Extended Results for Independence and Sensitivity of NIST Randomness Tests

Ali DOĞANAKSOY, Barış EGE, Köksal MUŞ

***Abstract*—Statistical tests are of crucial importance in determining the quality of pseudo random number generators. But these tests, when used together in a test suite, should be independent to have reliable results. In this study, we evaluate the dependency of the tests in the NIST test suite by experimental results. We also analyze the sensitivity of these tests to some basic transformations.**

***Keywords* —NIST, Randomness Tests, Independence.**

I. Introduction

Pseudo random number generators (PRNGs) are used in various subjects from cryptography to simulations. In cryptography, PRNGs are needed to provide security in authentication protocols, digital signature protocols, generation of encryption keys, etc. As a result of this, the quality of a PRNG is of crucial importance when used in cryptography. Therefore the quality of a PRNG should be carefully determined.

Since a theoretical approach to show the quality of a PRNG is not feasible, statistical testing of sample sequences are used for this purpose. There are various test suites [1], [2], [3], [4], [5] in literature which are collections of statistical randomness tests to evaluate various properties of a PRNG. However, as Soto stated in [6], the tests in a statistical test suite should be independent to achieve reliable results. In [7], the correlation among *approximate entropy*, *overlapping serial* and *universal* test is shown using defective sources. Recently in [8], it is shown that *frequency*, *overlapping template*, *longest run of ones*, *random walk height* and *maximum order complexity* tests are correlated for sequences of length $n = 20$ and $n = 30$, through observing all possible sequences. Also in [8], the concept of *sensitivity of tests to simple transformations* is introduced.

In this paper, since it is not feasible to observe all possible sequences for long sequences, we apply a new approach and extend the ideas in [8] to longer sequences to evaluate the independence and sensitivity of some chosen tests from the NIST Test Suite through experimental results.

In Section II, we provide basic descriptions of the tests we used in the study and statistical ideas used in NIST Test Suite. In Sections III and IV, experimental results on the independence and sensitivity of the tests are presented respectively. In the last section, we give some concluding remarks and point out some possible future work directions.

We would like to thank Meltem Sönmez Turan and members of the SADIST Workgroup (Onur Koçak, Dilek Arslan and Cihangir Tezcan) for their comments and support on our paper.

II. NIST Test Suite

NIST Test Suite consists of a total of 16 tests which evaluate the randomness of a given sequence or a random number generator. These tests focus on a variety of non-randomness properties in a sequence. The descriptions (from [1]) of the tests used for the study in this paper are given below.

- **Frequency (Monobits) Test:** The focus of the test is the proportion of zeros and ones for the entire sequence. The purpose of this test is to determine whether that number of ones and zeros in a sequence are approximately the same as would be expected for a truly random sequence. The test assesses the closeness of the fraction of ones to $\frac{1}{2}$, that is, the number of ones and zeros in a sequence should be about the same.
- **Test for Frequency Within a Block:** The focus of the test is the proportion of zeros and ones within m-bit blocks. The purpose of this test is to determine whether the frequency of ones is an m-bit block is approximately $\frac{m}{2}$.
- **Runs Test:** The focus of this test is the total number of zero and one runs in the entire sequence, where a run is an uninterrupted sequence of identical bits. A run of length k means that a run consists of exactly k identical bits and is bounded before and after with a bit of the opposite value. The purpose of the runs test is to determine whether the number of runs of ones and zeros of various lengths is as expected for a random sequence. In particular, this test determines whether the oscillation between such substrings is too fast or too slow.
- **Test for the Longest Run of Ones in a Block:** The focus of the test is the longest run of ones within m-bit blocks. The purpose of this test is to determine whether the length of the longest run of ones within the tested sequence is consistent with the length of the longest run of ones that would be expected in a random sequence. Note that an irregularity in the expected length of the longest run of ones implies that there is also an irregularity in the expected length of the longest run of zeros. Long runs of zeros were not evaluated separately due to a concern about statistical independence among the tests.
- **Random Binary Matrix Rank Test:** The focus of the test is the rank of disjoint sub-matrices of the entire sequence. The purpose of this test is to check for linear dependence among fixed length substrings of the original

sequence.

