

GINAR TEAM

-----



**GINAR**

## Test Report

---

# Diehard - Statistical Tests Results on GINAR's RNG

---

Tuong Nguyen Van  
HCMC, January 2019

## Contents

<b>1</b>	<b>Introduction</b>	<b>2</b>
<b>2</b>	<b>Diehard Tests</b>	<b>2</b>
2.1	The birthday spacings test . . . . .	2
2.2	Overlapping 5-Permutation Test (OPERM-5) . . . . .	2
2.3	Binary Rank Tests . . . . .	2
2.3.1	$31 \times 31$ Binary Matrix . . . . .	2
2.3.2	$32 \times 32$ Binary Matrix . . . . .	2
2.3.3	$6 \times 8$ Binary Matrix . . . . .	3
2.4	Bitstream Test . . . . .	3
2.5	The Tests OPSO, QQSO and DNA . . . . .	3
2.5.1	OPSO Overlapping Pairs Sparse Occupancy Test . . . . .	3
2.5.2	QQSO Overlapping Quadruples Sparse Occupancy Test . . . . .	3
2.5.3	DNA . . . . .	3
2.6	Count the 1's Test on a Stream of Bytes . . . . .	3
2.7	Count the 1's Test for Specific Bytes . . . . .	4
2.8	Parking Test . . . . .	4
2.9	Minimum Distance Test . . . . .	4
2.10	3D Spheres Test . . . . .	4
2.11	Squeeze Test . . . . .	4
2.12	Overlapping Sums Test . . . . .	4
2.13	Runs Test . . . . .	5
2.14	Craps Test . . . . .	5
<b>3</b>	<b>GINAR's Results</b>	<b>5</b>
3.1	Test Input . . . . .	5
3.2	Test Results . . . . .	5
	<b>References</b>	<b>17</b>

## List of Figures

## 1 Introduction

A model random number is said to be "good enough" if no adversary can distinguish it from the uniform distribution with a significant advantage.

Follow up the previous test, this paper is a report of the next statistical tests - Diehard - that GINAR uses to test our RNG. The report shows how the tests run and the result of GINAR RNG Service after running the tests. And we run the tests with raw data gotten directly from GINAR RNG Service.

## 2 Diehard Tests

Diehard tests are a suite of statistical tests for measuring the quality of random number generator. It contain 18 statistical tests which were developed by George Marsaglia. If a RNG passes Diehard statistical tests, then it can be used in more serious scientific researches.

### 2.1 The birthday spacings test

This test, we choose random  $m$  birthday in a year has  $n$  days. The spacing between the birthday was stored in a list and counted. If the number of values that occurred more than once in the list, it is the variable  $J$ , its distribution is approximate to Poisson distribution with mean  $\lambda = m^3/(4n)$ .

$n$  have to be very large so the results could be compared with the expected Poisson distribution with mean  $\lambda = m^3/(4n)$ . By default setup,  $n = 2^{24}$  and  $m = 2^9$ , so we can take the Poisson distribution with  $\lambda = m^3/(4n) = 2$  as the concrete distribution for  $J$ . For a sample of 500  $J$ 's a chi-square test is performed to provide a  $p$  - value. The first test uses the first bits from 1 - 24 (counting from left to right) from integers in the specified file and the file is closed and reopened. We do the same with the bits from 2 - 25 until the last sequence of bits from 9 - 32. Each set of bits provides a  $p$  - value, so we have 9  $p$  - value and then we do *Kolmogorov - Smirnov* ( $K - S$ ) test for the acquired 9  $p$ -values.

### 2.2 Overlapping 5-Permutation Test (OPERM-5)

This is the OPERM5 test. It looks at a sequence of one million 32 - bit random integers. Each set of five consecutive integers can be in one of 120 states, for the 5! possible orderings of five numbers. Thus the 5<sup>th</sup>, 6<sup>th</sup>, 7<sup>th</sup>, ... numbers each provide a state. As many thousands of state transitions are observed, cumulative counts are made of the number of occurrences of each state. Then the quadratic form in the weak inverse of the  $120 \times 120$  covariance matrix yields a test equivalent to the likelihood ratio test that the 120 cell counts came from the specified (asymptotically) normal distribution with the specified  $120 \times 120$  covariance matrix (with rank 99).

### 2.3 Binary Rank Tests

Binary rank tests use some of the characteristics of the matrixes and their ranks. N dimensional cube is taken using the columns of a matrix as axes. If the rank of the matrix is the same as the size of the matrix, then we can get to whatever point in the N dimensional cube. The actual values of the ranks are being compared with the ranks previously calculated. This is made by performing a chi-squared test to compare how well the sample fits the expected distribution.

#### 2.3.1 31 × 31 Binary Matrix

The leftmost 31 bits of 31 random integers from the sequence number are used to test. If the rank of the matrix is  $r$  then  $0 \leq r \leq 31$ . In practice,  $r$  are rarely less than 28. The sample of 40000 matrixes is taken and then a chi-squared test is performed to calculate the actual value of the ranks.

#### 2.3.2 32 × 32 Binary Matrix

Same the 31 × 31 Binary Matrix Test, this test take all 32 - bit and the rank  $r$  are rarely less than 29.

### 2.3.3 $6 \times 8$ Binary Matrix

This test generate matrix from 6 random integers and 8 bits from those integers. Rank  $r$  are rarely less than 4.

## 2.4 Bitstream Test

The file that is tested is considered as a stream of bits. So called 20 letters words are taken, overlapping between each other. The first word is from the 1<sup>st</sup> to 20<sup>th</sup> bit, the the second from 2<sup>nd</sup> to 21<sup>st</sup> bit. Then the number of the miss 20 letter words is counted in a string of  $2^{21}$  overlapping words. Their number is expected to be normally distributed with mean 144909 and sigma 428. It leads to a uniform  $[0, 1]$   $p - value$ .

