TECHNICAL ARTICLE

SIMULATION 72:3, 163-169

ISSN 0037-5497/99
Printed in the United States of America

On the CRAY–System Random Number Generator

Karl Entacher
University of Salzburg
Department of Mathematics
Salzburg, Austria
E-mail: *Karl.Entacher@sbg.ac.at*

We present a theoretical and empirical analysis of the quality of the CRAY-system random number generator RANF in parallel settings. Subsequences of this generator are used to obtain parallel streams of random numbers for each processor. We use the spectral test *to analyze the quality of lagged subsequences of RANF with step sizes* 2^l, $l \geq 1$, *appropriate for CRAY systems. Our results demonstrate that with increasing* l, *the quality of lagged subsequences is* strongly *reduced in comparison to the original sequence. The results are supported by a numerical Monte Carlo integration study. We also use the spectral test to exhibit the well known long-range correlations between consecutive blocks of random numbers obtained from RANF.*

Keywords: Random number generation, parallel random numbers, parallel and distributed simulation, lattice structure, spectral test, long-range correlations, leapfrog technique, CRAY systems

1. A Short Overview

In the present paper we study special subsequences of the CRAY-system random number generator RANF. Such subsequences are used to obtain parallel streams of random numbers. RANF is a linear congruential generator (LCG), and hence it is well known that overlapping s-tuples of random numbers generated from RANF produce *grid structures* in dimension $s \geq 2$. In Section 3 we give a formal description of the grid structures which are produced by subsequences of RANF or similar LCGs. Using the *spectral test*, which measures the coarseness of such grids, we analyze the quality of *lagged* subsequences with step sizes $k = 2^l$, $1 \leq l \leq 10$, which are relevant for CRAY systems. It turns out that the quality of subsequences with step sizes, especially for $l \geq 6$, is strongly reduced in comparison to the original sequence produced by RANF. A sample Monte Carlo integration study given in Section 4 verifies the unsatisfactory results obtained by the spectral test. In Subsection 3.2 we apply the spectral test to exhibit the well known long-range correlations obtained by splitting the output sequence of RANF into consecutive blocks. Section 2 gives the basic notation and references.

2. Basic Concepts

The multiplicative linear congruential pseudorandom number generator RANF with modulus $m = 2^{48}$,

[1] Research supported by the Austrian Science Fund (FWF projects no. P11143–MAT and P12441–MAT).

Table 1. Spectral tests S_s, $2 \le s \le 8$, of RANF-subsequences with lags 2^l

l	s = 2	3	4	5	6	7	8
0	0.8269	0.7416	0.3983	0.7307	0.6177	0.6670	0.5642
1	0.4130	0.7071	0.7243	0.3612	0.4488	0.5335	0.7384
2	0.6445	0.5519	0.6460	0.5288	0.6548	0.3528	0.5788
3	0.7877	0.5429	0.3204	0.6805	0.5510	0.6570	0.4324
4	0.6600	0.5093	0.5863	0.5182	0.5849	0.6376	0.6543
5	0.5957	0.6383	0.7469	0.6095	0.3881	0.3896	0.3292
6	0.6285	0.6489	0.5985	0.7557	0.1211	0.1297	0.1875
7	0.2917	0.8355	0.6459	0.2439	0.1359	0.1432	0.1524
8	0.4403	0.7542	0.7841	0.0350	0.0508	0.0913	0.0910
9	0.6008	0.7004	0.0988	0.0402	0.0571	0.1008	0.0993
10	0.7790	0.5691	0.0123	0.0152	0.0341	0.0467	0.0702

multiplier a = 44485709377909 and the underlying recurrence $x_n \equiv a \cdot x_{n-1} \pmod m$, $1 \le x_0 < m$, with period $p = 2^{46}$ is (was) implemented on CRAY systems[2]. For references or some theoretical and empirical studies on this generator, see [1 through 12]. Pseudorandom numbers in the unit interval [0, 1[are obtained by the transformation $u_n := x_n / m$. This type of LCG can be implemented very efficiently and provides an easy way to split its output sequence into distinct parallel streams (see below). Another advantage of LCGs is the possibility to assess correlations between consecutive pseudorandom numbers by studying the quality of the underlying *lattice structure* formed by all s-dimensional vectors $u_n^{(s)} = (u_n, ..., u_{n+s-1})$, $n \ge 0$, generated from the periodic sequence $x = (x_n)_{n \ge 0}$ (See Section 3).

