Higher-Dimensional Properties of Non-Uniform Pseudo-Random Variates

Josef Leydold[1⋆], Hannes Leeb[2⋆⋆], and Wolfgang Hörmann[3]

[1] Department for Statistics, WU Wien, Augasse 2–6, A-1090 Vienna, Austria
email: Josef.Leydold@statistik.wu-wien.ac.at
[2] ISOC, University of Vienna, Universitätsstraße 5, A-1010 Vienna, Austria
email: leeb@smc.univie.ac.at
[3] IE Department, Boğaziçi University Istanbul, 80815 Bebek-Istanbul, Turkey
email: Wolfgang.Hoermann@statistik.wu-wien.ac.at

Abstract. In this paper we present the results of a first empirical investigation on how the quality of non-uniform variates is influenced by the underlying uniform RNG and the transformation method used. We use well known standard RNGs and transformation methods to the normal distribution as examples. We find that except for transformed density rejection methods, which do not seem to introduce any additional defects, the quality of the underlying uniform RNG can be both increased and decreased by transformations to non-uniform distributions.

1 Introduction

The literature on random number generation falls into two main groups: (1) Uniform random number generation and (2) the generation of non-uniform random variates. The first group contains a large number of works dealing with the quality of different uniform pseudo-random number generators, e.g. the monograph of Niederreiter (1992), and the papers of L'Ecuyer et al. (1998), Leeb and Wegenkittl (1997) or Marsaglia (1985). In the second group most papers discuss the generation of non-uniform variates by transforming a sequence of independent identically distributed (iid) uniform random numbers and are mainly concerned with the speed or simplicity of the proposed algorithms. Concerning quality it is only stated that the method is exact, which means that perfect iid uniform random numbers (which are not available) would be transformed into independent random numbers of the correct distribution.

Investigations dealing with the effects that can occur when such an exact transformation method is combined with a pseudo-random sequence (this is done in every simulation which needs non-uniform random numbers) are very rare and are mainly discussing the quality of the one-dimensional distribution. (Section 3 gives references and a short summary of the literature.)

⋆ address of correspondence
⋆⋆ Research supported by the Austrian Science Foundation (FWF), project no. P11143-MAT

It is well known and accepted that one must investigate the distribution of n-tuples in several dimensions to assess the quality of a uniform random number generator, especially to check if the generated pseudo-random numbers really behave like independent random variables. This question was posed for non-uniform variates by the last author in his latest paper on this topic (Hörmann 1994b). But at that time he saw no possibility to investigate the distribution of n-tuples that are not forming a lattice.

The progress in computer power, the discussion of new quality measures like diaphony instead of discrepancy, and the new proposal of high-dimensional tests for random number generators give us the possibility to tackle this question now. It is our aim to investigate the quality of non-uniform pseudo-random variates by analyzing their multidimensional distribution. In particular we pose the question how the quality of the non-uniform variates is influenced by that of the uniform generator and the transformation method. To get an idea of the possible phenomena we have picked the normal distribution and have tested several transformation methods combined with different uniform pseudo-random number generators (uniform RNG). Thus this paper is intended as a preliminary study. Further theoretical and empirical studies have to be done.

Section 2 describes these used methods and uniform random number generators. Section 3 gives a short summary of the literature. Section 4 shows the results of our empirical tests. Section 5 summarizes our experiences.

2 Preliminaries

Uniform random number generators. There exists a huge number of different uniform RNGs (see e.g. L'Ecuyer (1994)). For our tests we have selected the following uniform random number generators:

- Linear congruential generators (LCG):
  - `fish` (Fishman and Moore 1986)
    $u_{n+1} = 950\,706\,376\,u_n \pmod{(2^{31}-1)}$ period: $2^{31}-2$
    remark: lattice optimal in dimensions 2 to 6.
  - `lcga` (Schmidt 1996)
    $u_{n+1} = 10\,767\,581\,u_n + 227\,623\,267 \pmod{2^{30}}$ period: 2^{30}
    remark: lattice bad for subsequence $\{u_0, u_2, u_4, \ldots\}$.
    results of spectral test in dimension 2 are: 0.963 and 0.051 for the sequence and subsequence, respectively.
  - `randu` (see Park and Miller 1988)
    $u_{n+1} = 65539\,u_n \pmod{2^{31}}$ period: 2^{29}
    remark: lattice: very bad in dimensions 3 and 4.
- Inversive congruential generators (ICG):
  ($\overline{u}$ denotes the multiplicative inverse of u mod M, with exception $\overline{0} = 0$)
  - `icg` (Eichenauer and Lehn 1986)
    $u_{n+1} = \overline{u_n} + 1 \pmod{(2^{31}-1)}$ period: $2^{31}-1$
    remark: no lattice.

  - `eicg1` (Eichenauer-Herrmann 1993)
    $u_n = \overline{n} \pmod{(2^{31}-1)}$ period: $2^{31}-1$
    remark: no lattice.
- Twisted GFSR generator:
  - `tt800` (Matsumoto and Kurita 1994)
    period: $2^{800}-1$
    remark: excellent equidistribution properties up to dimension 25.

