Bad subsequences of well-known linear congruential pseudorandom number generators

Karl Entacher

Austrian Science Foundation (FWF project no. P11143-MAT)

We present a spectral test analysis of full-period subsequences with small step sizes generated by well-known linear congruential pseudorandom number generators. Subsequences may occur in certain simulation problems or as a method to get parallel streams of pseudorandom numbers. Applying the spectral test, it is possible to find bad subsequences with small step sizes for almost all linear pseudorandom number generators currently in use.

Categories and Subject Descriptors: G.3 [**PROBABILITY AND STATISTICS**]: Random number generation; G.3 [**PROBABILITY AND STATISTICS**]: Statistical software; I.6.0 [**SIMULATION AND MODELING**]: General

General Terms: Algorithms

Additional Key Words and Phrases: Lattice structure, linear congruential generator, parallel pseudorandom number generator, random number generation, spectral test, stochastic simulation

1. INTRODUCTION

Linear congruential generators (LCGs) are the best analyzed and most widely used pseudorandom number generators (PRNGs). We will denote this PRNG with underlying recursion $y_{n+1} = ay_n + b \pmod m$ and seed y_0 by $LCG(m, a, b, y_0)$, $a, b, y_0 \in \mathbf{Z}_m$. LCGs allow an easy (number-) theoretical analysis based on the lattice structure formed by s-dimensional vectors $\mathbf{x}_n^{(s)} = (x_n, \ldots, x_{n+s-1}), n \geq 0$, generated from the periodic sequence $\mathbf{x} = (x_n)_{n\geq 0}$, $x_n = y_n/m$. The quality of LCGs heavily depends on the coarseness of the lattice (e.g. see [Knuth 1981]).

In order to find "optimal" parameters for LCGs, several figures of merit for 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

Affiliation: Institut für Mathematik, Universität Salzburg
Address: Hellbrunnerstr. 34, A-5020 Salzburg, Austria. WWW: http://random.mat.sbg.ac.at/
e-mail: Karl.Entacher@sbg.ac.at

$\mathbf{x}_n^{(s)}$ (see [Coveyou and MacPherson 1967; Knuth 1981; L'Ecuyer 1988; Fishman 1996]). Several LCGs have been proposed due to their good spectral test results in different dimensions. To compare spectral test results among dimensions Fishman and Moore [1986] introduced a normalized spectral test $S_s := d_s^*/d_s$, for which $0 \leq S_s \leq 1$. The constants d_s^* are absolute lower bounds on d_s for $s \leq 8$ [Knuth 1981, p. 105]. With this, Fishman and Moore made an exhaustive search for LCGs whose normalized spectral tests in dimensions 2 to 6 exceed 0.8. Lower bounds d_s^* for dimensions $s > 8$ are given in [L'Ecuyer 1998]. However, simulations of Afflerbach and Gruber [1994] show that the number of LCGs with normalized spectral test values exceeding 0.8 (or for example falling below 0.1, compare Section 3) decreases very rapidly with the dimension.

Another aspect should be discussed as well: why do people analyze merely the lattice of *overlapping* vectors $\mathbf{x}_n^{(s)}$, in order to get "good" LCGs. More general vectors might be considered, for example:

$$\mathbf{x}_{kn+i}^{(s)} := (x_{kn+i}, x_{k(n+1)+i}, \ldots, x_{k(n+s-1)+i}), \qquad k \geq 1, \quad 0 \leq i \leq k-1\,.$$

The examination of the structures of these vectors leads to a correlation analysis of subsequences

$$(x_{kn+i})_{n\geq 0}, \quad k \geq 1, \quad 0 \leq i \leq k-1, \tag{1}$$

of the sequence $\mathbf{x}$. Subsequences may occur in simulations or when parallel streams of PRNs are obtained by splitting (see [Anderson 1990]).

Section 3 of this paper presents bad (in terms of the spectral test) full-period subsequences with *small* step sizes for many LCGs that were proposed in scientific papers and that have extensively been used in simulation.

From our results we conjecture that for almost all linear pseudorandom number generators currently in use, bad subsequences with small step sizes occur. It is necessary to draw attention to this property of linear methods. Even for top generators from earlier tables containing parameters for LCGs we found subsequences with lattice structures that are even worse than those of RANDU.

Our spectral tests have been calculated using the dual lattice approach [Dieter 1975] and a *Mathematica* implementation of the Fincke-Pohst algorithm for finding the shortest vector in a lattice by Wilberd van der Kallen[1].

