PRNG - Statistical testing

Maciej Szczutko

2024-12-11

Statistical test description

Testing binary expansion of constans

In this section we perform frequency monobit test for number $\pi, e, \sqrt{2}$. More formally we will use their binary expansion as the random bit sequence. We use provided files with binary expansions. For inference we will follow instruction from official **NIST** report.

Some important notes from report about most basic test.

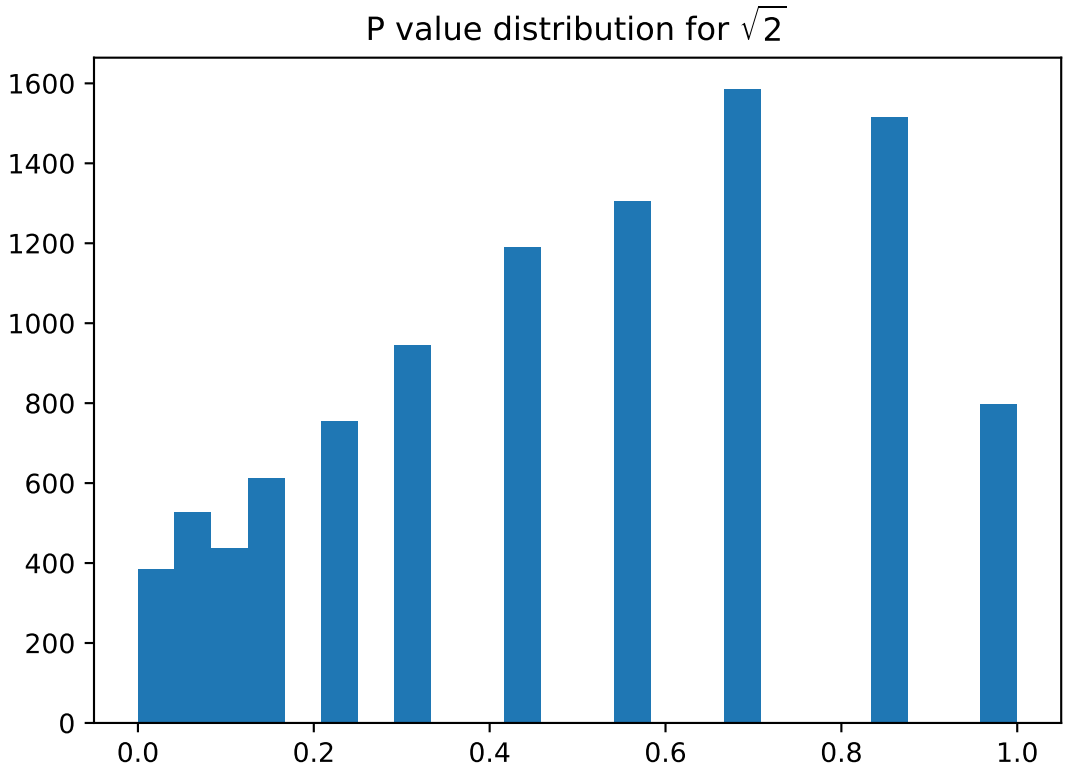
> 2.1.5 Decision Rule (at the 1% Level)
>
> If the computed P-value is < 0.01, then conclude that the sequence is non-random. Otherwise, conclude that the sequence is random.
>
> 2.1.7 Input Size Recommendation
>
> It is recommended that each sequence to be tested consist of a minimum of 100 bits (i.e., $n \geq 100$).

Constant name	p_{value}	Input Size
π	0.612315825298478	1004858
e	0.928460306674579	1004858
$\sqrt{2}$	0.817749242838411	1004859

The size of out data is aligned with **NIST** recommendations. Authors recommend 0.01 as significance level for PRNG testing. From above table we conclude that binary expansion of each mentioned constants could be considered as random bit sequence.

Because the size of sample are quite big we can try another approach. We split the sequence into a lot of smaller samples. We use the smallest recommended $n = 100$ for this test. The split method will be very straightforward. We simply take first 100 bits for first sample, another 100 for second sample and so on.

```
## (array([ 385.,  526.,  436.,  612.,    0.,  754.,    0.,  944.,    0.,
##            0., 1190.,    0.,    0., 1304.,    0.,    0., 1585.,    0.,
##            0.,    0., 1514.,    0.,    0.,  798.]), array([2.66914980e-05, 4.16922460e-02, 8.33578005e
##         1.66688910e-01, 2.08354464e-01, 2.50020019e-01, 2.91685573e-01,
##         3.33351128e-01, 3.75016682e-01, 4.16682237e-01, 4.58347791e-01,
##         5.00013346e-01, 5.41678900e-01, 5.83344455e-01, 6.25010009e-01,
##         6.66675564e-01, 7.08341118e-01, 7.50006673e-01, 7.91672227e-01,
##         8.33337782e-01, 8.75003336e-01, 9.16668891e-01, 9.58334445e-01,
##         1.00000000e+00]), <BarContainer object of 24 artists>)
```


P value distribution for $\sqrt{2}$
1600
1400
1200
1000
800
600
400
200
0
0.0
0.2
0.4
0.6
0.8
1.0