

Basic statistical test of bit sequences

=====

Date/Time: 14.04.2014,12:35 hour

file: xor3.rnd size: 10240000 Bytes

Test of null-hypothesis:

Bit stream ist a stream of truly randomly drawn number 0,1 with same probability p = 0.5

Non-overlapping byte count:

00	40093	39829	40224	40106	39821	40195	40453	39983
08	39773	39710	40129	39852	40105	40140	39672	39923
10	39764	39974	39998	39677	40094	40146	39829	39971
18	40098	39804	39974	39569	39897	40115	40077	40139
20	40007	40095	39761	40029	39711	39868	40000	40208
28	40020	40140	40082	40124	40049	40107	40116	40026
30	40173	40127	39998	40137	39745	39997	39913	39980
38	40094	39997	40061	40105	39739	39886	39947	39678
40	39949	40372	39827	40094	39879	40041	39991	40194
48	40244	40034	39599	40174	39761	39969	40083	39991
50	40002	40202	39869	39980	39876	39819	39730	40022
58	40326	40244	39936	40065	39806	39865	39907	40153
60	40155	40020	40050	39475	40517	39870	39869	39839
68	40149	39747	39834	40433	39644	40036	39915	39772
70	40628	40196	39960	40084	39985	39922	39964	40309
78	39772	40208	40071	39823	39903	40034	39886	40075
80	40031	40233	39648	39529	40434	39979	39750	39894
88	40191	39893	40203	40132	40000	40235	39949	39784
90	39934	39936	39731	39902	40174	40146	39947	40100
98	39925	40012	40103	39602	39988	39852	40180	39923
a0	39824	40058	40417	39810	40042	40308	39968	39855
a8	40095	39858	39505	40313	39971	39936	39830	40203
b0	39874	39839	40000	39729	40096	40247	40364	39722
b8	40189	40222	39929	40209	40139	39849	40036	40012
c0	39796	40213	40163	40073	40040	39837	40049	40009
c8	39939	40068	39778	39919	39753	40092	39846	40012
d0	40147	39734	40211	39894	39788	40126	39871	39675
d8	40124	39927	40139	40465	40113	39818	39905	40047
e0	39650	40287	39977	40004	39949	40064	39889	39964
e8	40044	39963	40074	40286	40218	40193	39948	40222
f0	40014	39888	40032	39969	40190	40080	40227	40017
f8	40076	40017	40144	40130	39857	40076	39969	40019

Evaluation of count of 10240000 Bytes = 81920000 Bits:

Theoretical average of byte-frequencies: 40000
'63' = 39475 (minimum) '70' = 40628 (maximum)

Theoretical interval I of byte-frequencies:
I = (39609 to 40391) (for 95 % of 256 frequency)

Test 1:

The theoretical permissible number of the 5% outliers (average 13) from the interval I is between 6 and 20

The real number of the outliers from interval I:
smaller: 6 greater: 7 summary: 13

Test 2:

Evaluation of byte-frequencies
Chi-square non-overlapping:
Theoretical maximum chi-square = 293.25

Chi-square value = 221.91

Chi-square overlapping:

Theoretical maximum chi-square = 155.40

Chi-square value = 121.04

Test 3:

r = 0.50002259 (relative frequency of bit 1 in the bit stream)

For a truly random sequence, the probability for r to have values in the complement of the open interval (0.49997741 , 0.50002259) is $w = 0.68259442$.

If w is very small (e.g., $w < 0.05$), the null-hypothesis is rejected.

If more sequences can be tested, the probability w has to be ≥ 0.05 for about 95% of the tested bit sequences.

Test 4:

Frequencies of overlapping 2-tuples:

tuples 00: 20477430 tuples 01: 20480722

tuples 10: 20480721 tuples 11: 20481127

Check size: Chi-square of 2-bit patterns minus chi square of 1-bit patterns

Theoretical maximum chi-square = 5.99

Chi-square value = 0.27

Test 5:

Frequencies of 2-tuples on even places:

tuples 00: 10238522 tuples 01: 10240753

tuples 10: 10240354 tuples 11: 10240371

Theoretical maximum chi-square = 7.81

Chi-square value = 0.29

Test 6:

Frequencies of 2-tuples on odd places:

tuples 00: 10238908 tuples 01: 10239969

tuples 10: 10240367 tuples 11: 10240756

Theoretical maximum chi-square = 7.81

Chi-square value = 0.19

Result of statistical analysis of file xor3.rnd:

=====

The tests: 1 2 3 4 5 6 were fulfilled!

The null-hypothesis is accepted!