The quality of LCGs heavily depends on the coarseness of their lattices (e.g., see [8, 13]). In order to find "optimal" parameters for LCGs, several figures of merit for the quality of the lattice structure have been proposed. The most popular measure is the spectral test which gives the maximal distance d_s between adjacent parallel hyperplanes, the maximum being taken over all families of parallel hyperplanes that cover all vectors $u_n^{(s)}$ (see [1; 8 (Sec. 7.7); 13 (Sec. 3.3.4); 14]). In other words, d_s determines the maximal size of empty slices (without points $u_n^{(s)}$) within $[0, 1[^s$. The smaller d_s, the more uniform is the sample space of the points.

Also widely used is a normalized spectral test $S_s := d_s^* / d_s$, $2 \le s \le 8$, for which $0 \le S_s \le 1$. The latter figure of merit should be viewed as (normalized) correlation measure (values near 1 imply a "good" lattice structure, whereas values near 0 exhibit strong correlations within the generated sequence). The constants d_s^* are absolute lower bounds on d_s, see [8 (Sec. 7.7); 13 (pg. 105)]. L'Ecuyer [15] also proposed some lower bounds d_s^* for dimensions $s > 8$ in order to compute S_s for arbitrary dimensions.

[2] Homepage: *http://www.cray.com*

For the spectral test, RANF behaves almost as well as the best LCGs with modulus 2^{48} given in [1, 8, 15], except for a negligible deviation in dimension $s = 4$ (compare Table 1). Normalized spectral tests of RANF up to dimension $s = 8$ are also given in [1, 8].

But for certain applications it is not enough to analyze the lattice structure of LCGs only. Subsequences of the form

$$(x_{kn+j})_{n \ge 0}, \quad k \ge 2, \quad 0 \le j \le k-1 \tag{1}$$

should be analyzed as well, since these subsequences are used to get parallel streams of pseudorandom numbers for each processor (sometimes called the "leap-frog" technique, e.g., see [3, 16]). In the case of RANF, step sizes $k = 2^l$, $l \ge 1$ are of special interest, since such step sizes are implemented on CRAY systems (e.g., see the Cray Math Library Reference Manual SR–2080). The splitting process is easily verified by changing the multiplier in the recurrence in the following way. Let $w_n := x_{kn+j}$, then with $b := a^k \pmod m$ and $w_0 = a^j \cdot x_0 \pmod m$,

$$w_n \equiv b \cdot w_{n-1} \pmod m \tag{2}$$

A first analysis of RANF with respect to *full-period* subsequences ($b \equiv 5 \pmod 8$) is contained in [17]. It turned out that RANF behaves rather robustly with respect to full-period subsequences. The smallest full-period subsequence with *poor* spectral test results is the one with $k = 781$ for which we get the bad values $S_3 = 0.0212$ and $S_4 = 0.0587$. Note that in dimension three, the vectors $u_n^{(3)}$ generated from the subsequence lie on at most $n_3 = 1599$ hyperplanes, whereas the same vectors produced with the original sequence are placed on 49,107 hyperplanes. The latter estimates are obtained by a special variant of the spectral test [14]; see also [8, Sec. 7.8]. Therefore, the quality of the subsequence is strongly reduced in comparison to the structure of the