- **Overlapping (Periodic) Template Matching Test:** The focus of this test is the number of pre-defined target substrings. The purpose of this test is to reject sequences that show deviations from the expected number of runs of ones of a given length. For this test, an m-bit window is used to search for a specific m-bit pattern. If the pattern is not found, the window slides one bit position. For this test, when the pattern is found, the window again slides one bit, and the search is resumed.
- **Linear Complexity Test:** The focus of this test is the length of a generating feedback register. The purpose of this test is to determine whether or not the sequence is complex enough to be considered random. Random sequences are characterized by a longer feedback register. A short feedback register implies non-randomness.
- **Serial Test:** The focus of this test is the frequency of each and every overlapping m-bit patterns across the entire sequence. The purpose of this test is to determine whether the number of occurrences of the 2^m m-bit overlapping patterns is approximately the same as would be expected for a random sequence. The pattern can overlap.
- **Approximate Entropy Test:** The focus of this test is the frequency of each and every overlapping m-bit pattern. The purpose of the test is to compare the frequency of overlapping blocks of two consecutive/adjacent lengths (m and $m+1$) against the expected result for a random sequence.
- **Cumulative Sum (Cusum) Test:** The focus of this test is the maximal excursion (from zero) of the random walk defined by the cumulative sum of adjusted $(-1, +1)$ digits in the sequence. The purpose of the test is to determine whether the cumulative sum of the partial sequences occurring in the tested sequence is too large or too small relative to the expected behavior of that cumulative sum for random sequences. This cumulative sum may be considered as a random walk. For a random sequence, the random walk should be near zero. For non-random sequences, the excursions of this random walk away from zero will be too large.

A number of tests in the test suite have the *standard normal* and the *chi-square* (χ^2) as reference distributions. If the calculated test statistic falls in extreme regions of the reference distribution, the sequence under test is considered to be non-random. The standard normal distribution (i.e., the bell-shaped curve) is used to compare the value of the test statistic obtained from the random number generator with the expected value of the statistic under the assumption of randomness. The test statistic for the standard normal distribution is of the form $z = \frac{(x-\mu)}{\sigma}$, where x is the sample test statistic value, and μ and σ^2 are the expected value and the variance of the test statistic. The χ^2 distribution (i.e., a left skewed curve) is used to compare the goodness-of-fit of the observed frequencies of a sample measure to the corresponding expected frequencies of the hypothesized distribution. The test statistic is of the form $\chi^2 = \sum \left(\frac{(o_i - e_i)^2}{e_i} \right)$, where o_i and e_i are the observed and expected frequencies of occurrence of the measure, respectively.

III. Independence of Tests

Two tests T_1 and T_2 are called independent if the corresponding p-values of these tests are independent [8]. (i.e., the p-values obtained from T_1 by applying the test to the sequences that fail T_2, should be uniformly distributed.)

Also whenever the test statistic is lower than a fixed value $\alpha = 0.01$, we will call the tested sequence a failing sequence; and we will call the set of all failing sequences of a test, the rejection region of that test.

In this section, we analyze the dependency of the NIST tests, given in the previous section, by first looking at the rejection regions of the tests and then the p-value distributions of the individual tests in this rejection regions.

Note that cusum test described in Section II outputs two p-values, one from the sequence itself and one from the inverse of the same sequence. Similarly serial test also outputs two p-values regarding one for the transition from $(m-1)$-bit templates to m-bit templates and one for the transition from $(m-2)$-bit templates to $(m-1)$ and m-bit templates.

We have analyzed the tests through $m = 10^5$ sequences of length $n = 5000$ in our study. But this n value restricted our study to the tests given in Section II since *random excursions*, *random excursion variant* and *universal* tests do not produce a p-value for this input size. Moreover, we also excluded *discrete fourier transform (spectral)* and *non-overlapping template matching* tests since the former did not produce a large enough rejection region for our inputs and the latter for ease of computation. The $(i,j)^{th}$ entry of the Table II represents the proportion of the sequences that fail T_i and T_j to the sequences that fail T_j. The expected value of this proportion is 0.01 so we marked the values greater than 0.1 to show significant deviations from this value. The parameters we used for the tests are given in Table I.

