International Journal of Modern Physics C, Vol. 9, No. 4 (1998) 607–624

THE RANLUX GENERATOR: RESONANCES IN A RANDOM WALK TEST

LEV N. SHCHUR

Landau Institute for Theoretical Physics, 142432 Chernogolovka, Russia
E-mail: *lev@landau.ac.ru*

PAOLO BUTERA

Istituto Nazionale di Fisica Nucleare, Dipartimento di Fisica, Università di Milano
Via Celoria 16, 20133 Milano, Italy
E-mail: *butera@mi.infn.it*

Received 8 May 1998
Revised 13 May 1998

Using a recently proposed directed random walk test, we systematically investigate the popular random number generator RANLUX developed by Lüscher and implemented by James. We confirm the good quality of this generator with the recommended luxury level. At a smaller luxury level (for instance equal to 1) resonances are observed in the random walk test. We also find that the lagged Fibonacci and Subtract-with-Carry recipes exhibit similar failures in the random walk test. A revised analysis of the corresponding dynamical systems leads to the observation of resonances in the eigenvalues of Jacobi matrix.

Keywords: Random Numbers; Random Walks; Dynamical Systems; Anosov Systems.

Categories: PACS Nos.: 02.70.Lq, 02.50.Ng, 05.50+q, 06.20.Dk

1. Introduction

Large-scale Monte Carlo simulations need good quality random numbers.[1] The half-century long history of computer simulations shows successes and failures of many algorithms for pseudo-random number (PRN) generation.[2]

Usually, whenever a new test of randomness is proposed some algorithm for generating PRN's becomes obsolete. A somewhat different point of view is advocated here: using a recently proposed test we argue that all algorithms using feedbacks (or lags) have more or less the same defects and belong to the same "universality class of badness." This class of generators, however, should not be rejected and rather improved versions of them can still be considered reasonably safe (see the final section).

One of the most widely used PRN generators of this class is the shift register (SR) generator.[12] Correlations in SR generators were pointed out by Compagner[4]

but the warning was ignored by computational physicists who usually stick to very practical recipes.[3]

It has been observed later by Ferrenberg, Landau and Wong[5] that the statistical simulations of the 2D Ising model by the Wolff single cluster algorithm are very sensitive to the defects of the Kirkpatrick–Stoll generator[6] (the SR generator with $(p, q) = (250, 103)$).

Motivated by this difficulty, Lüscher[7] and James[8] have developed a random number generator called RANLUX which is based on the subtract-with-carry (SWC) recipe advocated by Marsaglia and Zaman.[9]

We review here some properties of the generator RANLUX using the random walk test recently developed in Ref. 10 by Blöte, Heringa and one of the authors.

First, we find analytically that the deviations computed using the random walk test are the same for SWC and the lagged Fibonacci recipes. This finding is in contrast to the common belief that the SWC generator gives better quality random numbers than recipes which use the exclusive OR operation (like the SR generators) or addition (like the lagged Fibonacci generator). Note, that the RANLUX generator with parameter of luxury equal to 0 is equivalent to the SWC generator.

Second, we have found numerically that correlations among random numbers on distances associated with the lag values are still visible for luxury level parameter equal to 1. However at a luxury level equal to 2 the correlations lie on the boundary of observed deviations (and this is in agreement with the Lüscher and James results).

Therefore, our third result, supporting the author's expectations, is that the RANLUX generator with luxury levels higher than 2 is still safe in runs using less than 10^{15} random numbers.

Next, we also revise the dynamical system description given by Lüscher in his original paper. Namely, we argue that the correlations responsible for the deviations found in the simulation of the two-dimensional Ising model and of the random walks are not due to the correlation of trajectories in the corresponding dynamical systems. These deviations are rather connected with the correlations between random numbers, on distances equal to the lag values, as we show using the random walk test.

We compute the full spectrum of eigenvalues for the RANLUX generator and for the lagged Fibonacci generator with different lags. Our fifth result is the observation of resonances in the eigenvalues, reflecting the complexity of the phase space in the area preserving (Hamiltonian) dynamical systems.

The paper is organized is follows. In Sec. 2 we recall the definitions of random number generators used here — Subtract-with-Carry (SWC), lagged Fibonacci (LF) and Shift register (SR), and review the random walk test. In Sec. 3 we apply the random walk test to the RANLUX generator and surprisingly find that the SWC generator obeys the same analytical solutions as the LF generator. Then we analyze how the correlations in random walks depend on the luxury levels of the RANLUX generator. In Sec. 4 we reanalyze the dynamical system

approach to RANLUX generator and find resonances in the eigenvalues of the Jacobi matrix associated with the complex structure of the manifolds. Finally, in Sec. 5 we discuss the attempts to improve the lagged random number generators.

2. Definitions and Notations

We recall here the definitions of several random number generators which have the common feature of using lag algorithms. We also recall the definition of the random walk test.

2.1. *Marsaglia–Zaman recipe and RANLUX generator*

The PRN generation algorithm of Marsaglia–Zaman[9] is defined by a recursion relation involving three fixed positive integers b, r, s where b is called the base and $r > s$ are called the lags. This algorithm is usually known as SWC generator. Given the first r PRN's $x_0, x_1, \ldots, x_{r-1}$ and the "carry bit" c_{r-1}, the nth PRN ($n \geq r$) is given by

$$\begin{aligned} &x_n = (x_{n-s} - x_{n-r} - c_{n-1}) \bmod b \\ &c_n = 0 \quad if \;\; x_{n-s} - x_{n-r} \geq 0 \\ &\text{and} \\ &c_n = 1 \quad \text{otherwise.} \end{aligned} \tag{1}$$

The maximum possible period of this generator is $M = b^r - b^s + 1$ and it is attained when M is prime and b is a primitive root modulo M.