LCGs are the most common generators. These generators possess a lattice structure, i.e. the set of all n-tuples form a lattice in $\mathbb{R}^n$. Figure 1 shows such a scatter plot of all overlapping tuples $(u_0, u_1), (u_1, u_2), (u_2, u_3), \ldots$ of the "baby" generator $u_{n+1} = 869\, u_n + 1 \pmod{1024}$. We have tested LCGs with good (`fish`) and bad (`randu`) lattice structure. For comparison we have selected ICG and EICG (new types of generators without any lattice structures) and the twisted GFSR generator.

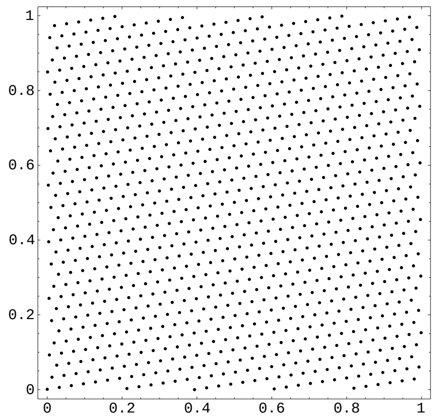


Fig. 1. Overlapping tuples of all terms of the LCG $u_{n+1} = 869\, u_n + 1 \pmod{1024}$

Transformation methods. To generate non-uniform random variates again a great variety of (exact) transformation methods are known and can be found in the monograph Devroye (1986) generally accepted as the "bible" in that field of research. Some basic methods for generation of normal variates are

- The *inversion method*, which transforms the uniform random number into a random variate of the desired distribution using the inverse of the cumulative distribution function F^{-1}. (Not efficient for the normal distribution).
- The *rejection method*, one of the oldest but still the most important and most flexible method for generating non-uniform random variates. It is necessary to specify a dominating or hat function and a method to generate variates from that hat.

- The *decomposition method* uses a discrete mixture of densities of easy to generate variates.
- A combination of decomposition and rejection we will call *patchwork-rejection*.

The following transformation methods are used for our tests (E(#URN) denotes the expected numbers of iid uniform random numbers U_i needed to generate one normal variate):

- `inversion` (only for comparison)
- `box-muller` (Box and Muller 1958)
  The *Box-Muller* method (only applicable for the normal distribution) uses a transformation between the two-dimensional uniform and the two-dimensional standard normal distribution ($Y_j \ldots$ normal variates):
  $$Y_i = \cos(2\pi\, U_{i+1}) \sqrt{-2 \log U_i}$$
  $$Y_{i+1} = \sin(2\pi\, U_{i+1}) \sqrt{-2 \log U_i}$$
  E(#URN) $= 1$ (2 for 2)
- `polar` (Marsaglia 1962)
  A variant of the Box-Muller method which uses an acceptance-rejection technique to avoid Sine and Cosine.
  $S = (2\,U_i - 1)^2 + (2\,U_{i+1} - 1)^2$, reject if $S = 0$ or $S > 1$, otherwise return
  $$Y_i = (2\,U_i - 1) \sqrt{-2 \log S / S}$$
  $$Y_{i+1} = (2\,U_{i+1} - 1) \sqrt{-2 \log S / S}$$
  E(#URN) $= \frac{4}{\pi} \approx 1.27$
- `nquo` (Kinderman and Monahan 1977)
  The *ratio of uniforms* method is a variant of rejection that uses the fraction of two uniforms to generate variates from the hat function. It is an application of the theorem:
  If (U, V) is uniformly distributed over $A = \{(u, v) \colon 0 \le u \le \sqrt{f(u/v)}\}$ then U/V has density proportional to f.
  Generate (U, V) by enclosing A in a rectangle; reject if $U > \sqrt{f(U/V)}$, otherwise return U/V.
  E(#URN) ≈ 2.72
- `nkira` (Kinderman and Ramage 1976)
  This patchwork-rejection method combines different methods by partitioning the area below the density function.
  E(#URN) ≈ 2.16
- `nacr` (Hörmann and Derflinger 1990)
  Another patchwork-rejection method that combines an acceptance-complement method with ratio of uniforms.
  E(#URN) ≈ 1.48

– `ntdr`x (Devroye 1986; Hörmann 1995)
Transformed density rejection with x points of contact uses a dominating function that is constructed by the minimum of x tangents to the transformed density (see Fig. 2). Variates with density proportional to the hat function are generated by inversion. For large x the expected number of uniform random numbers for generating one normal variate tends to 2 (Tab. 1). Thus for large x acceptance is almost sure and this method is near to the inversion method. Notice that this is an inversion from the step 2 subsequence $\{u_0, u_2, u_4, \ldots\}$, called `sub2` in Tab. 3 and 4.