TABLE I
Parameters used for the tests.

Test Name	Block Length
Block Frequency	128
Overlapping Template Matching	9
Approximate Entropy	8
Serial	9
Linear Complexity	500

According to Table II, *frequency*, *cusum1* and *cusum2* tests are closely related. Also *approximate entropy*, *serial1* and *serial2* tests also look related from this table, however the relation values between approximate entropy and serial tests seem to be deficient since the symmetric entries of the table are expected to have similar values [8]. But the relation between serial1 and serial2 is clear from the table as well as in theory.

In addition to this, we have made another observation that even though the most of the tests look uncorrelated in Table II, the distribution of the p-values in the rejection regions of each other are usually non-uniform. So we computed the values in

TABLE II
RELATION OF THE TESTS FOR $n = 5000$ AND $m = 10^5$.

	Frequency	Block Frequency	Cumulative Sums1	Cumulative Sums2	Runs	LongestRun	Rank	Overlapping Template	Approximate Entropy	Serial1	Serial2	Linear Complexity
Frequency	-	0,0089	0,7607	0,7332	0,0161	0,1568	0,0064	0,0159	0,0168	0,0218	0,0112	0,0093
Block Frequency	0,0158	-	0,0418	0,0461	0,0122	0,0177	0,0096	0,0097	0,0108	0,0129	0,0172	0,0099
Cumulative Sums1	0,7646	0,0456	-	0,6421	0,0193	0,1475	0,0103	0,0167	0,0156	0,0198	0,0091	0,0079
Cumulative Sums2	0,782	0,0533	0,6792	-	0,0193	0,1506	0,009	0,0159	0,0164	0,0198	0,0122	0,0099
Runs	0,0164	0,0133	0,0193	0,0182	-	0,0498	0,0083	0,0115	0,02	0,0159	0,0051	0,0096
LongestRun	0,1546	0,0189	0,1446	0,1392	0,0487	-	0,0096	0,0079	0,0104	0,0248	0,0091	0,0096
Rank	0,0102	0,0167	0,0163	0,0134	0,0132	0,0156	-	0,0141	0,0128	0,0089	0,0071	0,0152
Overlapping Template	0,0184	0,0122	0,0193	0,0175	0,0132	0,0093	0,0103	-	0,014	0,0149	0,0172	0,0116
Approximate Entropy	0,043	0,03	0,0397	0,0393	0,0508	0,053	0,0205	0,0308	-	0,9454	0,4452	0,0243
Serial1	0,0225	0,0144	0,0204	0,0192	0,0163	0,026	0,0058	0,0132	0,3806	-	0,2951	0,011
Serial2	0,0113	0,0189	0,0092	0,0115	0,0051	0,0093	0,0045	0,015	0,1753	0,2887	-	0,0093
Linear Complexity	0,0318	0,0089	0,0285	0,0336	0,0345	0,0153	0,0347	0,0161	0,0343	0,0387	0,0335	-

TABLE III
DISTRIBUTIONS OF p-VALUES IN THE REJECTION REGIONS OF EACH OTHER.

	Frequency	Block Frequency	Cumulative Sums1	Cumulative Sums2	Runs	LongestRun	Rank	Overlapping Template	Approximate Entropy	Serial1	Serial2	Linear Complexity
Frequency	0	0	0	0	0,503267786	0	0,838428658	0,153649214	0	0	0,154254592	0,115512794
Block Frequency	0	0	0	0	0,400661406	0	0,998699262	0,001281768	0,33294793	0,399385805	0,749219278	0,026748897
Cumulative Sums1	0	0	0	0	0,3591381	0	0,021851052	0,000978598	0,00022268	0,001347489	0,322986247	0,21817639
Cumulative Sums2	0	0	0	0	0,895744957	0	0,025116599	0,150631953	0	0,000116086	0,223634068	0,215472661
Runs	0,032927289	0,357729143	0,005383382	0,087158458	0	0	0,910395725	0,666446443	0	0,000163194	0,818661461	0,21817639
LongestRun	0	0	0	0	0	0	0,180756771	0,035429947	0	0	0,904611301	0,597139639
Rank	0	0	0	0	0	0	0	0	0	0	0	0
Overlapping Template	0	0	0	0	0	0	0	0	0	0	0	0
Approximate Entropy	0	0	0	0	0	0	0	0	0	0	0	0
Serial1	0	0,028391685	0	0	0	0	0,812198232	0,516052045	0	0	0	0,069809752
Serial2	0,965499914	0,668286822	0,940114784	0,708439694	0,022645968	0,318625796	0,833972426	0,371593238	0	0	0	0,252140898
Linear Complexity	0	0	0	0	0	0	0	0	0	0	0	0