In order to improve the properties of this algorithm which fails to pass some correlation tests, Lüscher proposed[7] to discard some of the PRN's produced by the MZ recursion and to use only the remaining ones. James has then defined[8] four levels of rejection (called "luxury levels"), characterized by an integer $p \geq 24$ in which the generator produces 24 PRN's, then discards the successive $p - 24$ and so on. Clearly the value $p = 24$ reproduces the original MZ recipe where all PRN's are kept and it is called luxury level zero. The values $p = 48, 97, 223, 389$ define the luxury levels $1, 2, 3, 4$, respectively. It has been suggested[7] that level 3 has a good chance of being optimal.

2.2. *Lagged Fibonacci generator*

The Fibonacci lagged generator (LF) is defined by the recursion relation

$$x_n = (x_{n-s} + x_{n-r}) \bmod 2^w, \tag{2}$$

where again s and $r > s$ are the lags and 2^w is the base. Brent gave conditions,[11] under which the above relation generates a sequence of PRN's having the maximum possible period $T = 2^{w-1}(2^r - 1)$. (T is simply the product of the reduced computer word length and of the number of possible initial seeds. The latter is the number of possible r bit seeds excluding zero.)

2.3. *Shift register generator*

The generalized feedback shift register (SR) method is defined by the recursion rule[12]

$$x_n = x_{n-s} \oplus x_{n-r}, \tag{3}$$

where $\oplus$ denotes the *exclusive-or* operation (bitwise sum modulo 2), s and $r > s$ are the lags. This sequence has maximum period $T = 2^r - 1$ if its characteristic polynomial is irreducible (for details, see Chap. 2 of Golomb's book[12]).

2.4. *Random walk test*

Let us consider the one-dimensional directed random walk model[10]: a walker starts at some site of an one-dimensional lattice and, at discrete times i, either he takes a step in a fixed direction with a probability μ_i or he stops with a probability $1 - \mu_i$. In the latter case a new walk begins. The probability of a walk with length n is then

$$P(n) = \left(\prod_{i=1}^{n-1} \mu_i \right) (1 - \mu_n).$$

In the case in which all probabilities are equal $\mu_i = \mu$, the probability for a walk of length n is

$$P(n) = \mu^{n-1} (1 - \mu) \tag{4}$$

and the mean walk length is given by

$$\langle n \rangle = \frac{1}{1 - \mu}. \tag{5}$$

Comparing μ with $\tanh(J/k_B T)$ it immediately follows that the mean walk size diverges as $\mu \to 1$ in the same way as the mean cluster size diverges as the temperature $T \to 0$ in the 1D Ising model.[10]

3. Random Walk in a Correlated Environment

The production rules for the SR and LF generators with the pair (p, q) of lags give rise to correlations on distances $l_c = ip + jq$, where i and j are integers.[4,10] We can treat these correlations as some kind of impurities, placed on the bonds of the 1D lattice and thus influencing the walk probabilities μ_i.

In some cases, it is possible to get exact analytical results for the deviations of walk probabilities from their values in the pure case.

In addition, correlations in the PRN sequences can be nicely detected by simulation of this model on the computer and by comparing the observed frequency $P^*(n)$ of walks of length n with their expected (pure) probability $P(n)$. In what follows we will plot the measured deviations

$$\delta P(n) \equiv \frac{P^*(n)}{P(n)} - 1 \tag{6}$$

versus n, for various PRN generators and briefly comment on why they occur.

For all PRN generators we will consider here, biases are brought out in the directed random walk model by the obvious fact that the end of a walk and the beginning of a new one are strictly correlated: as a result probability deviations will occur at walk lengths related to the lag values in the production rule. To be definite, suppose for example that in our PRN sequence the nth term x_n is generated from x_{n-r} and x_{n-s} with $r > s$ and let us assume for simplicity that the stepping probability in our model has the value $\mu = 1/2$. In other words the ideal walker would proceed after tossing a good coin, while the real walker will have to resort to our deterministic PRN generator with lags r and s. Let us now suppose that the real walker stops after k steps, so that $x_k > \mu$. Since the production rule gives x_k in terms of x_{k-r} and x_{k-s}, both of which have to be less than μ, it follows that the probability of the kth step of the real walker is biased by his previous history.

The first study of this new correlation test in the case of the shift register and lagged Fibonacci generators has been performed in Ref. 10.

3.1. *Random walk and luxury levels*

Here we shall test the RANLUX generator with different levels of luxury in the simulation of the directed random walk model.

To begin let us choose luxury level 0 and step probability $\mu = 31/32$. In Fig. 1 we have plotted versus n the deviation $\delta P(n)$ (defined by Eq. (6)) of the frequency of the walks of length n from their expected probability. We notice strong signals for $n_1 = r = 24$ and $n_2 = 2r = 48$. A sizable deviation is also clearly visible for all walk lengths exceeding the largest lag r.

We should stress that our choice of the value of the step probability has no special meaning and that our results depend smoothly on μ.

