

# EMPIRICAL SPECTRAL ANALYSIS OF RANDOM NUMBER GENERATORS

DAVID ZEITLER - SIEMENS DEMATIC, JOSEPH MCKEAN - WESTERN MICHIGAN UNIVERSITY, AND JOHN KAPENGA - WESTERN MICHIGAN UNIVERSITY

ABSTRACT. Computer simulation procedures have become a staple of research and development in many fields, including statistics. The generation of random number sequences is critical to these procedures. The validity of research results often depend on the underlying validity of the generator being used. In this work we develop the theory for the Empirical Spectral Test (EST). The EST is a class of tests of spatial uniformity based on a multi-dimensional Fourier transform of the empirical probability density function. The test can be applied to sequences from any random number generator, can be adapted to specific user requirements and has the added advantage that its computational complexity is relatively independent of the number of data points being tested.

## 1. THE NATURE OF PSEUDO RANDOM NUMBER GENERATORS

Pseudo random number generators are recursive integer equations that produce deterministic sequences which exhibit apparently random characteristics. Examples are:

- \* Congruential:  $s(x) = (ax + c) \text{ mod } m$  [E.G.  $a = 137, c = 187, m = 256$ ]
- \* Shift register:  $y_{n+k} = \sum_{i=0}^{k-1} a_i y_{n+i} \text{ mod } p$
- \* Combinations of generators can also be used to improve the sequence properties.

Use of a single generator in a simulation at more than one point will effectively partition the sequence as if it were generating points in a multi-dimensional space. Examples of partitions schemes which arise in these situations include block and leap frog illustrated below.

<b>Subsequence</b>	1	1	1	1	1	2	2	2	2	2
--------------------	---	---	---	---	---	---	---	---	---	---

<b>Generator</b>	1	2	3	4	5	6	7	8	9	10
------------------	---	---	---	---	---	---	---	---	---	----

Block Partitioning:

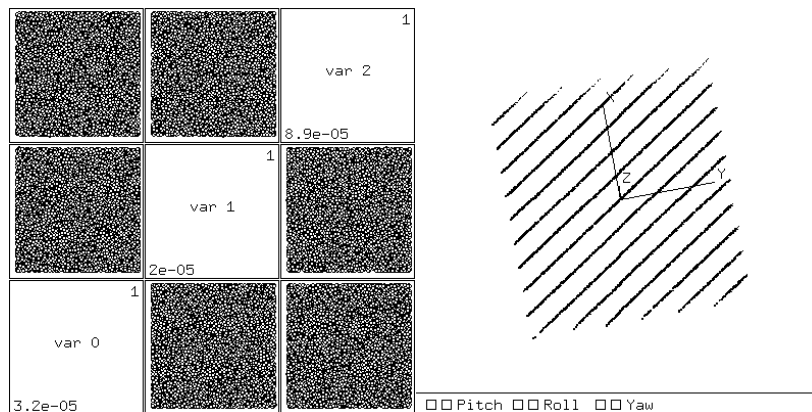
<b>Subsequence</b>	1	2	1	2	1	2	1	2	1	2
--------------------	---	---	---	---	---	---	---	---	---	---

<b>Generator</b>	1	2	3	4	5	6	7	8	9	10
------------------	---	---	---	---	---	---	---	---	---	----

Leap-Frog Partitioning

## 2. 10,000 POINTS FROM RANDU IN 3 DIMENSIONS

An example of what can go wrong with random number generators is illustrated well by the RANDU generator used in many early systems. This generator was found to exhibit relatively good behavior in one or two dimensions as seen in Figure 2.1a, but as can be seen in Figure 2.1b, it's spatial distribution breaks down to parallel hyper-planes in 3 dimensions. This is true of all congruential generators. The closer the planes, the better the quality of the generator.



(a) 2D orthogonal views of data

(b) Parallel hyperplanes in 3D RANDU

FIGURE 2.1.

