LCELLs* como búferes de inversor. Las Figs. 6.12 y 6.13 muestran cómo esta primitiva es implementada por el compilador *Quartus II*.

Para lograr que cada *RO* tenga comportamientos distintos, cada uno debe ser ubicado en posiciones distintas en el chip. Para esto debe asignarse a una *LogicLock region* definida previamente.

La Fig. 6.14 muestra las 50 regiones *LogicLocks* utilizadas para este trabajo. Se asigna

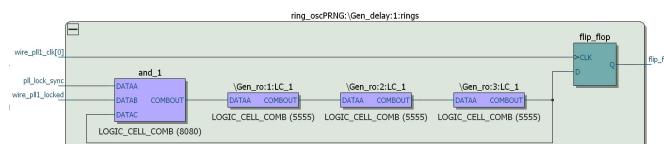


Figura 6.13: Technology map viewer (post mapping) de un ring con 3 inversores.

### 6.3. IMPLEMENTACIÓN Y ANÁLISIS ESTADÍSTICO DE TRNG BASADO EN ROS145

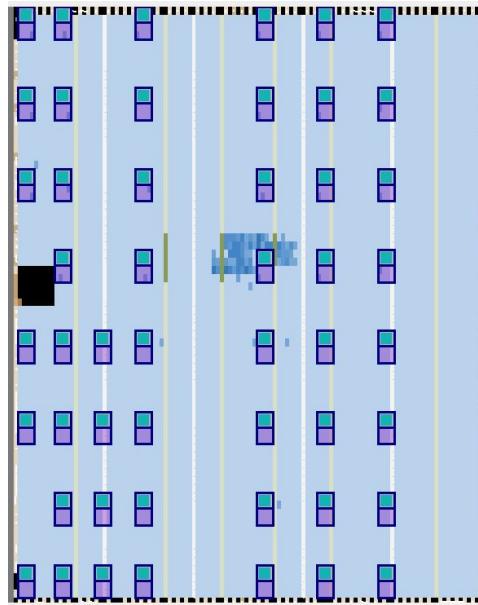
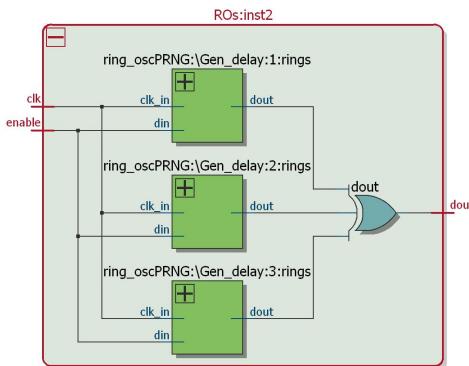


Figura 6.14: Vista de las regiones *LogicLock* del *Chip Planner*.

un *RO* a cada región. Las regiones se distribuyen sobre el chip para un análisis futuro de la importancia de la ubicación. Cada región tiene 16 *LABs*, lo que nos permite aumentar el número de inversores de cada anillo, este es un problema a estudiar en futuros trabajos.

Hay muchos factores que determinan la frecuencia de cada *RO*, y contribuye a la imprevisibilidad de la salida:

1. Ubicación dentro de *LAB*: las diferentes ubicaciones entre los anillos pueden dar como resultado diferencias de tiempo.
2. Conexiones: incluso teniendo exactamente colocación idéntica de una *LUT* con respecto a la otra en un anillo dado, no es posible tener exactamente el mismo *uso de recursos de enrutamiento* en las conexiones.
3. Selección de entrada: durante la etapa de enrutamiento el *fitter* elegirá qué entrada del *LUT* se utiliza. Como el retraso a través del *LUT* depende de cuál de las cuatro entradas se utiliza, los anillos tienen diferentes retardos.
4. Neighborhood: incluso si todo es bloqueado físicamente, el retardo puede cambiar dependiendo de lo que se coloca y enruta alrededor del anillo.

Figura 6.15: *RTL* de *PRNG* con 3 *ROs*.

