PRNG - Statistical testing

Maciej Szczutko

2024-12-10

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

NIST 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.