Table III by evaluating the distributions of p-values through χ^2 distribution. The $(i,j)^{th}$ entry in Table III represents the χ^2 value of the distribution of p-values of T_i in the rejection region of T_j. In this table, the values less than 0.0001 are represented as 0 and values less than 0.01 are marked to show non-uniform distribution of p-values. The tables which these results were derived are also given in Appendix A.

IV. SENSITIVITY OF TESTS

Correlation coefficient is used to measure correlation between two random variables. There are number of different coefficients for different situations. In this section of our study, Pearson product-moment correlation coefficient [9] is implemented to find the correlation between the p-values of sequences and transformed sequences under basic transformations such as:

- **Inversion:** Taking the sequence in reverse order.
- **Complement:** Complementing every bit of the sequence.
- **1-Shifting:** 1 bit left shifting.
- **8-Shifting:** 8 bit left shifting.

The Pearson product-moment correlation coefficient r_{xy} is

$$r_{xy} = \frac{cov(X,Y)}{\sigma(x)\sigma(y)} = \frac{\sum x_i y_i - \sum x_i \sum y_i}{\sqrt{n\sum x_i^2 - (\sum x_i)^2}\sqrt{n\sum y_i^2 - (\sum y_i)^2}}$$

where x_i's and y_i's are the i^{th} block of sequences which we are investigating the correlation and n is the number of used p-values in a sequence.

Pearson product-moment correlation coefficient can be computed only if both of the standard deviations are finite and both of them are nonzero. And it is a result of Cauchy-Schwarz inequality that the absolute value of correlation coefficient cannot be larger than 1.

The coefficients reveal the degree of linear dependence between the p-values. The closer the absolute value of the coefficient is 1, the correlation between the corresponding tests become stronger. Independency of the corresponding tests implies that the correlation coefficient is 0. But converse is not true in general. Actually, having correlation coefficient 0 only means that there is no linear relation between the p-values [10].

The correlation coefficients of p-values through basic transformations are given in Table IV.

TABLE IV
CORRELATION COEFFICIENTS UNDER BASIC TRANSFORMATIONS.

	Inverse	Complement	1-Shift	8-Shift
Frequency	1	1	1	1
Block Frequency	0,869472	1	0,98266	0,869472
Cumulative Sums 1	0,723222	1	0,999438	0,995701
Cumulative Sums 2	0,723222	1	0,999437	0,995707
Runs	1	1	0,999121	0,999112
Longest Run	1	0,059991	0,473792	1
Rank	-0,003203	0,086677	0,086092	-0,00155
Overlapping Template	0,370533	-0,004004	0,993046	0,96608
Approximate Entropy	1	1	1	1
Serial 1	1	1	1	1
Serial 2	1	1	1	1
Linear Complexity	0,639843	0,404223	0,481013	0,00491

The entries of the Table IV show the correlation between the corresponding test results of a sequence and its transformed form. We have highlighted the values greater than 0.80 to point out correlated p-values. In this respect, the frequency, block frequency, runs, approximate entropy, serial 1 and serial 2 tests are strong against these transformations as they produce correlated p-values. But although cumulative sums tests are strong against complement, 1-shift and 8-shift transformations, it can be seen from the table that the correlation coefficient does not give a strong result for the inverse transformation. In addition, longest run of ones test is strong against inverse and 8-shift transformations, but we can only say that a linear relation of the p-values with 1-shifted ones are unlikely as in complemented ones. Similarly, overlapping template matching test is strong against shifting transformations but again it is unlikely to have a linear relation for inverse and complement transformed results. Finally, for the rank and linear complexity tests a linear relation between the raw p-values and transformed ones are unlikely to have.

