

Implementación de Renyi Maps acoplados y aplicación de pruebas NIST.

Marcos Daniel Calderón Calderón

Abstract

En este reporte, se explica a detalle la implementación de varios mapas caóticos acoplados. En este caso, se utilizará el mapa Renyi.

1. Introducción: Sistemas acoplados.

Un sistema acoplado puede estar representado por medio de ecuaciones diferenciales o discretas. En este tipo de sistemas, las razones de cambio dependen de más variables. Un ejemplo sencillo puede ser el siguiente sistema de ecuaciones diferenciales:

$$\frac{dC}{dt} = \alpha C - \beta CZ \quad \frac{dZ}{dt} = -\gamma Z + \delta CZ \quad (1)$$

Un ejemplo de sistema discreto acoplado es el siguiente:

$$X_{i,j} = (1 - \epsilon)f(X_{i,j-1}) + \epsilon H(X_{i,j-1}, \dots, X_{N,j-1}) \quad (2)$$

donde:

$$H(X_{i,j-1}, \dots, X_{N,j-1}) = \sum_{i=1}^N w_i X_{i,j-1}. \quad (3)$$

El índice i representa cada una de los N mapas que se van a acoplar, el índice j representa a las evaluaciones anteriores de cada uno de los mapas.

2. Criterios utilizados para el acoplamiento de mapas.

Se utilizaron diversas maneras para el acoplamiento de los mapas; a continuación, explicamos cada una de ellas.

Email address: marcos.calderon@cimat.mx (Marcos Daniel Calderón Calderón)

2.1. Criterio 1.

El primer criterio utilizado es el siguiente:

$$X_{i,j} = f(X_{i,j-1}) + \epsilon H(X_{i,j-1}, \dots, X_{N,j-1}) \quad (4)$$

donde:

$$H(X_{i,j-1}, \dots, X_{N,j-1}) = \sum_{i=1}^N (X_{i,j-1} \text{ mód } 256). \quad (5)$$

además, ϵ es un valor aleatorio del conjunto: $\{-1, 0, 1\}$

2.2. Criterio 2.

El segundo criterio utilizado es el siguiente:

$$X_{i,j} = f(X_{i,j-1}) + \epsilon H(X_{i,j-1}, \dots, X_{N,j-1}) \quad (6)$$

donde:

$$H(X_{i,j-1}, \dots, X_{N,j-1}) = \bigoplus_{i=1}^N (X_{i,j-1}). \quad (7)$$

donde \bigoplus representa la operación XOR , además ϵ es un valor aleatorio del conjunto: $\{-1, 0, 1\}$

2.3. Criterio 3.

El tercer criterio utilizado es el siguiente:

$$X_{i,j} = \hat{\gamma} \bigoplus f(X_{i,j-1}) + \gamma \bigoplus H(X_{i,j-1}, \dots, X_{N,j-1}) \quad (8)$$

donde:

$$H(X_{i,j-1}, \dots, X_{N,j-1}) = \bigoplus_{i=1}^N (X_{i,j-1}). \quad (9)$$

donde \bigoplus representa la operación XOR , además para el cálculo del valor de γ , necesitamos un ϵ que será un valor aleatorio donde $1 \geq \epsilon \geq 32$, el rango es establecido de acuerdo al tipo de dato utilizado cuando se traduce el sistema a un lenguaje de programación elegido. Ahora, podemos calcular γ de la siguiente manera:

$$\gamma = 2^\epsilon - 1 \quad (10)$$

$$\hat{\gamma} = M - \gamma \quad (11)$$

donde $M = 2^{32} - 1$.

3. Detalles de implementación.

A continuación, se especifican algunos detalles importantes a tomar en cuenta a la hora de la implementación de los mapas acoplados:

- El lenguaje de programación utilizado será **C**.
- Se trabajará con el tipo de dato **unsigned long**; por lo tanto, se dispone de 32 bits (4 bytes) para la representación de los datos. Por lo tanto, tenemos un rango de $(0 - 4,294,967,295 = 2^{32} - 1)$.
- Se buscaron 80000 valores en la ejecución del programa; además, cada valor está compuesto de 32 bits cuando se guarda la información en un archivo binario. Por las características mencionadas anteriormente, se pueden leer **2,560,000 bits** para la aplicación de las pruebas NIST.
- Para equipos de cómputo de 32 bits, se utilizó el tipo de dato **unsigned long**, que está conformado de 4 bytes. Si el equipo de cómputo utilizado es de 64 bits, se recomienda utilizar el tipo de dato **unsigned int**, todavía no hay un estándar definido para el tamaño de los tipos de datos en los equipos de 64 bits.

4. Resultados.

4.1. Aplicación de las pruebas NIST a los mapas acoplados del Criterio 1.

Recordemos que el criterio 1 era el siguiente:

$$X_{i,j} = f(X_{i,j-1}) + \epsilon H(X_{i,j-1}, \dots, X_{N,j-1}) \quad (12)$$

donde:

$$H(X_{i,j-1}, \dots, X_{N,j-1}) = \sum_{i=1}^N (X_{i,j-1} \text{ mód } 256). \quad (13)$$

además, ϵ es un valor aleatorio del conjunto: $\{-1, 0, 1\}$

Se ejecutó el siguiente código:

- **./assess 2560000**
- User Prescribed Input File: **binarioSUMA.dat**
- Enter 0 if you DO NOT want to apply all of the statistical tests to each sequence and 1 if you DO. Enter choice: **1**
- How many bitstreams? **1**
- Input File Format: [0] ASCII - A sequence of ASCII 0's and 1's [1] Binary - Each byte in data file contains 8 bits of data
Select input mode: **1**

Se obtuvieron los siguientes resultados:

Cuadro 1: Resultados de las pruebas de aleatoriedad NIST a los datos binarioSUMA.dat .

