

Generadores pseudoaleatorios

Alberto Benavides
6 de octubre de 2020

1. INTRODUCCIÓN

Una máquina es determinista y, por sí misma, no puede generar números aleatorios. Existen estrategias para conseguirlo, como las utilizadas por RANDOM.ORG [1] que lo hace a partir de ruido ambiental. De todas formas, existen algoritmos que se utilizan para generar números pseudoaleatorios. Entre ellos figuran un generador definido por el *método de Box–Muller* o el llamado *generador lineal congruencial*.

2. MÉTODO BOX–MULLER

El método de Box–Muller parte de dos números pseudoaleatorios u_1 y u_2 obtenidos de una distribución uniforme con media 0 y desviación estándar 1. Estos valores u_1, u_2 son usados para generar dos números independientes

$$z_0 = \sqrt{-2 \log(u_1) \cos(2\pi u_2)}$$

$$z_1 = \sqrt{-2 \log(u_1) \sin(2\pi u_2)}$$

según el pseudocódigo descrito en la entrada dedicada a Box–Muller en Wikipedia [2], que luego serán multiplicados por una desviación estándar σ y se les sumará una media μ para generar números pseudoaleatorios provenientes de una distribución normal.

2.1. DIFERENCIA CUALITATIVA ENTRE z_0 Y z_1

Lo primero que se desea experimentar es si los valores obtenidos a partir de z_0 y z_1 son cualitativamente distintos. Para ello, se realiza un experimento en el que se obtienen 100000 pares de valores obtenidos por este algoritmo con $\mu = 7$ y $\sigma = 3$. Los diagramas de cajas y bigotes, mostrados en la figura 2.1 (p. 3), evidencian la similitud de los valores generados por ambos números z_0, z_1 .

2.2. CAMBIOS EN DISTRIBUCIONES DE u_1 Y u_2

Se probará ahora utilizar otras distribuciones de las que partan los valores de u_1 y u_2 . Se prueban las distribuciones normal, binomial y Poisson, normalizando posteriormente los valores obtenidos de cada distribución entre $[0, 1]$. Se comparan entre sí los diagramas de cajas y bigotes de estos resultados utilizando sólo los generados a partir de las z_0 s de cada distribución, lo cual puede revisarse en la figura 2.2 (p. 4).

2.3. VALORES DEPENDIENTES PARA u_1 Y u_2

Por último, se explora cómo se comportan los números generados cuando u_2 depende de u_1 . Se exploran las siguientes dependencias:

1. $u_2 = 1 - u_1$,
2. $u_2 = u_1/2$,
3. $u_2 = 0.1u_1$,
4. $u_2 = 0.9u_1$.

Los resultados para cada z_0, z_1 de estas dependencias se muestran en la figura 2.3 (5). Como puede constatarse, cuando los valores de u_1 y u_2 son dependientes, los números generados z_0, z_1 tienen distribuciones distintas que varían según la dependencia entre las variables.

3. CONCLUSIONES

Mientras los valores generadores u_1, u_2 sean independientes, los números pseudoaleatorios generados a partir de z_0, z_1 mantienen distribuciones similares, contrario a lo que sucede cuando u_1, u_2 no son independientes entre sí.

REFERENCIAS

- [1] RANDOM.ORG. RANDOM.ORG – True Random Number Service. <https://www.random.org>, 2020.
- [2] Wikipedia. Box-Muller transform. https://en.wikipedia.org/wiki/Box%E2%80%9393Muller_transform, 2020.