V. CONCLUSION

Statistical testing is an important aspect on determining the quality of a PRNG. To achieve this purpose, several test suites are proposed. But as well as having many tests to examine different randomness properties of sequences, having these tests independent is also of crucial importance in designing a test suite. In this work, we experimentally show that, looking at the failing sequences from NIST tests, we may conclude that most tests in this suite are independent. But as we have observed through the distribution of the p-values taken from the rejection regions of the tests, there is a relation, in this sense, among most tests. We also examined the sensitivity of NIST tests to some basic transformations. It is of interest to extend these ideas further to commonly used randomness tests which are not included in the NIST test suite as future work.

REFERENCES

[1] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo. A statistical test suite for random and pseudorandom number generators for cryptographic applications. 2001. http://www.nist.gov.

[2] D. E. Knuth. *Seminumerical Algorithms*, volume 2 of *The Art of Computer Programming*. Addison-Wesley, 1981.

[3] W. Caelli, E. Dawson, L. Nielsen, and H. Gustafson. CRYPT–X statistical package manual, measuring the strength of stream and block ciphers, 1992.

[4] G. Marsaglia. The Marsaglia random number CDROM including the DIEHARD battery of tests of randomness. 1996.

[5] Pierre L'Ecuyer and Richard Simard. Testu01: A c library for empirical testing of random number generators. *ACM Trans. Math. Softw.*, 33(4):22, 2007.

[6] J. Soto. Randomness testing of the AES candidate algorithms, 1999.

[7] P. Hellekalek and S. Wegenkittl. Empirical evidence concerning aes. *ACM Trans. Model. Comput. Simul.*, 13(4):322–333, 2003.

[8] Meltem Sönmez Turan, Ali Doganaksoy, and Serdar Boztas. On independence and sensitivity of statistical randomness tests. In Solomon W. Golomb, Matthew G. Parker, Alexander Pott, and Arne Winterhof, editors, *SETA*, volume 5203 of *Lecture Notes in Computer Science*, pages 18–29. Springer, 2008.

[9] Joseph L. Rodgers and Alan W. Nicewander. Thirteen ways to look at the correlation coefficient. *The American Statistician*, 42(1):59–66, 1988.

[10] David S. Moore. *The Basic Practice of Statistics with Cdrom*. W. H. Freeman & Co., New York, NY, USA, 1999.

APPENDIX A
p-VALUE DISTRIBUTION TABLES

Below are the tables used to derive the values in Table III.

TABLE V
DISTRIBUTIONS OF p-VALUES IN THE REJECTION REGION OF THE FREQUENCY TEST.

	[0, 0.1]	(0.1, 0.2]	(0.2, 0.3]	(0.3, 0.4]	(0.4, 0.5]	(0.5, 0.6]	(0.6, 0.7]	(0.7, 0.8]	(0.8, 0.9]	(0.9, 1]
BlockFrequency	271	192	151	117	71	67	49	33	21	5
CumulativeSums2	977	0	0	0	0	0	0	0	0	0
CumulativeSums2	977	0	0	0	0	0	0	0	0	0
Runs	97	112	92	98	98	90	86	93	130	81
LongestRun	593	177	89	57	21	16	13	7	4	0
Rank	94	48	95	0	189	154	245	152	0	0
OverlappingTemplate	87	92	83	121	76	175	139	73	131	0
ApproximateEntropy	262	168	118	108	91	63	56	43	42	26
Serial1	164	131	124	122	88	102	75	61	64	46
Serial2	109	98	95	99	102	96	97	89	91	101
LinearComplexity	124	64	50	63	86	88	107	100	93	202

TABLE VI
DISTRIBUTIONS OF p-VALUES IN THE REJECTION REGION OF THE BLOCK FREQUENCY TEST.