Table 1. Expected number of uniform random numbers for `ntdr`x

x	2	3	5	10	20	30	50	100
E(#URN)	2.63	2.26	2.10	2.026	2.0067	2.0030	2.0011	2.0002

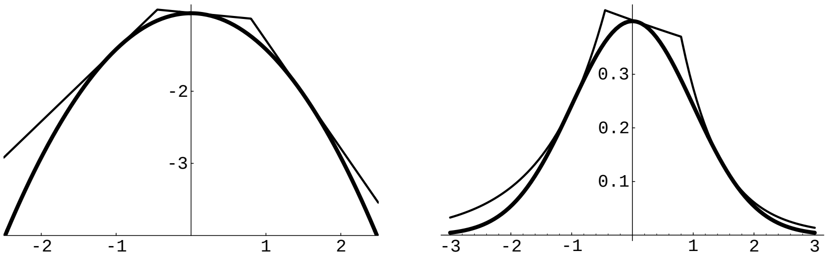
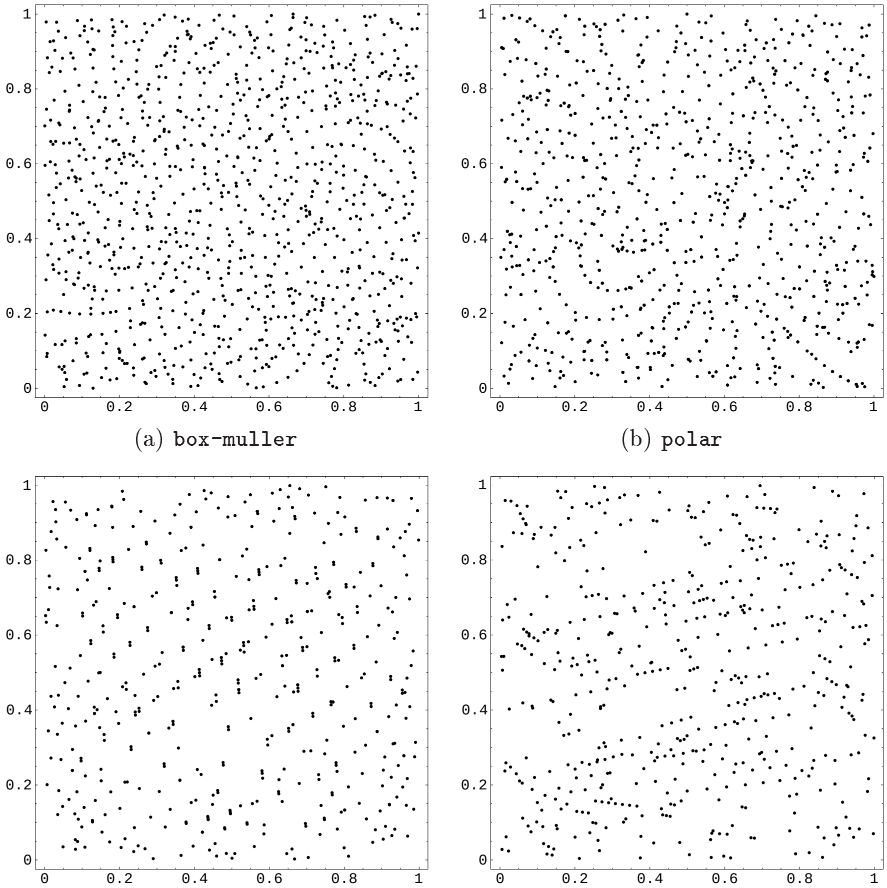


Fig. 2. Construction of a dominating function with 3 points of contact

Figures 3 and 4 show the effect of these transformation methods. The normal variates are transformed back to uniform variates by means of the cumulative distribution function F and plotted in the same way as the source sequence of uniform random numbers in Fig. 1. Notice that the number of different generated numbers differs between different methods.

It is necessary to define how we are going to measure the quality of generated random variates of different distributions. It turned out that the easiest way is to transform the random variates by the cumulative distribution function F into uniform random variates. Then we can use all tests and performance measures introduced for uniform generators.

As an immediate consequence of our approach it follows that the inversion method preserves the quality of uniform generators (in all dimensions), since $F(F^{-1}(U)) = U$.