One should notice the qualitative similarity of the deviations in Fig. 1 and Fig. 4, which refers to the case of a lagged Fibonacci generator. Moreover, it could be shown analytically that the deviations at $n = r$ and at $n = i$, satisfying

$$r < i < \begin{cases} r + s & \text{if } s < \dfrac{r}{2} \\ 2r - s & \text{if } s > \dfrac{r}{2} \end{cases} \tag{7}$$

coincide for the lagged Fibonacci and the SWC generators. We recall that the RANLUX generator with luxury level 0 is equivalent to the SWC generator. It also could be shown, that the mean value of the deviation for the SWC generators at $n = r$ is equal to that for the lagged Fibonacci generator obtained in Ref. 10

$$\delta P(r) = \frac{1 - 2\mu}{2\mu} \tag{8}$$

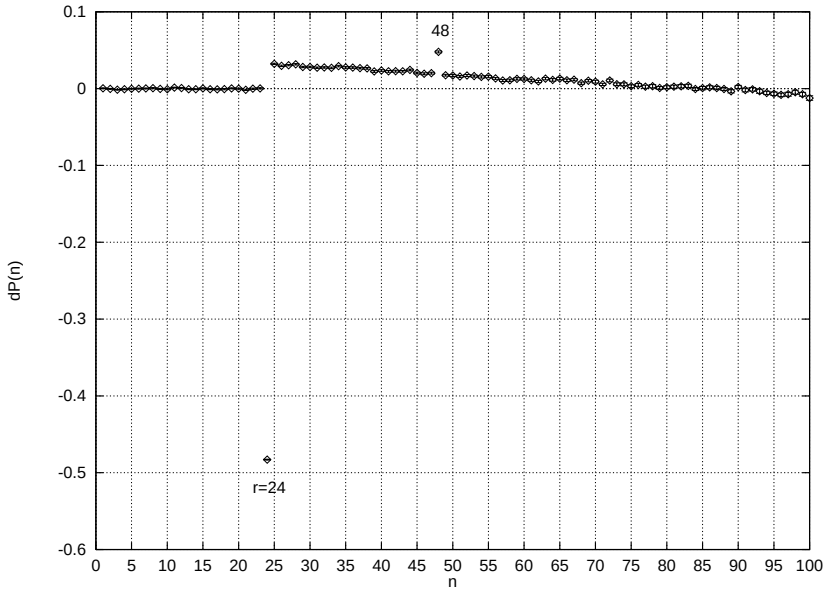

Fig. 1. Deviation δP of the probability of a walk length n from the value for uncorrelated random numbers versus walk length. We have used the RANLUX random number generator with lag values $r = 24$ and $s = 10$ and luxury level 0. The step probability is $\mu = 31/32 = 0.968750$. The result of averaging over 10^8 walks is shown.

and that the mean value of the deviation at $n = r + 1$ is

$$\delta P(r+1) = \frac{(3\mu - 1)^2}{4\mu^4} - 1. \tag{9}$$

In order to check that point, in Table 1 we have presented a comparison of the observed values of the deviations obtained using either the RANLUX generator with luxury level 0 or the lagged Fibonacci generator for two values of the step probability with the expected values given by Eqs. (8) and (9). All data agree within the statistical errors.

In contrast to common belief this result shows that there are no differences in the accuracy of the data obtained using the LF and the SWC generators,

Table 1. Comparison of probability deviations, computed using directed random walk test with lagged Fibonacci (LF) and subtract-with-carry (SWC) random number generators, and predicted by formulas (8) and (9).

	$\mu = 31/32$		$\mu = 15/16$	
	$\delta P(r)$	$\delta P(r+1)$	$\delta P(r)$	$\delta P(r+1)$
Expected	$-0.48387\ldots$	$0.03146\ldots$	$-0.4666\ldots$	$0.06319\ldots$
LF	$-0.48304(55)$	$0.03221(81)$	$-0.46636(47)$	$0.06290(85)$
SWC	$-0.48299(64)$	$0.03122(81)$	$-0.46696(63)$	$0.06243(113)$

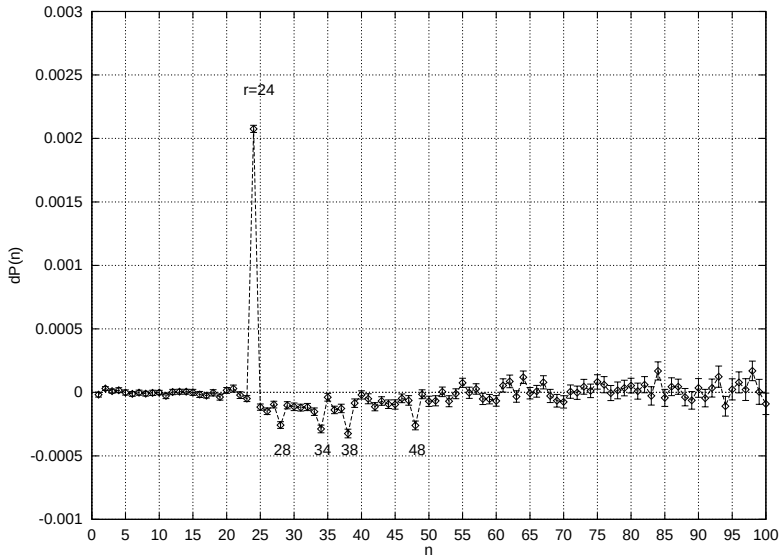

Fig. 2. Deviation δP of the probability of a walk length n from the value for uncorrelated random numbers versus walk length. We have used the RANLUX random number generator with lag values $r = 24$ and $s = 10$ and luxury level 1. The step probability is $\mu = 31/32 = 0.968750$. The result of averaging over 10^{11} walks is shown.

