Análisis del Generador Renyi Map.

Marcos Daniel Calderón Calderón

Abstract

En este reporte, se hacen algunas pruebas del tamaño de ciclo del mapa caótico Renyi.

1. Características a tomar en cuenta para la realización de las pruebas.

1. Siempre ocurrió que $j \geq n$ para que el mapa se comporte como un generador congruencial lineal (LCG).
2. Otra cosa que se debe de tener en cuenta es lo siguiente, al igual que en las pruebas del paper, es necesario que $i = j$.
3. Ahora, lo que hacemos es definir el valor de q como *impar*.

Con las características mencionadas arriba, lo que se busca es obtener un período máximo de $2^n - 1$. De acuerdo a diversos estudios realizados, para obtenener un tamaño máximo de ciclo, es necesario que la función sea invertible (biyectiva y suprayectiva). Esto sólo se logra si $i = j$.

La proposición 1 del artículo [1] demuestra que el mapa caótico Renyi es invertible cuando $i = j$, y que si cumple esta condición, es posible encontrar siclos de tamaño máximo.

Además, al utilizar $i = j = n$, obtenemos una simplificación del mapa caótico:

$$f(k) = qk \mod 2^n \tag{1}$$

1. **unsigned long** Es un tipo de dato utilizado en C, es una variable para almacenar números en 32 bits (4 bytes). Por el contrario que las variables long estándar, las unsigned long no almacenan números negativos, haciendo que su rango sea de 0 a 4,294,967,295 ($2^{32} - 1$).
2. **Máscaras.** Son secuencias de bits que tienen la finalidad de ocultar o mostrar bits específicos de otra secuencia de bits. Esto se logra al aplicar un operador lógico a la máscara con la secuencia original.
3. **Hexadecimales en C.** La representación de Hexadecimales en C se realiza al anteponer los caracteres "0x" al número que estará en Hexadecimal.
4. **Operacion módulo en bits.** A la hora de utilizar esta operación en generación de números pseudoaleatorios, se utiliza la operación lógica de & con una máscara de bits.

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

2. Resultados.

2.1. Ejemplo 1. $i = j = 31, n = 32$

A continuación mostramos una tabla en donde se observan los tamaños de ciclo obtenidos para algunos valores de q.

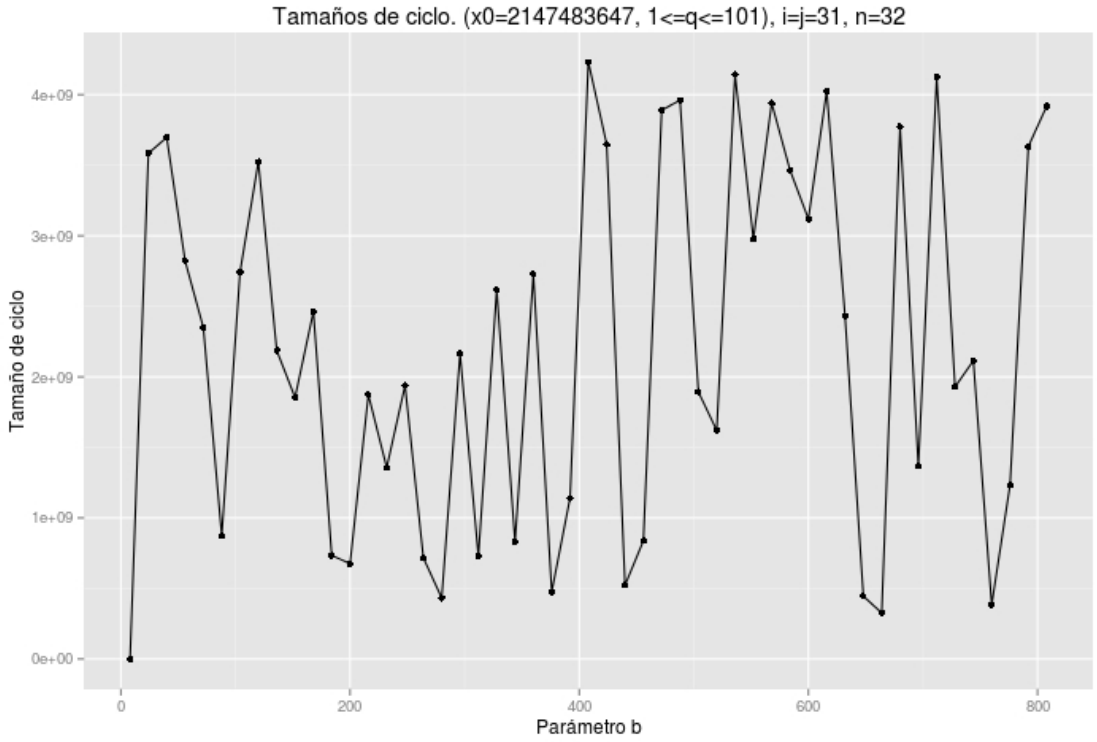

Figura 1: Mapa caótico Renyi.