### 3. ROOTS OF SPECTRAL TESTING OF RNG'S

The spectral test of Coveyou and MacPherson[3, 10] determines the hyper-plane separation in congruential generators. To do this it applies a Fourier analysis to the full period of the generator using the actual generator equations. This type of test is referred to as a theoretical test and is generally applicable only to a single class of generators. While theoretical in nature, considerable computation is required for any particular parameterization of the generator and is practical only with computer algorithms to complete the calculations.

Another theoretical test applicable to lattice structure generators is the discrepancy tests due to Niederreiter[11]. These tests look for the maximum discrepancy from expected counts over sequences of  $s$ -dimensional subregions of the unit hypercube. For example:  $\overline{T^s}$ :  $\Pi_{i-1}^s [0, u_i] \Rightarrow D^*$  (star),  $\Pi_{i-1}^s [u_i, v_i] \Rightarrow D$  (extreme). As with the spectral test this theoretical test requires considerable computation for any particular parameterization of a generator and has been shown to have a computational complexity of  $O(N^k)$ .

A more recent relative of discrepancy is the weighted spectral test [Diaphony][8] developed by Hellekalek and Niederreiter. This test has computational complexity  $O(kN^2)$ .

### 4. PROPOSED TEST

7	56	57	58	59	60	61	62	63
6								
5								
4								
3								
2								
1	8	9	10	11	12	13	14	15
0	0	1	2	3	4	5	6	7
	0	1	2	3	4	5	6	7

FIGURE 4.1.

**Algorithm 4.1.** *Empirical Spectral Test (EST)*<sup>1</sup>:

- 1) Collect the  $k$ -dimensional empirical PDF from generated uniform data over  $b$  cells per dimension giving a  $b^k$  uniform spatial grid as illustrated in Figure 4.1 for the case of  $k = 2$  and  $b = 8$ .
- 2) Use a  $k$ -dimensional FFT to obtain the complex DFT coefficients.
- 3) Test the coefficients for a significant difference from expectation using a comparison of the sum of squares against the Chi-Squared distribution.
- 4) If #3 fails to reject examine the individual coefficients using a Bonferroni interval.

This algorithm has been implemented in a preliminary form using C, Numerical Recipes in C[12] and R[9]. A future implementation integrated better with R and using FFTW[4, 5] is planned.

**4.1. POTENTIAL EFFECTIVENESS OF THE EST.** The EST provides a new view of the uniformity of the generated data which combines spectral and discrepancy features. It looks for structure in the empirical PDF rather than directly in the data and finds 'density' structure in the  $k$ -dimensional data set. It can also potentially benefit from special purpose FFT hardware and software which is readily available. The EST's computational complexity is a function not of  $N$ , but of  $k$  &  $b$ :  $O(kb \log_2 b)$ . Perhaps more importantly, the EST is equally applicable to any form of uniform random sequence, including integer data, binary sequences, and hardware generated sequences.

To explore the potential of the test, FFT's were generated for two well known generators. The first is Marsaglia's Super-Duper which is known to be quite good (although not as good as his later Multiply-With-Carry generators). In the graphics of Figure 4.2, FFT's in each of the first three dimensions were generated and both the coefficients (on the left) and a Q-Q normal plot of all but the first coefficient were plotted. Expected behavior for data with no structure is for the first coefficient to be equal to the mean with the rest being zero. Initial exploratory work indicated that the coefficients appeared to be normally distributed, hence the normal Q-Q plots. Note that Super-Duper appears to behave well, as does RANDU in 1 and 2 dimensions. However RANDU deviates drastically in three dimensions. It appears the EST can be an excellent indicator of at least this type of structure.

<sup>1</sup>The Empirical Spectral Test (EST) is discussed in more detail in [14, 15]. For the purposes of this article, we will be providing only a brief summary.

