

Statistischer-Basistest PRG620 AES128 (PTG.3) IBB, 18.02.2015

Basic statistical test of bit sequences

=====
Date/Time: 22.01.2015,16:22 hour

file: PRG620_2.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	40364	39714	40202	40185	39999	40035	40165	39897
08	40222	39925	39916	39721	39871	40254	40176	40039
10	39989	39718	40208	39756	40050	39864	40148	40103
18	39730	40299	39864	39716	40167	40000	40336	40078
20	39859	40260	39788	40113	40064	39711	39679	39874
28	39858	39706	40313	40216	39585	39973	40351	40247
30	39695	40127	40130	39905	39844	40031	40078	39930
38	39922	39950	39937	39951	39886	39978	39518	40214
40	39886	39983	39967	39893	40045	40030	40152	40187
48	40076	39781	40108	39968	40154	39879	40112	40112
50	40154	40008	40263	40433	40217	40017	39931	39786
58	39644	40120	40014	39726	39821	40364	39977	39938
60	39796	39906	39859	40200	40112	40056	39968	40081
68	39874	40184	39938	40199	40157	40136	40099	39634
70	39850	39690	39858	39928	39870	40094	39835	40153
78	40040	40239	39936	39881	39930	40037	40243	39795
80	39950	40106	39756	40076	40056	39839	40189	39978
88	40296	39911	39822	39986	40043	39995	39982	39714
90	40393	39623	40163	39783	40121	40044	40018	40061
98	39982	39860	39782	39925	39711	40164	40024	40099
a0	39908	40024	39759	40022	39960	40078	39863	40043
a8	39868	40434	40097	40281	40191	40020	40198	39791
b0	39881	39955	39916	39658	39670	39751	40075	39688
b8	40081	39960	39953	40479	40070	39962	39946	39832
c0	40064	39821	40043	39863	40062	39758	39987	39924
c8	40154	39908	40198	40040	39819	40041	39806	40017
d0	40405	39817	40004	40156	40087	40257	40221	40272
d8	39979	40317	40051	40196	39705	40070	39816	40184
e0	40468	39716	40049	39893	40084	39896	39964	40267
e8	39852	40147	40438	39948	39616	40056	39958	40015
f0	39679	40308	40015	39832	39854	40090	40158	40348
f8	40152	39680	40050	40157	40396	39706	39692	39880

Evaluation of count of 10240000 Bytes = 81920000 Bits:

Theoretical average of byte-frequencies: 40000
'3e' = 39518 (minimum) 'bb' = 40479 (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: 2 greater: 8 summary: 10

Test 2:

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

Chi-square value = 232.41

Chi-square overlapping:

Theoretical maximum chi-square = 155.40

Chi-square value = 152.99

Test 3:

r = 0.50001091 (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 (0.49998909 , 0.50001091) is $w = 0.84347576$.

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: 20475988 tuples 01: 20483118

tuples 10: 20483117 tuples 11: 20477777

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

Theoretical maximum chi-square = 5.99

Chi-square value = 1.94

Test 5:

Frequencies of 2-tuples on even places:

tuples 00: 10237707 tuples 01: 10242105

tuples 10: 10241586 tuples 11: 10238602

Theoretical maximum chi-square = 7.81

Chi-square value = 1.38

Test 6:

Frequencies of 2-tuples on odd places:

tuples 00: 10238281 tuples 01: 10241013

tuples 10: 10241531 tuples 11: 10239175

Theoretical maximum chi-square = 7.81

Chi-square value = 0.68

Result of statistical analysis of file PRG620_2.rnd:

=====

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

The null-hypothesis is accepted!