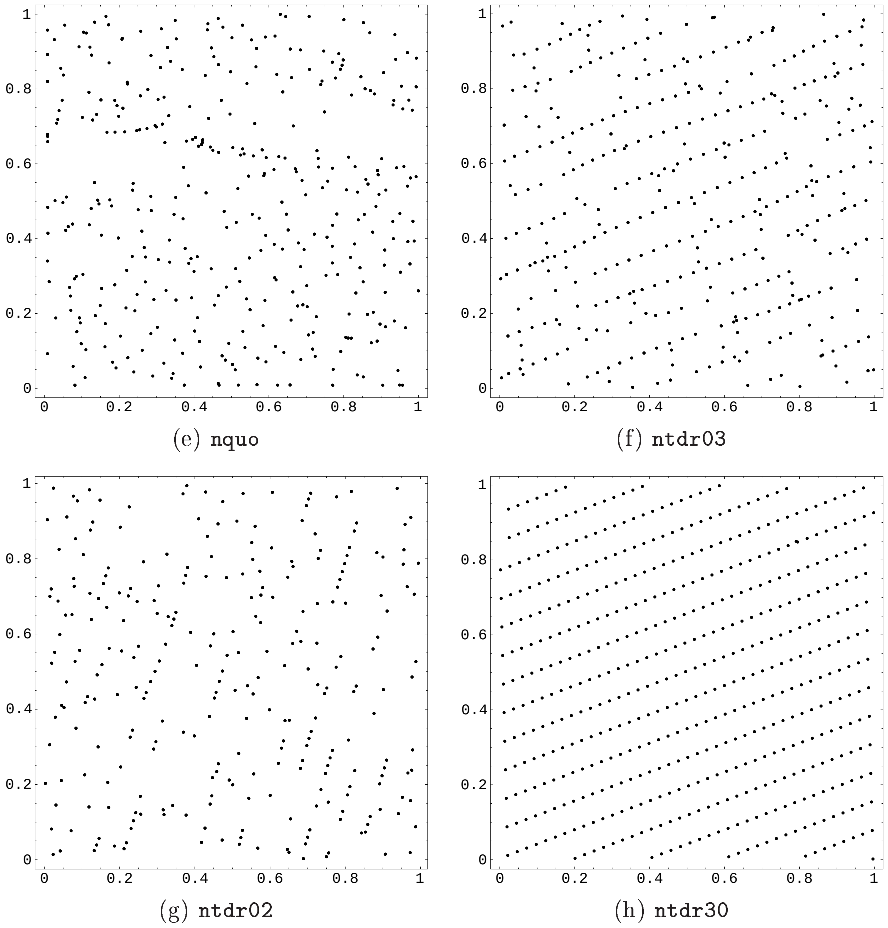
(a) box-muller (b) polar

(c) nkira (d) nacr

Fig. 3.

3 Known facts on the quality of random variates

Devroye (1982) derives some measures for the error that is committed when the exact density f is approximated by a density g and gives some bounds. Monahan (1985) discusses the problem of accuracy that is caused by approximations and discretization error on a digital computer, but the randomness of the pseudo-random number generator is not an issue. Deng and Chhikara (1992) propose a new criterion of *robustness* to compare the effects of imperfect uniform RNGs on different transformation methods and give some examples. (No RNG produces a truly random uniform sequence, i.e. the true distribution of such uniform RNG differs slightly from uniform distribution.) But none of these papers considers the combination of transformation methods with uniform generators used in practice.



(e) nquo (f) ntdr03

(g) ntdr02 (h) ntdr30

Fig. 4.

The first transformation method, whose quality was considered in the literature is the Box-Muller method. After papers in the seventies (e.g. Neave 1973) containing warnings against the use of that method, it was demonstrated in (Afflerbach and Wenzel 1988) that the method can be viewed as a two-dimensional inversion method. The two-dimensional structure of the uniform generator is not preserved but transformed into a system of intersecting spirals (see Fig. 3(a) and 3(b)). Thus the structure of the normal variates is different from the structure of the uniform random numbers but the quality of the uniform generator is preserved.

The last author studied the quality of non-uniform random variates already between 1990 and 1993. His results (Afflerbach and Hörmann 1992; Hörmann and Derflinger 1993; Hörmann 1994a; Hörmann 1994b) are restricted to the one-dimensional distribution and to LCGs only.

For the ratio of uniforms method it turned out that the combination with an LCG always results in a defect. Due to the lattice structure of random pairs generated by an LCG there is always a hole without a point with probability of the order $1/\sqrt{M}$, where M is the modulus of the LCG.

For the rejection method combined with an LCG the empirical results for the one-dimensional distribution were found to be satisfactory. Only if an LCG with a small multiplier (about $\sqrt{M}$) is used the micro structure of the one dimensional distribution becomes bad. This can be seen using a simple geometric argument together with the fact that the two-dimensional lattice of an LCG with small multiplier is covered by about $\sqrt{M}$ lines almost parallel to the vertical axis. Therefore the accepted points lie in one small interval, the rejected points in the next small interval thus ruining the micro structure of the distribution. All other transformations combined with LCGs showed no special problems of the one-dimensional distribution.

Recently considerations about the quality of an RNG become more and more important. E.g. Herendi et al. (1997) investigated performance and the randomness of their new Gaussian RNG.

4 An empirical investigation

We have used the following model:

1. Use a uniform RNG to generate a sequence $u_0, u_1, u_2, \ldots$.
2. Use a transformation method to produce a sequence $g_0, g_1, g_2, \ldots$ (These numbers should be Gaussian iid random numbers).
3. Apply the cumulated distribution function F to this sequence.

The resulting sequence $F(g_0), F(g_1), F(g_2), \ldots$ should then be a sequence of uniform iid random numbers. Thus we can use techniques for testing uniform RNGs.

We have used 2-level tests with the following combinations

level 1	*level 2*
• M-Tuple test	• Kolmogorov-Smirnov
• Diaphony	• Diaphony
• Walsh-Diaphony	• χ^2

The number of repetitions of the test in the first level is given by the "samples" parameter in Tab. 2–5. The number of bins for the χ^2 test was selected, s.t. the expected number of hits was at least 6.

M-Tuple test. (Good 1953; Marsaglia 1985)
We have used an overlapping serial test as described in Leeb and Wegenkittl (1997) where the partition in a given dimension d is defined by partitioning each axis into 2^s intervals of equal length. s is the size parameter in Tab. 2–4,

and the sample size was set to $3 \cdot 2^{s\,d}$. Table 2 shows some results of our tests. The darkness of the fields indicates the minimum of the p-values of the three level 2 tests.

