ComScire QNG Model PQ4000KU
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 PQ4000KU 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 PQ4000KU using 1.27 trillion random bits. All metatest results for the device are recorded in the following Table 1.

ComScire QNGmeter 1.27 Trillion Bits Test Testing QNG Device S/N QWR40010			
Run Time Information		Autocorrelation	
Bits Tested	1.27E+12	Order	p (χ2 ≤ x)
Time Elapsed	3:16:45:00	1	0.685
Throughput	4.00E+06	2	0.227
Meter	38.2+	3	0.531
1/0 Balance		4	0.682
p (z ≤ x)	0.746	5	0.998
p (χ2 ≤ x)	0.510	6	0.015
Entropy Test		7	0.492
p (z ≤ x)	0.881	8	0.567
p (χ2 ≤ x)	0.123	9	0.419
Serial Test		10	0.074
p (z ≤ x)	0.652	11	0.844
p (χ2 ≤ x)	0.524	12	0.153
OQSO (Monkey Test)		13	0.008
p (z ≤ x)	0.206	14	0.601
p (χ2 ≤ x)	0.495	15	0.854
AC Meta KS- Test		16	0.617
KS-	0.997	17	0.791
Meta KS Test		18	0.082
KS+	0.601	19	0.025
KS-	0.646	20	0.579
		21	0.197
		22	0.475
		23	0.934
		24	0.345
		25	0.776
		26	0.687
		27	0.273
		28	0.394
		29	0.832
		30	0.909
		31	0.117
		32	0.779

Table 1 — QNGmeter continuous test results for PQ4000KU.

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 PQ4000KU (SN: QWR40005) 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	0.564639
Block Frequency (m = 128)	0.246750
Cumulative Sums-Forward	0.996677
Cumulative Sums-Reverse	0.295391
Runs	0.009467
Long Runs of Ones	0.208837
Rank	0.065230
Spectral DFT	0.562591
Non-overlapping Templates (m = 9)	0.486609
Overlapping Templates (m = 9)	0.751866
Universal	0.200115
Approximate Entropy (m = 10)	0.607993
Random Excursions	0.010239
Random Excursions Variant	0.896669
Linear Complexity (m = 500)	0.000876
Serial (m = 16, $\nabla\Psi^2_m$)	0.508172
Serial (m = 16, $\nabla^2\Psi^2_m$)	0.066465

Table 2 — NIST Test Suite Results for PQ4000KU.

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 PQ4000KU (SN: QWR40001) 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	0.983146
Overlapping 5-Permutation	0.815226
Binary Rank (31x31)	0.474647
Binary Rank (32x32)	0.750961
Binary Rank (6x8)	0.679387
Bitstream	0.522100
OPSO	0.371200
OQSO	0.965900
DNA	0.753400
Count-the-1's (byte stream)	0.440757
Count-the-1's (specified bytes)	0.268900
This is a Parking Lot	0.479416
The Minimum Distance	0.870736
3DSpheres	0.894333
Squeeze	0.531706
Overlapping Sums	0.090995
Runs (up)	0.728846
Runs (down)	0.663521
Craps (no. of wins)	0.599130
Craps (throws/game)	0.134858

Table 3 — DIEHARD Test Suite Results for PQ4000KU.

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