ComScire QNG Model R2000KU
Validation Tests of Randomness
(Representative Test Results)

ComScire QNGmeter: Continuous Random Number Tester

The ComScire QNGmeter (earlier versions are RNGmeter) is a continuous statistical tester that uses five powerful and fundamentally different tests on the input data. Unlike other statistical test suites it is designed to measure the quality of randomness of a continuous sequence of bits up to hundreds of Terabits in length. The QNGmeter automatically performs metatests of subsequences, which would have to be done manually by other popular test suites. Every QNG Model R2000KU is tested extensively after production and finally just before shipment using the QNGmeter test suite.

The five tests are:

1) 1/0 Balance – nominal expected value is p(0) = p(1) = 0.5.

2) Auto Correlation – orders 1 up to 32, nominal expected value is 0.0 for all orders.

3) Entropy Test – nominal expected value is H = 1.0, an update of U. Maurer's "Universal Test" (J-S Coron, *LNCS*, Vol. 1560, pp 29-42, 1999).

4) Serial Test – (Good, I. J, The serial test for sampling numbers and other tests for randomness, *Proc. Camb. Philos. Soc*. Vol. 49, 1953).

5) OQSO – Overlapping-Quadruples-Sparse-Occupancy test, nominal expected value for the mean = 141909.47* and standard deviation (by simulation) = 294.63* (G. Marsaglia and A. Zaman, *Computers Math. Applic.*, Vol. 26, No. 9, pp 1-10, 1993). *Our empirical tests indicate the actual mean and standard deviation are closer to 141909.195 and 294.656 respectively.

The z-scores, p-values, and chi-square (metatest) p-values are presented for each test. In addition, current test run time information, such as the *Bit Count*, *Elapsed Time*, and *Throughput*, is displayed by the tester. *Bit Count* is the total number of bits tested. *Elapsed Time* is the time from the start of the current test run. *Throughput* is the input data rate in bits per second.

Each test uses blocks of data of varying lengths, depending on the specific test. The 1/0 Balance and Auto Correlation tests use a block size of 65536 bits. The Serial test has a block size of 262144 bits. The Entropy test has 4194304 bits in a block. The OQSO test uses 10485775 bits per block.

A z-score is calculated for every test for each data-block. The z-scores are converted to probabilities with the assumption they are normally distributed. The z-scores of the 1/0

Balance, Auto Correlation and Serial tests and their associated p-values displayed are cumulative for all blocks. The z-scores of the Entropy and OQSO tests are combined by summing the z-scores of all blocks and dividing by the square root of the number of blocks, respectively.

A second level of testing is applied to the p-values calculated from the z-scores for each block of data. The z-scores are expected to be normally distributed and hence their associated p-values are expected to be uniformly distributed. A chi-square test is applied to the individual p-values from each of the five tests. The chi-square tests are cumulative and their results are displayed as probabilities. If these chi-square p-values converge to 0.0 or 1.0 for any test, the assumption of randomness fails, indicating non-random patterns in the data being tested.

A third level of testing is applied to all of the individual chi-squared tests. A Kolmogorov-Smirnov (KS) test is first applied to the probabilities of chi-squared results of all orders of auto correlation being tested to reduce the auto correlation results to a single number. A meta KS test is finally calculated using the auto correlation KS result and the probabilities of the chi-squared results of the remaining tests. The meta KS(+) and KS(-) probabilities are displayed. Convergence toward 1.0 or 0.0 indicates failure.

If any cumulative z-score exceeds ±4.265 standard deviations the generator will be determined as failed. Failure is also pronounced if the probability of any chi squared test is less than 0.00001 or greater than 0.99999, or if the probability of either of the Meta KS results is less than 0.0001 or greater than 0.9999.

For the hardware validation report, the QNGmeter tests were completed on four randomly selected QNG R2000KU devices for a minimum of 1 trillion random bits each. All test results and run time information for each device are recorded in the following tables.