We have also tested the effect of increasing the numbers of touching points for the transformed density rejection. The results are given in Tab. 3 and 4.

Diaphony. (Zinterhof 1976; Leeb and Hellekalek 1998)
The test statistics for this test is given by

$$F_n = \left(\frac{1}{n^2} \sum_{i,j=1}^{n} g(\mathbf{x}_i - \mathbf{x}_j) \right)^{1/2}$$

where n is the sample size and $g(\mathbf{x}) = \prod_{i=1}^{d} \big(f(\mathbf{x}^{(i)}) + 1\big) - 1$, where $f(x) = -\pi^2/6 + \pi^2/2(1 - 2\,\{x\})^2$. $\{x\}$ denotes the fractional part of x and $\mathbf{x}^{(i)}$ the i-th coordinate of $\mathbf{x}$. Table 5 shows some results of our tests.

Walsh-Diaphony. (Hellekalek and Leeb 1997; Leeb and Hellekalek 1998)
The test statistics is similar to that of the Diaphony tests. The results for the Walsh-Diaphony tests are very similar to the results of the Diaphony tests and thus omitted here.

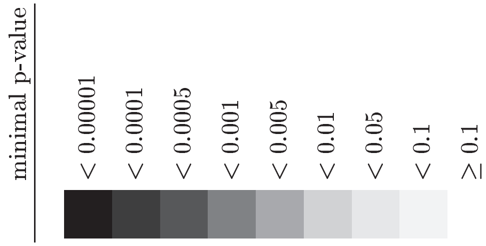
5 Summary and concluding remarks

The results of these empirical tests can be interpreted in different ways:

About transformation methods.

- Transformations which preserve global structure inherit the quality and defects of the uniform generator, i.e. their behavior is more transparent (compare e.g. the results for `lcga` in Tab. 2 for the `ntdr`x methods (structure preserving) with `nquo`; see also Tab. 3).
- The quality of subsequences of the uniform RNG is (sometimes) crucially important for the quality of the non-uniform RNG (compare e.g. `inv` and `sub2` in Tab. 3 and 4).
- We suggest transformed density rejection with many touching points together with an uniform RNG with a high quality step 2 subsequence when the quality of the non-uniform pseudo-random numbers should be guaranteed without making investigations on the used pair generator/method.
- Global structures are not preserved by all methods except by inversion and inversion-rejection methods (e.g. `ntdr`).
- Thus there is no strong correlation between quality of uniform RNG and the corresponding non-uniform generator for most of these transformation methods (i.e. the non-uniform generator might be better or sometimes worse). For example the results for `randu` and `ntdr03` are worse than the corresponding subsequence `sub2`, see Tab. 3 and 4.

Table 2. M-Tuple test



test	dim	size	samples
1	3	4	512
2	3	6	512
3	4	4	512
4	5	4	512

sample size $= 3 \times 2^{\text{size} \cdot \text{dim}}$

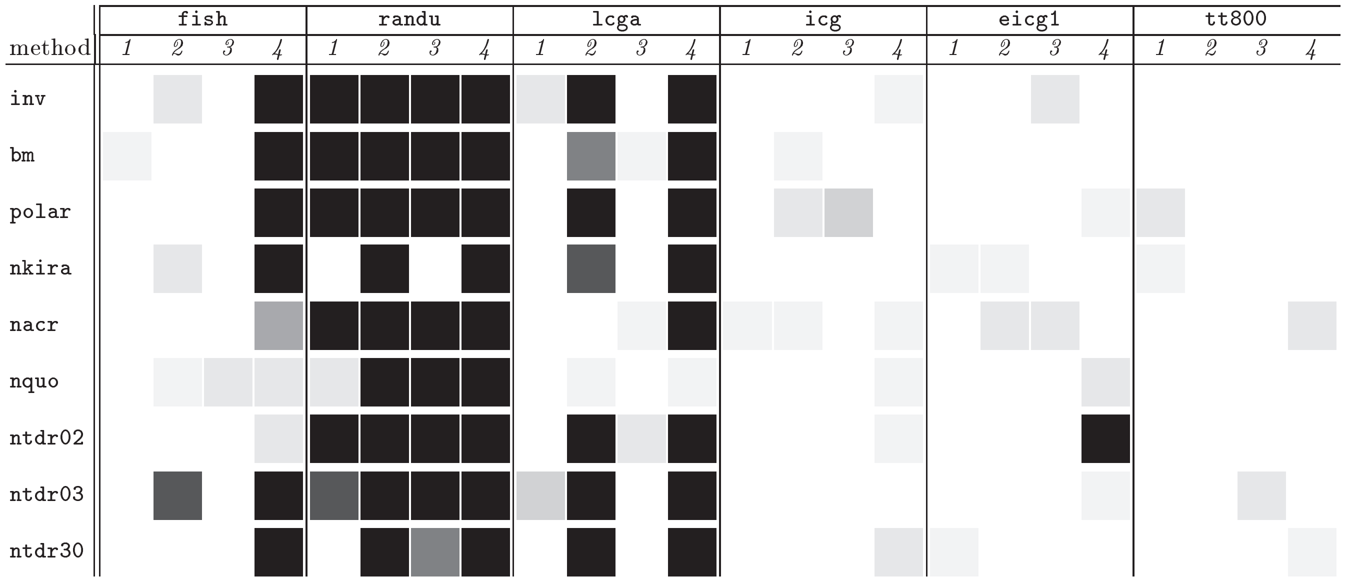
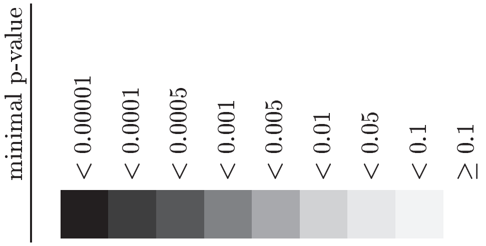