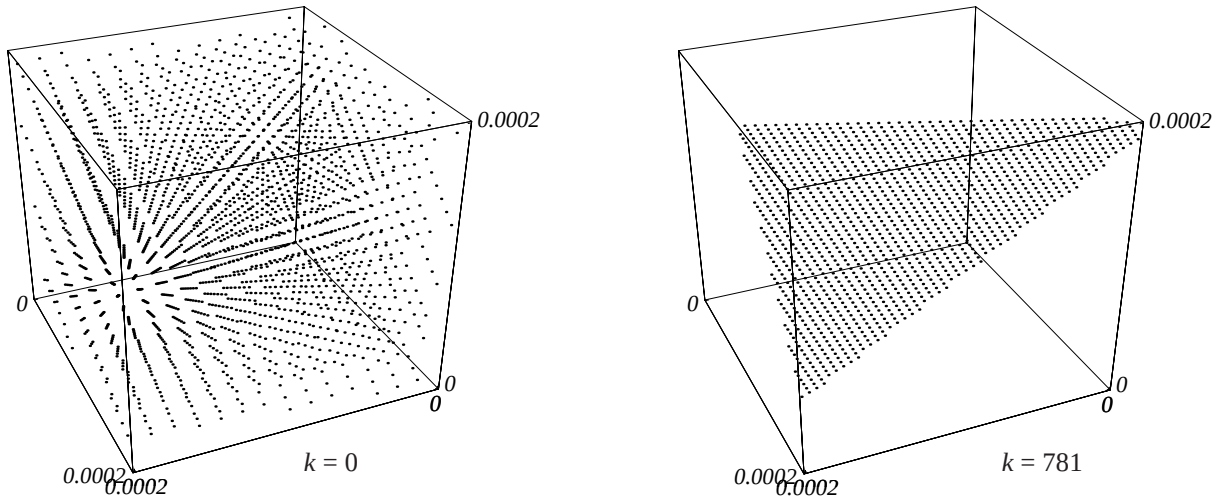

Figure 1. A zoom into the lattice structure of RANF and the RANF-subsequence with step size 781 in dimension three

original generator. Figure 1 demonstrates this reduction by zooms into the three-dimensional unit cube consisting of all vectors $u_n^{(3)}$ of RANF and the RANF-subsequence with step size 781.

What about non-full-period subsequences with step sizes, for example, $k = 2^l$, $l \geq 1$, which are relevant for CRAY architectures? In this case the period of the subsequence equals 2^{46-l}. Therefore, the underlying lattice structure differs from those of full-period subsequences with respect to this constant (see below).

In the following section we recall a formal description of the lattice structure formed by overlapping vectors from 2^l-subsequences of LCGs with power-of-two moduli. From this analysis we obtain a method to calculate the spectral test for such subsequences. We will perform a power-of-two subsequence analysis for RANF. The results show *strong* quality reductions of the lattices for step sizes $k = 2^l$, $l \geq 6$. More detailed lattice analyses of subsequences from LCGs are given in [18] and vectors with arbitrarily shifted indices from multiple recursive generators are studied in [19].

3. Lattice Analysis

The present section contains a lattice analysis of RANF-subsequences with step sizes 2^l, $l \geq 0$. Note that this analysis applies to an arbitrary linear congruential pseudorandom number generator with power-of-two moduli as well. For the three standard parameterization schemes of LCGs [20, pg. 169] (see also [1, 8, 11]) the set of vectors $\{u_n^{(s)} : n \geq 0\}$ forms a grid structure. In the case of RANF, a multiplicative LCG with power-of-two modulus $m = 2^\beta$ and $a \equiv 5 \pmod 8$, the set of all vectors $u_n^{(s)}$ is equal to the intersection of the s-dimensional unit cube $[0, 1[^s$ with the shifted lattice

$$\frac{1}{4} e_1 + G \text{ with } G = \{x \in R^s : x = \sum_{i=1}^{s} v_i \cdot e_i,\ v_i \in Z\} \quad (3)$$

and lattice basis $B = \{e_1, ..., e_s\}$, defined by the vectors

$$e_1=(1,a,...,a^{s-1}) \bmod 2^{\beta-2},\ e_2=(0,1,0,...,0),...,\ e_s=(0,0,...,0,1)$$

For the proof, see [11, 14, or 20, Thm. 7.6]. The spectral test measures the coarseness of lattice G. The calculation of this test[3] is realized using the dual lattice of G, since the maximal distance of adjacent hyperplanes d_s is equal to one over the length of the shortest vector of the dual lattice pointed out by Dieter [14]. An efficient implementation of the spectral test for multiple recursive generators which supports subsequence analyses is given in [19].

We now describe the lattice structure obtained by subsequences (1) with step sizes $k = 2^l$, $l \geq 1$. Recall the basic recurrence of RANF $x_n \equiv a \cdot x_{n-1} \pmod m$, $m = 2^\beta$, and without loss of generality, $x_0 = 1$. From [11, Prop. 1] (see also [8, pg. 599]), we get $x_n = 4 \cdot x_n^* + 1$ where $x_n^* \equiv a \cdot x_{n-1}^* + (a-1)/4 \pmod{2^{\beta-2}}$, $x_0^* = 0$, which, by the way, yields the period $p = 2^{\beta-2}$ of x. Using equation (4) in [13, pg. 12], it follows that for $k = 2^l$, $l \geq 1$,

$$x_{kn+j}^* = y_j + k \cdot z_n,\ n,\ z_n \in \{0,...,2^{\beta-l-2} - 1\} \quad (4)$$