Total logic elements	847/119,088	(< 1 %)
Total combinational functions	629/119,088	(< 1 %)
Dedicated logic registers	617/119,088	(< 1 %)
Total registers	617	
Total memory bits	131,072/3,981,312	(3 %)

Cuadro 6.1: Compilation Report, *RO*-based *PRNG* using 15 *ROs* and 3 inverters each.

En la Fig. 6.15 (vista RTL) se muestra un *PRNG* usando 3 *ROs* seguido por una puerta XOR.

Para tener una idea de la ocupación en el dispositivo, la tabla 6.1 muestra el informe de compilación de un *TRNG* usando 15 *ROs* cada uno con 3 inverters.

#### 6.3.4. Resultados

La herramienta *Embedded Logic Analyzer* se utiliza para recopilar las secuencias aleatorias generadas. Constituye una *herramienta de depuración a nivel de sistema*, proporcionada por *Altera* [68], que captura y almacena el comportamiento de la señal en tiempo real y permite observar las interacciones entre el hardware y el software en los diseños del sistema. Después de adquirir los datos y guardarlos en un archivo *SignalTap II*, pueden ser analizado o visto como una forma de onda. Con este procedimiento ni jitter adicional, ni la distorsión se introducen en la señal medida de la cadena de adquisición de datos.

Se utilizaron archivos de datos con 917504 bits cada uno para cada *TRNG*. Consideramos conjuntos de  $N_{RO}$  anillos, cada uno con 3 inversores;  $N_{RO} = 2, 3, 4, 5, 6, 7, 15, 25$  y 50.

Los datos de *SignalTap* se procesaron usando *Matlab* <sup>©</sup>. Se agruparon los datos en

### 6.3. IMPLEMENTACIÓN Y ANÁLISIS ESTADÍSTICO DE TRNG BASADO EN ROS147

pañabras de 6 bits sin superposición, por lo que se generaron archivos con 152917 datos cada uno. Se calcularon los cuantificadores descritos en la sección 3 para todos los archivos generados

También evaluamos otros generadores de ruidos conocidos para comparar su calidad con la de los *PRNG* basados en *RO*. Los ruidos analizados son:

- Mersenne Twister pseudo-random number generator, [49].
- Dos algoritmos empleados para generar datos aleatorios por Matlab (método congruente multiplicativo) [?] y Excel [?].
- Dos *ruidos físicos*: ruido de decaimiento radiactivo [81] y ruido atmosférico [82]. Los archivos de datos para estos ruidos están disponibles en los online en los sitios referidos.
- Dos mapas caóticos  $M^1$  y sus versiones iteradas  $M^2$  a  $M^8$  [9] para el mapa logístico (*LOGISTIC*) y el *three way Bernoulli map (TWBM)*.

La Fig. 6.16 muestra los resultados en el plano de doble entropía  $H_{BP} \times H_{hist}$  para todos estos ruidos. Se puede ver que los ruidos físicos, el algoritmo *Mersenne Twister* y los *PRNGs* utilizados en *Matlab* <sup>©</sup> (función *rand*) y en *Excel* <sup>©</sup> (*RAND*), tienen el valor máximo para  $H_{BP}$ , lo que indica que todos los patrones de orden aparecen casi el mismo número de veces. Sin embargo, estos cinco ruidos presentan un comportamiento muy diferente con respecto al cuantificador  $H_{hist}$ . El *decaimiento radiactivo* es el peor, con  $H_{hist} \sim 0,5$ , que indica que esta secuencia no muestra todos los valores posibles en la misma proporción. Los números al lado de cada marcador para las secuencias caóticas, indican el número de iteraciones. Los mapas iterados tienen mayor  $H_{BP}$  debido a su propiedad de mezcla [9]. El plano de entropía dual muestra que un aumento en el número de *ROs* mejora tanto  $H_{BP}$  como  $H_{hist}$ .

