

#####

THE NIST STATISTICAL TEST SUITE

#####

1. FREQUENCY TEST

Computational information:

- (a) The nth partial sum = -1010
- (b) S_n/n = -0.001010

p_value = 0.312495, SUCCESS

2. BLOCK FREQUENCY TEST

Computational information:

- (a) χ^2 = 125400.500000
- (b) # of substrings = 125000
- (c) block length = 8

p_value = 0.211427, SUCCESS

3. CUMULATIVE SUMS TEST

Cumulative sums forward test:

Computational information:

- (a) The maximum partial sum =

p_value = 0.235161, SUCCESS

Cumulative sums reverse test:

Computational information:

- (a) The maximum partial sum =

p_value = 0.474414, SUCCESS

4. RUNS TEST

Computational information:

- (a) π = 0.499495
- (b) V_{n_obs} (Total # of runs) = 500010
- (c) $V_{n_obs} - 2 n \pi (1-\pi)$
----- = 0.014863
 $2 \sqrt{(2n) \pi (1-\pi)}$

p_value = 0.983230, SUCCESS

5. LONGEST RUNS OF ONES TEST

Computational information:

(a) N (# of substrings) = 100
(b) M (Substring Length) = 10000
(c) Chi² = 3.667991

Frequency

```
-----  
<=10    11    12    13    14    15    >=16  
-----  
      9    22    20    16    16     9     8
```

p_value = 0.721502, SUCCESS

6. RANK TEST

Computational information:

(a) Probability P_32 = 0.288788
(b) P_31 = 0.577576
(c) P_30 = 0.133636
(d) Frequency F_32 = 287
(e) F_31 = 550
(f) F_30 = 139
(g) # of matrices = 976
(h) Chi² = 0.990795
(i) NOTE: 576 BITS WERE DISCARDED.

p_value = 0.609329, SUCCESS

7. DFT TEST

Computational information:

(a) Percentile = 95.019800
(b) N_l = 475099.000000
(c) N_o = 475000.000000
(d) d = 0.642397

p_value = 0.520616, SUCCESS

8. NONOVERLAPPING TEMPLATES TEST

Computational information:

LAMBDA = 122.061523
M = 125000, N = 8, m = 10, n = 1000000

```
Template  W_1  W_2  W_3  W_4  W_5  W_6  W_7  W_8  
-----  
1100100100 113  129  136  126  116  126  111  115
```

chi2_value = 4.711998
p_value = 0.787868, SUCCESS

9. OVERLAPPING TEMPLATE OF ALL ONES TEST

Computational information:

(a) n (sequence_length) = 1000000
(b) m (block length of 1s) = 10
(c) M (length of substring) = 1032
(d) N (number of substrings) = 968

(e) lambda [(M-m+1)/2^m] = 0.999023
(f) eta = 0.499512

Frequency:

```
-----  
0   1   2   3   4   >=5   Chi^2  
-----  
590 144 110  48  25  51    7.6086
```

p_value = 0.179167, SUCCESS

10. UNIVERSAL TEST

Computational information:

(a) L = 7
(b) Q = 1280
(c) K = 141577
(d) sum = 877279.002910
(e) sigma = 0.002768
(f) variance = 3.125000
(g) exp_value = 6.196251
(h) phi = 6.196480
(i) WARNING: 1 bits were discarded.

p_value = 0.934083, SUCCESS

11. APPROXIMATE ENTROPY TEST

Computational information:

(a) m (block length) = 5
(b) n (sequence length) = 1000000
(c) Chi^2 = 29.506126
(d) Phi(m) = -3.465723
(e) Phi(m+1) = -4.158855
(f) ApEn = 0.693132
(g) Log(2) = 0.693147

p_value = 0.593368, SUCCESS

12. RANDOM EXCURSIONS TEST

Computational information:

(a) Number Of Cycles (J) = 0248
(b) Sequence Length (n) = 1000000

WARNING: TEST NOT APPLICABLE. THERE ARE AN
INSUFFICIENT NUMBER OF CYCLES.

13. RANDOM EXCURSIONS VARIANT TEST

Computational information:

(a) Number Of Cycles (J) = 248
(b) Sequence Length (n) = 1000000

WARNING: TEST NOT APPLICABLE. THERE ARE AN
INSUFFICIENT NUMBER OF CYCLES.

14. SERIAL TEST

Computational information:

(a) Block length (m) = 5
(b) Sequence length (n) = 1000000
(c) Ψ_m = 26.025216
(d) Ψ_{m-1} = 10.126784
(e) Ψ_{m-2} = 3.588192
(f) Del_1 = 15.898432
(g) Del_2 = 9.359840

p_value1 = 0.460072, SUCCESS

p_value2 = 0.312855, SUCCESS

15. LEMPEL-ZIV COMPRESSION TEST

Computational information:

(a) W (# of words) = 69582

p_value = 0.234318, SUCCESS