In our experiments, the test is repeated 20 times and we perform a K-S Test on 20  $p - value$

## 2.5 The Tests OPSO, OQSO and DNA

### 2.5.1 OPSO Overlapping Pairs Sparse Occupancy Test

In this test a 2-letter words from an alphabet of 1024 letters are being considered. Each of the 2 letters are determined by a specified 10 bits from a 32 bit integers in the sequence to be tested. With OPSO,  $2^{21}$  overlapping words are being generated and then the number of the missing words (i.e. 2-letter words which do not appear in the entire sequence) is counted. This number is almost normally distributed with mean 141909 and a standard deviation sigma 290. It leads to a uniform  $[0, 1]$  p-value. The test is executed 23 times, first using the bits from 1 to 10, then 2-11, 3-12, , 23-32 bits of the  $2^{21} + 1$  keystrokes.

### 2.5.2 OQSO Overlapping Quadruples Sparse Occupancy Test

Similar as in OPSO, in this test a 4-letter words from an alphabet of 32 letters are being considered. Each of the 4 letters are determined by a specified 5 bits from a 32 bit integers. With OQSO  $2^{21}$  overlapping words are being generated and then the number of the missing words is counted. This number is almost normally distributed with mean 141909 and a standard deviation sigma 295 determined by simulation. Again, p-value is uniformly distributed on  $[0, 1]$ . The test is executed 28 times, first using the bits from 1 to 5, then 2-6, 3-7, ..., 28-32 bits of the  $2^{21} + 3$  keystrokes.

### 2.5.3 DNA

Like the previous 2 tests, in this test a 10-letter words from an alphabet of 4 letters C, G, A, T are being considered. Each of the 10 letters are determined by a specified 2 bits from a 32 bit integers. With DNA  $2^{21}$  overlapping words are being generated and then the number of the missing words in the whole sequence is counted. This number is almost normally distributed with mean 141909 and a standard deviation sigma 339 determined by simulation. As previous, p-value is uniformly distributed on  $[0, 1]$ . The test is executed 31 times, first using the bits from 1 to 2, then 2-3, 3-4, ..., 31-32 bits of the  $2^{21} + 9$  keystrokes.

## 2.6 Count the 1's Test on a Stream of Bytes

In this test as its name suggests the number of 1's in a stream of bytes is counted. Each byte can contain from 0 to 8 1's with different probabilities:  $\frac{1}{256} ; \frac{8}{256} ; \frac{28}{256} ; \frac{56}{256} ; \frac{70}{256} ; \frac{56}{256} ; \frac{28}{256} ; \frac{8}{256} ; \frac{1}{256}$ . The stream of bytes provides a string of overlapping 5-letter words. Each letter takes value A, B, C, D, E. The letters are determined by the number of 1's, in that byte: 0, 1, or 2  $\rightarrow$  A, 3  $\rightarrow$  B, 4  $\rightarrow$  C, 5  $\rightarrow$  D, and 6, 7 or 8  $\rightarrow$  E. So, which letter will be taken depends from the number of 1's in the stream. The number of 5 letters overlapping words is  $5^5$ . From a string of 256000 five letter words, frequencies for each word are being counted. The quadratic form in the weak inverse of the covariance matrix of the cell counts provides a chi-square test (the ordinary Pearson sums of  $(OBS - EXP)^2 / EXP$  on counts for 5- and 4-letter cell counts). The test returns 2 p-values for both 5- and 4-letter cell counts.

## 2.7 Count the 1's Test for Specific Bytes

In this test as its name suggests the number of 1's in specific bytes from each 32 integer are being counted. From each integer, a specific byte is chosen, say the left-most: bits 1 to 8. Each byte can contain from 0 to 8 1's with different probabilities:  $\frac{1}{256}; \frac{8}{256}; \frac{28}{256}; \frac{56}{256}; \frac{70}{256}; \frac{56}{256}; \frac{28}{256}; \frac{8}{256}; \frac{1}{256}$ . The letters are determined by the number of 1's, in that byte: 0, 1, or 2  $\rightarrow$  A, 3  $\rightarrow$  B, 4  $\rightarrow$  C, 5  $\rightarrow$  D, and 6, 7 or 8  $\rightarrow$  E. So, which letter will be taken depends from the number of 1's in that byte. So the words of 5 letters are being formed from the specified bytes from successive integers. The number of 5 letters overlapping words (each letter taking values A, B, C, D, E) is  $5^5$ . From a string of 256 000 five letter words frequencies for each word are being counted. The quadratic form in the weak inverse of the covariance matrix of the cell counts provides a chi-square test (the ordinary Pearson sums of  $(OBS - EXP)^2 / EXP$  on counts for 5- and 4-letter cell counts). The test is executed 25 times, first using first byte (bits from 1 to 8), then second byte (bits 2-9), ...,  $25^{th}$  byte (bits 25-32) and the corresponding p-values of Pearson chi-square tests are found.

## 2.8 Parking Test

In this test we park a car (it is a circle with radius 1) in a square of side 100 (so the square is with  $100 \times 100$  size). Then we do the same with the second, third car and so on. If a crash occurs when we try to park a car, the process for that particular car is repeated from the beginning choosing different random location for parking. The number of successfully parked cars is being counted after 12 000 attempts. This number has approximately normal distribution with the average of 3 523 with sigma 21.9. At the end a Kolmogorov-Smirnov (K-S) test for 10 obtained p-values is performed to check whether they all together are uniformly distributed at  $[0,1)$ .