La Fig. 6.17 es una vista con más detalle de la Fig. 6.16 alrededor del punto ideal (1, 1). Allí, se muestra la evolución de las secuencias cuando la cantidad de *ROs* aumenta de 5 a 50. Se puede observar que a medida que aumenta el número de anillos los datos aumentan su mezcla y también el histograma tiende a ser más uniforme, por lo tanto, ambas propiedades mejoran. Se puede determinar un umbral en el número de anillos, ya que los puntos se saturan en alrededor de (0,997, 1), por lo que este es el mejor *PRNG* posible, usar más de 15 *ROs* no presenta ninguna mejora. Como se dijo anteriormente, el cuantificador  $H_{hist}$  detecta la variación del histograma de la secuencia, y el cuantificador  $H_{BP}$  refleja la

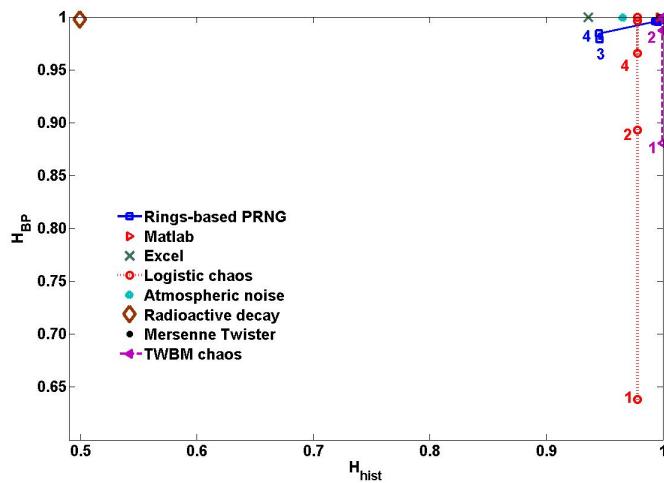


Figura 6.16: Plano  $H_{hist} \times H_{BP}$  para distintos RNGs. Los números que siguen a cada cuadrado indican la cantidad de ROs utilizado en cada TRNG. Los números al lado de cada punto en las secuencias caóticas *Logistic* y *TWBM* indican el número de iteración para el mapa caótico (ver texto).

mejora en la mezcla de datos. Finalmente, las secuencias de Mersenne Twister y Matlab presentan un valor idéntico, ideal  $H_{BP}$  y un valor alto de  $H_{hist}$ ; no obstante, el histograma no es perfectamente uniforme (los valores no son equiprobables).

## 6.4. Conclusiones

Los TRNGs basados en RO implementados aquí han demostrado satisfacer las propiedades estadísticas deseadas para un RNG. Son comparables a otros RNGs utilizados y en algunos casos son mejores. Emplean pocos recursos del dispositivo y se implementan de forma muy simple en una plataforma digital.

Se demostró que para esta arquitectura la cantidad de ROs establece las propiedades estadísticas del TRNG. Se vio que para 15 ROs el histograma y la mezcla, eran casi ideales, haciendo innecesario el aumento de la cantidad de anillos.

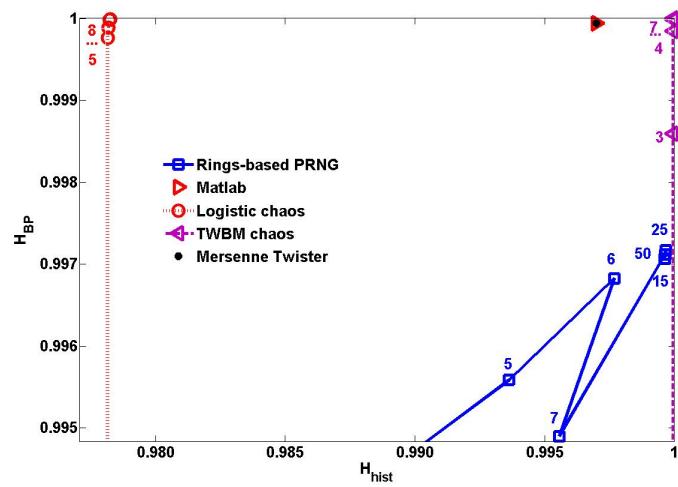


Figura 6.17: Detalle de la Fig. 6.16 alrededor del punto ideal (1, 1).



