Università di Catania

Metodi Matematici e Statistici

Test for Python's Numbers Generator

Autore:
Marco Ardizzone

Matricola:
X81001077

March 2021

Contents

1 Introduction **2**

2 Python PRNG: Mersenne Twister **2**

3 Uniformity Test **2**
3.1 Chi-Squared Test 3
3.2 Uniformity Test Results 4

4 Up and Down Test **5**
4.1 Up and Down Test Results 6

5 Conclusion **6**

References **7**

1 Introduction

*Pseudo*random numbers are used for so many purposes, such as gambling, banking and internet security. But does Python's Numbers Generator produce numbers which follow a Uniform Distribution? This project is meant to test this, using a *Uniformity Test* and an *Up and Down Test*. Source code from this project is available here

2 Python PRNG: Mersenne Twister

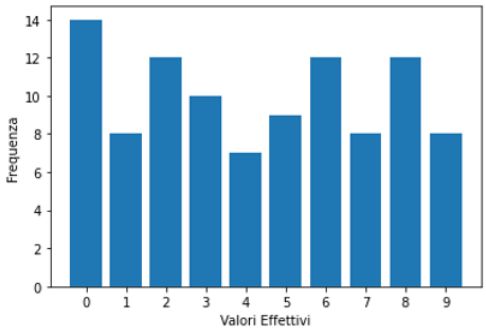
Python's PRNG algorithm is *Mersenne Twister*. This algorithm has a very long period $T = 2^{19937} - 1$, a necessary condition for having a great PRNG. Its function is reversible, which is not safe cryptographically speaking, but it makes the algorithm very efficient in computation [1] [2].

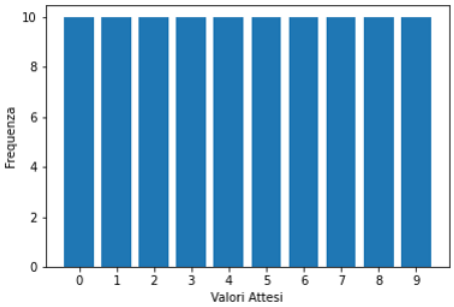
3 Uniformity Test

For testing whether or not the output of Python's PRNG is random, a χ^2 test is performed. It is used to check whether a population follows a given distribution [3]. In this case, a Uniform Distribution.

3.1 Chi-Squared Test

It splits the set $[0, 9]$ in k subsets (in this case, $k = 10$). It must be prove that there are the same number of elements in each subset.





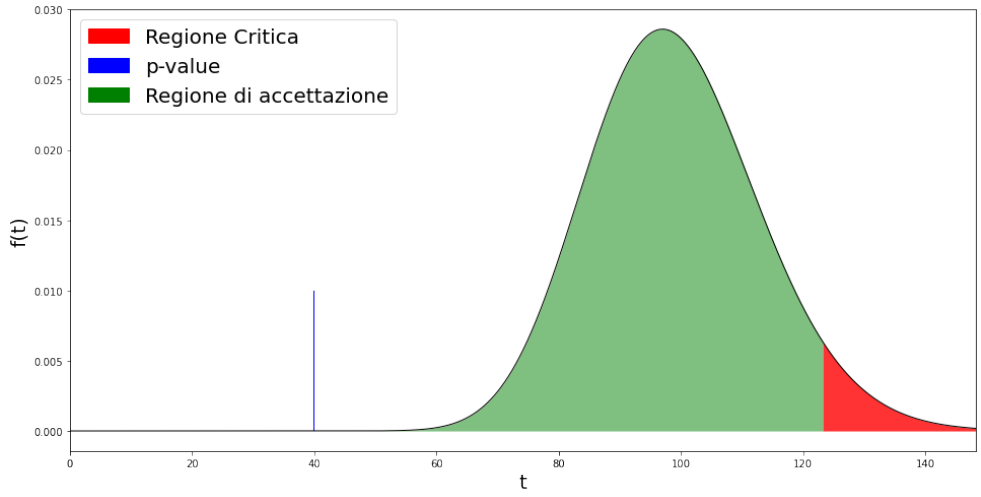
We assume X_i is the i-th element from the sample, O_i is the count of observations and A_i is the expected count. Let us introduce W as:

$$W = \sum_{k=1}^{K} \frac{(O_k - A_k)^2}{A_k}$$

If null hypotesis is true, so these numbers follow a Uniform Distribution, and W follows a χ^2 with $k - 1$ degrees of freedom. Null hypotesis is accepted if $W < W_{1-alpha}$, where $W_{1-alpha}$ is $1 - alpha - th$ quantile, where the reject region begins. For ease we introduce *p-value*, the area under the curve is $[W, +\infty[$. Null hypotesis is accepted if $p - value > alpha$.

