

#####

THE NIST STATISTICAL TEST SUITE

#####

-----  
1. FREQUENCY TEST  
-----

Computational information:

- (a) The nth partial sum = -696
- (b)  $S_n/n$  = -0.000696

p\_value = 0.486429, SUCCESS

-----  
2. BLOCK FREQUENCY TEST  
-----

Computational information:

- (a)  $\chi^2$  = 125107.000000
- (b) # of substrings = 125000
- (c) block length = 8

p\_value = 0.414778, SUCCESS

-----  
3. CUMULATIVE SUMS TEST  
-----

Cumulative sums forward test:

Computational information:

- (a) The maximum partial sum =

p\_value = 0.260548, SUCCESS

Cumulative sums reverse test:

Computational information:

- (a) The maximum partial sum =

p\_value = 0.621921, SUCCESS

-----  
4. RUNS TEST  
-----

Computational information:

- (a)  $\pi$  = 0.499652
- (b)  $V_n$ \_obs (Total # of runs) = 499753
- (c)  $V_n$ \_obs -  $2n\pi(1-\pi)$   
----- = 0.348968  
 $2\sqrt{2n}\pi(1-\pi)$

p\_value = 0.621648, SUCCESS

-----  
5. LONGEST RUNS OF ONES TEST  
-----

Computational information:

- (a) N (# of substrings) = 100

(b) M (Substring Length) = 10000  
(c) Chi^2 = 14.486128

Frequency

```
-----  
<=10    11    12    13    14    15    >=16  
-----  
    10    17    22    13    15     7    16  
-----
```

p\_value = 0.024653, 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 = 292  
(e) F\_31 = 553  
(f) F\_30 = 131  
(g) # of matrices = 976  
(h) Chi^2 = 0.571146  
(i) NOTE: 576 BITS WERE DISCARDED.

p\_value = 0.751584, SUCCESS

-----  
7. DFT TEST  
-----

Computational information:

(a) Percentile = 94.975800  
(b) N\_l = 474879.000000  
(c) N\_o = 475000.000000  
(d) d = -0.785152

p\_value = 0.432365, 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 147 127 116 117 129 151 124 118  
-----
```

chi2\_value = 13.476101  
p\_value = 0.096485, 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  
-----  
555 162  90  74  23  64    15.8159
```

p\_value = 0.007390, FAILURE

-----  
10. UNIVERSAL TEST  
-----

Computational information:

```
(a) L           = 7  
(b) Q           = 1280  
(c) K           = 141577  
(d) sum         = 876596.643014  
(e) sigma       = 0.002768  
(f) variance    = 3.125000  
(g) exp_value   = 6.196251  
(h) phi         = 6.191660  
(i) WARNING: 1 bits were discarded.
```

p\_value = 0.097268, SUCCESS

-----  
11. APPROXIMATE ENTROPY TEST  
-----

Computational information:

```
(a) m (block length) = 5  
(b) n (sequence length) = 1000000  
(c) Chi^2             = 32.945824  
(d) Phi(m)            = -3.465723  
(e) Phi(m+1)          = -4.158854  
(f) ApEn              = 0.693131  
(g) Log(2)            = 0.693147
```

p\_value = 0.420609, SUCCESS

-----  
12. RANDOM EXCURSIONS TEST  
-----

Computational information:

```
(a) Number Of Cycles (J) = 0967  
(b) Sequence Length (n) = 1000000  
(c) Rejection Constraint = 500.000000
```

```
x = -4 chi^2 = 2.076411 p_value = 0.838474, SUCCESS  
x = -3 chi^2 = 4.669460 p_value = 0.457535, SUCCESS  
x = -2 chi^2 = 6.692494 p_value = 0.244533, SUCCESS  
x = -1 chi^2 = 2.433299 p_value = 0.786505, SUCCESS  
x = 1 chi^2 = 3.359876 p_value = 0.644688, SUCCESS  
x = 2 chi^2 = 6.802188 p_value = 0.235772, SUCCESS  
x = 3 chi^2 = 5.475592 p_value = 0.360630, SUCCESS  
x = 4 chi^2 = 5.961328 p_value = 0.310000, SUCCESS
```

-----  
13. RANDOM EXCURSIONS VARIANT TEST  
-----

Computational information:

```
(a) Number Of Cycles (J) = 967  
(b) Sequence Length (n) = 1000000
```

(x = -9) Total visits = 830; p-value = 0.449914  
SUCCESS  
(x = -8) Total visits = 831; p-value = 0.424591  
SUCCESS  
(x = -7) Total visits = 786; p-value = 0.253659  
SUCCESS  
(x = -6) Total visits = 778; p-value = 0.195045  
SUCCESS  
(x = -5) Total visits = 764; p-value = 0.123884  
SUCCESS  
(x = -4) Total visits = 769; p-value = 0.088808  
SUCCESS  
(x = -3) Total visits = 848; p-value = 0.226227  
SUCCESS  
(x = -2) Total visits = 910; p-value = 0.454269  
SUCCESS  
(x = -1) Total visits = 926; p-value = 0.351182  
SUCCESS  
(x = 1) Total visits = 1014; p-value = 0.285190  
SUCCESS  
(x = 2) Total visits = 1084; p-value = 0.124533  
SUCCESS  
(x = 3) Total visits = 1176; p-value = 0.033556  
SUCCESS  
(x = 4) Total visits = 1219; p-value = 0.030325  
SUCCESS  
(x = 5) Total visits = 1219; p-value = 0.056123  
SUCCESS  
(x = 6) Total visits = 1255; p-value = 0.048319  
SUCCESS  
(x = 7) Total visits = 1294; p-value = 0.039181  
SUCCESS  
(x = 8) Total visits = 1231; p-value = 0.121143  
SUCCESS  
(x = 9) Total visits = 1137; p-value = 0.348474  
SUCCESS

-----  
14. SERIAL TEST  
-----

Computational information:

(a) Block length (m) = 5  
(b) Sequence length (n) = 1000000  
(c) Psi\_m = 25.661120  
(d) Psi\_m-1 = 7.098272  
(e) Psi\_m-2 = 2.676960  
(f) Del\_1 = 18.562848  
(g) Del\_2 = 14.141536

p\_value1 = 0.291982, SUCCESS

p\_value2 = 0.078150, SUCCESS

-----  
15. LEMPEL-ZIV COMPRESSION TEST  
-----

Computational information:

(a) W (# of words) = 69587

p\_value = 0.444155, SUCCESS