## 2.9 Minimum Distance Test

Again we take a square but now with a side of 10 000 choosing 8 000 random points in it. If we denote the minimum distance between  $\frac{n(n-1)}{2}$  pairs of random points with  $d$ , and if the points are independent and uniformly distributed, then  $d^2$  should be exponentially distributed with mean 0.995. Then  $1 - e(-d^2/0.995)$  should also be uniform on  $[0,1)$  and a Kolmogorov-Smirnov test on the resulting uniform values serves as a test of uniformity for random points in the square. The Kolmogorov-Smirnov test is based on the full set of 100 random choices of 8000 points in the  $10000 \times 10000$  square.

## 2.10 3D Spheres Test

Here we take a cube with side 10 000 and choose 4 000 random points in it. At each point, center a sphere large enough to reach the next closest point. Then the distribution of the volume of the smallest such a sphere is found and it is approximately exponentially distributed with mean  $\frac{120\pi}{3}$ . Then the cube of radius  $r^3$  is also exponential with mean 30 (obtained by extensive simulation). With this test, we generated 20 times by 4 000 such spheres. Next, using the transformation  $1 - e(-r^3/30)$  each minimum cube of radius  $r^3$  lead to a uniform distributed variable on  $[0, 1)$ . Then a K-S test is done on the 20 p-values.

## 2.11 Squeeze Test

In this test random integers are floated to get uniform distributions on  $[0, 1)$ . Starting with  $k = 2^{32}$ , the test finds J, the number of iterations necessary to reduce  $k$  to 0 using the reduction  $k = \lfloor kU \rfloor$ , where U is a random uniform. A sample of 100 000 J's is used for  $\chi^2$ -test of the cell frequencies.

## 2.12 Overlapping Sums Test

Let  $m \geq 100$  be a fixed integer. Take a sequence of independent and identically distributed  $U(0, 1)$  random variables  $U_1, U_2, \dots$  and form the overlapping sums  $S_1 = U_1 + U_2 + \dots + U_m$ ,  $S_2 = U_2 + U_3 + \dots + U_{m+1}$ , and so on. The random variables  $S_i$ ,  $i = 1, 2, \dots, m$  are virtually normal with a covariance matrix which is easy to calculate. Clearly,  $E(S_i) = m/2$ , and  $D(S_i) = m/12$ ,  $i = 1, 2, \dots, m$ . Furthermore, if  $1 \leq i < j \leq m$ , then  $S_i$  and  $S_j$  have a sum  $S$  of  $m - j + i$  uniform values in common with  $X = S_i - S$ ,  $S$ , and  $Y = S_j - S$ .

being mutually independent. Therefore,  $cov(S_i, S_j) = (m - j + i)/12$ . Thus, if  $C$  denotes the  $m \times m$  covariance matrix of the  $S_i$ 's, the matrix  $12C$  is *Toeplitz* with diagonals  $m, m - 1, \dots, 1$ . A cholesky factorization yields  $C = VV^T$ , where  $V$  is lower triangular. Since  $V^{-1}$ , the inverse of a lower triangular matrix is easily computed, we can convert the vector  $S$  of  $S_i$ 's to independent normal variables via the linear transformation  $X = V^{-1}S$  which can be tested for normality or uniformity after converting to uniforms via the normal cumulative distribution function. After 10 times applying of K-S test, another K-S test is performed on the obtained 10 p-values. The combination of the two Kolmogorov-Smirnov (K-S) tests expands the size of the detected circuits.

### 2.13 Runs Test

The RUNS test counts the number of runs up and run downs in a sequence of 10 000 uniform variables  $[0,1)$  acquired by floating the 32-bit integers from the specified file. Because the covariance matrix for the runs up and runs down is known, a chi-square test may be carried out for quadratic forms in a weak inverse of the matrix in order to get a p-value. Performing this 10 times the p-values are obtained, and then for these 10 p-values a K-S test is executed. After that the whole test is performed again.

### 2.14 Craps Test

This test is somehow connected with the Craps game. The test plays  $n \geq 200000$  games of craps and counts the number of wins and the number of throws necessary to end each game. The number of wins should be very close to normal with mean  $np$  and variance  $np(1-p)$  where  $p = 244/495$ . Throws necessary to complete the game can vary from 1 to  $\infty$ , but all throws  $\geq 21$  are lumped together. A  $\chi^2$ -test is made on the number-of-throws cell counts. Each 32-bit integer from the test file provides the value for the throw of a dice, by floating to  $[0,1)$ , multiplying by 6 and taking 1 plus the integer part of the result. Note that the most of the tests in DIEHARD return a p-value, which should be uniform on  $[0,1)$  if the input file contains truly independent random bits. Those p-values are obtained by  $p = F(X)$ , where  $F$  is the assumed cumulative distribution function of the sample (random variable  $X$ ) - often normal. But that assumed  $F$  is just an asymptotic approximation, for which the fit will be worst in the tails. Therefore  $p < 0.025$  or  $p > 0.975$  means that the RNG has failed the test at the 0.05 level.

## 3 GINAR's Results

### 3.1 Test Input

We have tested over 1 billion random bit using the *dieharder* debian package written by Robert G. Brown. Or you can test with original C code of diehard test which we publish in our *github* repository.