Related correlation analysis for large step sizes (long range correlations) for LCGs have been made by [De Matteis and Pagnutti 1992; De Matteis and Pagnutti 1995]. Recently, L'Ecuyer [1997] studied bad lattice structures for special vectors of non-successive values produced by some linear recurrences. An efficient algorithm of the spectral test which facilitates the analysis of lattices generated by vectors of successive or non-successive values produced by linear congruential generators with moduli of essentially unlimited sizes was derived by L'Ecuyer and Couture [1997]. A modified spectral test to analyze the independence of parallel streams of linear pseudorandom number generators was proposed by MacLaren [1989]. The latter paper is the basis for 273 combined multiplicative LCGs implemented in the Nag PVM Library (Chapter G05).

[1] The package ShortestVector.m and related Packages are available on the World-Wide-Web at `http://www.math.ruu.nl/people/vdkallen/kallen.html` and `http://random.mat.sbg.ac.at/`.

2. WELL-KNOWN LCGS

In this section we present classical and recent LCGs that were implemented in commercial software, used in applications, and some of which have extensively been tested. Further references for these generators (including implementations, empirical tests and lattice analysis) are given in [Entacher 1997a].

(1) $LCG(2^{31}, 1103515245, 12345, 12345)$ is the generator employed by the ANSI C `rand()` function [Park and Miller 1988; Ripley 1990].

(2) $LCG(2^{31}-1, 7^5 = 16807, 0, 1)$ was proposed by Lewis, Goodman, and Miller [1969]. Park and Miller [1988] suggested to use this LCG as a "minimal standard" generator. For implementations in commercial software and empirical tests see the latter paper and [Fishman 1996; Dudewicz and Ralley 1981; Ripley 1990; L'Ecuyer 1988; Vattulainen et al. 1995].

(3) $LCG(2^{31}-1, 630360016, 0, 1)$ was proposed by Payne, Rabung, and Bogyo [1969] and implemented in the SIMSCRIPT II simulation programming language [Fishman and Moore 1986; Fishman 1996; Ripley 1990; L'Ecuyer 1988].

(4) $LCG(2^{31}-1, 397204094, 0, 1)$ is one of the best LCGs from a study of Hoaglin [1976] and was for example implemented in the SAS and IMSL Lib. [Fishman and Moore 1986].

(5) The LCG (a) $LCG(2^{32}, 69069, 0, 1)$ also implemented as (b) $LCG(2^{32}, 69069, 1, 0)$, is called Super-Duper and was implemented on IBM computers (see [Fishman and Moore 1986; Fishman 1996; De Matteis and Pagnutti 1992]). The version (b) for example is part of the VAX VMS-Library [Ripley 1990] and was implemented by the Convex Corp [Vattulainen et al. 1995].

(6) $LCG(2^{32}, 3141592653, 1, 0)$ is implemented in the mathematical software *Derive* (`http://www.derive.com`). Note, that this generator performs a bad spectral test in dimension 2 (see the table below). The multiplier probably stems from Knuth [1981] who considered a similar generator with modulus 2^{35}.

(7) $LCG(2^{35}, 5^{15} = 30517578125, 7261067085, 0)$ was studied in [Knuth 1981]. It was implemented in the BCSLIB (Boeing Computer Services LIB) [Anderson 1990]. The multiplicative version of this LCG was implemented in the programming language SIMULA. A long range correlation analysis of this version is given in [De Matteis and Pagnutti 1992].

(8) $LCG(2^{35}, 5^{13} = 1220703125, 0, 1)$ [Knuth 1981] was implemented on Apple computers [Jennergren 1983].

(9) The top five LCGs respectively modulus $2^{31}-1$, 2^{32} and 2^{48} from an exhaustive study of [Fishman and Moore 1986; Fishman 1990; Fishman 1996]. We present results of the following four examples which exhibited the worst subsequence behavior: (a) $LCG(2^{31}-1, 950706376, 0, 1)$, (b) $LCG(2^{32}, 2396548189, 0, 1)$, (c) $LCG(2^{32}, 3934873077, 0, 1)$, (d) $LCG(2^{48}, 55151000561141, 0, 1)$

(10) $LCG(10^{12}-11, 427419669081, 0, 1)$ is implemented in the mathematical software *Maple* [Karian and Goyal 1994].

(11) $LCG(2^{48}, 25214903917, 11, 0)$ is the ANSI C system generator `drand48()`.