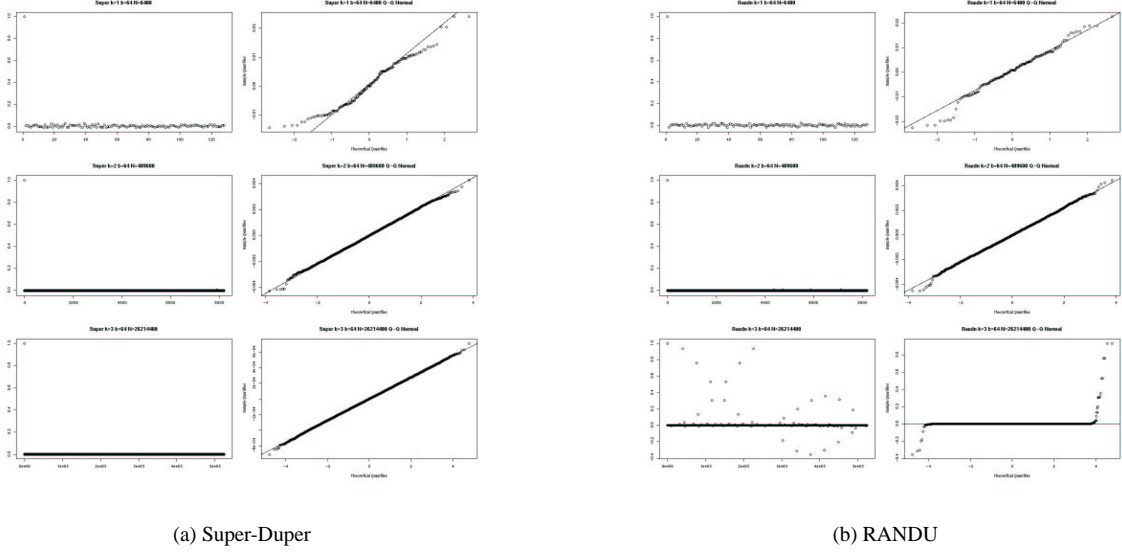


FIGURE 4.2.

## 5. DISTRIBUTION THEORY

In order to provide an objective test, we need the distribution of the transformed data under the null hypothesis. Our null will be independent uniformity of the sequence. This will require determining the distribution of the complex coefficients of the DFT. This will be accomplished by using the known asymptotic behavior of the cell counts and applying linear statistical theory to the resulting structures. Our first step is then to derive a linear algebraic form for the DFT from which we can more easily apply asymptotic distribution theory. Note that a similar matrix formulation can be found in section 14.4 of Garg[6].

**5.1. MATRIX FORM OF THE  $k$ -DIMENSIONAL DFT.** The  $k$ -dimensional DFT is defined for each of the  $T = b^k$  combinations,  $\mathbf{n} = (n_1, \dots, n_k)$ , of Fourier Frequencies as  $f_{\mathbf{n}} = \sum_{l_1=0}^{b-1} \dots \sum_{l_k=0}^{b-1} e^{i\frac{2\pi}{b}n_1l_1} \dots e^{i\frac{2\pi}{b}n_kl_k} y_{l_1, \dots, l_k}$ . We first reorganize the terms to get an inner product in the exponent for each element

$$f_{\mathbf{n}} = \sum_{l_1=0}^{b-1} \dots \sum_{l_k=0}^{b-1} e^{i\frac{2\pi}{b}[l_1n_1+l_2n_2+\dots+l_kn_k]} \cdot y_{l_1, \dots, l_k} = \sum_{l_1=0}^{b-1} \dots \sum_{l_k=0}^{b-1} e^{i\frac{2\pi}{b}\mathbf{l}'\mathbf{n}} \cdot y_{l_1, \dots, l_k}$$

Then define a  $T$  element complex vector of these summations  $\{a_{\mathbf{n}}\}_{l_1, \dots, l_k} = e^{i\frac{2\pi}{b}\mathbf{l}'\mathbf{n}}$  with each of the  $T$  Fourier coefficients now defined as  $f_{\mathbf{n}} = \mathbf{a}_{\mathbf{n}}'\mathbf{y}$ . Then we combine these vectors into the rows of a matrix  $\mathbf{A}$  allowing us to write the DFT as  $\mathbf{f} = \mathbf{A}\mathbf{y}$ .

