

Pruebas a generadores de números aleatorios

Maicol Parrado Rodríguez

March 7, 2016

Abstract

A random number generator 'RNG' is a computational or physical device designed to generate a sequence of numbers or symbols that can not be reasonably predicted better than by a random chance. The Kolmogorov-Smirnov test (KS-test) tries to determine if two datasets differ significantly. The KS-test has the advantage of making no assumption about the distribution of data. Chi-square is a statistical test commonly used to compare observed data with data we would expect to obtain according to a specific hypothesis. The Wald Wolfowitz run test is a non-parametric test or method that is used in cases when the parametric test is not in use. In this test, two different random samples from different populations with different continuous cumulative distribution functions are obtained

1 Introducción

Desde la antigüedad el tema de la aleatoriedad ha sido un asunto de bastante importancia tanto desde el punto de vista de la teoría como del punto de vista filosófico. La mayoría de generadores de números aleatorios que se usan en la actualidad utilizan lo que se llama "secuencias aleatorias" pero en realidad no son más que el resultado de algoritmos deterministas, por lo que técnicamente se les denomina generadores de números pseudoaleatorios. Estos generadores a veces contienen secuencias que no muestran una aleatoriedad suficiente y generan repeticiones, que no pasan algunos test de aleatoriedad. El uso de malos generadores de números aleatorios, debido a su falta de aleatoriedad puede dar lugar a experimentos erróneos.

2 Procedimiento y resultados

2.1 Randu

$$X_{i+1} = 65539X_i \bmod 2^{31}$$

- Test de Kolmogorov-Smirnov

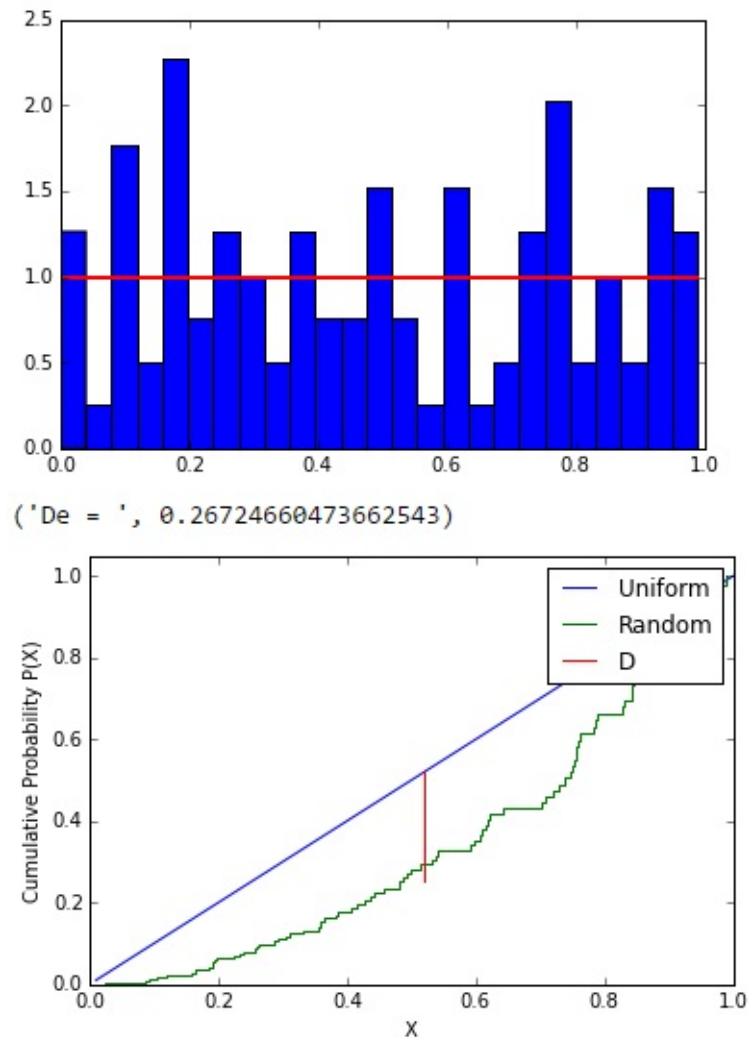


Figure 1:

- Test de Chi cuadrado. 6.919999999999998 Como el estimado = 6.92 es menor que el valor proporcionado por la tabla $T = 18.307$, SE ACEPTA LA UNIFORMIDAD DE LA SECUENCIA DE VALORES.
- Test de rachas. Rachas = [' ', 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1]