(12) $LCG(2^{48}, 44485709377909, 0, 1)$ was implemented on CRAY systems (see [Anderson 1990; De Matteis and Pagnutti 1995; De Matteis and Pagnutti 1992])

and used in PASCLIB, a collection of utility subprograms that are callable from PASCAL on CDC CYBER computers (see [Fishman 1990]).

(13) $LCG(2^{59}, 13^{13}, 0, 123456789 \cdot (2^{32}+1))$ is the basic generator for PRNGs in many different distributions implemented in the NAG Library [The Numerical Algorithms Group Limited 1991, Sect. G05], see also [Afflerbach and Gruber 1994; Vattulainen et al. 1995].

(14) LCGs from the studies [L'Ecuyer 1988; L'Ecuyer et al. 1993]. These generators have been chosen according to their good lattice structure. We give results for the LCGs (a) $LCG(2147483563, 40014, 0, 1)$, (b) $LCG(2147483399, 40692, 0, 1)$ (see also [Fishman 1996]) and (c) $LCG(2^{63}-25, 2307085864, 0, 1)$.

3. BAD SUBSEQUENCES

In this section we present results of a spectral test analysis of full-period subsequences (1) with step sizes $1 \le k \le 1000$ for the LCGs above. Supplementing results are available via internet [Entacher et al. ; Entacher 1997b]. Consider a mixed linear congruential generator $LCG(m, a, b, 0)$ with maximal period T. For this generator, the subsequence (1) is also produced by (see also [Ripley 1990; L'Ecuyer 1994])

$$LCG\left(m,\ a^k \pmod m,\ b \cdot \tfrac{a^k-1}{a-1} \pmod m, b \cdot \tfrac{a^i-1}{a-1} \pmod m\right), \qquad 0 \le i \le k-1.$$

For the multiplicative $LCG(m, a, 0, 1)$, the corresponding LCG which produces the subsequence (1) is given by

$$LCG(m,\ a^k \pmod m,\ 0, a^i \pmod m), \qquad 0 \le i \le k-1.$$

Note that the period of these subsequences equals $T/gcd(k, T)$. Even if one chooses subsequences with maximal period T, the quality of these sequences may be significantly reduced.

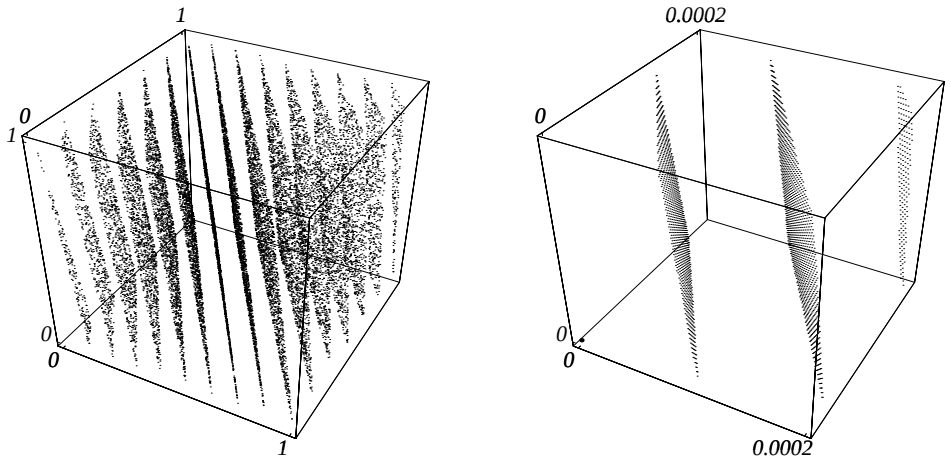
In the tables below we present results of the normalized spectral test S_s in dimensions $2 \le s \le 8$ for full period subsequence-LCGs generated from the LCGs given in Section 2. We give those results for step sizes $1 \le k \le 500$ and $i = 0$ where at least one value is lower than 0.1, and some mentionable results for step sizes $501 \le k \le 1000$.