### 3.2 Test Results

Our test results contain *p-value*, *histogram* of *p-value* and some additional information. All test assessment are "PASSED".

```
#=====
#           dieharder version 3.31.1 Copyright 2003 Robert G. Brown           #
#=====
# rng_name      | filename      | rands/second |
# file_input | new_test.bin | 6.19e+06 |
#=====
# Histogram of test p-values #
#=====
# Bin scale = 0.100000
# 20 | | | | | | | | | | | |
#   | | | | | | | | | | | |
# 18 | | | | | | | | | | | |
#   | | | | | | | | | | | |
```



```
# 16| | | | | | | | | | | |
# | | | | | | | | | | | |
# 14| | | | | | | | | | | |
# | |****| | | |****| | |****|
# 12| |****|****| | |****| | |****|
# | |****|****| | |****|****| |****|
# 10| |****|****| | |****|****| |****|
# |****|****|****|****| |****|****| |****|
# 8|****|****|****|****| |****|****| |****|****|
# |****|****|****|****| |****|****|****|****|****|
# 6|****|****|****|****| |****|****|****|****|****|
# |****|****|****|****|****|****|****|****|****|****|
# 4|****|****|****|****|****|****|****|****|****|****|
# |****|****|****|****|****|****|****|****|****|****|
# 2|****|****|****|****|****|****|****|****|****|****|
# |****|****|****|****|****|****|****|****|****|****|
# |-----|
# | 0.1| 0.2| 0.3| 0.4| 0.5| 0.6| 0.7| 0.8| 0.9| 1.0|
#=====#
#=====#
# test_name |ntup| tsamples |psamples| p-value |Assessment
#=====#
# diehard_birthdays| 0| 100| 100|0.89925936| PASSED
#=====#
# Histogram of test p-values #
#=====#
# Bin scale = 0.100000
# 40| | | | | | | | | | | |
# | | | | | | | | | | | |
# 36| | | | | | | | | | | |
# | | | | | | | | | | | |
# 32| | | | | | | | | | | |
# | | | | | | | | | | | |
# 28| | | | | | | | | | | |
# | | | | | | | | | | | |
# 24| | | | | | | | | | | |
# | | | | | | | | | | | |
# 20| | | | | | | | |****| |
# | | | | | | | | |****| |
# 16| | | | | | | | |****| |
# | | | | | | | | |****| |
# 12| |****| |****|****| |****| |****| |
# | |****| |****|****|****|****|****|****|
# 8| |****| |****|****|****|****|****|****|****|
# | |****| |****|****|****|****|****|****|****|
# 4|****|****|****|****|****|****|****|****|****|****|
# |****|****|****|****|****|****|****|****|****|****|
# |-----|
# | 0.1| 0.2| 0.3| 0.4| 0.5| 0.6| 0.7| 0.8| 0.9| 1.0|
#=====#
#=====#
# test_name |ntup| tsamples |psamples| p-value |Assessment
#=====#
# diehard_operm5| 0| 1000000| 100|0.11982399| PASSED
#=====#
# Histogram of test p-values #
```

```

=====
# Bin scale = 0.100000
# 20| | | | | | | | | |
# | | | | | | | | | |
# 18| | | | | | | | | |
# | | | | | | | | | |
# 16| | | | | | | | | |
# | | | | | | | | | |
# 14| |****| | | | | | | |
# | |****| | |****|****| | | |
# 12| |****| | |****|****| | | |
# | |****| | |****|****|****| | | |
# 10| |****| | |****|****|****| |****| |
# | |****| |****|****|****|****| |****|****|
# 8| |****|****|****|****|****|****| |****|****|
# |****|****|****|****|****|****|****| |****|****|
# 6|****|****|****|****|****|****|****|****|****|****|
# |****|****|****|****|****|****|****|****|****|****|
# 4|****|****|****|****|****|****|****|****|****|****|
# |****|****|****|****|****|****|****|****|****|****|
# 2|****|****|****|****|****|****|****|****|****|****|
# |****|****|****|****|****|****|****|****|****|****|
# |-----|
# | 0.1| 0.2| 0.3| 0.4| 0.5| 0.6| 0.7| 0.8| 0.9| 1.0|
=====
#
# test_name |ntup| tsamples |psamples| p-value |Assessment
=====
# diehard_rank_32x32| 0| 40000| 100|0.90849955| PASSED
=====
# Histogram of test p-values #
#
# Bin scale = 0.100000
# 20| | | | | | | | | |
# | | | | | | | | | |
# 18| | | | | | | | | |
# | | | | | | | | | |
# 16| | | | | | | | | |
# | | | | | | | | | |
# 14| | | | |****| |****| | | |
# |****| | | |****|****| | | |
# 12|****| | | |****|****| | | |
# |****|****| | |****|****| |****| |
# 10|****|****| | |****|****|****| |****| |
# |****|****|****| |****|****|****| |****| |
# 8|****|****|****| |****|****|****| |****| |
# |****|****|****| |****|****|****|****|****|****|****|
# 6|****|****|****| |****|****|****|****|****|****|****|
# |****|****|****| |****|****|****|****|****|****|****|
# 4|****|****|****|****|****|****|****|****|****|****|
# |****|****|****|****|****|****|****|****|****|****|
# 2|****|****|****|****|****|****|****|****|****|****|
# |****|****|****|****|****|****|****|****|****|****|
# |-----|
# | 0.1| 0.2| 0.3| 0.4| 0.5| 0.6| 0.7| 0.8| 0.9| 1.0|
=====