**5.2. The distribution of the DFT.** The empirical PDF with resolution  $\frac{1}{b} \times k$  of a uniform pseudo random number generator is a  $k$  dimensional multivariate and hence asymptotically normal. We will represent this as a  $T$ -vector  $\mathbf{y} \sim AN_T(\mathbf{1}p, \frac{1}{N}(\mathbf{p}\mathbf{I} - \mathbf{p}\mathbf{p}'\mathbf{J}))$ . We then apply the DFT to this vector to get a  $T$ -vector  $\mathbf{f} \sim AN_T^c(\delta_0, \frac{1}{N}(\mathbf{I} - \delta_0\delta_0'))$  where  $AN_T^c$  denotes a  $T$ -dimensional complex normal distribution<sup>2</sup>. Next we expand our complex distribution into a  $2T$  multivariate normal  $\mathbf{f} = \text{Re}\mathbf{f} + i\text{Im}\mathbf{f}$  with covariance  $\mathbf{S} = \frac{1}{N}(\mathbf{I} - \delta_0\delta_0') = \text{Re}\mathbf{S} + i\text{Im}\mathbf{S}$ , where we have  $\text{Im}\mathbf{S} = \mathbf{0}$ , then we create a  $2T$ -vector  $\mathbf{z} = \begin{pmatrix} \text{Re}\mathbf{f} \\ \text{Im}\mathbf{f} \end{pmatrix} \sim AN_{2T}(\delta_0, \frac{1}{2} \begin{pmatrix} \mathbf{S} & \mathbf{0} \\ \mathbf{0} & \mathbf{S} \end{pmatrix})$ .

**5.3. Overall TEST.** Before writing out the test, we first separate out the two degenerate elements from the coefficient vector using a generalized inverse or simple projection  $\mathbf{P}$ . Define  $\mathbf{g} = \mathbf{P}\mathbf{z}$  where  $\mathbf{P}$  is a  $2(T-1) \times 2T$  matrix defined as:

$$\mathbf{P} = \begin{bmatrix} \mathbf{0}_{\frac{r}{2}} & \mathbf{I}_{\frac{r}{2}} & \mathbf{0}_{\frac{r}{2}} & \mathbf{0}_{\frac{r}{2}} \\ \mathbf{0}_{\frac{r}{2}} & \mathbf{0}_{\frac{r}{2}} & \mathbf{0}_{\frac{r}{2}} & \mathbf{I}_{\frac{r}{2}} \end{bmatrix}, r = 2(T-1)$$

This gives us the asymptotic normal distribution for  $\mathbf{g} \sim AN_{2(T-1)}(\mathbf{0}, \frac{1}{2N}\mathbf{I})$  &  $\mathbf{h} = \begin{pmatrix} z_0 \\ z_T \end{pmatrix} \sim AN_2(\delta_0, \mathbf{0})$ . Using quadratic forms from these two vectors and recombining these into  $X = \mathbf{g}'[\frac{1}{2N}\mathbf{I}]^{-1}\mathbf{g} + [2N(\mathbf{h} - \delta_0)]^2 \sim \chi_{2T-2}^2$  we have a common quadratic form with a chi-squared (asymptotic) distribution. This allows us to use a standard rejection region where we reject  $H_0: (p_i = \frac{1}{T} \forall i)$ , if  $P(X = 2N \sum_{l=0}^{2T-1} z_l^2 - 1 < C) > 1 - \alpha$ .

<sup>2</sup>See Brillinger[1] or Brockwell and Davis[2] or covered in somewhat greater detail by Goodman [7]. Detail of the derivation of the PDF and characteristic function for this distribution is available in Wooding [13].