De acuerdo a la gráfica anterior, **un valor de q adecuado para este caso es el siguiente:** $400 \leq q \leq 600$.

2.2. Ejemplo 1. $i = j = 5, n = 32$

Ahora, vamos a relaizar otra prueba, en este caso $i = j = 5$, los resultados obtenidos son los siguientes.

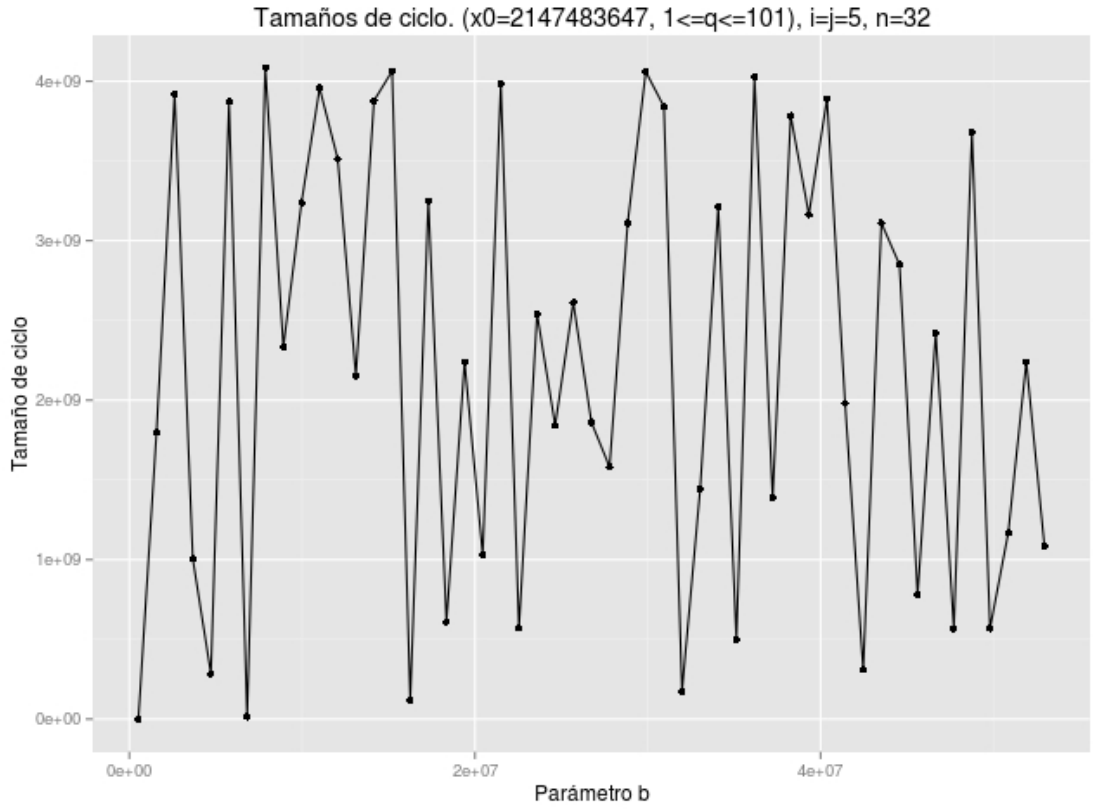

Figura 2: Mapa caótico Renyi.

Hay muchos tamaños de ciclo que son muy grandes, sin embargo, no se puede identificar un patrón específico respecto al valor de q y el cálculo de parámetro.

3. Referencias.

Referencias

[1] A. Fort A. Pasini S. Rocchi T. Addabbo, M. Alioto and V. Vignoli. A class of maximum-periodo nonlinear congruential generators derived from the rényi chaotic map. *IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS*, 54(4):816–828, 2007.