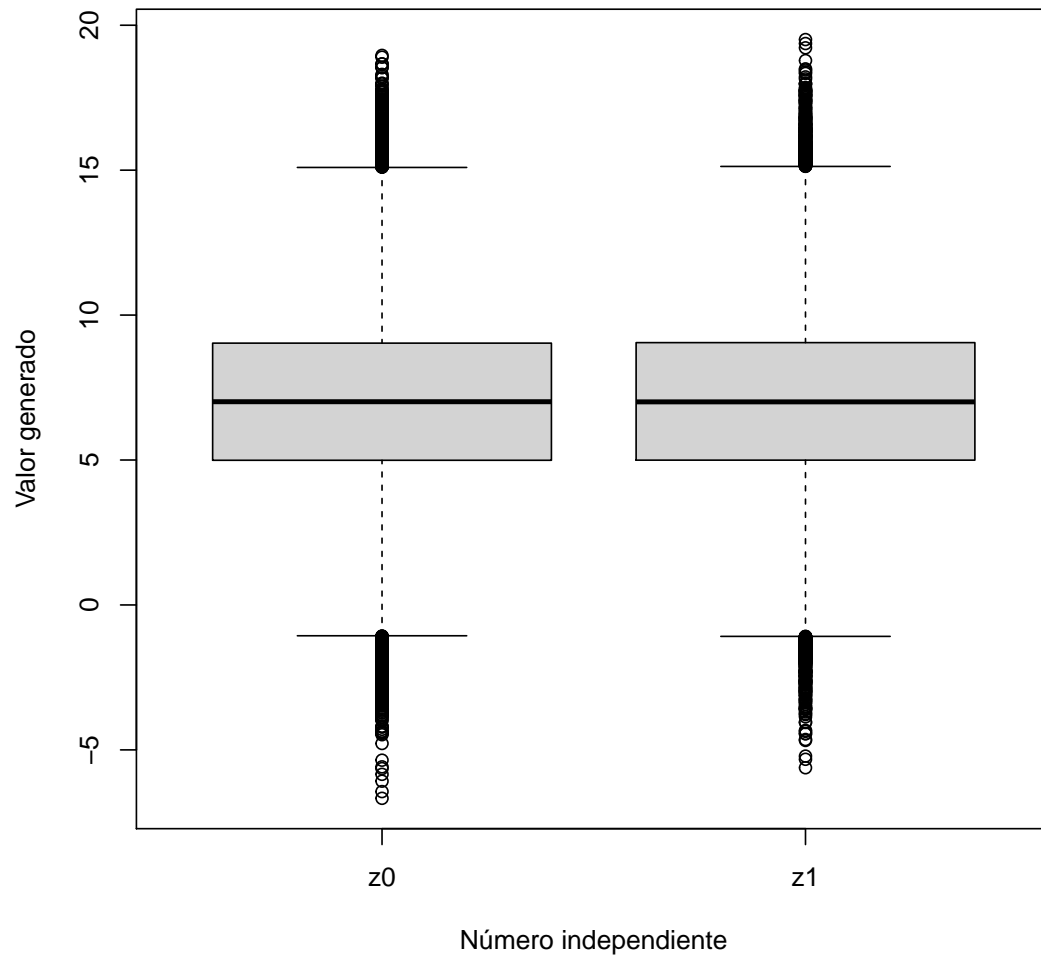


Figura 2.1: Diagramas de cajas y bigotes de 100000 valores generados de dos números independientes z_0, z_1 a partir de un algoritmo que parte del método de Box–Muller.