and $y_j \equiv a \cdot y_{j-1} + (a-1)/4 \pmod k$, $y_0 = 0$. Let j be fixed; therefore, the set $\{x_{kn+j} : n \geq 0\}$ equals $\{4 \cdot k \cdot u + v : u = 0,...,2^{\beta-l-2} - 1,\ v = 4y_j + 1\}$. The latter result and property (2), applied in exactly the same calculation as in [14, Sec. 4] yields that the set of overlapping vectors $u_{kn+j}^{(s)}$ consists of all points of the intersection of the s-dimensional unit cube $[0, 1[^s$ with the shifted lattice $v \cdot e_1 / 2^{l+2} + G$ with vector $e_1 = (1, b,..., b^{s-1}) /$

[3] Our spectral tests have been calculated using a *Mathematica* implementation of the Fincke-Pohst algorithm for finding the shortest vector in a lattice by Wilberd van der Kallen (*http://www.math.ruu.nl/people/vdkallen/kallen.html*).

2^{46-l}, $b = a^k \pmod m$. Therefore, the spectral test of the 2^l-subsequences has to be calculated using vector e_1 (with constant $1/2^{46-l}$!).

Note that if one uses constant $1/2^{46}$ for the calculation, this would give the spectral test for the union of all subsequence-grids. This is not the appropriate way to assess the subsequence structure. For example, the RANF–subsequence with step size $k = 2^8$ yields the weak spectral test $S_5 = 0.03502$ whereas for the union of the subsequence-grids $S_5 = 0.6625$.

3.1 Spectral Test and Lagged Subsequences of RANF

We applied the normalized spectral test S_s, $2 \le s \le 8$, to RANF subsequences with step sizes $k = 2^l$, $1 \le l \le 10$. Table 1 shows the results. The original sequence of RANF behaves very well with respect to this test, but the results for subsequences start to worsen considerably for $l \ge 6$. The latter quality reduction of the subsequences is easily verified with our simple Monte Carlo integration study given below.

Whenever the leapfrog method is applied to power-of-two LCGs, it should only be performed with "full-period" lags where the corresponding subsequences previously have been tested with the spectral test. Suppose one wants to distribute 2^8 parallel streams from RANF to the same number of processors. For example, consider full-period lagged-subsequences (1) of RANF with step size $k = 2^8 + 3$ and $0 \le j \le 2^8 - 1$. Therefore, the spectral test of each subsequence shows almost the same quality as for RANF, and from the spectral test results of RANF itself, we can easily conclude that there are no conspicuous correlations between the parallel streams.

3.2 Spectral Test and Long-Range Correlations

A different method to get parallel streams of pseudo-random numbers is to vary the seed x_0 and therefore partition the output sequence x into consecutive blocks $(x_{kL+n})_{n=0}^{L-1}$, $k \ge 0$, of a given length L. This approach was studied extensively by DeMatteis et al. [4, 6, 21, 22]. It turns out that only small fractions of sequences produced by an LCG can safely be used because of the well known long-range correlations which may impose unwanted correlations between the parallel streams. Long-range correlations of RANF have been studied in the latter papers.

Using the spectral test to assess such correlations was already suggested by Durst [7] and related concepts can be found in [5, 10][4]. Similar to DeMatteis et al., the latter authors applied their concepts only in dimension two for computational and mathematical reasons.

We will perform a "long-range" correlation analysis of RANF also in higher dimensions s. Thus we have to analyse the grid structure which contains all vectors:

$$(x_i, x_{i+L}, x_{i+2 \cdot L}, \ldots, x_{i+(s-1) \cdot L}),\ i \ge 0,\ s \ge 2 \qquad (5)$$

Elementary calculations yield that the spectral test can be applied to the same lattice as in (3), but with vector $e_1 = (1, b, \ldots, b^{s-1})/2^{46}$, $b = a^L \pmod m$.