```



```

=====#
test_name |ntup| tsamples |psamples| p-value |Assessment
=====#
diehard_rank_6x8| 0| 100000| 100|0.72390601| PASSED
=====#
# Histogram of test p-values #
=====#
# Bin scale = 0.100000
# 20| | | | | | | | | | |
# | | | | | | | | | | |
# 18| | | | | | | | | | |
# | | | | | | | | | | |
# 16| | | | | | | | | | |
# | | | | | | | | | | |
# 14| | | | | | | |****|
# | | | | |****| |****|****|
# 12| |****| |****| |****|****| |****|****|
# | |****| |****| |****|****| |****|****|
# 10| |****| |****| |****|****| |****|****|
# | |****| |****| |****|****| |****|****|
# 8| |****| |****| |****|****| |****|****|
# |****|****| |****| |****|****| |****|****|
# 6|****|****|****|****| |****|****|****|****|****|
# |****|****|****|****|****|****|****|****|****|****|
# 4|****|****|****|****|****|****|****|****|****|****|
# |****|****|****|****|****|****|****|****|****|****|
# 2|****|****|****|****|****|****|****|****|****|****|
# |****|****|****|****|****|****|****|****|****|****|
# |-----|
# | 0.1| 0.2| 0.3| 0.4| 0.5| 0.6| 0.7| 0.8| 0.9| 1.0|
=====#
=====#
test_name |ntup| tsamples |psamples| p-value |Assessment
=====#
diehard_bitstream| 0| 2097152| 100|0.31065992| PASSED
=====#
# Histogram of test p-values #
=====#
# Bin scale = 0.100000
# 20| | | | | | | | | | |
# | | | | | | | | | | |
# 18| | | | | | | | | | |
# | | | | | | | |****|
# 16| | | | | | | |****|
# | | | | | | | |****|
# 14| | | | | | | |****|****|
# | | | |****| |****| |****|****|
# 12| | | |****| |****| |****|****|
# | | | |****|****|****| |****|****|
# 10| | | |****|****|****| |****|****|
# | | |****|****|****| |****|****|
# 8| | |****|****|****|****| |****|****|****|
# | | |****|****|****|****| |****|****|****|
# 6| | |****|****|****|****| |****|****|****|
# |****|****|****|****|****|****|****|****|****|****|
# 4|****|****|****|****|****|****|****|****|****|****|

```

```

#      |****|****|****|****|****|****|****|****|****|****|
#      2|****|****|****|****|****|****|****|****|****|****|
#      |****|****|****|****|****|****|****|****|****|****|
#      |-----|
#      | 0.1| 0.2| 0.3| 0.4| 0.5| 0.6| 0.7| 0.8| 0.9| 1.0|
#=====
#
#      test_name  |ntup| tsamples |psamples|  p-value |Assessment
#=====
#      diehard_opso|  0|   2097152|    100|0.11445373|  PASSED
#=====
#
#                               Histogram of test p-values
#=====
# Bin scale = 0.100000
#      20|      |      |      |      |      |      |      |      |      |      |
#      |      |      |      |      |      |      |      |      |      |      |
#      18|      |      |      |      |      |      |      |      |      |      |
#      |      |      |      |      |      |      |      |      |      |      |
#      16|      |      |      |      |      |      |      |      |      |      |
#      |      |      |      |      |      |****|      |      |      |      |
#      14|      |      |      |      |      |****|      |****|      |      |
#      |      |      |      |      |      |****|      |****|      |      |
#      12|      |****|      |      |****|****|      |****|      |      |
#      |      |****|      |      |****|****|      |****|      |      |
#      10|      |****|      |      |****|****|      |****|      |      |
#      |      |****|****|      |****|****|****|      |****|      |      |
#      8|****|****|****|      |****|****|****|****|****|      |      |
#      |****|****|****|      |****|****|****|****|****|****|****|
#      6|****|****|****|****|****|****|****|****|****|****|****|
#      |****|****|****|****|****|****|****|****|****|****|****|
#      4|****|****|****|****|****|****|****|****|****|****|****|
#      |****|****|****|****|****|****|****|****|****|****|****|
#      2|****|****|****|****|****|****|****|****|****|****|****|
#      |****|****|****|****|****|****|****|****|****|****|****|
#      |-----|
#      | 0.1| 0.2| 0.3| 0.4| 0.5| 0.6| 0.7| 0.8| 0.9| 1.0|
#=====
#
#      test_name  |ntup| tsamples |psamples|  p-value |Assessment
#=====
#      diehard_oqso|  0|   2097152|    100|0.93719497|  PASSED
#=====
#
#                               Histogram of test p-values
#=====
# Bin scale = 0.100000
#      20|      |      |      |      |      |      |      |      |      |      |
#      |      |      |      |      |      |      |      |      |      |      |
#      18|      |      |      |      |      |      |      |      |      |      |
#      |      |      |      |      |      |      |      |      |      |      |
#      16|      |      |      |      |****|      |      |      |      |      |
#      |      |      |      |      |****|      |      |      |      |      |
#      14|      |      |      |      |****|      |      |      |      |      |
#      |      |      |      |      |****|      |      |      |      |      |
#      12|      |****|      |****|****|      |      |      |      |      |
#      |      |****|      |****|****|      |****|****|      |      |
#      10|      |****|****|****|****|      |****|****|      |      |

