***Abstract*—**

***Index Terms*—Monte Carlo, congruencia lineal, pseudo-aleatoriedad , estocástico,**

I. Introducción

Antes de la aparición de las computadoras y su capacidad de cálculo en procesos estocásticos, existieron diferentes métodos para la generación de números aleatorios, estos estaban basados en procedimientos mecánicos que generaban enormes tablas de números (Tippett, Kendall y Babbington, Rand Corporation, etc). Más adelante al rededor de los anõs 50 del siglo pasado aparecen técnicas matemáticas para la simulación de variables aleatorias y procesos no deterministas, dicho método lleva por nombre Monte Carlo.

Por otro lado existen dos tipos de generadores para números aleatorios, los que se basan en fenómenos físicos tales como el ruido atmosférico, que tiene un alto grado de entropía (ya que no se conocen las condiciones iniciales que generan estos ruidos), estos son denominados generadores de verdaderos números aleatorios (TRNG),en contrariedad con este método los generadores pseudoaleatorios (PRNG) [1], necesitan de un estado inicial para generar los números mediante una secuencia algorítmica, por esto carecen de entropía, es decir, si se conoce el estado inicial es muy probable que se pueda recalcular una secuencia de números, es por esto que un buen generador pseudoaleatorio debe de incorporar algún grado de entropía dentro de su ecuación,por lo tanto este tipo de técnica debe de incluir alguna complejidad adicional.

En este proyecto utilizaremos métodos de congruencia lineal y no lineal [2] para la generación de nuestros números pseudoaleatorios y compararemos los datos obtenidos para cada uno de estos algoritmos.

II. Estado del arte

En el artículo Random Number Generation: Types and Techniques [2] se describe dos métodos de generación de números aleatorios, la primera se basa en tomar como modelo fenomenos del entorno fisico cuyos patrones no son aleatorios, hay quienes discrepan sobre esta aleatoriedad, ya que para que se dé un fenómeno debe de existir efectos que lo causen, si se llegara a conocer las condiciones iniciales que causan estos fenómenos, estos dejarían de ser no deterministas, sin embargo, esto es casi imposible ya que los factores causantes de un fenómeno son prácticamente infinitos, esto se puede describir como un efecto mariposa, es decir, que si se produjera una pequeña perturbación en las condiciones iniciales los cambios en los fenómenos de la naturaleza serían enormes. Entre los fenómenos físicos tomados como fuente de aleatoriedad tenemos: ruido atmosférico, decaimiento radiactivo, lasers y circuitos osciladores.

Por otro lado también existen generadores que no dependen de fenómenos de la realidad, a estos se los conoce como generadores pseudoaleatorios, estos generadores en principio parecen producir secuencias aleatorias para cualquiera que no conozca el valor inicial secreto. En un generador pseudoaleatorio básico, el valor inicial es el único factor en que se introduce la entropía al sistema. A diferencia de los verdaderos generadores de números aleatorios (que toman la entropía de un fenómeno y lo transforman en números), un generador pseudoaleatorio necesita encontrar alguna entropá para mantenerse impredecible. Las tácticas clásicas para lograr esto incluyen tomar la hora del día, la ubicación del mouse o la actividad en el teclado, esto no nos asegura que alguien no pueda replicar una secuencia conociendo los valores iniciales, ya que un humano puede replicar estas tácticas. Un generador pseudoaleatorio confiable es aquel que no nos permite replicar con facilidad una secuencia de números, este debe de tener variables intermedias que no puedan determinarse con facilidad.

El método de congruencia lineal de Lehmer [3] es uno de los métodos más conocidos para la generación de números pseudoaleatorios, consiste en escoger convenientemente una semilla $X0$, un multiplicador

III. Diseño del experimento

-

modificando el archivo

Acknowledgment

References

[1] David DiCarlo (2012), Random Number Generation: Types and Techniques, [archivo PDF]. Disponible en: https://pdfs.semanticscholar.org

[2] James E. Gentle, Random Number Generation and Monte Carlo Methods, 2da ed., Estados Unidos, 2005, pp.11–38.

[3]