Table 2. Correlation analysis of consecutive blocks from RANF with $L = 2^j$ using the spectral test S_s, $2 \le s \le 8$

j	s = 2	3	4	5	6	7	8
10	0.7636	0.8322	0.8468	0.0115	0.0202	0.0413	0.0455
11	0.5808	0.4564	0.1662	0.0115	0.0202	0.0413	0.0455
12	0.7154	0.6941	0.0208	0.0115	0.0202	0.0413	0.0455
13	0.9788	0.5488	0.0026	0.0044	0.0121	0.0191	0.0322
14	0.2435	0.8288	0.0013	0.0044	0.0121	0.0191	0.0322

Table 3. Correlation analysis of consecutive blocks from RANF with $L = 3^j$ using the spectral test S_s, $2 \le s \le 8$

j	s = 2	3	4	5	6	7	8
7	0.4162	0.4491	0.4660	0.6344	0.5289	0.6972	0.6243
8	0.5914	0.6040	0.4525	0.6902	0.5179	0.7217	0.6115
9	0.7761	0.4099	0.3770	0.6642	0.7332	0.7578	0.6622
10	0.8316	0.6327	0.4392	0.3713	0.5662	0.5703	0.4853
11	0.9358	0.5259	0.7078	0.6060	0.6647	0.6780	0.5116

[4] In these papers, the parallel streams are initialized via the additive term of the LCG. Related concepts applied to prime LCGs have recently been published by Mascagni [31].