```

```

#      |      | ****| ****| ****| ****| ****| ****| ****|      |      |
#      8| ****| ****| ****| ****| ****| ****| ****| ****| ****|      |
#      | ****| ****| ****| ****| ****| ****| ****| ****| ****|      |
#      6| ****| ****| ****| ****| ****| ****| ****| ****| ****|      |
#      | ****| ****| ****| ****| ****| ****| ****| ****| ****|      |
#      4| ****| ****| ****| ****| ****| ****| ****| ****| ****|      |
#      | ****| ****| ****| ****| ****| ****| ****| ****| ****| ****|
#      2| ****| ****| ****| ****| ****| ****| ****| ****| ****| ****|
#      | ****| ****| ****| ****| ****| ****| ****| ****| ****| ****|
#      |-----|
#      | 0.1| 0.2| 0.3| 0.4| 0.5| 0.6| 0.7| 0.8| 0.9| 1.0|
#=====
#
#      test_name      |ntup| tsamples |psamples|  p-value |Assessment
#=====
#      diehard_dna|    0|   2097152|     100|0.20084658|  PASSED
#=====
#
#                               Histogram of test p-values
#=====
# Bin scale = 0.100000
#      20|      |      |      |      |      |      |      |      |      |
#      |      |      |      |      |      |      |      |      |      |
#      18|      |      |      |      |      |      |      |      |      |
#      |      |      |      |      |      |      |      |      |      |
#      16|      |      |      |      |      |      |      |      |      |
#      |      |      |      |      |      |      | ****|      |      |
#      14| ****|      | ****|      |      |      | ****|      |      |
#      | ****|      | ****|      |      |      | ****|      |      |
#      12| ****|      | ****|      |      |      | ****|      |      |
#      | ****|      | ****|      |      |      | ****|      |      |
#      10| ****|      | ****| ****|      |      | ****|      |      | ****|
#      | ****|      | ****| ****|      | ****| ****| ****| ****| ****|
#      8| ****|      | ****| ****|      | ****| ****| ****| ****| ****|
#      | ****| ****| ****| ****|      | ****| ****| ****| ****| ****|
#      6| ****| ****| ****| ****|      | ****| ****| ****| ****| ****|
#      | ****| ****| ****| ****|      | ****| ****| ****| ****| ****|
#      4| ****| ****| ****| ****|      | ****| ****| ****| ****| ****|
#      | ****| ****| ****| ****| ****| ****| ****| ****| ****| ****|
#      2| ****| ****| ****| ****| ****| ****| ****| ****| ****| ****|
#      | ****| ****| ****| ****| ****| ****| ****| ****| ****| ****|
#      |-----|
#      | 0.1| 0.2| 0.3| 0.4| 0.5| 0.6| 0.7| 0.8| 0.9| 1.0|
#=====
#
#      test_name      |ntup| tsamples |psamples|  p-value |Assessment
#=====
#      diehard_count_1s_str|    0|   256000|     100|0.61825849|  PASSED
#=====
#
#                               Histogram of test p-values
#=====
# Bin scale = 0.100000
#      20|      |      |      |      |      |      |      |      |      |
#      |      |      |      |      |      |      |      |      |      |
#      18|      |      |      |      |      |      |      |      |      |
#      |      |      |      |      |      |      |      |      | ****|
#      16|      |      |      |      |      |      |      |      | ****|

```

```

#      |      |      |      |      |      |      |      |      |      |      |
#    14|****|      |      |      |      |      |      |      |      |      |****|
#      |****|      |****|      |      |      |      |      |      |      |****|
#    12|****|      |****|      |      |      |      |      |      |      |****|
#      |****|      |****|      |      |      |      |      |      |****|****|
#    10|****|      |****|      |      |****|      |****|****|****|
#      |****|      |****|      |      |****|      |****|****|****|
#     8|****|      |****|****|****|****|      |****|****|****|
#      |****|      |****|****|****|****|      |****|****|****|
#     6|****|      |****|****|****|****|      |****|****|****|
#      |****|****|****|****|****|****|      |****|****|****|
#    4|****|****|****|****|****|****|****|****|****|****|
#      |****|****|****|****|****|****|****|****|****|****|
#    2|****|****|****|****|****|****|****|****|****|****|
#      |****|****|****|****|****|****|****|****|****|****|
#      |-----|
#      | 0.1| 0.2| 0.3| 0.4| 0.5| 0.6| 0.7| 0.8| 0.9| 1.0|
#=====
#=====
#      test_name      |ntup| tsamples |psamples|  p-value |Assessment
#=====
diehard_count_1s_byt|   0|   256000|    100|0.34506044|  PASSED
#=====
#                               Histogram of test p-values                               #
#=====
# Bin scale = 0.100000
#    20|      |      |      |      |      |      |      |      |      |      |
#      |      |      |      |      |      |      |      |      |      |      |
#    18|      |      |      |      |      |      |      |      |      |      |
#      |****|      |      |      |      |      |      |      |      |      |
#    16|****|      |      |      |      |      |      |      |      |      |
#      |****|      |      |      |      |      |      |      |      |      |
#    14|****|      |      |      |      |      |      |      |      |      |
#      |****|      |      |      |      |      |      |      |****|      |
#    12|****|      |      |      |      |      |      |      |****|      |
#      |****|      |      |      |      |****|****|****|      |      |
#    10|****|      |****|      |      |****|****|****|      |      |
#      |****|      |****|      |      |****|****|****|****|****|
#     8|****|      |****|      |      |****|****|****|****|****|
#      |****|****|****|      |****|****|****|****|****|****|****|
#     6|****|****|****|****|****|****|****|****|****|****|****|
#      |****|****|****|****|****|****|****|****|****|****|****|
#     4|****|****|****|****|****|****|****|****|****|****|****|
#      |****|****|****|****|****|****|****|****|****|****|****|
#     2|****|****|****|****|****|****|****|****|****|****|****|
#      |****|****|****|****|****|****|****|****|****|****|****|
#      |-----|
#      | 0.1| 0.2| 0.3| 0.4| 0.5| 0.6| 0.7| 0.8| 0.9| 1.0|
#=====
#=====
#      test_name      |ntup| tsamples |psamples|  p-value |Assessment
#=====
diehard_parking_lot|   0|   12000|    100|0.25013948|  PASSED
#=====
#                               Histogram of test p-values                               #
#=====

