TESTING THE NIST STATISTICAL TEST SUITE ON ARTIFICIAL PSEUDORANDOM SEQUENCES

A.A. Serov, A.M. Zubkov
Steklov Mathematical Institute of RAS
Moscow, RUSSIA
e-mail: serov@mi.ras.ru, zubkov@mi.ras.ru

Abstract

We discuss the results of experiments with the well-known NIST Statistical Test Suite designed for testing the hypothesis on the uniformity and independence of binary sequence elements. In particular, we investigate conditions on the parameters of piecewise merging of two linear recurrent sequences under which such combined sequences successfully pass all tests of the NIST package.
Keywords: data science, pseudorandom sequence, statistical test

1 Introduction

Generators of random and pseudo-random sequences are used in different fields of science and technology, including the cryptography. The most strict conditions on the quality of generated sequences are used in cryptography: to ensure the information security it is necessary for the generated sequences to be indistinguishable (or to be difficult to distinguish) from the equiprobable Bernoulli sequences. So the development and investigation of methods to test the closeness of the binary sequence properties to that of the equiprobable Bernoulli sequence is an actual problem.

2 Statistical test packages

In practice the testing of statistical qualities of random sequences (the quality is the higher the closer the characteristics of the tested sequence are to that of random equiprobable sequence) begins with the application of some statistical test packages. There are several popular packages of statistical tests which are distributed with open source codes (e.g. TESTU01 see [4], DIEHARD see [1], NIST see [3], SPRNG see [2]), or with closed source codes (e.g. Crypt-X http://www.isrc.qut.edu.au /resource/cryptx/). These packages allow to perform the analysis and testing of random sequences and have significant intersections in the sets of tests.

3 Main results

From the statistical test packages listed above, the NIST statistical tests package was selected as one of the most popular, fully documented and actively used for generator certifications.

The NIST Statistical Test Suite consists of 15 tests "developed for the randomness testing of the binary sequences" (word-for-word from the manual). These 15 tests are listed in Table 1.

Table 1: List of NIST Statistical Tests

Number	Test Name
1	Frequency
2	Block Frequency
3	Runs
4	Longest Run
5	Binary Matrix Rank
6	Discrete Fourier Transform
7	Non-overlapping Template Matching
8	Overlapping Template Matching
9	Universal
10	Linear Complexity
11	Serial
12	Approximate Entropy
13	Cumulative Sums
14	Random Excursions
15	Random Excursions Variant

For testing the sequence it is divided into several sufficiently long blocks and for each statistical test a set of P-values corresponding to these blocks are produced. The sequence is considered as *accepted by the test* if the corresponding P-values look like independent random variables with the uniform distribution on $[0, 1]$, in particular, satisfy some statistical test of uniformity, and is considered as *rejected by the test* otherwise.

The critical values of statistics in the NIST Statistical Test Suite were computed by means of limit theorems, and it was recommended that analysed sequences should have sufficiently large lengths. All segments sequences that we have tested were of $33,554,431 = 2^{25} - 1$ bit length. The significance level $\alpha = 0.01$ determining the rule of acceptance/rejection of the hypothesis was selected by default.

We have tested the following types of pseudo-random sequences by the NIST Test Suite (a brief description of the test results are given in brackets):

- pseudo-random sequences generated by linear shift registers of the maximal period with feedbacks given by the following primitive polynomials of degrees 25 and 27 over GF(2):

$$\begin{aligned} f(x) &= x^{25} + x^3 + 1, \\ g(x) &= x^{27} + x^5 + x^2 + x + 1, \\ h(x) &= x^{27} + x^{19} + x^{18} + x^{17} + x^{11} + x^6 + 1, \\ m(x) &= x^{27} + x^{26} + x^{25} + x^{24} + x^{23} + x^{22} + x^{21} + x^{20} + x^{19} + x^{17} \\ &\quad + x^{15} + x^{13} + x^{11} + x^9 + x^7 + x^5 + x^3 + x + 1 \end{aligned}$$

  (the segments of the pseudorandom sequences obtained by the linear shift registers with the $g(x)$, $h(x)$ and $m(x)$ polynomials have successfully passed all the

tests from the NIST Test Suite except for The Binary Matrix Rank Test, The Discrete Fourier Transform Test and The Linear Complexity Test, where the P-values were less than 10^{-6}, with the significance level $\alpha = 0.01$, the sequence corresponding to the polynomial $f(x)$, in addition to the listed tests, did not pass the Tests for the Longest Run-of-Ones in a Block (P-value $6 \cdot 10^{-6}$) and Maurer's "Universal Statistical Test" (P-value $1.91 \cdot 10^{-4}$))

- pseudo-random sequences generated by the linear shift registers with additive noise (the only test from the NIST Test Suite that detects nonrandomness in the disjoint $2^{25} - 1$ bit segments of output sequences of linear shift registers with polynomials $f(x)$, $g(x)$, $h(x)$, $m(x)$ perturbed by the Bernoulli noise sequence with parameter $\frac{1}{4}$, turned out to be The Discrete Fourier Transform Test (the corresponding P-values were smaller 10^{-6}));

