

#####  
THE NIST STATISTICAL TEST SUITE  
#####

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

Computational information:  
(a) The nth partial sum = 474  
(b)  $S_n/n$  = 0.000474

p\_value = 0.635500, SUCCESS

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

Computational information:  
(a)  $\chi^2$  = 124960.500000  
(b) # of substrings = 125000  
(c) block length = 8

p\_value = 0.530957, SUCCESS

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

Cumulative sums forward test:

Computational information:  
(a) The maximum partial sum =

p\_value = 0.807587, SUCCESS

Cumulative sums reverse test:

Computational information:  
(a) The maximum partial sum =

p\_value = 0.849583, SUCCESS

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

Computational information:  
(a)  $\pi$  = 0.500237  
(b)  $V_{n\_obs}$  (Total # of runs) = 499582  
(c)  $V_{n\_obs} - 2 n \pi (1-\pi)$   
----- = 0.590983  
 $2 \sqrt{2n} \pi (1-\pi)$

p\_value = 0.403281, SUCCESS

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

Computational information:  
(a) N (# of substrings) = 100  
(b) M (Substring Length) = 10000  
(c)  $\chi^2$  = 8.991259

Frequency

-----  
<=10    11    12    13    14    15    >=16  
-----

7 17 24 24 14 2 12

p\_value = 0.174070, 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 = 297  
(e) F\_31 = 562  
(f) F\_30 = 117  
(g) # of matrices = 976  
(h) Chi^2 = 2.201311  
(i) NOTE: 576 BITS WERE DISCARDED.

p\_value = 0.332653, SUCCESS

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

Computational information:

(a) Percentile = 95.004000  
(b) N\_l = 475020.000000  
(c) N\_o = 475000.000000  
(d) d = 0.129777

p\_value = 0.896743, 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 116 116 114 130 113 122 143 144

chi2\_value = 10.043987  
p\_value = 0.261952, 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  
-----

573 154 92 59 34 56 1.2773

p\_value = 0.937254, SUCCESS

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

Computational information:

(a) L = 7  
(b) Q = 1280  
(c) K = 141577  
(d) sum = 876867.128880  
(e) sigma = 0.002768  
(f) variance = 3.125000  
(g) exp\_value = 6.196251  
(h) phi = 6.193570  
(i) WARNING: 1 bits were discarded.

p\_value = 0.332977, SUCCESS

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

Computational information:

(a) m (block length) = 5  
(b) n (sequence length) = 1000000  
(c) Chi^2 = 24.309741  
(d) Phi(m) = -3.465728  
(e) Phi(m+1) = -4.158863  
(f) ApEn = 0.693135  
(g) Log(2) = 0.693147

p\_value = 0.832989, SUCCESS

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

Computational information:

(a) Number Of Cycles (J) = 2512  
(b) Sequence Length (n) = 1000000  
(c) Rejection Constraint = 500.000000

x = -4 chi^2 = 11.598574 p\_value = 0.040722, SUCCESS  
x = -3 chi^2 = 1.362697 p\_value = 0.928350, SUCCESS  
x = -2 chi^2 = 1.130986 p\_value = 0.951324, SUCCESS  
x = -1 chi^2 = 3.262739 p\_value = 0.659551, SUCCESS  
x = 1 chi^2 = 4.167994 p\_value = 0.525491, SUCCESS  
x = 2 chi^2 = 3.276244 p\_value = 0.657481, SUCCESS  
x = 3 chi^2 = 6.225265 p\_value = 0.284913, SUCCESS  
x = 4 chi^2 = 2.899353 p\_value = 0.715499, SUCCESS

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

Computational information:

(a) Number Of Cycles (J) = 2512  
(b) Sequence Length (n) = 1000000

(x = -9) Total visits = 2558; p-value = 0.874929  
SUCCESS  
(x = -8) Total visits = 2612; p-value = 0.715653  
SUCCESS  
(x = -7) Total visits = 2570; p-value = 0.820462  
SUCCESS  
(x = -6) Total visits = 2456; p-value = 0.811715  
SUCCESS  
(x = -5) Total visits = 2403; p-value = 0.608230  
SUCCESS  
(x = -4) Total visits = 2450; p-value = 0.740938  
SUCCESS  
(x = -3) Total visits = 2479; p-value = 0.835064  
SUCCESS

(x = -2) Total visits = 2522; p-value = 0.935081  
SUCCESS  
(x = -1) Total visits = 2548; p-value = 0.611524  
SUCCESS  
(x = 1) Total visits = 2426; p-value = 0.225009  
SUCCESS  
(x = 2) Total visits = 2381; p-value = 0.285948  
SUCCESS  
(x = 3) Total visits = 2353; p-value = 0.315765  
SUCCESS  
(x = 4) Total visits = 2333; p-value = 0.339827  
SUCCESS  
(x = 5) Total visits = 2371; p-value = 0.507272  
SUCCESS  
(x = 6) Total visits = 2391; p-value = 0.606754  
SUCCESS  
(x = 7) Total visits = 2320; p-value = 0.452481  
SUCCESS  
(x = 8) Total visits = 2216; p-value = 0.280920  
SUCCESS  
(x = 9) Total visits = 2237; p-value = 0.346712  
SUCCESS

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

Computational information:

(a) Block length (m) = 5  
(b) Sequence length (n) = 1000000  
(c) Psi\_m = 15.867520  
(d) Psi\_m-1 = 5.523296  
(e) Psi\_m-2 = 2.093920  
(f) Del\_1 = 10.344224  
(g) Del\_2 = 6.914848

p\_value1 = 0.848045, SUCCESS

p\_value2 = 0.545847, SUCCESS

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

Computational information:

(a) W (# of words) = 69575

p\_value = 0.061457, SUCCESS