Table 3. M-Tuple tests for `ntdr`



test	dim	size	samples
1	3	4	32
2	3	4	128
3	3	4	512
4	3	4	2048
5	3	4	8192

test	dim	size	samples
6	3	6	32
7	3	6	128
8	3	6	512

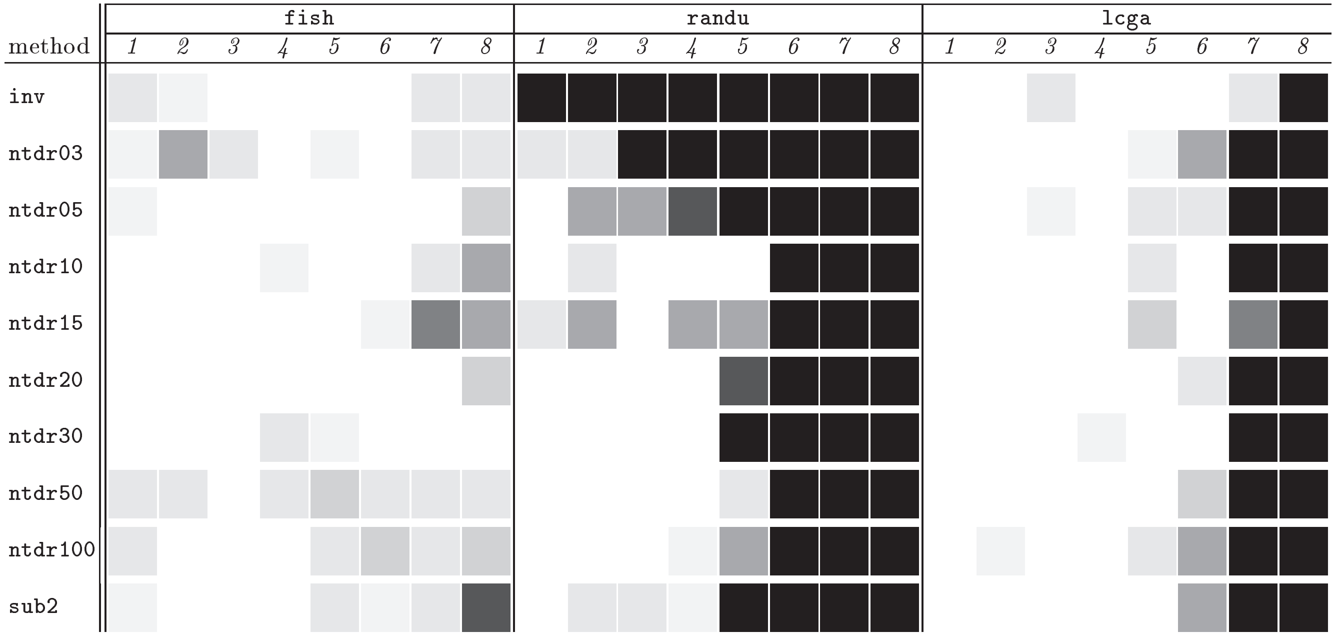
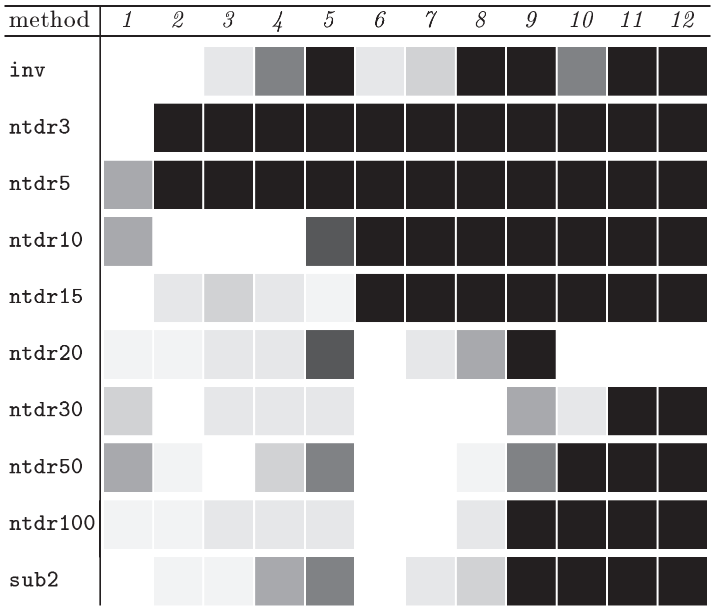