# Bibliografía

- [1] E. N. Lorenz. Deterministic non periodic flow. *Journal of the Atmospheric Sciences*, 20:130 – 141, 1963.
- [2] J Sprott. *Chaos and Time-Series Analysis*. Oxford University Press, 2003.
- [3] S Strogatz. *Nonlinear Dynamics and Chaos*. Perseus Books, 1994.
- [4] A. Kantz. A robust method to estimate the maximal lyapunov exponent of a time series. *Phys. Lett. A*, 185(77), 1994.
- [5] Ma Xian-Min. Detecting of coal gas weak signals using lyapunov exponent under strong noise background. *Intelligent System Design and Engineering Applications (ISDEA), 2013 Third International Conference on*, 2013.
- [6] S. M. Bruijna, D. J.J. Bregmanc, O. G. Meijerb, P. J. Beekb, and J. H. van Dieën. Maximum lyapunov exponents as predictors of global gait stability: A modelling approach. *Medical Engineering and Physics*, 2011.
- [7] Thomas Weise. *Global Optimization Algorithms*. 2009.
- [8] O. A. Rosso, L. De Micco, H. A. Larrondo, M. T. Martin, and A. Plastino. Generalized statistical complexity measure: a new tool for dynamical systems. *International Journal of Bifurcation and Chaos*, Vol. , No. 3 (2010) ., 20(3):775–785.
- [9] L. De Micco, C. M. González, H. A. Larrondo, M. T. Martin, A. Plastino, and O. A. Rosso. Randomizing nonlinear maps via symbolic dynamics. *Physica A*, 387:3373–3383, 2008.
- [10] K. Mischaikow, M. Mrozek, J. Reiss, and A. Szymczak. Construction of symbolic dynamics from experimental time series. *Phys. Rev. Lett.*, 82:1114–1147, 1999.

- [11] G. E. Powell and I. C. Percival. A spectral entropy method for distinguishing regular and irregular motion of hamiltonian systems. *J. Phys. A: Math. Gen.*, 12:2053–2071, 1979.
- [12] O. A. Rosso, S. Blanco, J. Jordanova, V. Kolev, A. Figliola, M. Schürmann, and E. Başar. Wavelet entropy: a new tool for analysis of short duration brain electrical signals. *Journal of Neuroscience Methods*, 105:65–75, 2001.
- [13] C. Bandt and B. Pompe. Permutation entropy: a natural complexity measure for time series. *Phys. Rev. Lett.*, 88:174102–1, 2002.
- [14] C. E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27:379–423 y 623–656., 1948.
- [15] D. P. Feldman, C. S. McTague, and P. Crutchfield. The organization of intrinsic computation: complexity-entropy diagrams and the diversity of natural information processing. *arxiv.org:0866.4789[nlin.CD]*, pages 1–18, junio 2008.
- [16] D. P. Feldman and J. P. Crutchfield. Measures of statistical complexity: why? *Physics Letters A*, 238:244–252, 1998.
- [17] P. W. Lamberti, M. T. Martín, A. Plastino, and O. A. Rosso. Intensive entropic non-triviality measure. *Physica A*, 334:119–131, 2004.
- [18] R. López-Ruiz, H. L. Mancini, and X. Calbet. A statistical measure of complexity. *Phys. Lett. A*, 209:321–326, 1995.
- [19] M. T. Martín, A. Plastino, and O. A. Rosso. Statistical complexity and disequilibrium. *Phys. Lett. A*, 311:126–132, 2003.
- [20] M. T. Martín and A. Plastino. Generalized statistical complexity measures: Geometrical and analytical properties. *Physica A*, 369:439–462, 2006.
- [21] M. T. Martin. *Ph.D. Thesis, Department of Mathematics*,. PhD thesis, Faculty of Sciences, University of La Plata, 2004.
- [22] S. Blanco, A. Figliola, R. Quian Quiroga, O. A. Rosso, and E. Serrano. Time-frequency analysis of electroencephalogram series (iii): Wavelet packets and information cost function. *Phys. Rev. E*, 57:932–940., 1998.

