

#####

THE NIST STATISTICAL TEST SUITE

#####

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

Computational information:

- (a) The nth partial sum = 762
- (b)  $S_n/n$  = 0.000762

p\_value = 0.446060, SUCCESS

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

Computational information:

- (a)  $\chi^2$  = 124508.500000
- (b) # of substrings = 125000
- (c) block length = 8

p\_value = 0.837186, SUCCESS

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

Cumulative sums forward test:

Computational information:

- (a) The maximum partial sum =

p\_value = 0.655013, SUCCESS

Cumulative sums reverse test:

Computational information:

- (a) The maximum partial sum =

p\_value = 0.394576, SUCCESS

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

Computational information:

- (a)  $P_i$  = 0.500381
- (b)  $V_{n\_obs}$  (Total # of runs) = 499870

$$\frac{(c) \sqrt{V_{n\_obs} - 2 n p_i (1-p_i)}}{2 \sqrt{2n} p_i (1-p_i)} = 0.183437$$

p\_value = 0.795312, SUCCESS

---

5. LONGEST RUNS OF ONES TEST

---

Computational information:

(a) N (# of substrings) = 100  
 (b) M (Substring Length) = 10000  
 (c) Chi^2 = 4.207545

Frequency

<=10	11	12	13	14	15	>=16
14	18	23	20	10	8	7

p\_value = 0.648613, 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 = 278  
 (e) F\_31 = 575  
 (f) F\_30 = 123  
 (g) # of matrices = 976  
 (h) Chi^2 = 0.701807  
 (i) NOTE: 576 BITS WERE DISCARDED.

p\_value = 0.704052, SUCCESS

---

7. DFT TEST

---

Computational information:

(a) Percentile = 95.041000  
 (b) N\_l = 475205.000000  
 (c) N\_o = 475000.000000  
 (d) d = 1.330216

p\_value = 0.183447, 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	126	137	113	122	118	131	134	127

chi2\_value = 4.875349  
p\_value = 0.770812, 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
594	142	83	60	43	46	3.9076

p\_value = 0.562801, SUCCESS

---

10. UNIVERSAL TEST

---

Computational information:  
(a) L = 7  
(b) Q = 1280  
(c) K = 141577  
(d) sum = 877699.416247  
(e) sigma = 0.002768  
(f) variance = 3.125000  
(g) exp\_value = 6.196251  
(h) phi = 6.199449  
(i) WARNING: 1 bits were discarded.

p\_value = 0.247951, SUCCESS

---

11. APPROXIMATE ENTROPY TEST

---

Computational information:  
(a) m (block length) = 5  
(b) n (sequence length) = 1000000

(c) Chi<sup>2</sup> = 30.995498  
(d) Phi(m) = -3.465723  
(e) Phi(m+1) = -4.158854  
(f) ApEn = 0.693132  
(g) Log(2) = 0.693147

p\_value = 0.517240, SUCCESS

---

12. RANDOM EXCURSIONS TEST

---

Computational information:

(a) Number Of Cycles (J) = 0695  
(b) Sequence Length (n) = 1000000  
(c) Rejection Constraint = 500.000000

x = -4 chi<sup>2</sup> = 6.368847 p\_value = 0.271964, SUCCESS  
x = -3 chi<sup>2</sup> = 6.532901 p\_value = 0.257760, SUCCESS  
x = -2 chi<sup>2</sup> = 5.117311 p\_value = 0.401732, SUCCESS  
x = -1 chi<sup>2</sup> = 4.464748 p\_value = 0.484614, SUCCESS  
x = 1 chi<sup>2</sup> = 6.047482 p\_value = 0.301626, SUCCESS  
x = 2 chi<sup>2</sup> = 3.078550 p\_value = 0.687877, SUCCESS  
x = 3 chi<sup>2</sup> = 3.453953 p\_value = 0.630366, SUCCESS  
x = 4 chi<sup>2</sup> = 3.018492 p\_value = 0.697135, SUCCESS

---

13. RANDOM EXCURSIONS VARIANT TEST

---

Computational information:

(a) Number Of Cycles (J) = 695  
(b) Sequence Length (n) = 1000000

(x = -9) Total visits = 951; p-value = 0.095841  
SUCCESS  
(x = -8) Total visits = 915; p-value = 0.127610  
SUCCESS  
(x = -7) Total visits = 886; p-value = 0.155355  
SUCCESS  
(x = -6) Total visits = 895; p-value = 0.105785  
SUCCESS  
(x = -5) Total visits = 894; p-value = 0.075207  
SUCCESS  
(x = -4) Total visits = 900; p-value = 0.037686  
SUCCESS

(x = -3) Total visits = 862; p-value = 0.045156  
SUCCESS

(x = -2) Total visits = 798; p-value = 0.110705  
SUCCESS

(x = -1) Total visits = 752; p-value = 0.126299  
SUCCESS

(x = 1) Total visits = 644; p-value = 0.171335  
SUCCESS

(x = 2) Total visits = 635; p-value = 0.352814  
SUCCESS

(x = 3) Total visits = 645; p-value = 0.548666  
SUCCESS

(x = 4) Total visits = 674; p-value = 0.831410  
SUCCESS

(x = 5) Total visits = 702; p-value = 0.950097  
SUCCESS

(x = 6) Total visits = 691; p-value = 0.974194  
SUCCESS

(x = 7) Total visits = 697; p-value = 0.988129  
SUCCESS

(x = 8) Total visits = 735; p-value = 0.781767  
SUCCESS

(x = 9) Total visits = 764; p-value = 0.653528  
SUCCESS

---

#### 14. SERIAL TEST

---

Computational information:

(a) Block length (m) = 5  
(b) Sequence length (n) = 1000000  
(c) Psi\_m = 26.562304  
(d) Psi\_m-1 = 9.599712  
(e) Psi\_m-2 = 4.369120  
(f) Del\_1 = 16.962592  
(g) Del\_2 = 11.732000

p\_value1 = 0.388022, SUCCESS

p\_value2 = 0.163568, SUCCESS

---

#### 15. LEMPEL-ZIV COMPRESSION TEST

---

Computational information:

(a) W (# of words) = 69584

p\_value = 0.311714, SUCCESS