Table 4. M-Tuple tests for `ntdr/randu`, dim=2



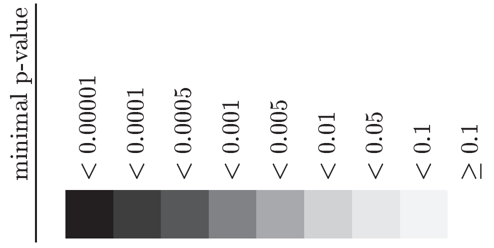
test	1	2	3	4	5	6	7	8	9	10	11	12
size	4	6	6	6	6	8	8	8	8	9	9	9
samples	2048	32	128	512	2048	32	128	512	2048	32	128	512

– Consequently each pair generator/method needs exhaustive investigations.

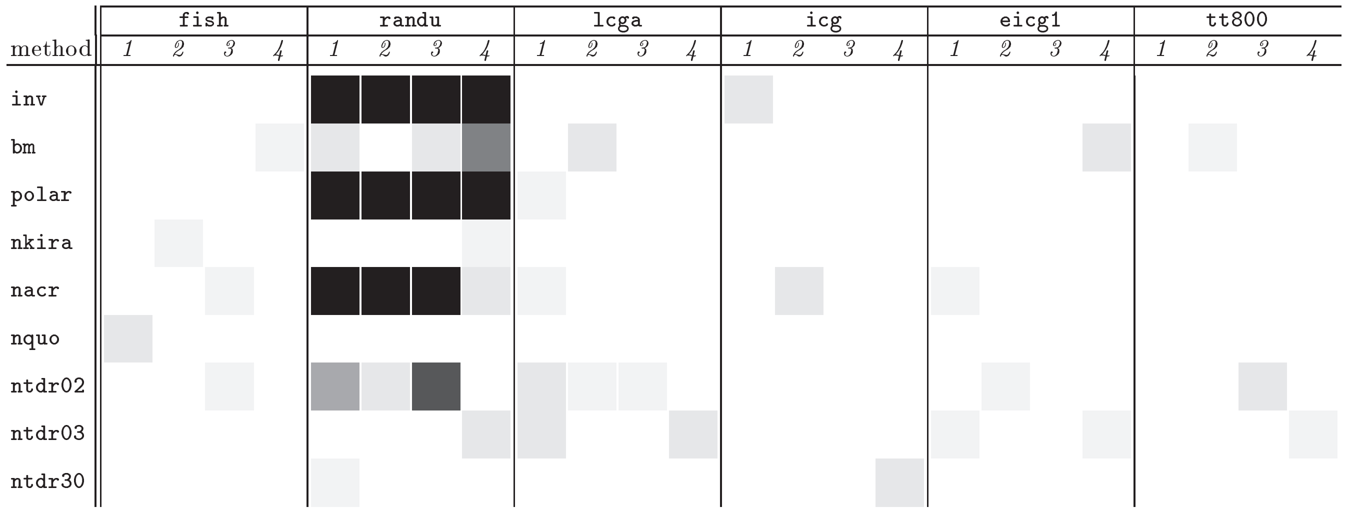
About Tests.

– The existing tests seem not to be very sufficient for this problem. Many tests have been developed to detect deficiencies in LCGs and are insensitive to non-linear structures. Thus most of the transformation methods seem to improve the "randomness" of the uniform RNG as they "mix" the structures of the uniform generator.
– The tests detect global structural deficiencies but fail to find local ones (e.g. `nquo`). We have also tested the hat function of `ntdr` as approximate density and have used inversion from the hat without rejection. Although the resulting random numbers are not normal any more, the M-Tuple test did not show any problems when we had at least 15 points of contact.

Table 5. Diaphony test



test	dim	sample size	samples
1	3	4096	512
2	3	8192	128
3	5	8192	128
4	8	8192	128



About Simulation.

- In spite of their deficiencies LCGs are commonly used RNGs (see L'Ecuyer (1994)). Reasons are: (1) they are simple and well studied; (2) only small fractions of the period are (*should be*) used (thus some of our tests used too many numbers); (3) nearly all models that are used for simulation are non-linear. A generally accepted rule states that this "improves" the quality of the resulting random variates. Although this is true in almost all cases, we have found some counter examples, where the resulting variate is "less random" than the underlying uniform LCG (e.g. `randu/ntdr03` in Tab. 4).

Acknowledgment

The authors wish to note their appreciation for help rendered by Karl Entacher. He suggested the use of the SIMPLEX generator. The tests in this study were performed using the pLAP-package developed in Peter Hellekalek's research project P11143-MAT. Thanks are due to Jürgen Eichenauer-Herrmann for his interest in this work.

References

Afflerbach, L. and Hörmann, W. 1992. Nonuniform random numbers: A sensitivity analysis for transformation methods. In G. C. Pflug and U. Dieter Eds., *Lecture Notes in Econom. Math. Systems*, Volume 374, pp. 135–144. New York: Springer.