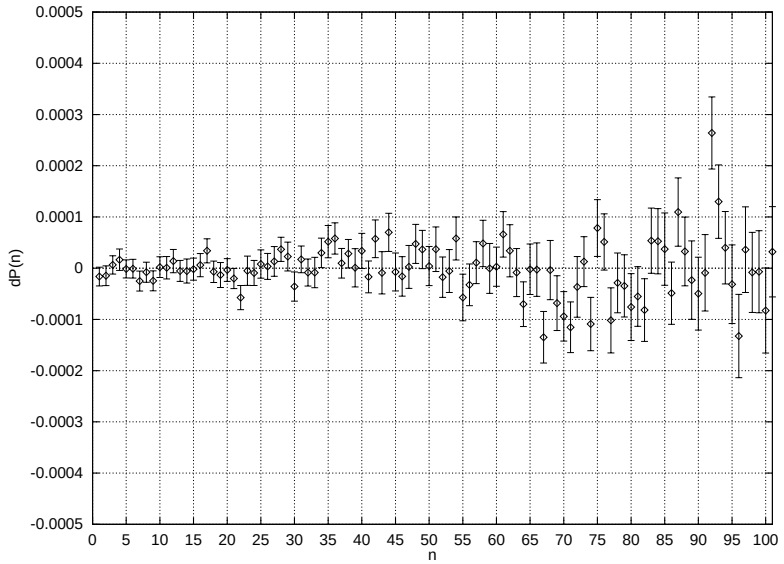

Fig. 3. Deviation δP of the probability of a walk length n from the value for uncorrelated random numbers versus walk length. We have used the RANLUX random number generator with lag values $r = 24$ and $s = 10$ and luxury level 2. The step probability is $\mu = 31/32 = 0.968750$. The result of averaging over 10^{11} walks is shown.

at least as far as the cluster formation processes or the random walks are simulated.

The next luxury level of the Lüscher and James RANLUX is 1. In this case only the first $r = 24$ random numbers are used out of each generated set of $p = 48$. The observed deviations Eq. (6) are plotted in Fig. 2. Clearly, a deviation at $n = r = 24$ still remains, but has opposite sign and a much smaller size in comparison with that observed for the luxury level 0.

Also at the values $n = 28, 34, 38, 48$, all of which are linear combinations of the lags with small integer coefficients, smaller deviations remain clearly visible.

We conclude that, at the luxury levels 0 and 1, the deviations have the same qualitative nature, the only difference being that the absolute value of the deviations is depressed for the higher levels of luxury.

This remark is confirmed by Fig. 3 where we have plotted the observed deviations for the case of luxury level 2, and the visible deviations are not larger than the statistical errors. Notice that in this case the average length of the walk is 32 and for the total number of 10^{11} walks approximately 10^{13} random numbers were used. We could extrapolate our result like in Ref. 13 and we expect that deviations will be visible even for the luxury level 2 if $\approx 10^{15}$ random numbers are used.

3.2. *Lagged Fibonacci with luxuries*

In Fig. 4 we present the results of a simulation using the plain lagged Fibonacci generator with lags $r = 24$ and $s = 10$. The plot shows features

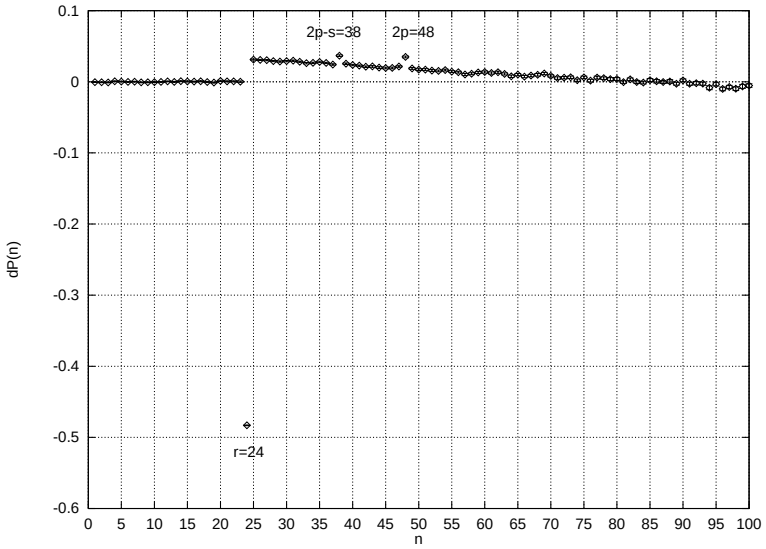

Fig. 4. Deviation δP of the probability of a walk length n from the value for uncorrelated random numbers versus walk length. We have used the lagged Fibonacci generator with lag values $r = 24$ and $s = 10$. The step probability is $\mu = 31/32 = 0.968750$. The result of averaging over 10^8 walks is shown.

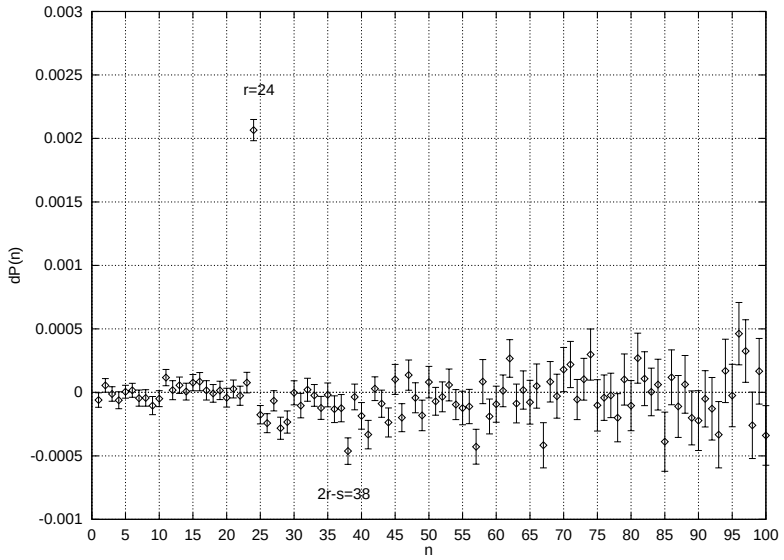

Fig. 5. Deviation δP of the probability of a walk length n from the value for uncorrelated random numbers versus walk length. We have used the lagged Fibonacci generator with lag values $r = 24$ and $s = 10$ and luxury level 1. The step probability is $\mu = 31/32 = 0.968750$. The result of averaging over 10^{10} walks is shown.