- filtered output sequences of linear shift registers of the maximal period (failed to pass a number of tests of NIST Test Suite, corresponding P-values in many cases were smaller than 10^{-6});

- pseudo-random sequences obtained by merging of outputs of two linear shift registers of maximal periods: A) the output sequence of the first register $\{x_1, x_2, \ldots\}$ corresponding to the polynomial $f(x)$ was divided into adjacent segments of $L_1 = 25$ bits, the output sequence of the second register $\{y_1, y_2, \ldots\}$ corresponding to the polynomial $g(x)$ was similarly divided into segments of $L_2 = 27$ bits; the tested sequence $\{z_1, z_2, \ldots\}$ of the first type was constructed by merging of obtained segments of two sequences:

  $$\{z_k\}_{k=0}^{2^{L_1}-1+\left[\frac{2^{L_1}-1}{L_1}\right]L_2} = \{x_1, \ldots, x_{L_1}, y_1, \ldots, y_{L_2}, x_{L_1+1}, \ldots, x_{2L_1}, y_{L_2+1}, \ldots\};$$

  B) the output register sequences were divided into adjacent segments of a variable lengths according to the following rule:

  $$\{w_1, w_2, \ldots\} = \{x_1, \ldots, x_{L_1}, y_1, \ldots, y_{L_1^*}, x_{L_1+1}, \ldots, x_{L_2}, y_{L_1^*+1}, \ldots, y_{L_2^*}, \ldots\},$$

  where $L_1 = 25$, $L_k^* = 16 + 2^3 x_{L_k-3} + 2^2 x_{L_k-2} + 2 x_{L_k-1} + x_{L_k}$, $L_{k+1} = 16 + 2^3 y_{L_k^*-3} + 2^2 y_{L_k^*-2} + 2 y_{L_k^*-1} + y_{L_k^*}$, $k \geq 1$ (the A type sequences had passed all tests with the exception of Discrete Fourier Transform Test: for this test P-values were smaller than 10^{-6}, while the B type sequences had passed all the tests with P-values being as a rule essentially larger than $\alpha = 0.01$);

- pseudo-random sequence generated by AES, each byte of the encrypted sequence was replaced by the corresponding bit depending on the byte value (four non-overlapping segments of the length $2^{25} - 1$ bits of the initial sequence of the length $2^{27} - 4$ bits passed all the tests from the NIST Test Suite in the aggregate);

- output sequence of shrinking generators composed of two linear shift registers; two tested sequences were obtained by extracting from the output sequence of the first linear shift register (with feedback polynomial $g(x)$) all bits corresponding to the nonzero bits in the output sequence of the second linear shift register (with

feedback polynomial $f(x)$ for the first type test sequence and the polynomial $h(x)$ for the second one). The first type sequence passed all the tests from the NIST Test Suite with the significance level $\alpha = 0.01$. The second type sequence passed all the tests except for the Serial Test: for this test P-values turned out to be smaller than 10^{-6}. Maybe this is the consequence of coincidence of orders of the source and control sequences.

Also three series of experiments for following binary sequences having some different probabilistic structures were performed:

- pseudo-random sequences generated by AES, these sequences are considered as almost perfect;
- output sequences of linear shift register with primitive polynomial of degree 32 filtered by the equiprobable Boolean function corresponding to the first bit of nonlinear substitution in AES;
- non-equiprobable sequences obtained from the AES pseudo-random sequences by replacement each byte with bit such that the probability of 1 is $\frac{127}{256}$.

In each series of experiments 128 binary sequences of length 2^{20} were generated, the above 15 tests of the NIST package were applied to each sequence and the statistics values of these tests were saved, after which sample correlation statistics matrices were constructed.

Large correlations of statistics of Frequency, Cumulative Sums, Random Excursions, Random Excursions Variant, Runs tests were observed. So, these tests cannot be considered as independent.

4 Conclusions

The set of experiments with different non-random pseudo-random sequences showed that the NIST Test Suite may detect some deviations of properties of analyzed sequences from that of ideal Bernoulli sequences, but may fail to detect non-randomness of deterministic sequences with not very complex artificial irregularities.

References

[1] Marsaglia G. (1996). *DIEHARD: a battery of tests of randomness.*

[2] Mascagni M. (2000). Algorithm 806: SPRNG: A scalable library for pseudorandom number generation. *ACM Trans. Math. Soft.* Vol. 26, pp. 436–461.

[3] Rukhin A. et al. (2010). *A statistical test suite for the validation of random number generators and pseudo random number generators for cryptographic applications.* NIST Special Publ. 800-22 Revision 1a. 27 April 2010. NIST, ed.: L. E. Bassham III.

[4] L'Ecuyer P., Simard R. (2013). *TestU01.* D'epartement d'Informatique et de Recherche Op'erationnelleUniversit'e de Montr'eal.