Analysis of the Discrete Fourier Transform statistical test

Asandoaiei David, Anghel Florin, Tabacaru Robert

Faculty of Computer Science
Alexandru Ioan Cuza University
Iasi, Romania

January 2022

Pseudo Random Number Generators

- Produces a sequence of bits that are uniquely determined.
- Initial value is called a seed.
- Output should be statistically indistinguishable from random values.

Applications of PRNGS

Random numbers are very useful in a variety of cryptographic applications, such as :

- key generation
- nonces
- salts in some signature schemes

Some protocols require a higher "quality" of randomness !

Requirements of Cryptographically Secure PRNGS

Every Cryptographically Secure PRNG should :

- Pass the *next-bit* test.
- Withstand *state compromise extensions*.

The Discrete Fourier Transform (Spectral) Test

The focus of this test is the peak heights in the Discrete Fourier Transform of the sequence. The purpose of the *DFT* test is to detect periodic features such as repetitive patterns that are near each other, in the tested sequence that would indicate a deviation from the assumption of randomness. We can try to achieve this purpose by detecting whether the number of peaks exceeding the 95% threshold is significantly different than 5%.

The Discrete Fourier Transform (Spectral) Test

- Function call : *DiscreteFourierTransform*(n)
  - n represents the length of the bit string
  - The function could take an additional parameter ϵ representing the sequence of bits generated by the *RNG* or *PRNG* being tested ; this exists as a global structure at the time of the function call : $\epsilon = \epsilon_1, \epsilon_2, ..., \epsilon_n$.

The Discrete Fourier Transform (Spectral) Test

- Test Statistic and Reference Distribution
  - We will denote d as the normalized difference between the observed and the expected number of frequency components that are beyond the 95% threshold
  - The reference distribution for the test statistic is the normal distribution

The Discrete Fourier Transform (Spectral) Test

- Test Description
  1. The zeros and ones of the input sequence (ϵ) will be converted into -1 and 1, obtaining the sequence $X = x_1, x_2, ..., x_n$, where $x_i = -1$ if $\epsilon_i = 0$ or $x_i = 1$ if $\epsilon_i = 1$.
  2. A Discrete Fourier Transform (DFT) is applied to X to produce $S = DFT(X)$.
  3. M is calculated as $M = modulus(S')$, where S' represents the sequence of the first $n/2$ elements in S and *modulus* function produces a sequence of peak heights.
  4. Calculate $T = \sqrt{(\log \frac{1}{0.05})n}$, which represents the 95% peak height threshold value. Under the assumption of randomness, 95% of the values obtained from the test should not exceed T.
  5. Calculate $N_0 = 0.95n/2$, which represents the expected theoretical (95%) number of peaks that are less then T (under the assumption of randomness).
  6. Calculate N_1 which is the actual number of peaks in M that are less than T.
  7. Compute $d = \frac{N_1 - N_0}{\sqrt{n(0.95)(0.05)/4}}$.
  8. Compute P-value $= erfc(\frac{|d|}{\sqrt{2}})$, where $erfc$ represents the complementary error function : $erfc(z) = \frac{2}{\sqrt{\pi}} \int_z^{\infty} e^{-u^2} du$.

The Discrete Fourier Transform (Spectral) Test

- With the final P-value resulted, we can conclude if a sequence is or is not random. If the P-value< 0.01 then the sequence is non considered random, otherwise the sequence is considered random.
- It is recommended that each sequence to be tested should consist of a minimum of 1000 bits ($n \geq 1000$).

Preliminaries

It is important to establish some preliminaries about the NIST STS before we move on.

- The main result of each individual test on a sequence comes in form of a $p - value$. This value represents the probability that a truly random sequence is less random than the one being tested.
- Each tested sequence passes as random if the resulting $p - value \geq 0.01$.
- For a test on multiple sequences, we will look at the uniformity of $p - values$ and the proportion of sequences that pass the test.