	[0, 0.1]	(0.1, 0.2]	(0.2, 0.3]	(0.3, 0.4]	(0.4, 0.5]	(0.5, 0.6]	(0.6, 0.7]	(0.7, 0.8]	(0.8, 0.9]	(0.9, 1]
Frequency	180	124	109	91	82	64	69	63	61	57
CumulativeSums1	231	133	116	90	85	88	53	55	32	17
CumulativeSums2	224	122	133	90	68	78	66	62	36	21
Runs	103	108	86	80	96	85	92	83	90	77
LongestRun	144	110	95	91	79	75	78	82	58	88
Rank	93	51	91	0	179	148	197	141	0	0
OverlappingTemplate	105	71	70	137	73	154	120	49	121	0
ApproximateEntropy	191	103	118	106	83	70	68	67	47	47
Serial1	119	103	85	90	88	91	89	85	84	66
Serial2	114	84	76	102	75	94	77	98	92	88
LinearComplexity	138	46	52	57	63	101	85	80	103	175

TABLE VII
DISTRIBUTIONS OF p-VALUES IN THE REJECTION REGION OF THE CUMULATIVE SUMS 1 TEST.

	[0, 0.1]	(0.1, 0.2]	(0.2, 0.3]	(0.3, 0.4]	(0.4, 0.5]	(0.5, 0.6]	(0.6, 0.7]	(0.7, 0.8]	(0.8, 0.9]	(0.9, 1]
Frequency	979	2	1	0	0	0	0	0	0	0
BlockFrequency	297	190	155	122	66	62	49	26	11	4
CumulativeSums2	973	8	1	0	0	0	0	0	0	0
Runs	111	115	97	98	109	82	79	85	124	82
LongestRun	557	168	103	61	26	27	22	10	6	2
Rank	102	55	101	0	178	151	235	160	0	0
OverlappingTemplate	95	95	81	117	76	178	149	64	127	0
ApproximateEntropy	273	160	109	101	93	69	58	53	36	30
Serial1	178	124	122	106	90	94	85	68	68	47
Serial2	106	105	91	100	99	107	90	95	94	95
LinearComplexity	115	68	49	62	88	93	104	104	99	200

TABLE VIII
DISTRIBUTIONS OF p-VALUES IN THE REJECTION REGION OF THE CUMULATIVE SUMS 2 TEST.

	[0, 0.1]	(0.1, 0.2]	(0.2, 0.3]	(0.3, 0.4]	(0.4, 0.5]	(0.5, 0.6]	(0.6, 0.7]	(0.7, 0.8]	(0.8, 0.9]	(0.9, 1]
Frequency	1031	8	3	0	0	0	0	0	0	0
BlockFrequency	315	209	163	117	76	68	44	31	16	3
CumulativeSums1	1017	21	4	0	0	0	0	0	0	0
Runs	109	104	97	109	112	89	103	96	134	89
LongestRun	582	184	95	71	37	29	16	18	6	4
Rank	111	57	96	0	203	163	250	162	0	0
OverlappingTemplate	89	97	85	138	80	186	142	76	149	0
ApproximateEntropy	266	171	122	117	104	70	66	58	40	28
Serial1	172	134	124	123	100	99	93	82	68	47
Serial2	116	109	106	104	116	93	102	94	94	108
LinearComplexity	136	72	56	67	90	95	109	99	106	212

TABLE IX
DISTRIBUTIONS OF p-VALUES IN THE REJECTION REGION OF THE RUNS TEST.

	[0, 0.1]	(0.1, 0.2]	(0.2, 0.3]	(0.3, 0.4]	(0.4, 0.5]	(0.5, 0.6]	(0.6, 0.7]	(0.7, 0.8]	(0.8, 0.9]	(0.9, 1]
Frequency	102	91	108	90	114	95	107	103	87	88
BlockFrequency	114	86	97	97	81	102	95	112	99	102
CumulativeSums1	105	81	103	95	106	114	92	100	84	105
CumulativeSums2	101	96	98	86	104	106	92	97	96	109
LongestRun	254	140	88	105	99	79	73	51	47	49
Rank	121	41	108	0	178	167	215	155	0	0
OverlappingTemplate	92	83	94	138	73	169	139	65	132	0
ApproximateEntropy	258	167	114	101	84	81	47	59	40	34
Serial1	164	133	122	102	87	108	71	79	60	59
Serial2	115	92	79	90	98	114	81	101	93	122
LinearComplexity	146	67	44	67	75	109	88	110	116	163

TABLE X
DISTRIBUTIONS OF p-VALUES IN THE REJECTION REGION OF THE LONGEST RUN OF ONES TEST.