Expected cell count	k	b	T	N	RNG values	Resolution	Volume
8	1	8192	8192	65536	65536	0.00012	0.00012
8	2	64	4096	32768	65536	0.01563	0.00024
5	3	16	4096	20480	61440	0.06250	0.00024
4	4	8	4096	16384	65536	0.12500	0.00024
12	5	4	1024	12288	61440	0.25000	0.00098

Table: 6

Generator	1	2	3	4	5
RANDU	0.003	0.982	0.000	0.000	0.055
Super-Duper	0.074	0.733	0.198	0.214	0.062

Table: 6

Generator	1	2	3	4	5
Marsaglia-Multi-carry	<b>0.075</b>	0.689	<b>0.057</b>	0.945	0.504
Super-Duper	0.347	0.838	0.847	0.800	0.137
Mersenne-Twister	0.172	0.246	0.912	0.863	0.761
Knuth-TAOCP	0.956	0.467	0.974	0.839	0.452
Wichmann-Hill	0.677	0.870	<b>0.031</b>	0.870	0.418

Table: 10

5.4. **Confidence INTERVALS.** Using a Fisher protected LSD procedure, we derive standard confidence intervals as well as intervals based on Bonferroni levels to use in the case that the overall test does not reject. The interval for the individual components is based on  $\mathbf{g}$  which is  $AN_{2T-2}(\mathbf{0}, \frac{1}{2N}\mathbf{I})$  and uses  $\sqrt{2N}g_j$ , which is a standard normal. This gives us a normal cutoff of  $K_1 : 1 - \Phi(K_1) < \frac{\alpha}{2}$ , and a Bonferroni cutoff,  $L_1 : 1 - \Phi(L_1) < \frac{\alpha}{4(T-1)}$ . In order to look at a combined value for each complex pair we also look at cutoffs based on the magnitude of the complex coefficient based on  $|f_j|^2 = (Re(f_j))^2 + (Im(f_j))^2$ . We use  $|\sqrt{2N}f_j|^2 \sim X_2^2$ , giving a normal cutoff of  $K_2 : P(2N|f_j|^2 < K_2) > 1 - \alpha$  and a Bonferroni cutoff,  $L_2$  which is the  $1 - \frac{\alpha}{T-1}$  quantile of the  $X_2^2$  distribution.

5.5. **Testing summary.** This then gives us the objective means to test for and identify coefficients which are indicators of unexpected structure within the  $k$ -dimensional data structure derived from the original sequence. Matching of the coefficients with associated frequencies can be used to identify the nature of the structure and hence the potential failure in the underlying generator or sequence. Note that this is not necessarily a test of the entire period of a generator, but only of the sequence we're interested in.

### 6. ANOTHER LOOK AT THE RANDU AND SUPER-DUPER GENERATORS

Tests using the parameterizations in table 6 were run against both RANDU and SUPER-DUPER. This table shows the p-values obtained from calculation of the EST to the indicated subsequences. As expected, RANDU rejects strongly in three dimensions and up. Note that it also fails in one dimension and at two dimensions did not reject. There were coefficients which exceeded the Bonferroni limits for even one and two dimensions.