LCG	k	s = 2	3	4	5	6	7	8
1	25	**0.0822**	0.7978	0.6059	0.7767	0.6327	0.5936	0.6096
	81	**0.0840**	0.6378	0.5062	0.7045	0.6193	0.4904	0.6850
	203	0.1499	**0.0600**	**0.0841**	0.1631	0.2624	0.4197	0.5863
	209	**0.0588**	0.3732	0.6954	0.4086	0.4421	0.7071	0.6951
	221	**0.0599**	0.8012	0.5197	0.7360	0.4368	0.3873	0.4915
	283	**0.0505**	0.8271	0.4279	0.6979	0.4271	0.6744	0.5981
	375	**0.0807**	0.2111	0.7582	0.6735	0.5900	0.6655	0.6430
	379	0.1874	**0.0888**	0.5023	0.7910	0.5700	0.6036	0.4962
	395	**0.0469**	0.5375	0.5623	0.3172	0.6193	0.5976	0.6357
	471	**0.0850**	0.5473	0.8368	0.5458	0.3519	0.4855	0.6321
	557	**0.0411**	0.5127	0.5025	0.4871	0.7188	0.6324	0.5620
	665	**0.0419**	0.7994	0.5932	0.4233	0.4228	0.6761	0.7497
	689	0.7866	0.5055	0.7553	**0.0870**	0.1142	0.1826	0.2550

LCG	k	s = 2	3	4	5	6	7	8
2	25	0.5967	**0.0783**	0.4427	0.5401	0.4780	0.5036	0.5600
	289	**0.0574**	0.5886	0.5451	0.4360	0.7706	0.5244	0.6058
3	431	**0.0725**	0.7368	0.6866	0.5817	0.5916	0.5804	0.6430
	719	0.4378	0.8154	**0.0776**	0.21959	0.4288	0.6857	0.7372
4	101	**0.0456**	0.4036	0.7808	0.5760	0.6238	0.7071	0.7277
	515	**0.0235**	0.8063	0.7670	0.6113	0.6991	0.6556	0.5345
	571	0.3566	**0.0790**	0.4125	0.4779	0.4484	0.6673	0.6430
5a	59	**0.0910**	0.6132	0.5992	0.7485	0.6342	0.5902	0.6648
	81	**0.0594**	0.6492	0.8133	0.6886	0.6249	0.6729	0.6771
	99	**0.0202**	0.20708	0.6000	0.29328	0.4180	0.4603	0.6350
	135	0.6758	0.6143	0.5708	**0.0999**	0.1281	0.2016	0.2781
	153	0.1729	**0.0567**	0.2795	0.7636	0.5872	0.5360	0.4071
	319	**0.0462**	0.3751	0.3507	0.6830	0.5382	0.7542	0.5757
	459	**0.0847**	0.3762	0.8955	0.7114	0.5327	0.5494	0.6812
	565	**0.0034**	**0.0678**	0.3617	0.5627	0.6806	0.6707	0.7012
	739	0.5703	**0.0095**	**0.0500**	0.1367	0.2608	0.4103	0.5660
5b	59	**0.0910**	0.7726	0.6663	0.6431	0.6518	0.7016	0.5590
	99	**0.0405**	0.3182	0.5635	0.6835	0.3863	0.6281	0.6092
	153	**0.0864**	0.1429	0.3797	0.6811	0.6310	0.5449	0.5413
	319	**0.0924**	0.8428	0.4814	0.7258	0.6108	0.6187	0.6495
	561	**0.0523**	0.7282	0.5033	0.25952	0.5186	0.5846	0.7235
	565	**0.0069**	**0.0854**	0.2773	0.4265	0.5597	0.7448	0.6124
	739	0.7771	**0.0238**	**0.0354**	0.1036	0.2070	0.3366	0.4760
6	1	**0.0972**	0.5552	0.5479	0.3216	0.6426	0.5210	0.6731
	33	0.4475	**0.0591**	0.1450	0.3601	0.3438	0.5590	0.6495
7	45	0.7494	0.7596	**0.0766**	0.2122	0.4544	0.7216	0.6590
	173	**0.0346**	0.5739	0.7012	0.4710	0.6424	0.7495	0.6430
	191	**0.0357**	0.6696	0.5452	0.5674	0.7189	0.6316	0.5843
	211	**0.0976**	0.6126	0.6051	0.6696	0.6798	0.6584	0.5600
	381	**0.0126**	0.6856	0.5985	0.4340	0.6231	0.6705	0.6764
	455	0.5334	**0.0822**	0.4893	0.7785	0.7579	0.5129	0.5662
	979	0.1972	**0.0953**	**0.0767**	0.1991	0.2416	0.4127	0.5191
8	137	**0.0852**	0.7675	0.8369	0.6168	0.6955	0.4886	0.6433
	347	**0.0742**	0.6361	0.4923	0.5889	0.6231	0.7238	0.5467
	389	**0.0842**	0.2864	0.6831	0.5616	0.4998	0.6828	0.6484
	473	**0.0390**	0.2830	0.7305	0.4483	0.7650	0.5517	0.6585
	999	0.4899	**0.0538**	0.2961	0.8791	0.7014	0.5869	0.7019
9a	29	**0.0903**	0.5806	0.2860	0.6150	0.7007	0.5815	0.5641
	377	**0.0890**	0.3379	0.8685	0.5384	0.7027	0.6343	0.6799
9b	65	**0.0968**	0.4785	0.5557	0.7437	0.4426	0.6962	0.7433
	105	0.9260	**0.0095**	**0.0500**	0.1367	0.2608	0.4103	0.5660
	393	**0.0819**	0.3344	0.3458	0.8119	0.5852	0.5414	0.7358
	475	0.7448	**0.0775**	0.3443	0.7041	0.6117	0.5599	0.6648
	615	0.6456	0.8049	**0.0673**	0.1839	0.3509	0.5223	0.7206
	619	0.6735	**0.0867**	0.3750	0.5578	0.4963	0.6166	0.4930
	857	**0.0440**	**0.0561**	0.2992	0.8176	0.4504	0.5278	0.5512