Hypothesis testing

- The null hypothesis H_0 - a certain sequence is random.
- The alternative hypothesis H_a - a certain sequence is not random.
- NIST's suite focuses on determining the probability of Type I errors. This probability is often denoted by α and its value is usually set to 0.01

Hypothesis testing

1. The input data is random.
   1. And our statistical test confirms that it is (accepts H_0). (desired behaviour)
   2. And our statistical test fails, accepting H_a. (Type I error)
2. The input is not random.
   1. And our statistical test states that it is random. (Type II error)
   2. And our statistical test confirms that it isn't. (desired behaviour)

Type II errors

The probability of Type II (denoted by β) errors is more complex to co calculate, and it is not a fixed value. This is because in practice, non-randomness can come in many forms, resulting in different values for β. However, we can estimate it.

$$\beta \quad (p_1) = P\left(u_{\frac{\alpha}{2}} \leq \frac{N_1 - 0.95 \cdot np_0}{\sqrt{np_0q_0 \cdot 0.95 \cdot 0.05}} \leq u_{1-\frac{\alpha}{2}} \middle| p = p_1\right) =$$

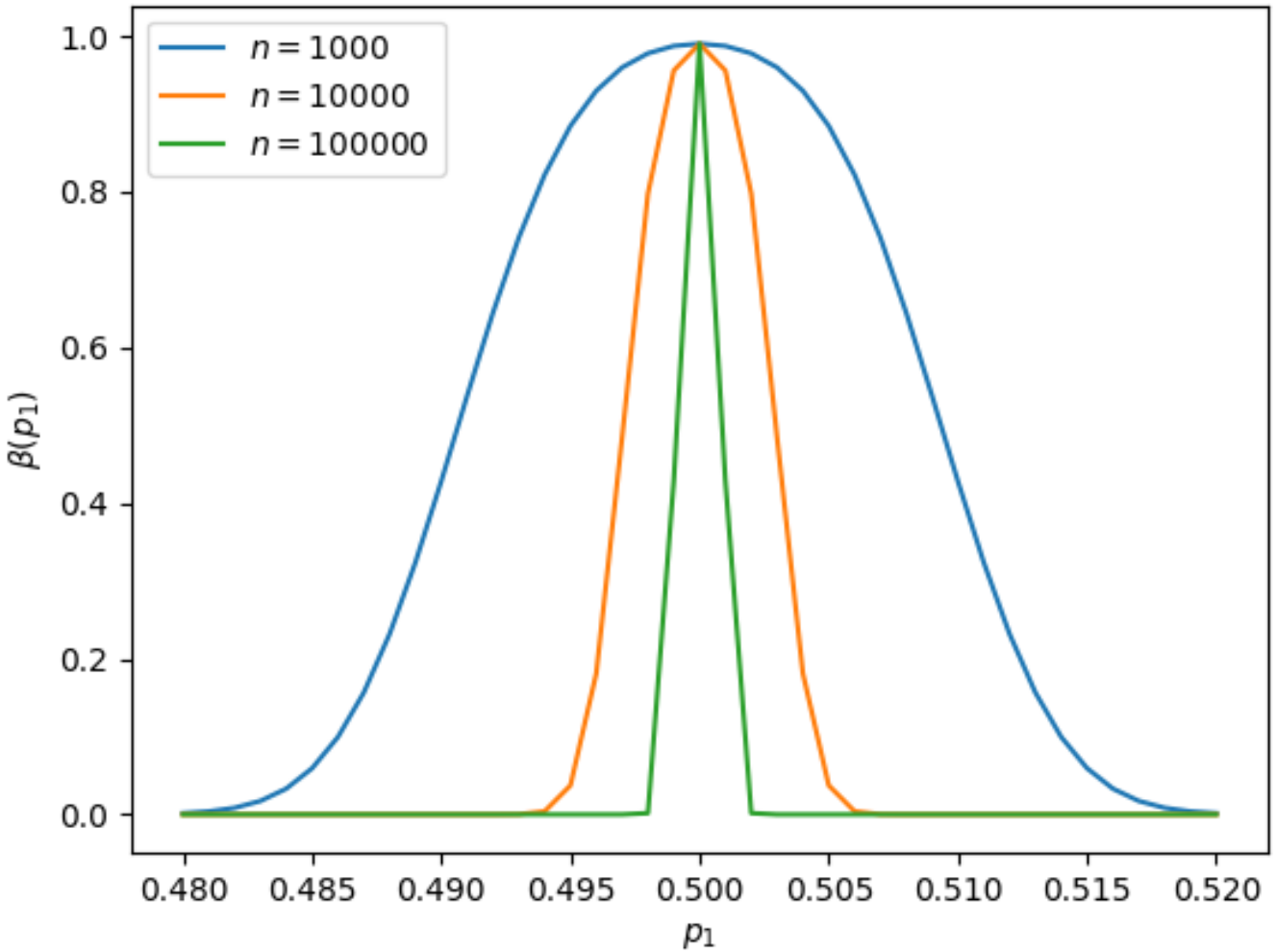
$$= P\left(u_{\frac{\alpha}{2}}\sqrt{\frac{p_0q_0}{p_1q_1}} + \frac{0.95 \cdot n(p_0 - p_1)}{\sqrt{np_1q_1 \cdot 0.95 \cdot 0.05}} \leq \frac{N_1 - 0.95 \cdot np_1}{\sqrt{np_1q_1 \cdot 0.95 \cdot 0.05}} \leq u_{1-\frac{\alpha}{2}}\sqrt{\frac{p_0q_0}{p_1q_1}} + \frac{0.95 \cdot n(p_0 - p_1)}{\sqrt{np_1q_1 \cdot 0.95 \cdot 0.05}}\right)$$