	[0, 0.1]	(0.1, 0.2]	(0.2, 0.3]	(0.3, 0.4]	(0.4, 0.5]	(0.5, 0.6]	(0.6, 0.7]	(0.7, 0.8]	(0.8, 0.9]	(0.9, 1]
Frequency	404	129	75	63	47	49	52	68	33	43
BlockFrequency	124	108	115	106	98	105	77	91	77	62
CumulativeSums1	384	110	88	69	51	55	42	58	58	48
CumulativeSums2	391	114	77	61	53	64	40	64	58	41
Runs	199	128	99	103	66	76	64	73	80	75
Rank	93	66	99	0	195	142	214	154	0	0
OverlappingTemplate	85	69	63	145	80	181	143	65	132	0
ApproximateEntropy	248	163	113	99	85	64	59	63	37	32
Serial1	158	126	103	107	94	92	80	76	74	53
Serial2	86	116	100	106	92	81	89	90	102	101
LinearComplexity	124	73	42	47	60	89	101	94	127	206

TABLE XI
DISTRIBUTIONS OF p-VALUES IN THE REJECTION REGION OF THE MATRIX RANK TEST.

	[0, 0.1]	(0.1, 0.2]	(0.2, 0.3]	(0.3, 0.4]	(0.4, 0.5]	(0.5, 0.6]	(0.6, 0.7]	(0.7, 0.8]	(0.8, 0.9]	(0.9, 1]
Frequency	164	150	150	172	164	156	150	146	144	162
BlockFrequency	155	158	158	163	160	146	156	155	155	152
CumulativeSums1	163	149	140	146	152	187	125	153	163	180
CumulativeSums2	156	158	134	185	138	169	137	161	141	179
Runs	152	158	146	141	154	169	161	155	157	165
LongestRun	160	167	169	145	135	164	133	174	146	165
OverlappingTemplate	106	133	100	221	116	277	229	117	259	0
ApproximateEntropy	292	186	169	164	148	147	133	122	113	84
Serial1	158	166	145	140	149	170	150	158	160	162
Serial2	138	164	158	169	156	153	149	160	147	164
LinearComplexity	221	125	80	85	118	172	149	151	173	284

TABLE XII
DISTRIBUTIONS OF p-VALUES IN THE REJECTION REGION OF THE OVERLAPPING TEMPLATE TEST.

	[0, 0.1]	(0.1, 0.2]	(0.2, 0.3]	(0.3, 0.4]	(0.4, 0.5]	(0.5, 0.6]	(0.6, 0.7]	(0.7, 0.8]	(0.8, 0.9]	(0.9, 1]
Frequency	135	113	109	111	110	100	136	117	106	98
BlockFrequency	135	137	133	126	92	114	99	104	109	86
CumulativeSums1	136	115	112	105	88	126	109	129	94	121
CumulativeSums2	135	102	119	116	107	122	94	129	103	108
Runs	106	110	100	133	114	121	112	119	113	107
LongestRun	114	125	134	101	123	85	111	115	99	128
Rank	126	62	126	0	232	162	239	188	0	0
ApproximateEntropy	208	137	142	110	112	106	96	95	74	55
Serial1	113	117	116	118	111	107	101	138	107	107
Serial2	119	109	103	99	112	130	118	102	112	131
LinearComplexity	158	82	58	71	90	123	119	98	104	232

TABLE XIII
DISTRIBUTIONS OF p-VALUES IN THE REJECTION REGION OF THE APPROXIMATE ENTROPY TEST.