3.2 Uniformity Test Results

Using 6*stats*'s library from *scipy* a chi squared test was performed to 100 random numbers. It outputted $W = 0.12599999$ and a $p-value = 0.9999999282$, so we can state that the numbers have been generated following a Uniform Distribution, the error chance is 5%.



It is possible to graphically notice that p-value stays in region of acceptance.

4 Up and Down Test

This test is meant to prove whether a given series is random generated or whether it follows a specific pattern. Given a series L of random numbers, we write a 1 if $x_i < median(L)$, 0 otherwise. A great random number generator must not produce long runs [4].
Let introduce Z as:

$$Z = \frac{R - \bar{R}}{S_R}$$

Where R is the number of observed run and $\bar{R}$ is the number of expected run, so:

$$\bar{R} = \frac{2n_1n_2}{n_1 + n_2} + 1$$

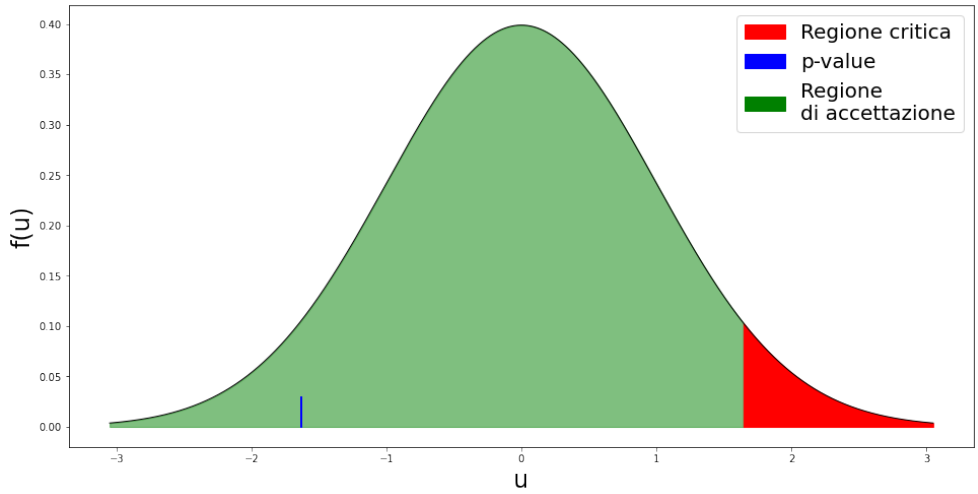
And S_R is standard deviation, so:

$$S_R^2 = \frac{2n_1n_2(2n_1n_2 - n_1 - n_2)}{(n_1 + n_2)^2(n_1 + n_2 - 1)}$$

Where n_1 and n_2 are, respectively, the count of 1 and 0 given from the test [5].
Null hypotesis, the numbers does not follow any pattern, is accepted at confidence level $1 - alpha\%$ if $Z < Z_{1-alpha}$.
Where $Z_{1-alpha}$ is $1 - alpha - th$ quantile, where the reject region begins [6].

4.1 Up and Down Test Results

Using *math* e *statistics* libraries we obtained $Z = 0.89915847$ and $Z_{1-alpha} = 0.94915847$, since $Z < Z_{1-alpha}$, we can state that our numbers are generated not following any pattern at confidence level $1 - alpha\%$



It is possible to graphically notice that p-value stays in region of acceptance.

5 Conclusion

It was proved that Python's PRNG generates numbers which follow an Uniform Distribuition and don't follow any pattern, so we can state its algorithm (Mersenne Twister) is a great PRNG.

References

[1] Wikipedia : Mersenne Twister
https://en.wikipedia.org/wiki/Mersenne_Twister

[2] Cryptologie.net : How does the Mersenne Twister work
https://www.cryptologie.net/article/331/how-does-the-mersennes-twister-work/

[3] Orazio Muscato : Metodi Matematici e Statistici
https://www.dmi.unict.it/muscato/MMStat.pdf

[4] Kinds on the Genius : What is Run Test
https://kindsonthegenius.com/blog/what-is-run-test-in-statistics
-a-simple-explanation-with-step-by-step-examples/

[5] Wikipedia : Wald Wolfowitz Run Test
https://en.wikipedia.org/wiki/Wald-Wolfowitz_runs_test

[6] Geeks for Geeks : Runs test of Randomness in Python
https://www.geeksforgeeks.org/runs-test-of-randomness-in-python/