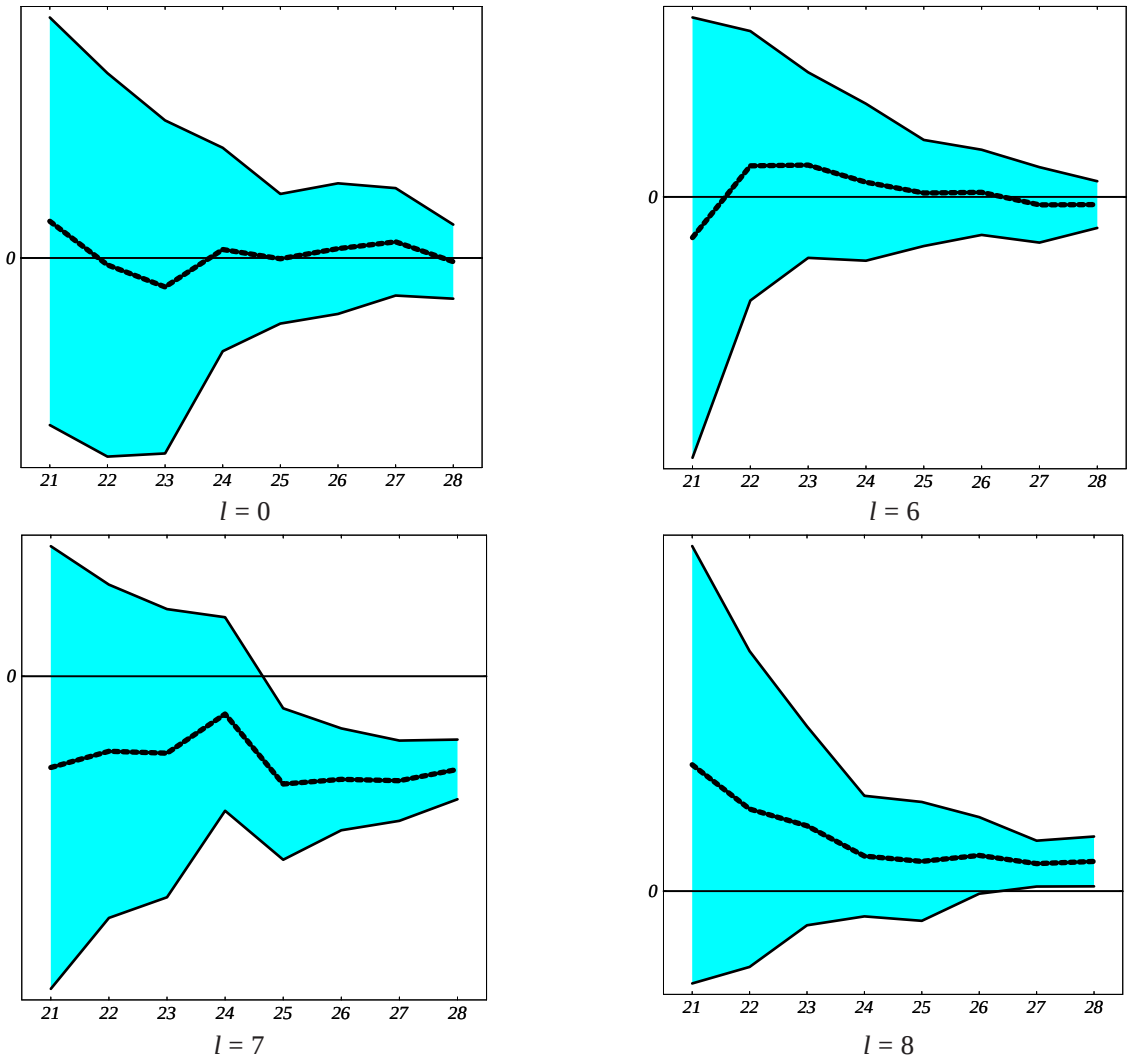

Figure 2. Monte Carlo integrations with RANF with sample sizes 2^{21} ,..., 2^{28}, dimension 8 and subsequences with step sizes $k = 2^l$, $l = 0, 6, 7, 8$

Table 2 shows normalized spectral test results for such lattices with block lengths $L = 2^j$, $10 \le j \le 14$. Note that these results are equal to spectral tests of the *union* of all lattices from lagged subsequences (1) with step size $k = L$ and $0 \le j < L$. As can be seen from Table 2, no practical relevant consecutive blocks of RANF with power-of-two block sizes should be used in practice.

Using odd block lengths L (hence the block length does not divide the period of the generator which also implies that the multiplicative LCG with multiplier a^L (mod m has full period) provides a simple way against correlations between consecutive blocks obtained from power-of-two LCGs. But previous testing is recommended in this case as well. Table 3 shows normalized spectral tests S_s, $2 \le s \le 8$, using RANF for block lengths $L = 3^j$, $7 \le j \le 11$. Similarly, as the results in Table 3, there are no conspicuous correlations for $12 \le j \le 29$.

4. Monte Carlo Integration

In order to demonstrate the effects of the splitting of RANF into subsequences with step sizes 64, 128, 256, we performed a sample Monte Carlo integration study. We consider the problem of numerical integration in dimension $s \ge 1$, see [20]. Denote by $n \in \mathrm{N}$ a sample size and choose a test function $f : I^s \to \mathrm{R}$, $I = [0, 1[$. Put:

$$\in(f,\psi,n) := S_n(f,\psi) - \int_{I^s} f(\xi)\, d\xi, \quad S_n(f,\psi) := \frac{1}{n} \sum_{i=0}^{n-1} f(\psi_i)$$

the integration error arising from the Monte Carlo approximation $S_n(f,\psi)$ with the sequence $\psi = (\psi_i)$, $i = 0, 1..., n-1$, $\psi_i \in I^s$ of integration nodes. Under the assumption that ψ is a sequence of independent random variables distributed uniformly on I^s and that $f \in L^1$, i.e., the integral exists and is finite, the strong law of large numbers guarantees almost sure convergence of the error to zero as n increases to infinity. As a test function we have chosen the polynomial $f(x_1, x_2, ..., x_s) = \prod_{i=1}^{s} g(x_i)$, with $g(x) := x^r - 1/(r-1)$, $r = 20$. The integral of this function equals zero. An analysis of the impact of the parameter r on integration results can be found in [23]. Similar results to those given below have been obtained also for small powers r (for $r = 5$, see [9]).

The graphics in Figure 2 show the results for dimension $s = 8$. The bold line reports the standard estimator for the integral based on 64 independent samples of

the Monte Carlo approximation for each sample size $n = 2^{21},...,2^{28}$, whereas the shaded area corresponds to an estimated 99% confidence interval based on the *t*-distribution (see [23, 24]). The horizontal line labeled with 0 represents the true value of the integral.

The first graphic shows the results for the original RANF-sequence. RANF shows almost optimal spectral test results. The empirical results are unsuspicious too, as the true value of the integral never lies outside the 99% confidence interval. For the RANF-subsequences with step sizes 128 and 256 (our parallel setup, i.e., the implementation of the splitting procedure is described in [23, 24]) the coarseness of the lattice in these dimensions clearly shows up in the empirical results where the generator is rejected at a 99% level of confidence in a large range of sample sizes. The reduced quality of the subsequence with step size 64 does not affect the Monte Carlo integration as can be seen from the second graphic.

5. Conclusion

Using the spectral test we have analyzed the quality reduction of subsequences of the CRAY system generator RANF. The results show that for serious simulation problems the usage of RANF subsequences with step sizes 64, 128, 256, 512, . . . may lead to bad simulation results, which is due to the reduced quality of the underlying lattice structures of overlapping vectors produced by such subsequences.