Numero de rachas de la secuencia = 61

2.2 Numerical reciepes

$$xi + 1 = 1664525xi + 1013904223 \bmod 23$$

- Test de Kolmogorov-Smirnov

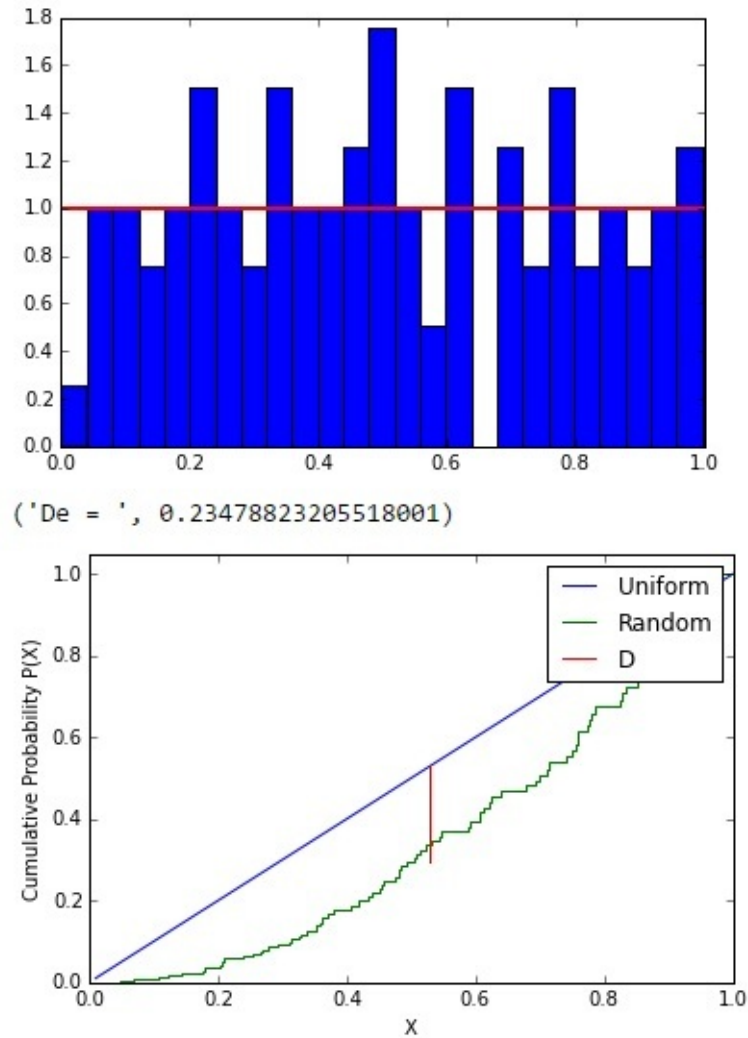


Figure 2:

- Test de Chi cuadrado. 5.1599999999999 Como el estimado = 5.16 es menor que el valor proporcionado por la tabla $T = 18.307$, SE ACEPTA LA UNIFORMIDAD DE LA SECUENCIA DE VALORES.
 - Test de rachas. Rachas = [' ', 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0]
- Numero de rachas de la secuencia = 60