LCG	k	s = 2	3	4	5	6	7	8
9c	23	0.2118	**0.0378**	**0.0500**	0.1367	0.2608	0.4103	0.5660
	43	0.8975	0.8154	0.3505	**0.0999**	0.1281	0.2016	0.2781
	91	**0.0313**	**0.0775**	0.1456	0.2213	0.4222	0.6642	0.6084
	121	0.7674	**0.0890**	0.4754	0.6995	0.5751	0.4788	0.6564
	155	0.7266	**0.0811**	0.3766	0.4948	0.5751	0.6374	0.6564
	275	**0.0352**	0.7249	0.5908	0.7370	0.5148	0.7863	0.6606
	497	**0.0644**	0.4851	0.5546	0.8111	0.4582	0.7208	0.6394
9d	23	0.2562	**0.0600**	**0.0114**	**0.0462**	0.1275	0.2031	0.2078
	43	**0.0863**	0.8345	0.5441	0.5609	0.7319	0.5805	0.6940
	243	**0.0247**	0.6995	0.5934	0.7342	0.4729	0.6175	0.6146
	263	0.8887	**0.0677**	0.4030	0.3487	0.7188	0.5005	0.6007
	361	**0.0454**	0.6792	0.5134	0.5375	0.6241	0.7147	0.6202
10	175	**0.0812**	0.3844	0.4763	0.4475	0.5110	0.6578	0.4791
	667	0.1870	**0.0823**	0.6566	0.7010	0.5559	0.4799	0.6663
	807	**0.0198**	0.3513	0.5817	0.7890	0.5221	0.6933	0.4904
11	37	**0.0928**	0.3579	0.7156	0.4162	0.4727	0.4237	0.6838
	179	**0.0369**	0.6996	0.7944	0.4642	0.5715	0.6699	0.6514
	201	0.7225	**0.0865**	0.4669	0.7351	0.7585	0.6044	0.6297
	221	**0.0693**	0.5557	0.5967	0.5030	0.6115	0.6153	0.5493
	245	**0.0986**	0.6502	0.4324	0.4937	0.6014	0.3779	0.4386
	455	**0.0595**	0.8079	0.8111	0.7490	0.6522	0.6518	0.6118
	477	**0.0851**	0.5524	0.7133	0.6256	0.3850	0.6207	0.5754
12	377	0.8594	**0.0657**	0.8311	0.5215	0.6745	0.5507	0.5781
	429	**0.0596**	0.3552	0.7118	0.5798	0.6514	0.4159	0.3579
	493	**0.0398**	0.8850	0.5762	0.8112	0.5623	0.4743	0.6661
	781	0.7646	**0.0212**	**0.0587**	0.2790	0.7514	0.6936	0.4664
	799	0.9011	**0.0488**	0.2179	0.3134	0.6285	0.4168	0.3933
13	13	**0.0875**	0.7036	0.2369	0.7165	0.6532	0.6219	0.5455
	621	0.5723	**0.0520**	0.4537	0.7085	0.5678	0.6709	0.6851
14a	17	**0.0759**	0.7824	0.6206	0.6302	0.4858	0.7311	0.6850
	151	**0.0367**	0.5127	0.3711	0.6548	0.5538	0.6831	0.6695
	341	0.4269	0.8898	**0.0964**	0.2727	0.5324	0.7799	0.7635
	355	**0.0836**	0.2856	0.8811	0.5787	0.6819	0.5036	0.7034
	451	**0.0633**	0.6104	0.6010	0.6135	0.6924	0.7838	0.5600
14b	33	**0.0088**	0.3013	0.3845	0.6992	0.6632	0.6371	0.5961
	87	**0.0996**	0.4503	0.6798	0.6872	0.4139	0.6418	0.6747
	137	0.5268	**0.0901**	0.5026	0.6123	0.7730	0.6162	0.6357
	173	0.6510	**0.0730**	0.4131	0.6512	0.7255	0.4282	0.5981
	175	**0.0928**	0.5712	0.7406	0.6979	0.3616	0.4952	0.6626
	821	**0.0510**	0.2872	0.4281	0.7266	0.7921	0.4564	0.5078
	929	**0.0661**	0.5085	0.5660	0.5613	0.8333	0.6036	0.6247
14c	227	0.6895	0.6913	**0.0447**	0.3830	0.5805	0.6518	0.6290
	313	**0.0748**	0.7943	0.6057	0.4944	0.5875	0.5186	0.6638
	613	**0.0363**	0.8497	0.7142	0.5218	0.5669	0.6098	0.6043
	923	0.5395	**0.0322**	0.4291	0.6869	0.4425	0.6472	0.4852