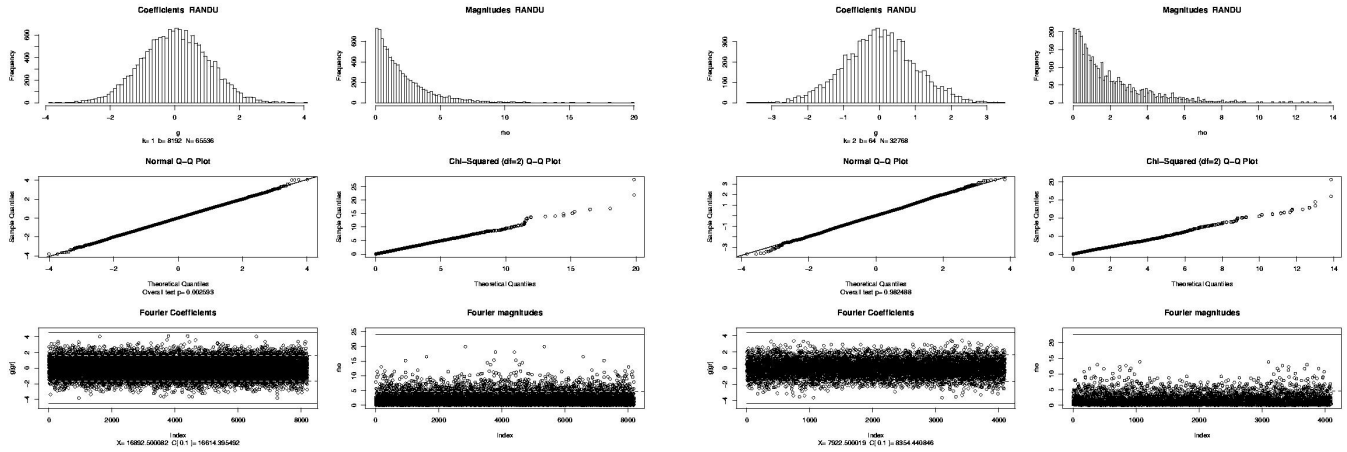
Super-Duper rejects at  $k=5$ , but not at the lower dimensions we looked at earlier.

### 7. TESTS RUN AGAINST THE GENERATORS IN R

We also ran the EST against the default generators available in the R statistical package using the same parameterization as in Table 6. These are readily available generators for statistical simulation and some of the best available today. Results are tabulated in table 7. When looking at this data, it is useful note a quote from Marsaglia's DIEHARD test descriptions "keep in mind that 'p happens'". When testing random number generators, one should never take a single rejection as an indictment of the generator. A rejection is simply a suggestion that a problem may exist and that further investigation is warranted.

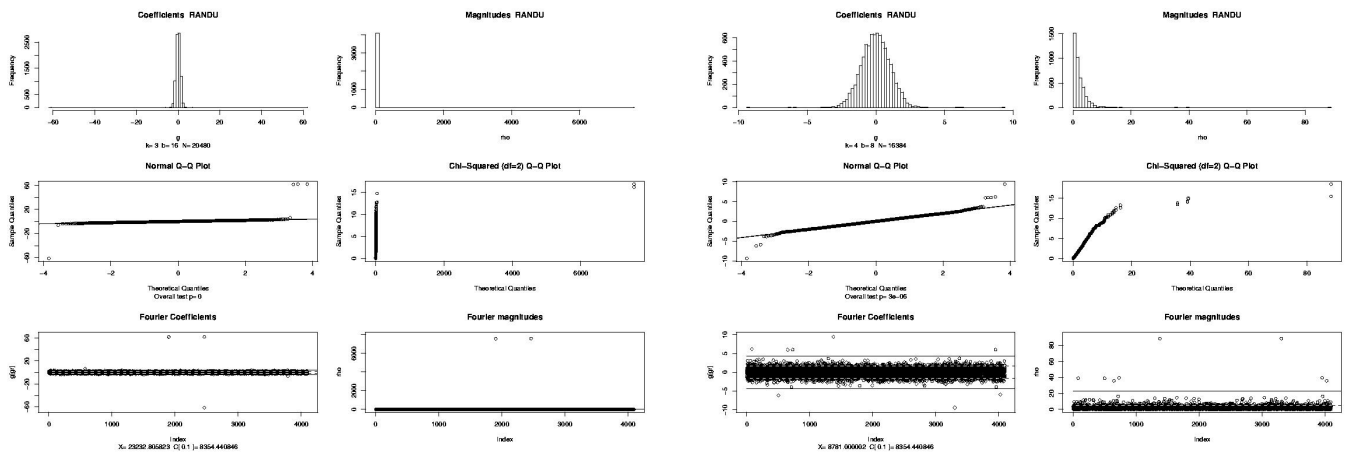
**Marsaglia-Multi-carry  $k=3$ :** Figure 7.1a shows results for  $k=3$  Marsaglia's multiply-with-carry RNG, it has a period of over  $2^{60}$  and has passed all of Marsaglia's tests. This is the default generator for R. By itself this rejection means little but is interesting. Further runs have suggested this failure may be significant, but the work is not yet complete.