- [23] W. Ebeling and R. Steuer. Partition-based entropies of deterministic and stochastic maps. *Stochastics and Dynamics*, 1(1):1–17, 2001.
- [24] K. Keller and M. Sinn. Ordinal analysis of time series. *Physica A*, 356:114–120, 2005.
- [25] J. M. Amigó, L. Kocarev, and I. Tomovski. Discrete entropy. *Physica D*, 228:77–85., 2007.
- [26] O. A. Rosso, L. Zunino, D. G. Pérez, A. Figliola, H. A. Larrondo, M. Garavaglia, Martín M. T., and A. Plastino. Extracting features of gaussian selfsimilar stochastic processes via the bandt & pompe approach. *Phys. Rev. E*, 76(6):061114, 2007.
- [27] O. A. Rosso, L. C. Carpi, P. M. Saco, M. Gómez Ravetti, A. Plastino, and H. A. Larrondo. Causality and the entropy complexity plane: Robustness and missing ordinal patterns. *Physica A*, 391:42–55, 2012.
- [28] J. M. Amigó, L. Kocarev, and J. Szczepanski. Order patterns and chaos. *Physics Letters A*, 355:27–31, 2006.
- [29] J. M. Amigó, S. Zambrano, and M. A. F. Sanjuán. Combinatorial detection of determinism in noisy time series. *Europhysics Letters*, 83:60005, 2008.
- [30] J. M. Amigó. *Permutation complexity in dynamical systems*. Springer-Verlag, Berlin, Germany, 2010.
- [31] Amigó et al. *Physica D*, 210:77, 2005.
- [32] L. De Micco, M. Antonelli, C.M. Gonzalez, and H.A Larrondo. Hardware implementation of maximum lyapunov exponent. In *Embedded Systems (SASE/CASE), 2013 Fourth Argentine Symposium and Conference on*, pages 1–4, Aug 2013.
- [33] Yu Gu, Andrew McCallum, and Don Towsley. Detecting anomalies in network traffic using maximum entropy estimation. In *Proceedings of the 5th ACM SIGCOMM Conference on Internet Measurement*, IMC ’05, pages 32–32, Berkeley, CA, USA, 2005. USENIX Association.
- [34] Arno Wagner and Bernhard Plattner. Entropy Based Worm and Anomaly Detection in Fast IP Networks. In *Proceedings of the 14th IEEE International Workshops on Enabling Technologies Infrastructure for Collaborative Enterprise*, 2005.

- [35] Subramanya Nagalakshmi. *Study of FPGA implementation of entropy norm computation for IP data streams*. PhD thesis, University of South Florida Scholar Commons, 2008.
- [36] Actel Corporation. *Core8051s Embedded Processor Hardware Development Tutorial, for Fusion Mixed-Signal FPGAs*, 2009.
- [37] Actel Corporation. *Fusion Embedded Development Kit*, 2009.
- [38] Actel Corporation. *Core8051s Embedded Processor Software Development Tutorial, for Fusion Mixed-Signal FPGAs*, 2009.
- [39] Issue 7 The Open Group Base Specifications. math.h: mathematical declarations, base definitions reference.
- [40] J. G. Fernández, H. A. Larrondo, H. A. Slavin, D. G. Levin, R. M. Hidalgo, and R. R. Rivera. Masking properties of apd communication systems. *Physica A*, 328:351–359, 2003.
- [41] G. Setti, R. Rovatti, and G. Mazzini. Performance of chaos-based asynchronous ds-cdma with different pulse shapes. *IEEE Communications Letters*, 8(7):416–418, July 2004.
- [42] L. De Micco, C. M. Arizmendi, and H. A. Larrondo. Zipping characterization of chaotic sequences used in spread spectrum communication systems. *Institute of Physics Conference Proceedings 913*, pages 139–144, 2007.
- [43] L. Kocarev and G. Jakimoski. Pseudorandom bits generated by chaotic maps. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 50(1):123–126, January 2003.
- [44] H. A. Larrondo, M. T. Martin, C.M. González, A. Plastino, and O. A. Rosso. Random number generators and causality. *Phys. Lett. A*, 352(4- 5):421–425, April 2006.
- [45] L. De Micco, H. A. Larrondo, A. Plastino, and O. A. Rosso. Quantifiers for randomness of chaotic pseudo random number generators. *Philosophical Transactions of the Royal Society A*, 367:3281–3296, 2009.