```

```

# Bin scale = 0.100000
# 20| | | | | | | | | |
# | | | | | | | | | |
# 18| | | | | | | | | |
# | | | | | | | | | |
# 16| | | | | | | | | |
# | | | | | | | | | |
# 14| |****| | | | | | | |
# | |****| | | | | | |****|
# 12| |****| |****|****| | |****|
# | |****| |****|****| | |****|
# 10| |****| |****|****| | |****|
# |****|****| |****|****| |****|****|****|
# 8|****|****| |****|****|****|****|****|****|****|
# |****|****| |****|****|****|****|****|****|****|
# 6|****|****|****|****|****|****|****|****|****|****|
# |****|****|****|****|****|****|****|****|****|****|
# 4|****|****|****|****|****|****|****|****|****|****|
# |****|****|****|****|****|****|****|****|****|****|
# 2|****|****|****|****|****|****|****|****|****|****|
# |****|****|****|****|****|****|****|****|****|****|
# |-----|
# | 0.1| 0.2| 0.3| 0.4| 0.5| 0.6| 0.7| 0.8| 0.9| 1.0|
#=====
#=====
# test_name |ntup| tsamples |psamples| p-value |Assessment
#=====
# diehard_2dsphere| 2| 8000| 100|0.75177792| PASSED
#=====
# Histogram of test p-values #
#=====
# Bin scale = 0.100000
# 20| | | | | | | | | |
# | | | | | | | | | |
# 18| | | | | | | | | |
# | | | | | | | | | |
# 16| | | | | | | | |****|
# | | | | | | | | |****|
# 14| | | | | | | | |****|
# | | | | | | | | |****|
# 12| | | | | | | |****|****|
# |****| | | | | | |****|****|
# 10|****| |****|****| | |****|****|****|
# |****| |****|****| |****|****|****|****|
# 8|****|****|****|****|****| |****|****|****|****|
# |****|****|****|****|****| |****|****|****|****|
# 6|****|****|****|****|****|****|****|****|****|****|
# |****|****|****|****|****|****|****|****|****|****|
# 4|****|****|****|****|****|****|****|****|****|****|
# |****|****|****|****|****|****|****|****|****|****|
# 2|****|****|****|****|****|****|****|****|****|****|
# |****|****|****|****|****|****|****|****|****|****|
# |-----|
# | 0.1| 0.2| 0.3| 0.4| 0.5| 0.6| 0.7| 0.8| 0.9| 1.0|
#=====
#=====

```

```

      test_name |ntup| tsamples |psamples| p-value |Assessment
#=====#
      diehard_3dsphere| 3|      4000|      100|0.45351699| PASSED
#=====#
#                               Histogram of test p-values                               #
#=====#
# Bin scale = 0.100000
#  40| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
#  36| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
#  32| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
#  28| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
#  24| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
#  20|****| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
#  16|****| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
#  12|****| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
#  8|****|****| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
#  4|****|****| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
#  |****|****|****|****|****|****|****|****|****|****|****|****|****|****|****|****|
#  |-----|
#  | 0.1| 0.2| 0.3| 0.4| 0.5| 0.6| 0.7| 0.8| 0.9| 1.0|
#=====#
#=====#
      test_name |ntup| tsamples |psamples| p-value |Assessment
#=====#
      diehard_squeeze| 0|    100000|      100|0.02666498| PASSED
#=====#
#                               Histogram of test p-values                               #
#=====#
# Bin scale = 0.100000
#  20| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
#  18| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
#  16|****| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
#  14|****| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
#  12|****| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
#  10|****|****|****|****| | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
#  8|****|****|****|****| | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
#  6|****|****|****|****|****| | | | | | | | | | | | | | | | | | | | | | | | | | | |
#  4|****|****|****|****|****|****|****|****|****|****|****|****|****|****|****|****|
#  |****|****|****|****|****|****|****|****|****|****|****|****|****|****|****|****|

```

```

#      2|****|****|****|****|****|****|****|****|****|****|
#      |****|****|****|****|****|****|****|****|****|****|
#      |-----|
#      | 0.1| 0.2| 0.3| 0.4| 0.5| 0.6| 0.7| 0.8| 0.9| 1.0|
#=====
#
#      test_name      |ntup| tsamples |psamples|  p-value |Assessment
#=====
#      diehard_sums|    0|      100|    100|0.13135493|  PASSED
#=====
#
#                               Histogram of test p-values
#=====
# Bin scale = 0.100000
#      20|      |      |      |      |      |      |      |      |      |      |
#      |      |      |      |      |      |      |      |      |****|      |
#      18|      |      |      |      |      |      |      |      |****|      |
#      |      |      |      |      |      |      |      |      |****|      |
#      16|      |      |      |      |      |      |      |      |****|      |
#      |      |      |      |      |      |      |      |      |****|      |
#      14|      |      |      |      |      |      |      |      |****|      |
#      |      |      |      |      |      |      |      |      |****|      |
#      12|      |****|      |      |****|      |      |****|      |
#      |      |****|      |      |****|****|      |****|      |
#      10|      |****|      |      |****|****|      |****|      |
#      |****|****|      |      |****|****|****|****|****|      |
#      8|****|****|      |      |****|****|****|****|****|****|
#      |****|****|      |****|****|****|****|****|****|      |
#      6|****|****|****|****|****|****|****|****|****|****|****|
#      |****|****|****|****|****|****|****|****|****|****|****|
#      4|****|****|****|****|****|****|****|****|****|****|****|
#      |****|****|****|****|****|****|****|****|****|****|****|
#      2|****|****|****|****|****|****|****|****|****|****|****|
#      |****|****|****|****|****|****|****|****|****|****|****|
#      |-----|
#      | 0.1| 0.2| 0.3| 0.4| 0.5| 0.6| 0.7| 0.8| 0.9| 1.0|
#=====
#=====
#      test_name      |ntup| tsamples |psamples|  p-value |Assessment
#=====
#      diehard_runs|    0|  100000|    100|0.67260064|  PASSED
#=====
#
#                               Histogram of test p-values
#=====
# Bin scale = 0.100000
#      20|      |      |      |      |      |      |      |      |      |      |
#      |      |      |      |      |      |      |      |      |      |      |
#      18|      |      |      |      |      |      |      |      |      |      |
#      |****|      |      |      |      |      |      |      |      |      |
#      16|****|      |      |      |      |      |      |      |      |      |
#      |****|      |      |      |      |      |      |      |      |      |
#      14|****|      |      |      |      |      |      |      |****|      |
#      |****|      |      |      |      |      |      |      |****|      |
#      12|****|      |      |      |      |      |      |      |****|      |
#      |****|      |      |      |      |****|      |      |****|      |
#      10|****|      |      |****|      |****|      |      |****|      |
#      |****|      |****|****|      |****|****|      |****|****|