**Wichmann-Hill  $k=3$ :** Figure 7.1b shows results for  $k=3$  on the Wichmann-Hill generator. Note the graphics show no clear outliers. A close examination of the histogram of magnitudes shows a distinctly heavy tail is causing the rejection.



(a) RANDU k=1

(b) RANDU k=2



(c) RANDU k=3

(d) RANDU k=4

FIGURE 6.1.

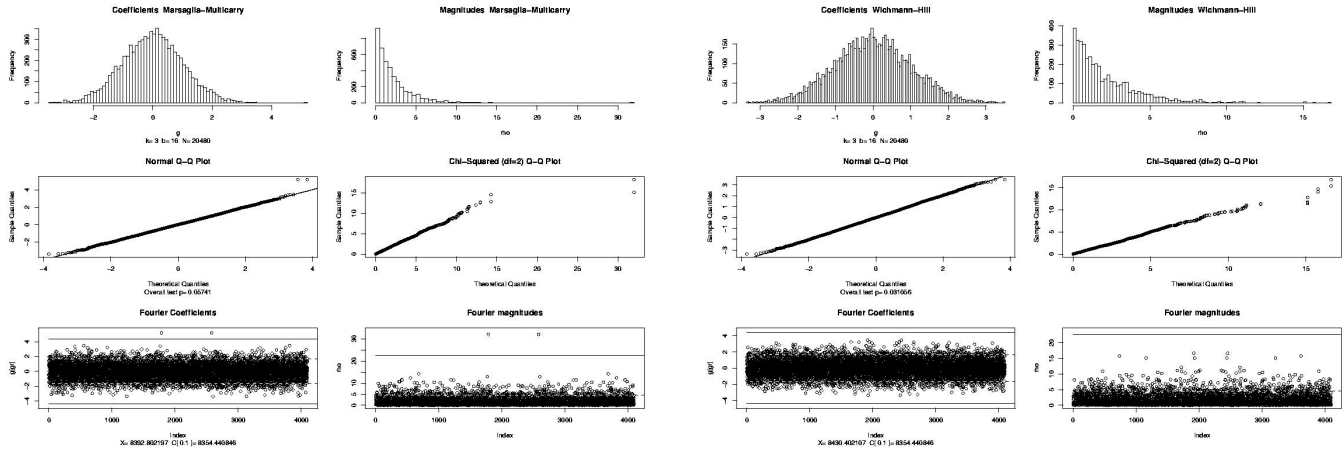
**Mersenne-Twister k=1:** Figure 7.2a shows the Mersenne-Twister at k=1. This is a twisted generalized feedback shift register generator with period  $2^{19937} - 1$  and equidistribution in 623 consecutive dimensions (over the whole period). Note outliers do show up above the Bonferroni 10% levels.

**Knuth-TAOCP k=4:** Figure 7.2b shows k=4 results for the Knuth-TAOCP generator. It's a generalized feedback shift register generator using lagged Fibonacci sequences with subtraction. The p value is high (0.870), but we have a hit on the Bonferroni limits.

REFERENCES

[1] David R. Brillinger. *Time Series Data Analysis and Theory*. Holt, Reinhart & Winston, Inc., 1975.  
 [2] Peter J. Brockwell and Richard A. Davis. *Time Series: Theory and Methods*. Springer-Verlag New York, Inc., second edition, 1991.  
 [3] R. R. Coveyou and R. D. Macpherson. Fourier analysis of uniform random number generators. *J. Assoc. Comput. Mach.*, 14:100–119, 1967.  
 [4] M. Frigo and S.G. Johnson. Fftw: An adaptive software architecture for the fft. In *ICASSP conference proceedings*, volume 3, pages 1381–1384, 1998.  
 [5] Matteo Frigo. A fast fourier transform compiler. In *ACM SIGPLAN Conference on Programming Language Design and Implementation*, 1999.  
 [6] Hari Krishna Garg. *Digital Signal Processing Algorithms: Number Theory, Convolution, Fast Fourier Transforms, and Applications*. CRC Press, 1998.