Note that spectral test results lower than 0.1 did occur only for dimensions $2 \leq s \leq 5$. The worst generators with respect to subsequence behavior are LCG 1, 5a, 9b, 9c and 9d. For these generators there exist "small" subsequences whose spectral test results have the same order of magnitude as RANDU's. The graphics in Figure 1 show the lattice structures in dimension three for the subsequences of the Fishman LCGs 9b with $k = 105$ (30000 overlapping vectors in $[0,1[^3$) and for LCG 9d with $k = 23$, Note, that the second graphics shows a zoom into $[0, 0.0002[^3$ containing all overlapping vectors.



LCG 9b LCG 9d

Fig. 1. The lattice structure of subsequences from LCG 9b and 9d in dim. three.

The LCGs 3, 12, 14c show the "best" subsequence behavior. Weak full-period subsequences for these generators occur only for "large" step sizes k. But if the subsequence-LCGs do not have full-period, the underlying lattice structure can be of reduced quality as well. We demonstrate this behavior using zooms into the unit square, see Fig. 2.

4. CONCLUSION

Many pseudorandom number generation methods are equivalent or closely equivalent to LCGs or multiple recursive generators [L'Ecuyer 1996; L'Ecuyer and Couture 1997; Tezuka et al. 1993; Couture and L'Ecuyer 1996; Couture and L'Ecuyer 1997; Niederreiter 1995]. Hence, almost all pseudorandom number generators used in simulations today are linear methods.

A disadvantage of many linear methods is their weakness with respect to subsequences, which restricts the use of these methods in parallel simulation.

We applied the spectral test to find small lags which result in bad subsequences for many well-known LCGs. Our results underline the necessity to run a-priori tests,

whenever subsequences of a linear generator are used for a particular simulation problem.

Finally, we want to note that inversive pseudorandom number generators guarantee the absence of lattice structures, see the surveys [Eichenauer-Herrmann 1992; Niederreiter 1995; Hellekalek 1995; L'Ecuyer 1994]. Especially explicit inversive congruential PRNGs are very robust with respect to splitting their output into subsequences. The splitting procedure is easy to handle. Inversive generators are significantly slower than LCGs [Leeb and Wegenkittl 1997]. Nevertheless, the properties of these generators differ substantially from those of LCGs and hence make them an alternative choice to verify simulation results obtained by linear methods.

ACKNOWLEDGMENTS

The author wants to thank his colleagues of the pLab research group, especially the head of the group Peter Hellekalek, and Otmar Lendl (his code made the production of the scatter plots feasible) for their support. Many thanks to Wilberd van der Kallen from the University of Utrecht, Netherlands for implementing the Fincke-Pohst algorithm in *Mathematica*.

REFERENCES

Afflerbach, L. and Gruber, G. 1994. Assessment of random number generators in high accuracy. In S. Morito, H. Sakasegawa, M. Fushimi, and K. Nakano Eds., *New Directions in Simulation for Manufacturing and Communications* (1994), pp. 128–133. OR Society of Japan.

Anderson, S. 1990. Random number generators on vector supercomputers and other advanced architectures. *SIAM Rev.* **32**, 221–251.

Couture, R. and L'Ecuyer, P. 1996. Orbits and Lattices for Linear Random Number Generators with Composite Moduli. *Math. Comp.* **65**, 189–201.