From our results we strongly suggest running *a priori* tests whenever subsequences of linear congruential generators are used. These types of generators are until now the best analyzed and most widely used pseudorandom number generators, and many up-to-date generation methods with high periods are equivalent or approximately equivalent to large size linear generators [16, 25]. However, even if the period is large, a variation in the parameters which is, for example, caused by the use of subsequences may lead to unexpected behavior (see also [26]).

Power-of-two LCGs such as RANF or the ANSI C generator drand48() [2, 3, 17, 25] are no longer relevant for actual simulation problems due to the strong regularities in the least significant bits [13, pg. 12] which are also responsible for the aforementioned bad quality of lagged subsequences with large power-of-two step sizes (see Equation (4)).

On parallel architectures one has to apply more up-to-date generators [27, 28] or explicit inversive congruential generators [29] which are slower than linear generators but known to be stable with respect to splitting [30].

6. Acknowledgements

The author wants to thank his colleagues of the pLab research group [32], University Salzburg, especially the head of the group Peter Hellekalek, for their support. Many thanks to Pierre L'Ecuyer for helping with the verification of some spectral test calculations and to Andreas Uhl and Stefan Wegenkittl for their assistance with parallel Monte Carlo integrations.

7. References

[1] Anderson, S.L. "Random Number Generators on Vector Supercomputers and Other Advanced Architectures." *SIAM Rev*., Vol. 32, pp 221-251, 1990.

[2] Coddington, P. "Analysis of Random Number Generators Using Monte Carlo Simulation." *International Journal of Modern Physics*, Vol. C 5, p 547, 1994.

[3] Coddington, P. "Random Number Generators for Parallel Computers." *NHSE Review*, Second Issue, Northeast Parallel Architectures Center, 1996. Available at: *http://nhse.cs.rice.edu/NHSEreview/RNG/*.

[4] DeMatteis, A., Pagnutti, S. "Parallelization of Random Number Generators and Long-Range Correlations." *Numer. Math*., Vol. 53, pp 595-608, 1988.

[5] DeMatteis, A., Pagnutti, S. "A Class of Parallel Random Number Generators." *Parallel Computing*, Vol. 13, pp 193-198, 1990.

[6] DeMatteis, A., Pagnutti, S. "Critical Distances in Pseudorandom Sequences Generated with Composite Moduli." *International Journal of Computer Mathematics*, Vol. 43, pp 189-196, 1992.

[7] Durst, M.J. "Using Linear Congruential Generators for Parallel Random Number Generation." In *Proceedings of the 1989 Winter Simulation Conference*, E.A. MacNair, K.J. Musselman, P. Heidelberger, editors, pp 462-466, 1989.

[8] Fishman, G.S. *Monte Carlo: Concepts, Algorithms, and Applications*, Volume 1 of Springer Series in Operations Research, Springer, New York, 1996.

[9] Hellekalek, P. "On the Assessment of Random and Quasi–Random Point Sets." In *Random and Quasi-Random Point Sets*, P. Hellekalek and G. Larcher, editors, Lecture Notes in Statistics, Springer-Verlag, New York, 1998.

[10] Percus, O.E., Kalos, M.H. "Random Number Generators for MIMD Parallel Processors." *Journal of Parallel and Distributed Computing*, Vol. 6, pp 477-497, 1989.

[11] Ripley, B.D. "The Lattice Structure of Pseudo-Random Number Generators." *Proceedings of the Royal Society of London*, Ser. A, Vol. 389, pp 197-204, 1983.

[12] Vattulainen, I., Kankaala, K., Saarinen, J., Ala-Nissila, T. "A Comparative Study of Some Pseudorandom Number Generators." *Comp. Phys. Comm*., Vol. 86, pp 209-226, 1995.

[13] Knuth, D.E. *The Art of Computer Programming, Volume 2: Seminumerical Algorithms*, Second Edition, Addison-Wesley, Reading, MA, 1981.

[14] Dieter, U. "How to Calculate Shortest Vectors in a Lattice." *Mathematics of Computation*, Vol. 29, No. 131, pp 827-833, 1975.

[15] L'Ecuyer, P. "Tables of Linear Congruential Generators of Different Sizes and Good Lattice Structure." *Mathematics of Computation*, Vol. 68, No. 225, pp 249-260, 1999.

[16] L'Ecuyer, P. "Uniform Random Number Generation." *Annals of Operations Research*, Vol. 53, pp 77-120, 1994.