$$\simeq \Phi\left(u_{1-\frac{\alpha}{2}}\sqrt{\frac{p_0q_0}{p_1q_1}} + \frac{0.95 \cdot n(p_0 - p_1)}{\sqrt{np_1q_1 \cdot 0.95 \cdot 0.05}}\right) - \Phi\left(u_{\frac{\alpha}{2}}\sqrt{\frac{p_0q_0}{p_1q_1}} + \frac{0.95 \cdot n(p_0 - p_1)}{\sqrt{np_1q_1 \cdot 0.95 \cdot 0.05}}\right)$$

Results on the NIST STS

PRNG	s	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	$p-value$	Proportion	Result
LCG	$1k$	116	99	112	90	95	108	113	191	80	86	0.13	0.984	✓
LCG	$10k$	1098 93 1064 ... 977										0.0	0.987	××
LCG	$100k$	11196 9701 10709 ... 10034										0.0	0.987	××
CBG	$1k$	127	90	117	78	88	104	95	121	76	104	0.0008	0.981	✓
CBG	$10k$	1280 1025 1099 ... 982										0.0	0.983	××
CBG	$100k$	12611 10138 10801 ... 9796										0.0	0.984	××
GSIIA1	$1k$	102	90	122	77	113	89	93	102	117	95	0.038	0.989	✓
GSIIA1	$10k$	1085 963 1103 ... 967										0.0	0.988	×
GSIIA1	$100k$	11075 9760 10772 ... 10115										0.0	0.987	××
Micali	$1k$	118	100	99	76	117	105	92	93	87	113	0.0543	0.981	✓
Micali	$10k$	1150 967 1050 ... 1031										0.0	0.987	×
Micali	$100k$	11019 9675 10749 ... 10274										0.0	0.987	××
QDR1	$1k$	111	97	108	84	106	90	107	102	88	107	0.502	0.981	✓
QDR1	$10k$	1108 965 1014 ... 1002										0.0	0.986	××
QDR1	$100k$	11250 9819 10811 ... 10010										0.0	0.987	××
QDR2	$1k$	113	81	112	86	105	94	104	109	94	102	0.298282	0.987	✓
QDR2	$10k$	1166 935 1055 ... 1043										0.0	0.986	××
QDR2	$100k$	11296 9761 10687 ... 9984										0.0	0.987	××
XOR	$1k$	732	42	46	30	28	31	26	29	15	21	0.0	0.375	××
XOR	$10k$	3895 874 787 ... 635										0.0	0.737	××
XOR	$100k$	4942 1220 1154 ... 988										0.0	0.968	××
BBS*	100	13	6	6	7	9	14	12	13	4	16	0.0855	1	✓
BBS*	$1k$	111	117	76	100	102	123	67	132	74	98	0.000002	0.993	×

Type II error calculation



Conclusions and Future Work

Based on our experimental results, we can draw the following conclusions :

1. The current version of the DFT statistical test can still be improved
   1. Include the type II error probability as a metric for determining the result of the test
   2. Improve the efficiency and reliability of correct results on larger inputs.
2. A good direction for future work would be that of trying to devise estimations for type II error for improved versions of the test, and comparing the results with other tests from the NIST STS.