```

```

#      8|****|      |****|****|****|****|****|      |****|****|
#      |****|      |****|****|****|****|****|****|****|****|
#      6|****|****|****|****|****|****|****|****|****|****|
#      |****|****|****|****|****|****|****|****|****|****|
#      4|****|****|****|****|****|****|****|****|****|****|
#      |****|****|****|****|****|****|****|****|****|****|
#      2|****|****|****|****|****|****|****|****|****|****|
#      |****|****|****|****|****|****|****|****|****|****|
#      |-----|
#      | 0.1| 0.2| 0.3| 0.4| 0.5| 0.6| 0.7| 0.8| 0.9| 1.0|
#=====
#=====
#      test_name      |ntup| tsamples |psamples|  p-value |Assessment
#=====
#      diehard_runs|    0|   100000|    100|0.50570010|  PASSED
#=====
#                               Histogram of test p-values                               #
#=====
# Bin scale = 0.100000
#      40|      |      |      |      |      |      |      |      |      |
#      |      |      |      |      |      |      |      |      |      |
#      36|      |      |      |      |      |      |      |      |      |
#      |      |      |      |      |      |      |      |      |      |
#      32|      |      |      |      |      |      |      |      |      |
#      |      |      |      |      |      |      |      |      |      |
#      28|      |      |      |      |      |      |      |      |      |
#      |      |      |      |      |      |      |      |      |      |
#      24|      |      |      |      |      |      |      |      |      |
#      |      |      |      |      |      |      |      |      |****|
#      20|      |      |      |      |      |      |      |      |****|
#      |      |      |      |      |      |      |      |      |****|
#      16|      |      |      |      |      |      |      |      |****|
#      |      |      |      |      |      |      |      |      |****|
#      12|      |      |      |      |      |****|****|      |****|
#      |      |****|      |      |****|****|****|      |****|
#      8|      |****|****|      |****|****|****|      |****|
#      |      |****|****|****|****|****|****|      |****|****|
#      4|****|****|****|****|****|****|****|****|****|****|
#      |****|****|****|****|****|****|****|****|****|****|
#      |-----|
#      | 0.1| 0.2| 0.3| 0.4| 0.5| 0.6| 0.7| 0.8| 0.9| 1.0|
#=====
#=====
#      test_name      |ntup| tsamples |psamples|  p-value |Assessment
#=====
#      diehard_craps|    0|   200000|    100|0.09042038|  PASSED
#=====
#                               Histogram of test p-values                               #
#=====
# Bin scale = 0.100000
#      20|      |      |      |      |      |      |      |      |      |
#      |      |      |      |      |      |      |      |      |      |
#      18|      |      |      |      |      |      |      |      |      |
#      |      |      |      |      |      |      |      |      |      |
#      16|      |      |      |      |      |      |      |      |****|
#      |      |      |      |      |      |      |      |      |****|

```



```

# 14| | | | | | | | | |****|****|
# | | | | | | | | | |****|****|
# 12| | |****| | | | |****|****|****|
# | | |****| | | | |****|****|****|
# 10| | |****|****| | |****|****|****|
# | | |****|****| | |****|****|****|
# 8|****|****|****| |****| |****|****|****|
# |****|****|****|****|****| |****|****|****|****|
# 6|****|****|****|****|****| |****|****|****|****|
# |****|****|****|****|****|****|****|****|****|****|****|
# 4|****|****|****|****|****|****|****|****|****|****|****|
# |****|****|****|****|****|****|****|****|****|****|****|
# 2|****|****|****|****|****|****|****|****|****|****|****|
# |****|****|****|****|****|****|****|****|****|****|****|
# |-----|
# | 0.1| 0.2| 0.3| 0.4| 0.5| 0.6| 0.7| 0.8| 0.9| 1.0|
#=====
#=====
# test_name |ntup| tsamples |psamples| p-value |Assessment
#=====
# diehard_craps| 0| 200000| 100|0.04995448| PASSED
#=====

```

## References

- [1] Wikipedia. [https://en.wikipedia.org/wiki/Diehard\\_tests](https://en.wikipedia.org/wiki/Diehard_tests)
- [2] *Sashe Gjorgjievski, Verica Bakeva, Vesna Dimitrievska Ristovska*: ICT Innovations 2016 - Relation Between Statistical Tests for Pseudo-Random Number Generators and Diaphony as a Measure of Uniform Distribution of Sequences.
- [3] *Robert G. Brown*, Dieharder. <https://webhome.phy.duke.edu/~rgb/General/dieharder.php>