[17] Entacher, K. "Bad Subsequences of Well–Known Linear Congruential Pseudorandom Number Generators." *ACM Transactions on Modeling and Computer Simulation*, Vol. 7, No. 1, pp 61-70, 1998.

[18] Entacher, K. "Parallel Streams of Linear Random Numbers in the Spectral Test." *ACM Transactions on Modeling and Computer Simulation*, to appear in 1999.

[19] L'Ecuyer, P., Couture, R. "An Implementation of the Lattice and Spectral Tests for Multiple Recursive Linear Random Number Generators." *INFORMS Journal on Computing*, Vol. 9, No. 2, pp 206-217, 1997.

[20] Niederreiter, H. "Random Number Generation and Quasi-Monte Carlo Methods." *SIAM*, Philadelphia, 1992.

[21] DeMatteis, A., Eichenauer-Herrmann, J., Grothe, H. "Computation of Critical Distances Within Multiplicative Congruential Pseudorandom Number Sequences." *Journal of Comp. Appl. Math.*, Vol. 39, pp 49-55, 1992.

[22] Eichenauer-Herrmann, J., Grothe, H. "A Remark on Long-Range Correlations in Multiplicative Congruential Pseudo Random Number Generators." *Numerical Mathematics*, Vol. 56, pp 609-611, 1989.

[23] Entacher, K., Uhl, A., Wegenkittl, S. "Linear Congruential Generators for Parallel Monte-Carlo: The Leap-Frog Case." *Monte Carlo Methods and Applications*, Vol. 4, No. 1, pp 1-16, 1998.

[24] Hellekalek, P. "Don't Trust Parallel Monte Carlo." In *Twelfth Workshop on Parallel and Distributed Simultation*, PADS'98, May 1998, pp 82-89, Banff, Alberta, Canada, 1998. IEEE Computer Society, Los Alamitos, California.

[25] Entacher, K. "A Collection of Selected Pseudorandom Number Generators with Linear Structures—Updated Version." Technical Report, Dept. of Mathematics, University of Salzburg, Austria, available at: *http://random.mat.sbg.ac.at/*, 1998. The previous version was published as Technical Report 97-1, ACPC-Austrian Center for Parallel Computation, University of Vienna, Austria, 1997.

[26] L'Ecuyer, P. "Bad Lattice Structures for Vectors of Non-Successive Values Produced by Some Linear Recurrences." *INFORMS Journal on Computing*, Vol. 9, pp 57-60, 1997.

[27] Ceperley, D., Mascagni, M., Srinivasan, A. *SPRNG: Scalable Parallel Random Number Generators.* NCSA, University of Illinois at Urbana-Champaign and University of Southern Mississippi, 1997. *http://www.ncsa.uiuc.edu/Apps/SPRNG/.*

[28] L'Ecuyer, P., Andres, T.H. "A Random Number Generator Based on the Combination of Four LCGs." *Mathematics and Computers in Simulation*, Vol. 44, pp 99-107, 1997.

[29] Eichenauer-Herrmann, J. "Statistical Independence of a New Class of Inversive Congruential Pseudorandom Numbers." *Math. Comp.*, Vol. 60, pp 375-384, 1993.

[30] Niederreiter, H. "New Developments in Uniform Pseudorandom Number and Vector Generation." In *Monte Carlo and Quasi-Monte Carlo Methods in Scientific Computing*, H. Niederreiter and P. Jau–Shyong Shiue, editors, Volume 106 of Lecture Notes in Statistics, Springer, 1995.

[31] Mascagni, M. "Parallel Linear Congruential Generators with Prime Moduli." *Parallel Computing*, Vol. 24, No. 5-6, pp 923-936, 1998.

[32] Hellekalek, P., Entacher, K., Leeb, H., Lendl, O., Wegenkittl, S. The PLAB www-server, Dept. of Mathematics, University of Salzburg, Austria. *http://random.mat.sbg.ac.at*, 1995. Also accessible via ftp.

Karl Entacher received BS and MS degrees, both in Mathematics, from the University of Salzburg. He completed his PhD in Mathematics at the same University. He is currently Research Assistant in the University's Department of Mathematics. His research interests include Monte Carlo and quasi-Monte Carlo methods, random number generation, parallel random numbers, and low discrepancy point sets. For details, see *http://random.mat.sbg.ac.at/team/*.