ComScire QNGmeter 1 Trillion Bits Test

Testing QNG Device S/N QWR20153

Run Time Information	
Bits Tested	1.37E+12
Elapsed Time	07:22:49:19
Throughput	2.00E+06
1/0 Balance	
p(1) = 0.499999676	
z-score	-0.76
p (z ≤ x)	0.224
p (χ2 ≤ x)	0.852
Entropy Test	
H = 1.000000217	
z-score	+0.63
p (z ≤ x)	0.734
p (χ2 ≤ x)	0.161
Serial Test	
z-score	-0.71
p (z ≤ x)	0.240
p (χ2 ≤ x)	0.766
OQSO (Monkey Test)	
z-score	-1.20
p (z ≤ x)	0.115
p (χ2 ≤ x)	0.460
Meta KS Test	
KS+	0.5115
KS-	0.3074

Autocorrelation			
Order	z-score	p (z ≤ x)	p (χ2 ≤ x)
1	-0.98	0.164	0.064
2	-0.67	0.251	0.745
3	+2.56	0.995	0.315
4	+0.04	0.517	0.810
5	-0.44	0.331	0.819
6	+1.90	0.971	0.759
7	-0.75	0.227	0.931
8	+0.98	0.837	0.004
9	+0.22	0.588	0.667
10	+0.54	0.705	0.364
11	-0.54	0.296	0.581
12	-0.02	0.491	0.751
13	-0.02	0.490	0.075
14	-0.27	0.395	0.494
15	+0.42	0.661	0.049
16	+0.45	0.674	0.300
17	+1.19	0.884	0.084
18	+1.21	0.886	0.047
19	+0.79	0.785	0.849
20	-0.53	0.299	0.223
21	+0.14	0.555	0.597
22	-0.54	0.294	0.091
23	-0.95	0.172	0.661
24	+0.35	0.638	0.014
25	-0.38	0.353	0.679
26	-1.12	0.132	0.312
27	-0.30	0.381	0.010
28	+0.16	0.565	0.113
29	-1.21	0.113	0.010
30	-0.23	0.408	0.020
31	+0.87	0.808	0.808
32	+0.94	0.826	0.012

ComScire QNGmeter 1 Trillion Bits Test

Testing QNG Device S/N QWR20154

Run Time Information	
Bits Tested	1.37E+12
Elapsed Time	07:22:49:18
Throughput	2.00E+06
1/0 Balance	
p(1) = 0.499999739	
z-score	-0.61
p (z ≤ x)	0.270
p (χ2 ≤ x)	0.112
Entropy Test	
H = 1.000000021	
z-score	+0.06
p (z ≤ x)	0.524
p (χ2 ≤ x)	0.818
Serial Test	
z-score	-0.57
p (z ≤ x)	0.285
p (χ2 ≤ x)	0.070
OQSO (Monkey Test)	
z-score	-0.94
p (z ≤ x)	0.173
p (χ2 ≤ x)	0.447
Meta KS Test	
KS+	0.8343
KS-	0.0910

Autocorrelation			
Order	z-score	p (z ≤ x)	p (χ2 ≤ x)
1	-1.83	0.033	0.639
2	+0.40	0.655	0.826
3	-0.86	0.195	0.756
4	-1.62	0.053	0.960
5	+0.20	0.579	0.610
6	-0.41	0.340	0.923
7	-0.89	0.187	0.603
8	-0.55	0.290	0.744
9	-0.82	0.206	0.051
10	-0.16	0.438	0.327
11	-0.55	0.290	0.250
12	-0.42	0.338	0.058
13	+1.64	0.949	0.868
14	+0.28	0.611	0.668
15	+0.78	0.782	0.107
16	-1.33	0.092	0.057
17	+1.86	0.968	0.717
18	+0.91	0.819	0.022
19	+1.33	0.909	0.750
20	+1.23	0.891	0.280
21	-2.45	0.007	0.082
22	+0.62	0.731	0.136
23	-0.36	0.360	0.952
24	+0.61	0.729	0.803
25	-1.37	0.085	0.656
26	+0.54	0.704	0.259
27	-0.39	0.348	0.791
28	-1.57	0.058	0.295
29	+1.46	0.928	0.038
30	+1.12	0.868	0.026
31	+0.95	0.829	0.259
32	+0.01	0.503	0.611