Afflerbach, L. and Wenzel, K. 1988. Normal random numbers lying on spirals and clubs. *Statistical Papers 29*, 237–244.

Box, G. E. P. and Muller, M. E. 1958. A note on the generation of random normal deviates. *Annals of Mathem. Stat. 29*, 2, 610–611.

Deng, L. Y. and Chhikara, R. S. 1992. Robustness of some non-uniform random variate generators. *Statistica Neerlandia 46*, 2–3, 195–207.

Devroye, L. 1982. A note on approximations in random variate generation. *J. Stat. Comput. Simul. 14*, 149–158.

Devroye, L. 1986. *Non-Uniform Random Variate Generation*. Springer-Verlag, New-York.

Eichenauer, J. and Lehn, J. 1986. A non-linear congruential pseudo random number generator. *Statistical Papers 27*, 315–326.

Eichenauer-Herrmann, J. 1993. Statistical independence of a new class of inversive congruential pseudorandom numbers. *Math. Comp. 60*, 375–384.

Fishman, G. S. and Moore, L. R. 1986. An exhaustive analysis of multiplicative congruential random number generators with modulus $2^{31} - 1$. *SIAM J. Sci. Stat. Comput. 7*, 24–45. see erratum, ibid. p. 1058.

Good, I. J. 1953. The serial test for sampling numbers and other tests for randomness. *Proc. Cambridge Philosophical Society 49*, 276–284.

Hellekalek, P. and Leeb, H. 1997. Dyadic diaphony. *Acta Arith. 80*, 187–196.

HERENDI, T., SIEGL, T., AND TICHY, R. F. 1997. Fast Gaussian random number generation using linear transformations. *Computing 59*, 163–181.

HÖRMANN, W. 1994a. A note on the quality of random variates generated by the ratio of uniforms method. *ACM TOMACS 4*, 1, 96–106.

HÖRMANN, W. 1994b. The quality of non-uniform random numbers. In H. DYCKHOFF, U. DERINGS, M. SALOMON, AND H. C. TIJMS Eds., *Operations Research Proceedings 1993* (Berlin, 1994), pp. 329–335. Springer Verlag.

HÖRMANN, W. 1995. A rejection technique for sampling from T-concave distributions. *ACM Trans. Math. Software 21*, 2, 182–193.

HÖRMANN, W. AND DERFLINGER, G. 1990. The ACR method for generating normal random variables. *OR Spektrum 12*, 181–185.

HÖRMANN, W. AND DERFLINGER, G. 1993. A portable uniform random number generator well suited for the rejection method. *ACM Trans. Math. Software 19*, 4, 489–495.

KINDERMAN, A. J. AND MONAHAN, F. J. 1977. Computer generation of random variables using the ratio of uniform deviates. *ACM Trans. Math. Soft. 3*, 3, 257–260.

KINDERMAN, A. J. AND RAMAGE, J. G. 1976. Computer generation of normal random variables. *J. Am. Stat. Assoc. 71*, 356, 893–898.

L'ECUYER, P. 1994. Uniform random number generation. *Ann. Op. Research 53*, 77–120.

L'ECUYER, P., CORDEAU, J.-F., AND SIMAND, R. 1998. Close-points spatial tests for random number generation. preprint.

LEEB, H. AND HELLEKALEK, P. 1998. Asymptotic properties of the spectral test, diaphony, and related quantities. preprint.

LEEB, H. AND WEGENKITTL, S. 1997. Inversive and linear congruential pseudorandom number generators in empirical tests. *ACM TOMACS 7*, 2, 272–286.

MARSAGLIA, G. 1962. Improving the polar method for generating a pair of random variables. Technical Report D1-82-0203, Boeing Sci. Res. Lab.

MARSAGLIA, G. 1985. A current view of random number generators. In L. BILLARD Ed., *Computer Science and Statistics: The Interface*, pp. 3–10. Amsterdam: Elsevier Science Publishers B.V.

MATSUMOTO, M. AND KURITA, Y. 1994. Twisted GFSR generators II. *ACM TOMACS 4*, 3, 254–266.

MONAHAN, F. 1985. Accuracy in random number generation. *Math. Comp. 45*, 172, 559–568.

NEAVE, H. R. 1973. On using the Box-Müller transformation with multiplicative congruential pseudo-random number generators. *Appl. Statist. 22*, 1, 92–97.

NIEDERREITER, H. 1992. *Random Number Generation and Quasi-Monte Carlo Methods*. SIAM, Philadelphia.

PARK, S. K. AND MILLER, K. W. 1988. Random number generators: good ones are hard to find. *Comm. ACM 31*, 1192–1201.

SCHMIDT, B. 1996. *Simplex II, Referenzhandbuch, Version 2.6*. Universität Passau. `http://www.uni-passau.de/~simplex/`.

ZINTERHOF, P. 1976. Über einige Abschätzungen bei der Approximation von Funktionen mit Gleichverteilungsmethoden. *Sitzungsber. Österr. Akad. Wiss. Math.-Natur. Kl. II 185*, 121–132.