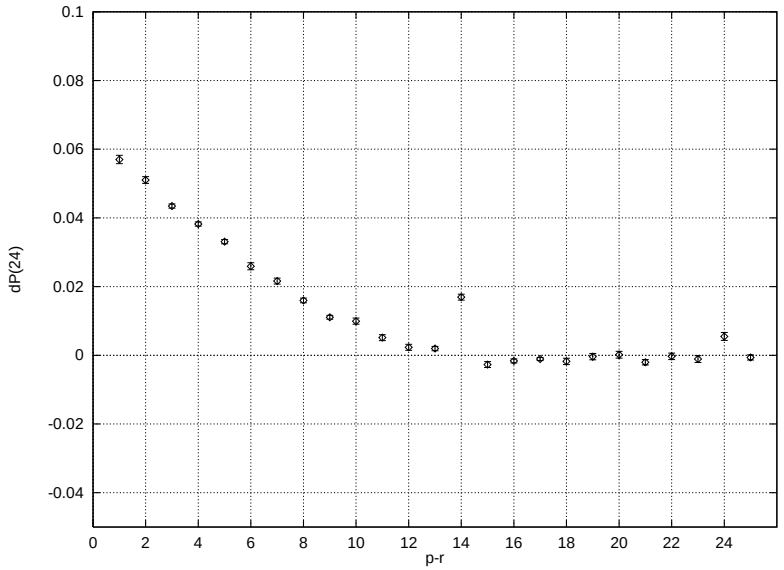

Fig. 6. Lagged Fibonacci generator with lags $r = 24$ and $s = 10$ and $\mu = 15/16$. The figure shows the deviation $\delta P(r)$ as a function of $p - r$ on the way from luxury level 0 ($p - r = 0$) to luxury level 1 ($p - r = 24$).

completely similar to those of Fig. 1 obtained with RANLUX at luxury level 0.

We can now extend to the lagged Fibonacci generator (LF) the procedure of decorrelation which discards 24 PRN's out of each generated set of 48, and call it following Lüscher[7] and Jamess'[8] luxury level 1. In Fig. 5 we have reported the results of a simulation using the LF generator with lags $r = 24$, $s = 10$ at luxury level 1. The results again show no qualitative difference from those reported in Fig. 2 obtained when RANLUX at the same luxury level was used: a strong deviation is observed when the walk length equals the value of the largest lag r and smaller but visible deviations occur for any $n > r$.

In order to understand how the decorrelation procedure works we also have studied intermediate luxury levels obtained by varying p between 24 and 48 in steps of one. In Fig. 6 we have plotted $\delta P(24)$ versus $p - r$. The value of $\delta P(24)$ decreases rapidly but peaks are still evident at $p - r = 10, 14, 24$ indicating the persistence of an interplay between p and the lags r and s.

4. Dynamical System

Lüscher justified his proposal of skipping some $p - r$ numbers using the language of dynamical systems.[7]

Let us then briefly recall here a few well known results from the dynamical system theory.

The production rules Eqs. (1), (2) and (3) can be rewritten[7] in the matrix form

$$\mathbf{v}_{n+1} = \mathbf{L}\mathbf{v}_n, \tag{10}$$

where the rule of matrix "multiplication" includes the "$\oplus$" operation for the shift register generator, the usual "$+$" operation for the lagged Fibonacci and the "$-$" operation for the SWC generators, and $\mathbf{v}_n = (x_{n-r+1}, x_{n-r+2}, \ldots, x_{n-1}, x_n)$ is an r-component vector.

The simplest example is the Fibonacci sequence

$$x_n = x_{n-1} + x_{n-2}, \tag{11}$$

which can be written in matrix form

$$\begin{pmatrix} x_n \\ x_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x_{n-1} \\ x_{n-2} \end{pmatrix}. \tag{12}$$

This shows that the dynamical system, corresponding to the Fibonacci random number generator with lags $r = 2$ and $s = 1$ is the famous Arnold's "cat map", acting on the unit torus, obtained by rewriting Eq. (10) in the form

$$\mathbf{v}_{n+2} = \mathcal{M}\mathbf{v}_n. \tag{13}$$

The matrix $\mathcal{M} = \mathbf{L}^r$ is called the monodromy matrix,

$$\mathcal{M} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}. \tag{14}$$

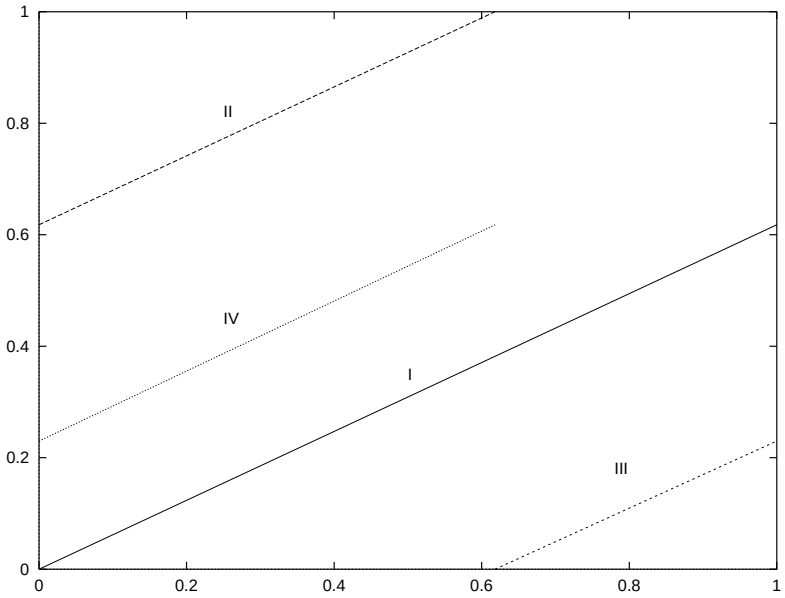

Fig. 7. Fibonacci sequence on torus: Arnold's cat map.