PRUEBA APLICADA	P-VALOR	EXITO?
APROXIMATE ENTROPY	0.241029	✓
BLOCK FREQUENCY	0.464753	✓
CUMULATIVE SUMS	FORWARD TEST: 0.628651, REVERSE TEST: 0.848525	✓
FFT	0.149985	✓
FREQUENCY	0.625019	✓
LINEAR COMPLEXITY	0.595287	✓
LONGEST RUN	0.511949	✓
NON OVERLAPPING TEMPLATE	P-VALORES ACEPTADOS: 145 DE 148	✓
OVERLAPPING TEMPLATE	0.037821	✓
RANDOM EXCURSIONS	P-VALORES ACEPTADOS: 8 DE 8	✓
RANDOM EXCURSIONS VARIANT	P-VALORES ACEPTADOS: 18 DE 18	✓
RANK	0.111388	✓
RUNS	0.957015	✓
SERIAL	P-VALORES ACEPTADOS: 2 DE 2	✓
UNIVERSAL	0.136601	✓

4.2. Aplicación de las pruebas NIST a los mapas acoplados del Criterio 2.

El criterio 2 era el siguiente:

$$X_{i,j} = f(X_{i,j-1}) + \epsilon H(X_{i,j-1}, \dots, X_{N,j-1}) \quad (14)$$

donde:

$$H(X_{i,j-1}, \dots, X_{N,j-1}) = \bigoplus_{i=1}^N (X_{i,j-1}). \quad (15)$$

donde \bigoplus representa la operación *XOR*, además ϵ es un valor aleatorio del conjunto: $\{-1, 0, 1\}$

Para el criterio 2, se ejecutó el siguiente código:

- `./assess 2560000`
- User Prescribed Input File: **binarioXOR.dat**
- Enter 0 if you DO NOT want to apply all of the statistical tests to each sequence and 1 if you DO. Enter choice: **1**
- How many bitstreams? **1**
- Input File Format: [0] ASCII - A sequence of ASCII 0's and 1's [1] Binary - Each byte in data file contains 8 bits of data
- Select input mode: **1**

Se obtuvieron los siguientes resultados:

Cuadro 2: Resultados de las pruebas de aleatoriedad NIST a los datos binarioXOR.dat .

PRUEBA APLICADA	P-VALOR	EXITO?
APROXIMATE ENTROPY	0.858228	✓
BLOCK FREQUENCY	0.118270	✓
CUMULATIVE SUMS	FORWARD TEST: 0.021856, REVERSE TEST: 0.035757	✓
FFT	0.787496	✓
FREQUENCY	0.022608	✓
LINEAR COMPLEXITY	0.791809	✓
LONGEST RUN	0.378018	✓
NON OVERLAPPING TEMPLATE	P-VALORES ACEPTADOS: 144 DE 148	✓
OVERLAPPING TEMPLATE	0.457920	✓
RANDOM EXCURSIONS	NOT APPLICABLE.	
RANDOM EXCURSIONS VARIANT	NOT APPLICABLE.	
RANK	0.278871	✓
RUNS	0.019569	✓
SERIAL	P-VALORES ACEPTADOS: 2 DE 2	✓
UNIVERSAL	0.249147	✓

4.3. Aplicación de las pruebas NIST a los mapas acoplados del Criterio 3.

EL criterio 3 era el siguiente:

$$X_{i,j} = \hat{\gamma} \bigoplus f(X_{i,j-1}) + \gamma \bigoplus H(X_{i,j-1}, \dots, X_{N,j-1}) \quad (16)$$

donde:

$$H(X_{i,j-1}, \dots, X_{N,j-1}) = \bigoplus_{i=1}^N (X_{i,j-1}). \quad (17)$$

Para el criterio 3, se ejecutó el siguiente código:

- ./assess 2560000
- User Prescribed Input File: **binarioXORcomp.dat**
- Enter 0 if you DO NOT want to apply all of the statistical tests to each sequence and 1 if you DO. Enter chice: **1**
- How many bitstreams? **1**
- Input File Format: [0] ASCII - A sequence of ASCII 0's and 1's [1] Binary - Each byte in data file contains 8 bits of data
- Select input mode: **1**

Se obtuvieron los siguientes resultados:

Cuadro 3: Resultados de las pruebas de aleatoriedad NIST a los datos binarioXORcomp.dat .

PRUEBA APLICADA	P-VALOR	EXITO?
APROXIMATE ENTROPY	0.979174	✓
BLOCK FREQUENCY	0.283892	✓
CUMULATIVE SUMS	FORWARD TEST: 0.320736, REVERSE TEST: 0.476676	✓
FFT	0.990848	✓
FREQUENCY	0.286876	✓
LINEAR COMPLEXITY	0.142002	✓
LONGEST RUN	0.106050	✓
NON OVERLAPPING TEMPLATE	P-VALORES ACEPTADOS: 145 DE 148	✓
OVERLAPPING TEMPLATE	0.879647	✓
RANDOM EXCURSIONS	P-VALORES ACEPTADOS: 8 DE 8	✓
RANDOM EXCURSIONS VARIANT	P-VALORES ACEPTADOS: 18 DE 18	✓
RANK	0.398102	✓
RUNS	0.964539	✓
SERIAL	P-VALORES ACEPTADOS: 2 DE 2	✓
UNIVERSAL	0.603939	✓

5. Conclusiones.

En general, los criterios 1 y 3 arrojan mejores resultados que el criterio 2. Si se tuviera que elegir entre el criterio 1 y el 3. Se puede concluir que el criterio 3 obtuvo un mejor desempeño de acuerdo a los p-valores obtenidos.

6. Anexos.