- [46] S. Callegari, R. Rovatti, and G. Setti. Chaos-based fm signals: application and implementation issues. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 50(8):1141–1147, August 2003.
- [47] L. Kocarev and U. Parlitz. General approach for chaotic synchronization with applications to communication. *Physical Review Letters*, 74(25):5028–5031, 1995.
- [48] R. M. Hidalgo, J. G. Fernández, R. R. Rivera, and H. A. Larrondo. Versatile dsp-based chaotic communication system. *Electronic Letters*, 37:1204–1205, 2001.
- [49] M. Matsumoto and T. Nishimura. Mersenne twister: A 623-dimensionally equidistributed uniform pseudorandom number generator. *ACM Trans. on Modeling and Computer Simulation*, 8(1):3–30, January 1998.
- [50] G. Marsaglia and A. Zaman. A new class of random number generators george marsaglia and arif zaman the annals of applied probability. *Institute of Mathematical Statistics Stable*, 1(3):462–480, August 1991.
- [51] J. Boyar. Inferring sequences produced by pseudo-random number generators. *Journal of the ACM*, 36(1):129–141, 1989.
- [52] J.B. Plumstead. Inferring sequences produced by pseudo-random number generators. *CRYPTO*, pages 317–319, 1982.
- [53] L. Kocarev and S. Lian. *Chaos-Based Cryptography: Theory, Algorithms and Applications*. Studies in Computational Intelligence. Springer, 2011.
- [54] A. Lasota and M. C. Mackey. *Chaos, Fractals, and Noise: Stochastic Aspects of Dynamics*. Applied Mathematical Sciences 97. Springer Verlag, 2nd. edition. edition, 1994.
- [55] G.A. Constantinides, P.Y.K. Cheung, and W. Luk. Optimum wordlength allocation. In *Field-Programmable Custom Computing Machines, 2002. Proceedings. 10th Annual IEEE Symposium on*, pages 219–228, 2002.
- [56] George A. Constantinides, Peter Y. K. Cheung, and Wayne Luk. Wordlength optimization for linear digital signal processing. *IEEE Trans. Computer-Aided Design of Integrated Circuits and Systems*, 22:1432–1442, 2003.