The eigenvectors $(\gamma^{-2}, 1)$ and $(\gamma^2 - 1, 1)$ of $\mathcal{M}$ define respectively the stable and the unstable directions of the origin, which is an unstable fixed point. The corresponding eigenvalues are

$$\begin{pmatrix} \lambda_1 \\ \lambda_2 \end{pmatrix} = \begin{pmatrix} \gamma^2 \\ \gamma^{-2} \end{pmatrix} \approx \begin{pmatrix} 2.618034\ldots \\ 0.381966\ldots \end{pmatrix}, \tag{15}$$

and $\gamma = (1 + \sqrt{5})/2$ is the golden mean.

Figure 7 demonstrates the idea of hyperbolicity of the "cat map." The points on the part I of the unstable manifold are mapped under a single application of the transformation Eq. (14) onto the four parts (in order, denoted by I, II, III and IV) of the same unstable manifold. Clearly, Fig. 7 shows a trajectory winding on the torus with the golden angle $\tan\phi = (\sqrt{5}-1)/2$. The distance between neighbor points along the unstable manifold is enlarged by a factor λ_1. In order to imagine the complexity of the trajectories, one needs to add the set of transversal lines representing the stable manifold. Along these lines the distances are contracted by a factor λ_2. Thus, according to the Poincaré theory, there is an infinite set of periodic points with zero measure in this system (we address interested readers to the figures on page 170 of Ref. 17.)

It is known[16] that the "cat map" is an Anosov system, which implies the following properties of randomness[17]: global instability (the Lyapunov exponent, which is the logarithm of λ_1 from Eq. (15), is positive), positivity of Kolmogorov-Sinai entropy (the trajectories are locally divergent), mixing (existence of equilibrium state

for the distribution function) and, finally, ergodicity (the equivalence of averaging over time and over space). Nevertheless, the "cat map" doesn't have the strongest property of randomness, namely, it is not a Bernoulli system, in other words it is not a system "whose motion is as random as a fair coin toss" (M. Tabor in Ref. 17, page 174).

In fact, the lagged Fibonacci generators (and the Marsaglia–Zaman SWC generators as well) are an r-dimensional generalization of a "cat map." A regular way to extend randomness properties to higher dimensions is not known. Nevertheless, in general, one should not expect from the generalized system stronger properties of randomness than in the case of a low-dimensional system. In fact, it is practically sufficient to analyze the eigenvalues of the corresponding monodromy matrix to be sure that a system is locally hyperbolic at any point of phase space (to have, at least, the properties of the weakly Anosov systems[18]).

The suggestion of Lüscher to improve the quality of the random numbers generated by rule (10) is based on the observation, that since the absolute value of the largest eigenvalue of the matrix L in (10) is greater than unity, we can construct a monodromy matrix $\mathcal{M} = \mathbf{L}^p$ with a relatively large modulus of the largest eigenvalue, whose logarithm is the Lyapunov exponent of the corresponding dynamical system on the r-dimensional torus.

Indeed, his Fig. 1 from Ref. 7 shows clearly the process of decorrelation (loss of memory). If we apply the monodromy matrix $\mathcal{M}$ to the shortest representable vector which has elements of order of 2^{-m}, the length of our vector will become the order of unity after a number of iterations n such that

$$2^{-m}\ \lambda^n \approx 1. \tag{16}$$

Knowing the Lüscher result for $n = 16$ and considering the case of 24-bit representation for the random numbers ($m = 24$), as in his paper, from Eq. (16) we could estimate λ as $\lambda \approx 2^{24/16} \approx 2.828\ldots$ in a good agreement with his direct calculation $\lambda = 2.746\ldots$.

This means, according to Lüscher, that the decorrelation time depends on the number of bits in the random number representation

$$n \approx m\ \frac{\log 2}{\log \lambda} \tag{17}$$

and leads to the prediction of an infinite decorrelation time in the limit $m \to \infty$. We could use the same arguments for the case of a "cat map" and would arrive at a contradiction with Arnold's result, that the "cat map" is a C-system with the strong ergodic properties cited above.

This means, that the values of the Lyapunov exponent are not directly connected with the process of decorrelation in random number sequences. We can support our idea considering the LCG generator which are known to have a lattice structure and introducing luxury levels in this case. It is clear, that the lattice structure will not disappear — increasing the luxury levels would enlarge eigenvalues, but the lattice structure would still persist.

Really, as we have demonstrated using the random walk test, the situation is more complicated and we need to consider also the correlations in the production rules on distances equal to the lags and to their linear combinations. This effect is clearly visible in Fig. 6, where one can see strong resonances at lag values $r = 24$ and $s = 10$, whereas the eigenvalues are increasing smoothly as λ_1^p with p.

It should be noted, that the deviations at $\delta P(r)$ do not vanish smoothly on the way from one luxury level to another, but they oscillate. We hope, nevertheless, that the amplitude of these oscillations vanishes.

4.1. *Eigenvalue spectrum*

Each state of the random number generators of interest is described by a set of r random numbers $v_i^0,\ (i = 1, 2, \ldots, r)$. After r applications of any of the rules Eqs. (1), (2) and (3), we will have completely refreshed the set of r random number $u_i^0,\ (i = 1, 2, \ldots, r)$. This defines the mapping of unit r-dimensional cube onto itself.[7]

We could construct numerically the Jacobi matrix,[16,19] as the matrix of the variations of the final set $u_i = u_i^0 + \delta u_i$ due to the variations of the initial set $v_i = v_i^0 + \delta v_i$:

$$J_{ij} = \frac{\delta u_i}{\delta v_j}, \tag{18}$$

which reflects the behavior of neighbor trajectories for all components of the set u_i.