Couture, R. and L'Ecuyer, P. 1997. Distribution Properties of Multiply-with-Carry Random Number Generators. *Math. Comp.* **66**, 591–607.

Coveyou, R. and MacPherson, R. 1967. Fourier analysis of uniform random number generators. *J. Assoc. Comput. Mach.* **14**, 100–119.

De Matteis, A. and Pagnutti, S. 1992. Critical distances in pseudorandom sequences generated with composite moduli. *Intern. J. Computer Math.* **43**, 189–196.

De Matteis, A. and Pagnutti, S. 1995. Controlling correlations in parallel Monte Carlo. *Parallel Comput.* **21**, 73–84.

Dieter, U. 1975. How to calculate shortest vectors in a lattice. *Math. Comp.* **29**, 827–833.

Dudewicz, E. and Ralley, T. 1981. *The Handbook of Random Number Generation and Testing With TESTRAND Computer Code*, Volume 4 of *American Series in Mathematical and Management Sciences*. American Sciences Press, Inc., Columbus, Ohio.

Eichenauer-Herrmann, J. 1992. Inversive congruential pseudorandom numbers: a tutorial. *Int. Statist. Rev.* **60**, 167–176.

Entacher, K. 1997a. A collection of selected pseudorandom number generators with linear structures. Technical Report 97-1, ACPC – Austrian Center for Parallel Computation, University of Vienna, Austria. Available at: `http://random.mat.sbg.ac.at/`.

Entacher, K. 1997b. The pLab Picturebook: Part III, Bad Subsequences of LCGs – The Results. Report no. 06, pLab – reports, University of Salzburg. Available on the internet at `http://random.mat.sbg.ac.at/team/`.

Entacher, K., Hellekalek, P., Leeb, H., Lendl, O., and Wegenkittl, S. The pLab www-server. `http://random.mat.sbg.ac.at`. Also accessible via ftp.

Fishman, G. 1990. Multiplicative congruential random number generators with modulus 2^β: an exhaustive analysis for $\beta = 32$ and a partial analysis for $\beta = 48$. *Math. Comp.* **54**, 331–344.

FISHMAN, G. 1996. *Monte Carlo: Concepts, Algorithms, and Applications*, Volume 1 of *Springer Series in Operations Research*. Springer, New York.

FISHMAN, G. AND MOORE, L. 1986. An exhaustive analysis of multiplicative congruential random number generators with modulus $2^{31} - 1$. *SIAM J. Sci. Statist. Comput.* **7**, 24–45. See erratum, ibid., **7**:1058, 1986.

HELLEKALEK, P. 1995. Inversive pseudorandom number generators. In C. ALEXOPOULOS AND D. G. K. KANG, W.R. LILEGDON Eds., *Proceedings of the 1995 Winter Simulation Conference* (1995).

HOAGLIN, D. 1976. *Theoretical Properties of Congruential Random-Number Generators: An Empirical View.* Memorandum NS-340. Harvard University, Department of Statistics.

JENNERGREN, L. 1983. Another method for random number generation on microcomputers. *Simulation* **41** , 79.

KARIAN, Z. AND GOYAL, R. 1994. Random number generation and testing. Technical Report 1, Maple Technical Newsletter, Birkhäuser Verlag, Switzerland.

KNUTH, D. 1981. *The Art of Computer Programming* (2nd ed.), Volume 2: Seminumerical Algorithms. Addison-Wesley, Reading, MA.

L'ECUYER, P. 1988. Efficient and portable combined random number generators. *Comm. ACM* **31**, 742–749 and 774.

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

L'ECUYER, P. 1996. Combined Multiple Recursive Random Number Generators. *Operations Research* **44**, 816–822.

L'ECUYER, P. 1997. Bad Lattice Structures for Vectors of Non-Successive Values Produced by Some Linear Recurrences. *INFORMS Journal on Computing* **9**, 57–60.

L'ECUYER, P. 1998. Tables of Linear Congruential Generators of Different Sizes and Good Lattice Structure. *Mathematics of Computation, to appear*.

L'ECUYER, P., BLOUIN, F., AND COUTURE, R. 1993. A Search for Good Multiple Recursive Generators. *ACM Transactions on Modeling and Computer Simulation* **3**, 87–98.

L'ECUYER, P. AND COUTURE, R. 1997. An Implementation of the Lattice and Spectral Tests for Multiple Recursive Linear Random Number Generators. *INFORMS Journal on Computing.* **9**, 2, 206–217.

