

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

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

Computational information:

- (a) The nth partial sum = -4
- (b)  $S_n/n$  = -0.000004

p\_value = 0.996808, SUCCESS

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

Computational information:

- (a)  $\chi^2$  = 124931.000000
- (b) # of substrings = 125000
- (c) block length = 8

p\_value = 0.554363, SUCCESS

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

Cumulative sums forward test:

Computational information:

- (a) The maximum partial sum =

p\_value = 0.963210, SUCCESS

Cumulative sums reverse test:

Computational information:

- (a) The maximum partial sum =

p\_value = 0.964954, SUCCESS

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

Computational information:

- (a)  $\pi$  = 0.499998
- (b)  $V_n$ \_obs (Total # of runs) = 500615
- (c)  $V_n$ \_obs -  $2 n \pi (1-\pi)$   
----- = 0.869741  
 $2 \sqrt{2n} \pi (1-\pi)$

p\_value = 0.218697, SUCCESS

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

Computational information:

- (a) N (# of substrings) = 100
- (b) M (Substring Length) = 10000
- (c)  $\chi^2$  = 4.396342

Frequency

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

-----  
11 20 22 25 8 8 6

p\_value = 0.623204, 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 = 267
- (e) F\_31 = 571
- (f) F\_30 = 138
- (g) # of matrices = 976
- (h) Chi^2 = 1.316848
- (i) NOTE: 576 BITS WERE DISCARDED.

p\_value = 0.517667, SUCCESS

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

Computational information:

- (a) Percentile = 95.022800
- (b) N\_l = 475114.000000
- (c) N\_o = 475000.000000
- (d) d = 0.739730

p\_value = 0.459464, 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 131 110 105 134 130 125 108 126

chi2\_value = 7.878544  
p\_value = 0.445423, 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  
-----  
614 150 82 47 31 44 5.2694

p\_value = 0.383897, SUCCESS

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

Computational information:

(a) L = 7  
(b) Q = 1280  
(c) K = 141577  
(d) sum = 877415.850774  
(e) sigma = 0.002768  
(f) variance = 3.125000  
(g) exp\_value = 6.196251  
(h) phi = 6.197446  
(i) WARNING: 1 bits were discarded.

p\_value = 0.665844, SUCCESS

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

Computational information:

(a) m (block length) = 5  
(b) n (sequence length) = 1000000  
(c) Chi^2 = 37.934112  
(d) Phi(m) = -3.465717  
(e) Phi(m+1) = -4.158845  
(f) ApEn = 0.693128  
(g) Log(2) = 0.693147

p\_value = 0.216944, SUCCESS

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

Computational information:

(a) Number Of Cycles (J) = 1777  
(b) Sequence Length (n) = 1000000  
(c) Rejection Constraint = 500.000000

x = -4 chi^2 = 8.146429 p\_value = 0.148348, SUCCESS  
x = -3 chi^2 = 6.348165 p\_value = 0.273799, SUCCESS  
x = -2 chi^2 = 5.622898 p\_value = 0.344658, SUCCESS  
x = -1 chi^2 = 4.843557 p\_value = 0.435270, SUCCESS  
x = 1 chi^2 = 4.206528 p\_value = 0.520080, SUCCESS  
x = 2 chi^2 = 3.328977 p\_value = 0.649408, SUCCESS  
x = 3 chi^2 = 2.352323 p\_value = 0.798552, SUCCESS  
x = 4 chi^2 = 1.572241 p\_value = 0.904586, SUCCESS

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

Computational information:

(a) Number Of Cycles (J) = 1777  
(b) Sequence Length (n) = 1000000

(x = -9) Total visits = 1671; p-value = 0.666291  
SUCCESS  
(x = -8) Total visits = 1670; p-value = 0.643060  
SUCCESS  
(x = -7) Total visits = 1726; p-value = 0.812449  
SUCCESS  
(x = -6) Total visits = 1771; p-value = 0.975791  
SUCCESS  
(x = -5) Total visits = 1754; p-value = 0.897673  
SUCCESS  
(x = -4) Total visits = 1722; p-value = 0.727313  
SUCCESS  
(x = -3) Total visits = 1658; p-value = 0.372020

SUCCESS  
(x = -2) Total visits = 1671; p-value = 0.304625  
SUCCESS  
(x = -1) Total visits = 1721; p-value = 0.347549  
SUCCESS  
(x = 1) Total visits = 1797; p-value = 0.737260  
SUCCESS  
(x = 2) Total visits = 1785; p-value = 0.938244  
SUCCESS  
(x = 3) Total visits = 1732; p-value = 0.735684  
SUCCESS  
(x = 4) Total visits = 1674; p-value = 0.513740  
SUCCESS  
(x = 5) Total visits = 1700; p-value = 0.666805  
SUCCESS  
(x = 6) Total visits = 1741; p-value = 0.855525  
SUCCESS  
(x = 7) Total visits = 1680; p-value = 0.651791  
SUCCESS  
(x = 8) Total visits = 1549; p-value = 0.323405  
SUCCESS  
(x = 9) Total visits = 1453; p-value = 0.187456  
SUCCESS

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

Computational information:

(a) Block length (m) = 5  
(b) Sequence length (n) = 1000000  
(c) Psi\_m = 37.579840  
(d) Psi\_m-1 = 17.977856  
(e) Psi\_m-2 = 4.012576  
(f) Del\_1 = 19.601984  
(g) Del\_2 = 5.636704

p\_value1 = 0.238684, SUCCESS  
p\_value2 = 0.687852, SUCCESS

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

Computational information:

(a) W (# of words) = 69594

p\_value = 0.750961, SUCCESS