- [57] M. A. Asseri, M. I. Sobhy, and P. Lee. Lorenz chaotic model using field programmable gate array. *The 2002 45th Midwest Symposium on Circuits and Systems, 2002. MWSCAS-2002*, 1:I – 527–30, 2002.
- [58] M.S. Azzaz, C. Tanougast, S. Sadoudi, A. Bouridane, and A. Dandache. Fpga implementation of new real-time image encryption based switching chaotic systems. *Signals and Systems Conference (ISSC 2009)*, pages 1 – 6, 2009.
- [59] L. De Micco, O. G. Zabaleta, C. M. González, C. M. Arizmendi, and H. A. Larrondo, editors. *Estocasticidad de un atractor caótico determinista implementado en FPGA*, 2010.
- [60] M.S. Azzaz, S. Tanougast, C. and Sadoudi, A. Bouridane, and A. Dandache. An fpga implementation of a feed-back chaotic synchronization for secure communications. *International Symposium on Communication Systems Networks and Digital Signal Processing (CSNDSP)*, pages 239 – 243, 2010.
- [61] C. M. González, H. A. Larrondo, C. A Gayoso, and L. J. Arnone. Generación de secuencias binarias pseudo aleatorias por medio de un mapa caótico 3d. In *Proceedings del IX Workshop de IBERCHIP*, 2003.
- [62] J. Soto. Statistical testing of random number generators. *available online at <http://csrc.nist.gov/groups/ST/toolkit/rng/documents/nissc-paper.pdf>.*
- [63] G. Marsaglia. The marsaglia random number cdrom including the diehard battery of tests of randomness. *<http://www.stat.fsu.edu/pub/diehard/>*, 1995.
- [64] H. M. Gustafson, E. P. Dawson, L. Nielsen, and W. J. Caelli. A computer package for measuring the strength of ciphers. *Computers and Security*, 13(8):687–697, 1994.
- [65] A.L. Rukhin. Testing randomness: a suite of statistical procedures. *Theory Probab. Appl.*, 45:111, 2000.
- [66] P. L'Ecuyer and R. Simard. Testu01: A c library for empirical testing of random number generators. *ACM Transactions on Mathematical Software*, 33(22), 2007.
- [67] R. G. Brown. dieharder: A random number test suite. *<http://www.phy.duke.edu/rgb/General/dieharder.php>*, 2012.
- [68] ALTERA. *Quartus II Handbook Version 9.1*, 2009.

- [69] Rathindra Nath Giri and M. K. Pandit. Pipelined floating-point arithmetic unit (fpu) for advanced computing systems using fpga. *International Journal of Engineering and Advanced Technology*, 1(4):168–174, 2012.
- [70] Gokul Govindu, Ling Zhuo, Seonil Choi, and Viktor Prasanna. Analysis of high-performance floating-point arithmetic on fpgas. 2004.
- [71] A. Lasota and J. A. Yorke. On the existence of invariant measure for piecewise monotonic transformations. *Trans. Amer. Math. Soc.*, 186:481–488, 1973.
- [72] Celso Grebogi, Edward Ott, and James A. Yorke. Roundoff-induced periodicity and the correlation dimension of chaotic attractors. *Phys. Rev. A*, 38:3688–3692, Oct 1988.
- [73] Julien Clinton Sprott. Automatic generation of strange attractors. *Computers & Graphics*, 17(3):325–332, 1993.
- [74] S. P. Dias, L. Longa, and E. Curado. Influence of the finite precision on the simulations of discrete dynamical systems. *Communications in Nonlinear Science and Numerical Simulations*, 16:1574–1579, March 2011.
- [75] N. Nagaraj, M. C. Shastry, and P. G. Vaidya. Increasing average period lengths by switching of robust chaos maps in finite precision. *The European Physical Journal Special Topics*, 165:73–83, 2008.
- [76] Xinzhi Liu, Kok-Lay Teo, Hongtao Zhang, and Guanrong Chen. Switching control of linear systems for generating chaos. *Chaos, Solitons and Fractals*, 30:725–733, 2006.
- [77] E. Gluskin. The nonlinear-by-switching systems (a heuristic discussion of some basic singular systems). <http://arxiv.org/abs/0801.3652>, 2008.
- [78] M. Antonelli and L. De Micco. Cripto-codificación caótica variante en el tiempo. *uEA2012*, 2012.
- [79] M. Antonelli. Emulating a ring oscillator with jitter. [www.mathworks.com/matlabcentral/fileexchange/54021-jitter-samples-n-r-sigma-](http://www.mathworks.com/matlabcentral/fileexchange/54021-jitter-samples-n-r-sigma-), 2015.
- [80] ALTERA. ip-basesuite.html. <http://www.altera.com/products/ip/design/basesuite/ip-basesuite.html>., 2008.

- [81] John Walker. HotBits: Genuine random numbers, generated by radioactive decay.  
*online at www.fourmilab.ch/hotbits*, 2001.
- [82] Mads Haahr. Random.org.