ComScire QNG Model PQ32MS
Validation Tests of Randomness

Table of Contents

ComScire QNGmeter: Continuous Random Number Tester.

The ComScire QNGmeter is a continuous real-time 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 PQ32MS 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 $p(1) = p(0) = 0.5$.
2) Auto Correlation - orders 1 through 32, nominal expected value is 0.5 for all orders.
3) Entropy Test – nominal expected value is H = 1.0, an update of U. Maurer's "Universal Test" [Cor99].
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) = 294.656 (G. Marsaglia and A. Zaman, *Computers Math. Applic.*, Vol. 26, No. 9, pp 1-10, 1993).

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 *Bits Tested, Elapsed Time, Throughput,* and *Bits Tested %,* is displayed by the tester. *Bits Tested* 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. *Bits Tested %* is the percent of the total bits tested. This value might be less than 100% due to limited CPU resources.

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 65,536 bits. The Serial test has a block size of 262,144 bits. The Entropy test has 4,194,304 bits in a block. The OQSO test uses 10,485,775 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 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 probability. A meta-meta

KS test is finally calculated using the auto correlation KS result and the probabilities of the chi-squared metatest results of all the other tests. The meta-meta KS+ and KS- probabilities are displayed. Convergence toward 1.0 or 0.0 indicates failure.

For the hardware validation report, the QNGmeter tests were completed on a QNG Model PQ32MS using 4.82 trillion random bits. All metatest results for the device are recorded in the following Table 1.

ComScire QNGmeter 4.82 Trillion Bits Test
Testing QNG Device S/N QWR50011

Run Time Information	
Bits Tested	4.82E+12
Time Elapsed	3:16:45:00
Throughput	32.0E+06
Meter	40.1+
1/0 Balance	
p (z ≤ x)	0.930
p (χ2 ≤ x)	0.028
Entropy Test	
p (z ≤ x)	0.581
p (χ2 ≤ x)	0.421
Serial Test	
p (z ≤ x)	0.245
p (χ2 ≤ x)	0.492
OQSO (Monkey Test)	
p (z ≤ x)	0.573
p (χ2 ≤ x)	0.074
AC Meta KS- Test	
KS-	0.111
Meta KS Test	
KS+	0.949
KS-	0.031

Autocorrelation	
Order	p (χ2 ≤ x)
1	0.207
2	0.415
3	0.281
4	0.374
5	0.452
6	0.116
7	0.004
8	0.359
9	0.902
10	0.777
11	0.470
12	0.708
13	0.719
14	0.720
15	0.256
16	0.603
17	0.472
18	0.660
19	0.546
20	0.773
21	0.973
22	0.972
23	0.959
24	0.018
25	0.215
26	0.531
27	0.373
28	0.033
29	0.890
30	0.512
31	0.474
32	0.813

Table 1 — QNGmeter continuous test results for PQ32MS.

NIST Statistical Test Suite for the Validation of Random Number Generators.

The National Institute of Standards and Technology (NIST) provides a statistical testing suite, specified in Special Publication 800-22rev1a, consisting of 15 tests that were developed to test the randomness of binary sequences generated by a TRNG or PRNG. The NIST Statistical Test Suite (NIST STS) software and documentation can be downloaded from their Cryptographic Toolkit web page.

The NIST STS source code was compiled on a computer running Ubuntu 18.04. A number of tests were completed to confirm the functionality of the software. The test suite contains sample data files of 1,000,000 bits in length to be analyzed. These include the binary expansions of constants *e*, π, √2 and √3. For each sample file, the NIST STS battery of tests were performed and compared to the empirical results found in the SP800-22rev1a documentation Appendix B. Following the confirmation that the test suite is operating properly, a binary file of 1 billion raw random bits in length was generated using our QNG Model PQ32MS (SN: QWR50117) to be analyzed.

All test results are recorded in the following Table 2. The Block Frequency, Non-overlapping Template Matching, Overlapping Template Matching, Approximate Entropy, Linear Complexity and Serial tests require user prescribed input parameters. The exact values used in these examples have been included in parenthesis beside the name of the statistical test. In the case of the Non-overlapping Templates test, a Kolmogorov-Smirnov test (KS-test) was performed for the collection of 148 *P-values*. In the case of the Random Excursions and Random Excursions Variant tests, KS-tests for the collection of 8 and 18 *P-values*, respectively, have been reported.

NIST Battery of Tests Results	
Statistical Test	**P-value**
Frequency	0.151190
Block Frequency (m = 128)	0.562591
Cumulative Sums-Forward	0.084037
Cumulative Sums-Reverse	0.167184
Runs	0.967382
Long Runs of Ones	0.313041
Rank	0.152044
Spectral DFT	0.904708
Non-overlapping Templates (m = 9)	0.334514
Overlapping Templates (m = 9)	0.471146
Universal	0.705466
Approximate Entropy (m = 10)	0.916599
Random Excursions	0.640335
Random Excursions Variant	0.804067
Linear Complexity (m = 500)	0.554420
Serial (m = 16, $\nabla\Psi^2_m$)	0.176657
Serial (m = 16, $\nabla^2\Psi^2_m$)	0.101311

Table 2 — NIST Test Suite Results for PQ32MS.

DIEHARD: A Battery of Tests of Randomness.

The DIEHARD Battery of Tests of Randomness, developed by Prof. George Marsaglia, contains a collection of 15 tests to examine the randomness of binary sequences generated by a TRNG or PRNG. The complete testing suite, including documentation and software, can be found from the DIEHARD archived website[1]. Windows executable files are provided for simple use of the testing suite. The DIEHARD tests require a large binary file of random integers, at least 80 million bits, to be tested. Therefore, a binary file of 80 million raw random bits in length was generated using our QNG Model PQ32MS (SN: QWR50001) to be analyzed.

For the generated random data file all of the statistical tests were applied and the resulting *p-values* recorded in the following Table 3. In the case of the Birthday Spacings, Binary Rank (6x8 matrices), OPSO, OQSO, DNA, Count-the-1's (specified bytes), This is a Parking Lot, The Minimum Distance, 3DSpheres, Overlapping Sums, and Runs (up & down) tests, only the K-S tests are reported here.

DIEHARD Battery of Tests Results	
Statistical Test	**p-value**
Birthday Spacings	0.584316
Overlapping 5-Permutation	0.023375
Binary Rank (31x31)	0.700515
Binary Rank (32x32)	0.703387
Binary Rank (6x8)	0.586651
Bitstream	0.512400
OPSO	0.852800
OQSO	0.235200
DNA	0.403800
Count-the-1's (byte stream)	0.800646
Count-the-1's (specified bytes)	0.251800
This is a Parking Lot	0.975336
The Minimum Distance	0.421422
3DSpheres	0.119535
Squeeze	0.813194
Overlapping Sums	0.102156
Runs (up)	0.612206
Runs (down)	0.039565
Craps (no. of wins)	0.611182
Craps (throws/game)	0.237462

Table 3 — DIEHARD Test Suite Results for PQ32MS.

[1] https://web.archive.org/web/20160113163414/http://stat.fsu.edu/pub/diehard/diehard.zip