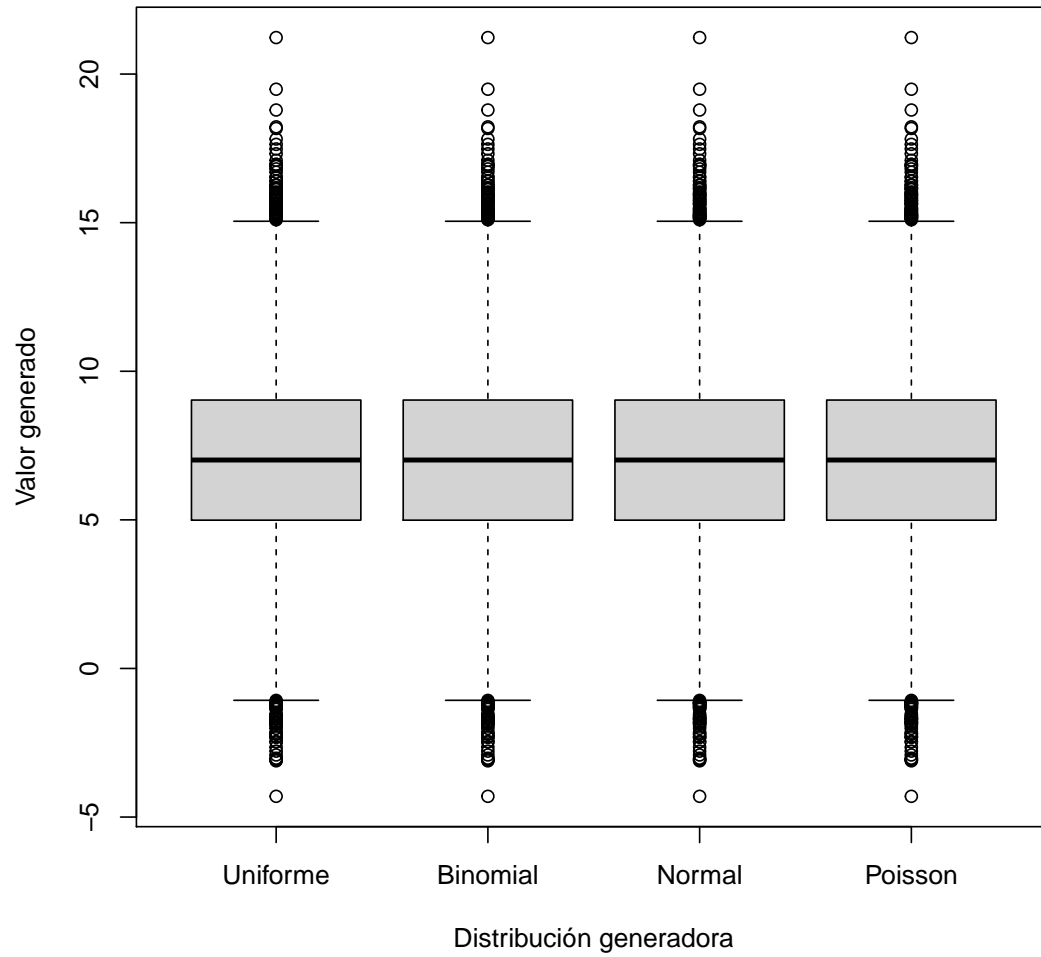


Figura 2.2: Diagramas de cajas y bigotes de 10000 valores generados de un números independientes z_0 a partir de un algoritmo que parte del método de Box–Muller con u_1, u_2 generados a partir de distintas distribuciones.

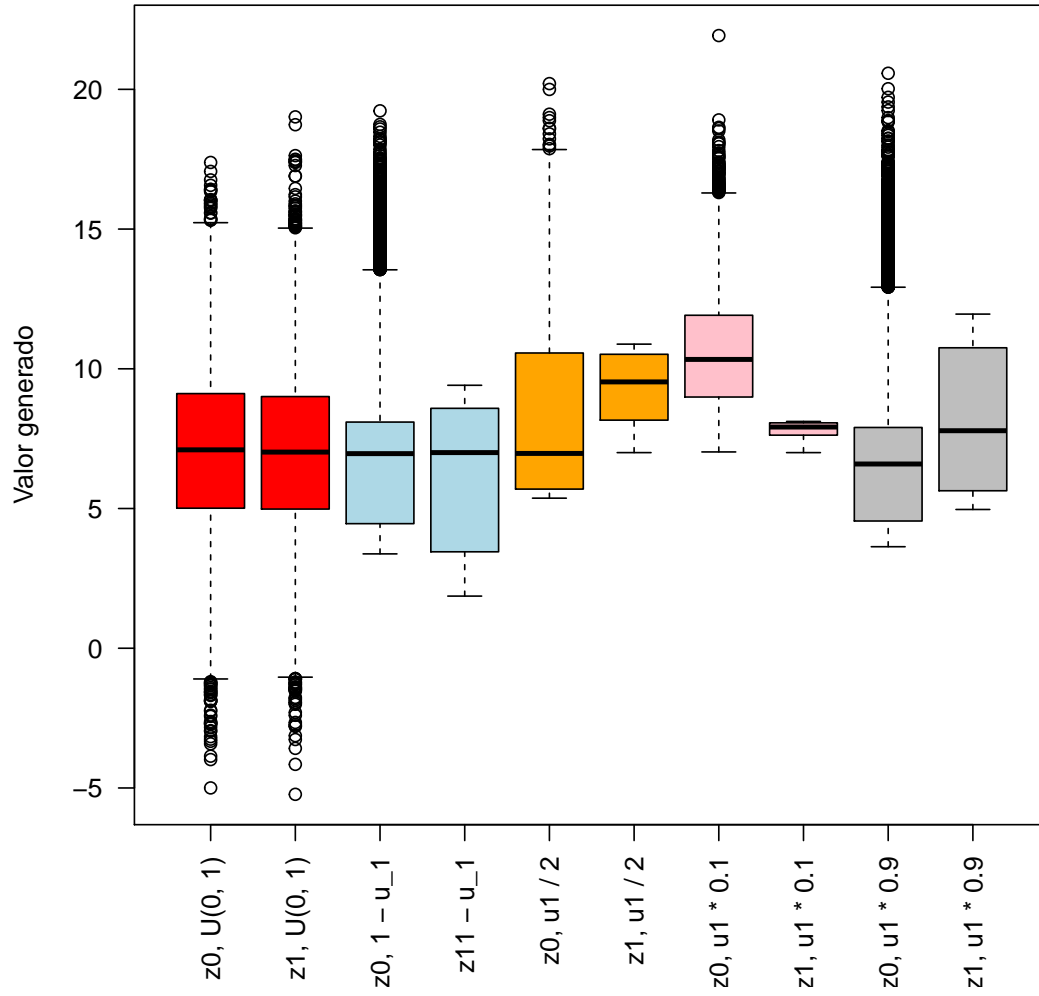


Figura 2.3: Diagramas de cajas y bigotes de 10000 valores generados de un números independientes z_0, z_1 a partir de un algoritmo que parte del método de Box-Muller con u_2 generado a partir de u_1 .