

Generador mediante el algoritmo **Tausworthe**

Est. Douglas Bryan Sarmiento Basurto

Asignatura: Simulación, P60



Generador de Tausworthe - Consideraciones

Se basa en la utilización de bits para generar números pseudoaleatorios.

- Guarda relación con métodos criptográficos.
- Pueden obtener secuencias de longitud considerable.
- Tienen un periodo máximo de $2^q - 1$



Generador de Tausworthe - Pasos (I)

1. Se define un valor "**r**", y una secuencia inicial de "**q**" dígitos binarios. ($B_1, B_2, B_3, \dots, B_q$)

Se tiene que tener en cuenta que el valor de "r" debe ser menor a "q".

2. Posteriormente, se continúa con la secuencia, teniendo en cuenta la siguiente fórmula:

$$B_i = (B_{i-r} + B_{i-q}) \bmod 2 = B_{i-r} \text{ XOR } B_{i-q} \quad 0 < r < q$$



Generador de Tausworthe - Pasos (II)

Recordando las reglas de XOR, tenemos que:

B_{i-r}	B_{i-q}	$B_{i-r} \text{ XOR } B_{i-q}$
0	0	0
0	1	1
1	0	1
1	1	0

Por lo tanto, los valores de B_i serían:

$$B_i = \begin{cases} 0 & B_{i-r} = B_{i-q} \\ 1 & B_{i-r} \neq B_{i-q} \end{cases}$$



Generador de Tausworthe - Pasos (III)

3. Se transforman los números binarios a valores entre 0 y 1.

Para ello se utiliza la siguiente fórmula:

$$\frac{l}{2^l}$$

donde, "l" es una cantidad determinada de bits sobre los que se dividirá la secuencia generada.



Generador de **Tausworthe** - Ejemplo (I)

Hója de cálculo: [Click aquí](#)

Cuaderno de Jupyter: [Click aquí](#)

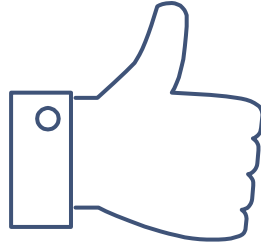


Referencias bibliográficas

[1] L. Q. Aguilera, “Generación de números aleatorios”, Docplayer.es, 2017. [En línea]. Disponible en: <https://docplayer.es/22534154-Generacion-de-numeros-aleatorios.html>. [Consultado: 29-abr-2022].

[2] M. Schlenker, “Generating uniform random numbers - OMSCS notes”, Omscs-notes.com. [En línea]. Disponible en: <https://www.omscs-notes.com/simulation/generating-uniform-random-numbers/>. [Consultado: 29-abr-2022].

[3] C. Alexopoulos y D. Goldsman, “Generating Uniform Random Numbers”, Gatech.edu, 2009. [En línea]. Disponible en: <https://www2.isye.gatech.edu/~sman/courses/Mexico2010/Module06-RandomNumberGeneration.pdf>. [Consultado: 29-abr-2022].



¡Gracias!

Carrera de Computación
Douglas Bryan Sarmiento Basurto
dsarmientob1@est.ups.edu.ec