The eigenvalues of RANLUX with luxury level 0 are plotted on Fig. 8 together with the eigenvalues for the corresponding lagged Fibonacci generator with lags $(24, 10)$. It is clear that eigenvalues will collapse on a single curve changing the sign of $\mathrm{Re}(\lambda)$. These eigenvalues could be determined directly from the characteristic polynomial for the productions rules, which reads as

$$\lambda_0^{24} - \lambda_0^{14} \pm 1 = 0 \tag{19}$$

with the plus sign for the Marsaglia–Zaman generator and the minus sign for the Fibonacci generator. In Fig. 8 we have plotted λ_0^{24} (we remind the reader that the dynamical system is obtained as the mapping of the r-dimensional unit cube onto itself, after p iterations of the production rule. The luxury level 0 corresponds to $p = 24$.)

Figure 9 demonstrates how the eigenvalues change going from the luxury level 0 to the luxury level 1 in the case of the RANLUX generator.

Below we will produce data for the lagged Fibonacci generator with $p > r$ (we generate p random numbers and use only the last r of them) taking into account the similarity in many aspects of the lagged Fibonacci and the RANLUX generators described in this paper.

First, we show how the eigenvalues depend on the value of the lag r. Figure 10 shows, in particular, that the eigenvalues for (24, 10) and (250, 103) lie almost on

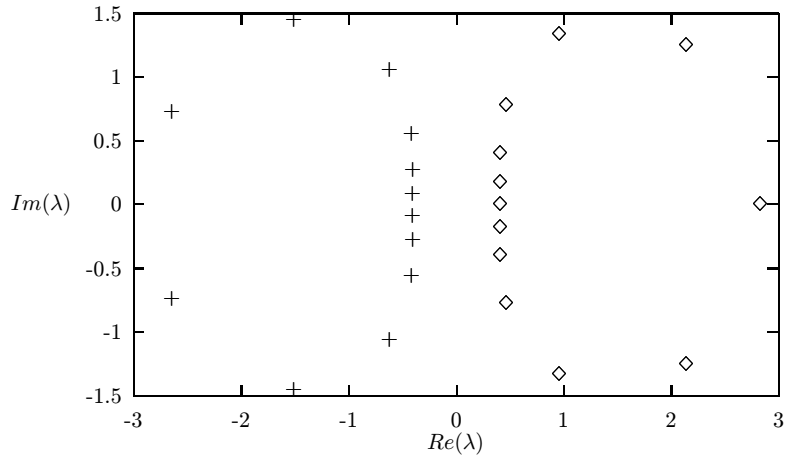

Fig. 8. Eigenvalues of the Jacobi matrixes corresponding to the RANLUX generator with luxury level 0 (marked with pluses +). The same for lagged Fibonacci generator with lags (24, 10) (marked with diamonds ⋄).

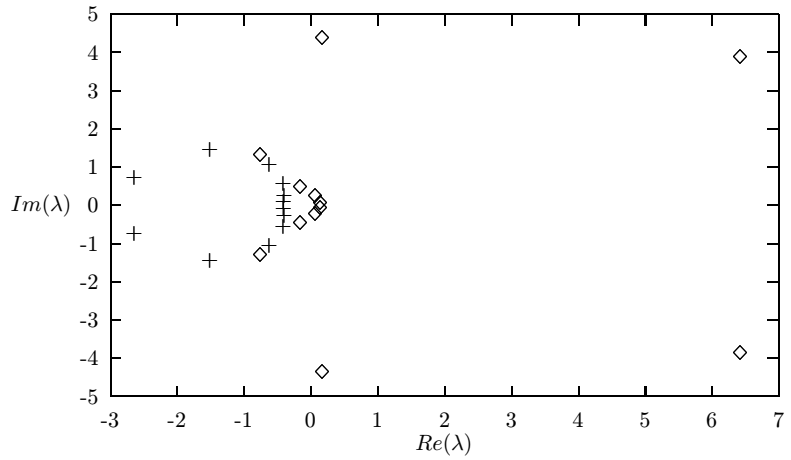

Fig. 9. Eigenvalues of the Jacobi matrixes corresponding to the RANLUX generator with luxury level 0 (pluses +) and to the RANLUX generator with luxury level 1 (diamonds ⋄).

the same curve. We will plot below the eigenvalues for the last case in order to have more detailed pictures.

In Figs. 11–14 we show how the eigenvalues change when the parameter p is varied. One clearly sees that the resonances in eigenvalues reflect the interplay of the lags (r, s) and the parameter p. These pictures reflect in some sense the complexity of the phase space of our dynamical systems.

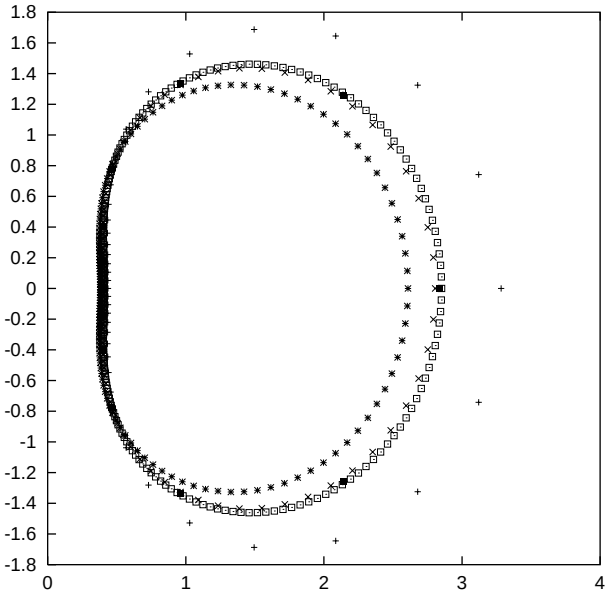

Fig. 10. The complex plane eigenvalues of the Jacobi matrices corresponding to the lagged Fibonacci generator with lags (24, 10), (36, 11), (89, 38), (127, 64) and (250, 103) indicated by $(\Box, +, \times, *, \Box)$ respectively.