LEEB, H. AND WEGENKITTL, S. 1997. Inversive and linear congruential pseudorandom number generators in selected empirical tests. *ACM Transactions on Modeling and Computer Simulation* **7**, 2, 272–286.

LEWIS, P., GOODMAN, A., AND MILLER, J. 1969. A pseudo-random number generator for the System/360. *IBM Syst. J.* **8** , 136–146.

MACLAREN, N. 1989. The Generation of Multiple Independent Sequences of Pseudorandom Numbers. *Appl. Statist.* **38**, 351–359.

NIEDERREITER, H. 1995. New developments in uniform pseudorandom number and vector generation. In H. NIEDERREITER AND P. JAU-SHYONG SHIUE Eds., *Monte Carlo and Quasi-Monte Carlo Methods in Scientific Computing*, Volume 106 of *Lecture Notes in Statistics* (1995). Springer.

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

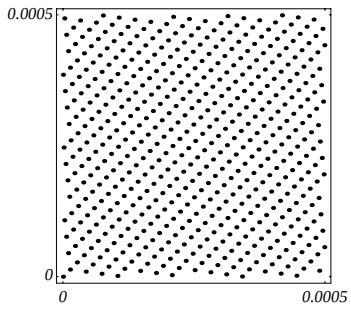
PAYNE, W., RABUNG, J., AND BOGYO, T. 1969. Coding the lehmer pseudo-random number generator. *Communications of the ACM* **12** , 85–86.

RIPLEY, B. 1990. Thoughts on pseudorandom number generators. *J. Comput. Appl. Math.* **31**, 153–163.

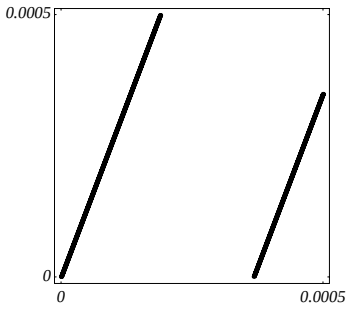
TEZUKA, S., L'ECUYER, P., AND COUTURE, R. 1993. On Add-with-Carry and Subtract-with-Borrow Random Number Generators. *ACM Transactions on Modeling and Computer Simulation* **3**, 315–331.

The Numerical Algorithms Group Limited. 1991. *The NAG Fortran Library Manual, Mark 15* (1 ed.). The Numerical Algorithms Group Limited.

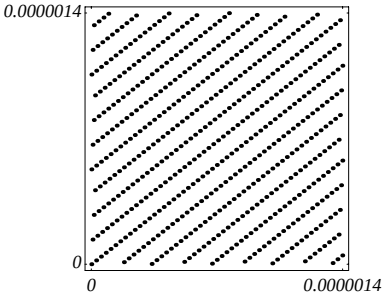
VATTULAINEN, I., KANKAALA, K., SAARINEN, J., AND ALA-NISSILA, T. 1995. A comparative study of some pseudorandom number generators. *Comp. Phys. Comm.* **86**, 209–226.



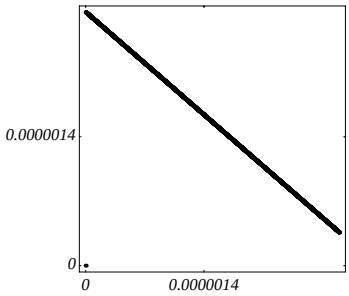
LCG 3



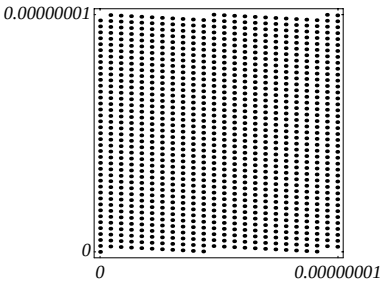
LCG 3 subsequence with $k = 78$



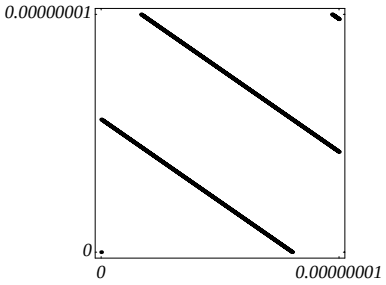
LCG 12



LCG 12 subsequence with $k = 36$



LCG 14c



LCG 14c subsequence with $k = 50$

Fig. 2. Subsequences with reduced quality for LCG 3, 12 and 14c