ComScire QNG Model PQ128MU
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 PQ128MU 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 PQ128MU using 103 trillion random bits. All metatest results for the device are recorded in the following Table 1.

ComScire QNGmeter 103 Trillion Bits Test Testing QNG Device S/N QWR70004			
Run Time Information		Autocorrelation	
Bits Tested	103E+12	Order	p (χ2 ≤ x)
Time Elapsed	21:22:01:00	1	0.750
Throughput	128E+6	2	0.886
Meter	44.5+	3	0.939
1/0 Balance		4	0.099
p (z ≤ x)	0.963	5	0.071
p (χ2 ≤ x)	0.172	6	0.836
Entropy Test		7	0.987
p (z ≤ x)	0.582	8	0.323
p (χ2 ≤ x)	0.385	9	0.040
Serial Test		10	0.336
p (z ≤ x)	0.539	11	0.346
p (χ2 ≤ x)	0.885	12	0.466
OQSO (Monkey Test)		13	0.570
p (z ≤ x)	0.169	14	0.441
p (χ2 ≤ x)	0.966	15	0.413
AC Meta KS- Test		16	0.075
KS-	0.213	17	0.207
Meta KS Test		18	0.711
KS+	0.452	19	0.386
KS-	0.623	20	0.154
		21	0.460
		22	0.023
		23	0.786
		24	0.951
		25	0.407
		26	0.835
		27	0.801
		28	0.637
		29	0.974
		30	0.786
		31	0.485
		32	0.413

Table 1 — QNGmeter continuous test results for PQ128MU.

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 PQ128MU (SN: QWR70001) 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	0.415422
Block Frequency (m = 128)	0.709558
Cumulative Sums-Forward	0.968863
Cumulative Sums-Reverse	0.448424
Runs	0.368587
Long Runs of Ones	0.278461
Rank	0.208837
Spectral DFT	0.106246
Non-overlapping Templates (m = 9)	0.673334
Overlapping Templates (m = 9)	0.163513
Universal	0.115387
Approximate Entropy (m = 10)	0.474986
Random Excursions	0.770736
Random Excursions Variant	0.264284
Linear Complexity (m = 500)	0.036833
Serial (m = 16, $\nabla\Psi^2_m$)	0.883171
Serial (m = 16, $\nabla^2\Psi^2_m$)	0.086109

Table 2 — NIST Test Suite Results for PQ128MU.

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 PQ128MU (SN: QWR70004) 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	0.026053
Overlapping 5-Permutation	0.717986
Binary Rank (31x31)	0.320859
Binary Rank (32x32)	0.394794
Binary Rank (6x8)	0.966855
Bitstream	0.878749
OPSO	0.682987
OQSO	0.561982
DNA	0.645468
Count-the-1's (byte stream)	0.745519
Count-the-1's (specified bytes)	0.089936
This is a Parking Lot	0.310429
The Minimum Distance	0.319546
3DSpheres	0.291031
Squeeze	0.476844
Overlapping Sums	0.701413
Runs (up)	0.303256
Runs (down)	0.071091
Craps (no. of wins)	0.623129
Craps (throws/game)	0.147330

Table 3 — DIEHARD Test Suite Results for PQ128MU.

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