	[0, 0.1]	(0.1, 0.2]	(0.2, 0.3]	(0.3, 0.4]	(0.4, 0.5]	(0.5, 0.6]	(0.6, 0.7]	(0.7, 0.8]	(0.8, 0.9]	(0.9, 1]
Frequency	326	288	276	244	259	218	219	249	198	227
BlockFrequency	250	244	246	261	213	246	275	245	261	263
CumulativeSums1	302	283	255	256	258	250	211	258	221	210
CumulativeSums2	329	267	267	262	226	284	216	213	216	224
Runs	331	290	274	238	258	223	225	229	225	211
LongestRun	370	291	263	251	244	230	226	212	214	203
Rank	258	142	277	0	466	432	569	360	0	0
OverlappingTemplate	211	215	187	324	191	442	374	154	406	0
Serial1	2497	7	0	0	0	0	0	0	0	0
Serial2	1595	446	194	103	79	37	25	16	8	1
LinearComplexity	355	182	126	158	166	257	236	277	276	471

TABLE XIV
DISTRIBUTIONS OF p-VALUES IN THE REJECTION REGION OF THE SERIAL 1 TEST.

	[0, 0.1]	(0.1, 0.2]	(0.2, 0.3]	(0.3, 0.4]	(0.4, 0.5]	(0.5, 0.6]	(0.6, 0.7]	(0.7, 0.8]	(0.8, 0.9]	(0.9, 1]
Frequency	138	125	109	104	103	79	77	102	76	95
BlockFrequency	100	114	92	98	83	90	111	109	101	110
CumulativeSums1	136	115	86	115	96	93	84	108	88	87
CumulativeSums2	145	117	100	106	89	103	84	98	88	78
Runs	132	131	111	89	108	97	89	80	90	81
LongestRun	170	117	100	98	75	91	86	89	100	82
Rank	87	47	115	0	208	170	226	155	0	0
OverlappingTemplate	98	90	60	120	81	184	149	64	162	0
ApproximateEntropy	1008	0	0	0	0	0	0	0	0	0
Serial2	781	133	46	20	14	8	3	2	1	0
LinearComplexity	156	75	48	53	61	99	109	108	108	191

TABLE XV
DISTRIBUTIONS OF p-VALUES IN THE REJECTION REGION OF THE SERIAL 2 TEST.

	[0, 0.1]	(0.1, 0.2]	(0.2, 0.3]	(0.3, 0.4]	(0.4, 0.5]	(0.5, 0.6]	(0.6, 0.7]	(0.7, 0.8]	(0.8, 0.9]	(0.9, 1]
Frequency	106	113	85	100	92	92	100	108	77	113
BlockFrequency	96	91	94	95	93	97	119	100	97	104
CumulativeSums1	89	119	103	87	103	101	81	102	99	102
CumulativeSums2	116	101	86	96	85	110	97	112	99	84
Runs	106	110	107	90	93	99	96	89	93	103
LongestRun	97	111	91	106	90	105	96	96	98	96
Rank	119	53	104	0	178	188	191	153	0	0
OverlappingTemplate	91	72	59	147	71	191	129	71	155	0
ApproximateEntropy	913	54	15	2	2	0	0	0	0	0
Serial1	843	96	31	11	3	2	0	0	0	0
LinearComplexity	126	77	51	54	63	107	101	103	109	195

TABLE XVI
DISTRIBUTIONS OF p-VALUES IN THE REJECTION REGION OF THE LINEAR COMPLEXITY TEST.

	[0, 0.1]	(0.1, 0.2]	(0.2, 0.3]	(0.3, 0.4]	(0.4, 0.5]	(0.5, 0.6]	(0.6, 0.7]	(0.7, 0.8]	(0.8, 0.9]	(0.9, 1]
Frequency	330	375	358	385	345	329	347	387	321	364
BlockFrequency	330	305	400	378	364	373	347	351	333	360
CumulativeSums1	333	337	343	363	345	389	352	367	326	386
CumulativeSums2	355	332	387	339	339	360	357	373	320	379
Runs	349	361	365	385	377	308	341	364	344	347
LongestRun	379	369	335	377	345	344	334	352	365	341
Rank	378	180	382	0	637	616	785	563	0	0
OverlappingTemplate	268	310	245	458	270	626	551	247	566	0
ApproximateEntropy	576	472	427	365	329	324	303	269	246	230
Serial1	338	350	347	370	332	312	386	354	356	396
Serial2	357	342	340	351	323	357	387	342	350	392