2.3 Borland C/C++

$$xi + 1 = 22695477xi + 1 \bmod 232$$

- Test de Kolmogorov-Smirnov

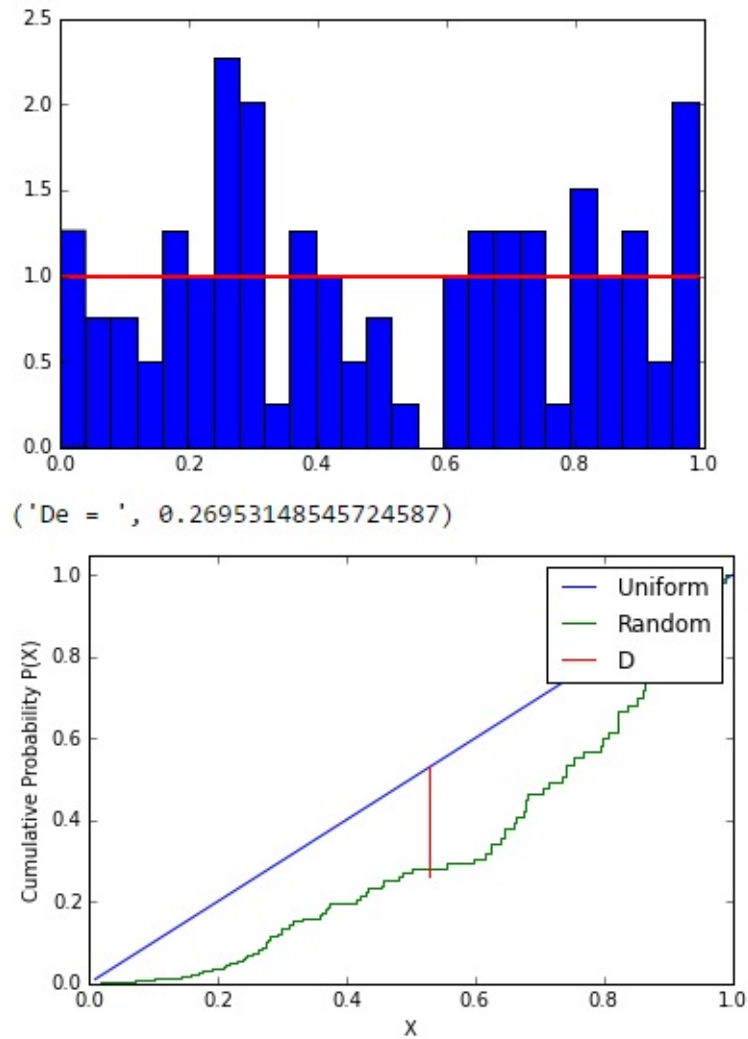


Figure 3:

- Test de Chi cuadrado. 9.5599999999999 Como el estimado = 9.56 es menor que el valor proporcionado por la tabla $T = 18.307$, SE ACEPTA LA UNIFORMIDAD DE LA SECUENCIA DE VALORES.
- Test de rachas. Rachas = [' ', 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1]

Numero de rachas de la secuencia = 67

2.4 Sinclair ZX81

$$xi + 1 = 75ximod(216 + 1)$$

- Test de Kolmogorov-Smirnov

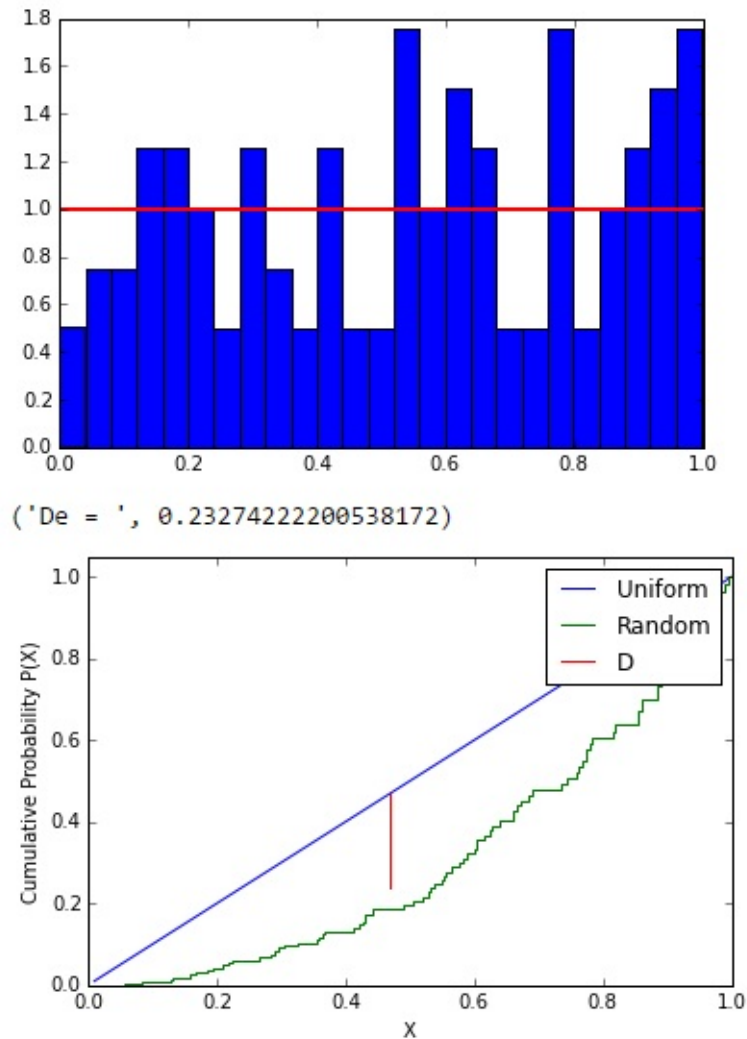


Figure 4:

- Test de Chi cuadrado. 5.8199999999999 Como el estimado = 5.82 es menor que el valor proporcionado por la tabla T = 18.307, SE ACEPTA LA UNIFORMIDAD DE LA SECUENCIA DE VALORES.
- Test de rachas. Rachas = [' ', 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1,

0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1,
1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1]

Numero de rachas de la secuencia = 71

3 Referencias

- David Ríos, Sixto Ríos, Jacinto Martín. Simulación, Métodos y aplicaciones. Editorial Alfaomega, 2000.