ComScire QNGmeter 1 Trillion Bits Test

Testing QNG Device S/N QWR20155

Run Time Information	
Bits Tested	1.37E+12
Elapsed Time	07:22:49:17
Throughput	2.00E+06
1/0 Balance	
p(1) = 0.500000138	
z-score	+0.32
p (z ≤ x)	0.627
p (χ2 ≤ x)	0.980
Entropy Test	
H = 1.000000465	
z-score	+1.34
p (z ≤ x)	0.911
p (χ2 ≤ x)	0.698
Serial Test	
z-score	-0.29
p (z ≤ x)	0.384
p (χ2 ≤ x)	0.126
OQSO (Monkey Test)	
z-score	-1.11
p (z ≤ x)	0.134
p (χ2 ≤ x)	0.927
Meta KS Test	
KS+	0.0979
KS-	0.9427

Autocorrelation			
Order	z-score	p (z ≤ x)	p (χ2 ≤ x)
1	-0.42	0.336	0.937
2	+0.65	0.742	0.138
3	+0.52	0.698	0.791
4	+1.32	0.906	0.632
5	-0.99	0.162	0.746
6	+0.78	0.783	0.710
7	-0.69	0.246	0.805
8	-0.03	0.488	0.290
9	+1.09	0.861	0.960
10	-0.29	0.388	0.408
11	-1.03	0.151	0.424
12	-0.12	0.454	0.687
13	+1.02	0.847	0.418
14	-0.10	0.462	0.532
15	+0.26	0.602	0.191
16	-0.03	0.487	0.295
17	-0.54	0.294	0.305
18	+1.44	0.925	0.899
19	+0.08	0.533	0.029
20	+1.82	0.966	0.793
21	+2.47	0.993	0.225
22	+1.29	0.901	0.424
23	+0.53	0.701	0.565
24	+0.90	0.817	0.697
25	-0.50	0.308	0.279
26	-0.48	0.317	0.278
27	-0.65	0.258	0.570
28	+0.22	0.586	0.971
29	-1.70	0.045	0.101
30	+0.02	0.509	0.578
31	-0.40	0.345	0.569
32	-0.01	0.497	0.015

ComScire QNGmeter 1 Trillion Bits Test

Testing QNG Device S/N QWR20156

Run Time Information	
Bits Tested	1.37E+12
Elapsed Time	07:22:49:16
Throughput	2.00E+06
1/0 Balance	
p(1) = 0.500000090	
z-score	+0.21
p (z ≤ x)	0.584
p (χ2 ≤ x)	0.897
Entropy Test	
H = 1.000000069	
z-score	+0.20
p (z ≤ x)	0.579
p (χ2 ≤ x)	0.799
Serial Test	
z-score	-1.43
p (z ≤ x)	0.077
p (χ2 ≤ x)	0.027
OQSO (Monkey Test)	
z-score	-0.80
p (z ≤ x)	0.212
p (χ2 ≤ x)	0.152
Meta KS Test	
KS+	0.5321
KS-	0.4118

Autocorrelation			
Order	z-score	p (z ≤ x)	p (χ2 ≤ x)
1	-1.25	0.106	0.541
2	-1.26	0.104	0.342
3	-0.05	0.482	0.828
4	+0.35	0.638	0.621
5	-0.91	0.182	0.622
6	-0.78	0.219	0.316
7	+1.38	0.916	0.102
8	+0.44	0.671	0.721
9	+0.36	0.640	0.760
10	-0.36	0.358	0.955
11	-0.54	0.293	0.851
12	-0.60	0.273	0.766
13	+0.94	0.825	0.819
14	+0.28	0.610	0.507
15	-0.07	0.471	0.298
16	-0.01	0.495	0.138
17	-0.70	0.241	0.999
18	-1.59	0.056	0.078
19	-0.43	0.334	0.164
20	-0.06	0.474	0.870
21	+0.21	0.584	0.957
22	+0.95	0.829	0.304
23	+0.59	0.723	0.343
24	+0.20	0.581	0.613
25	+0.06	0.523	0.467
26	-1.44	0.075	0.002
27	+0.98	0.836	0.235
28	-1.17	0.120	0.111
29	-0.96	0.169	0.429
30	+0.28	0.612	0.021
31	-1.25	0.106	0.450
32	-1.20	0.115	0.129