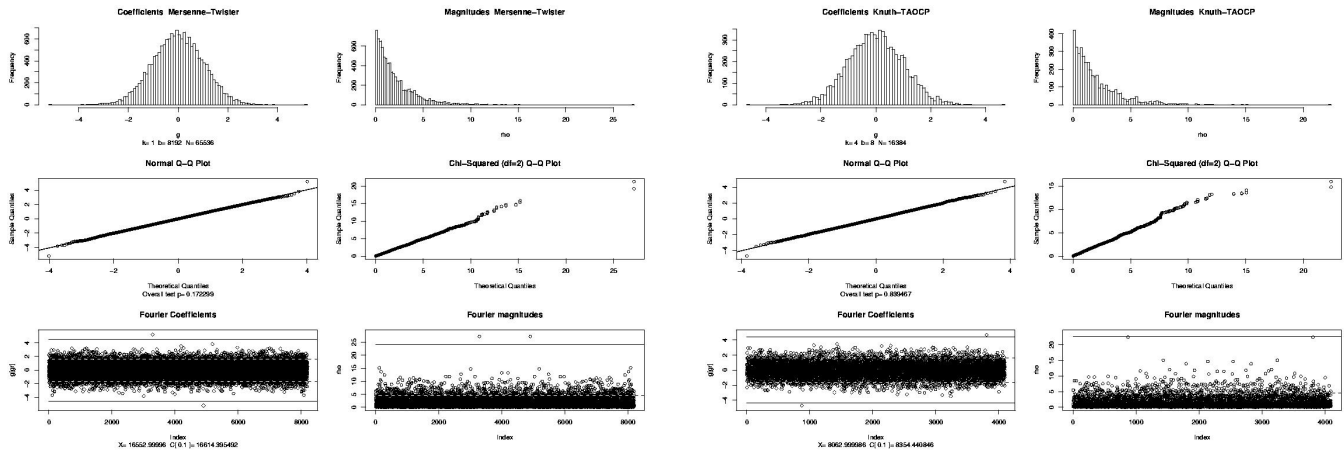
- [7] N. R. Goodman. Statistical Analysis Based on a Certain Multivariate Complex Gaussian Distribution (An Introduction). *Annals of Mathematical Statistics*, 34(1):152–177, 1963.
- [8] H. Hellekalek, P.: Niederreiter. The weighted spectral test: diaphony. *ACM Transactions on Modeling and Computer Simulation*, 8(1), Jan 1998.
- [9] Ross Ihaka and Robert Gentleman. R: A language for data analysis and graphics. *Journal of Computational and Graphical Statistics*, 5(3):299–314, 1996.
- [10] D.E. Knuth. *The art of computer programming, vol. 2: seminumerical algorithms*, volume 2. Addison Wesley Longman, Reading, MA, 3 edition, 1997.
- [11] Harald Niederreiter. *Random Number Generation and Quasi-Monte Carlo Methods*. SIAM, Philadelphia, PA, 1992.
- [12] William H. Press, Saul A. Teukolsky, William T. Vetterling, and Brian P. Flannery. *Numerical Recipes in C: The Art of Scientific Computing*. Cambridge University Press, 2nd edition, 1992.
- [13] R. A. Wooding. The Multivariate Distribution of Complex Normal Variables. *Biometrika*, 43(1/2):212–215, June 1956.
- [14] David Zeitler. *Empirical Spectral Analysis of Random Number Generators*. Thesis, Western Michigan University, 2001.
- [15] David Zeitler, Joseph McKean, and John Kapenga. Empirical spectral test (est) of random number sequences. Unpublished, 2002.



(a) Marsaglia-Multicarry k=3

(b) Wichmann-Hill k=3

FIGURE 7.1.



(a) Mersenne-Twister k=1

(b) Knuth-TAOCP k=4

FIGURE 7.2.