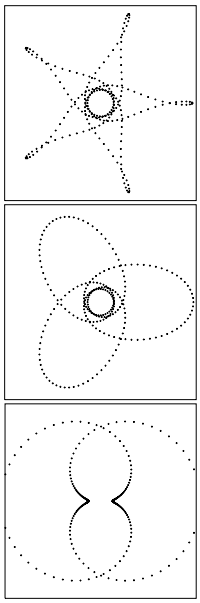

Fig. 11. Complex plane eigenvalues for the lagged Fibonacci generator with lags (250 ,103). The number of discarded PRN's is 3, 5 and 22 going from top to bottom.

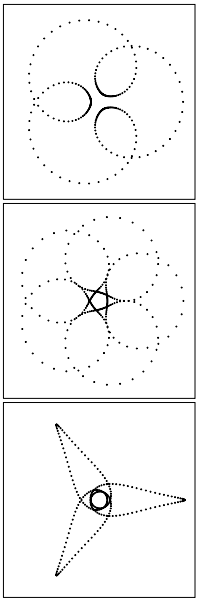

Fig. 12. Complex plane of eigenvalues for the lagged Fibonacci generator with lags (250, 103). The number of discarded PRN's is 49, 50 and 54 going from top to bottom.

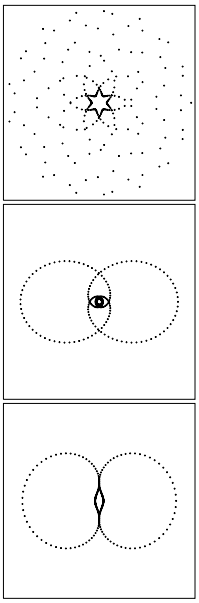

Fig. 13. Complex plane of eigenvalues for the lagged Fibonacci generator with lags (250, 103). Number of discarded PRN's is 71, 92 and 125 going from top to bottom.

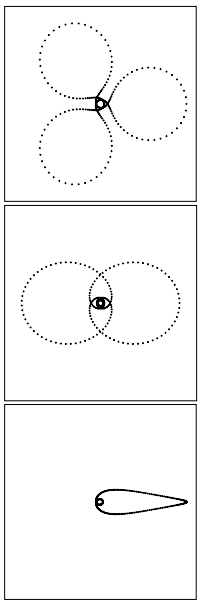

Fig. 14. Complex plane of eigenvalues for the lagged Fibonacci generator with lags (250, 103). The number of discarded PRN's is 152, 184 and 206 going from top to bottom.

5. Conclusions

In this paper we have shown that the sequences of random numbers generated using both the lagged Fibonacci and the subtract-with-carry generators have equivalent correlation properties, at least as far as the random walk and the cluster algorithms are concerned.

We have argued that correlations in random numbers on the lag distances decrease with increase of the luxury levels, although not monotonically. There are also resonances when the number $p - r$ of discarded random numbers coincides with linear combinations of lags. We also have argued that correlations on these distances are more important than correlations between "trajectories" of random numbers in phase space.

Comparisons of lagged Fibonacci and shift register generators have been presented in Ref. 10 and our analysis demonstrates that they behave in a qualitatively similar way.

One can conclude, that all recipes using lags will produce sequences of random numbers with the same qualitative features. It is important that knowing these bad properties we can avoid possible deviations either using the idea of luxury levels,[7,8] or decimated sequences[4,13] or combinations of two or more random number generators[4,13,14] or generators with a larger number of lags.[4,15]

Therefore rephrasing Orwell: "All algorithms for generating random numbers are equally bad, but some of them are more equal than others."[20]

Acknowledgments

The authors are thankful to G. Marchesini whose reasonable question on RANLUX initiated this work. Discussions and help from M. Comi, M. Enriotti, S. A. Krashakov and G. Salam were very important. LNS thanks to Theoretical Group of Milan University for the kind hospitality and Italian Ministry for Foreign Affairs for a Fellowship. This work has also been partially supported by grants from RFBR, INTAS and NWO.

References

1. K. Binder and D. W. Heermann, *Monte Carlo Simulation in Statistical Physics* (Springer-Verlag, Berlin, 1997).
2. D. E. Knuth, *The art of Computer Programming*, Vol. 2 (Addison-Wesley, Cambridge, 1981).
3. As a result, the section on random number generation is the most alterable part of the successive editions of the popular handbook by W. H. Press, D. P. Flannery, S. A. Teukolsky, and W. T. Vetterling, *Numerical Recipes* (Cambridge Univ. Press).
4. A. Compagner, *J. Stat. Phys.* **63**, 883 (1991); A. Compagner, *Am. J. Phys.* **59**, 700 (1991); A. Compagner, *The ABC of random number generation*, Delft University preprint CP-95-001 (1995); A. Compagner, *Phys. Rev.* **E52**, 5634 (1995).
5. A. M. Ferrenberg, D. P. Landau, and Y. J. Wong, *Phys. Rev. Lett.* **69**, 3382 (1992); W. Selke, A. L. Talapov, and L. N. Shchur, *JETP Lett.* **58**, 665 (1993); P. D. Coddington, *Int. J. Mod. Phys.* **C5**, 547 (1994); I. Vattulainen, T. Ala-Nissila, and K. Kankaala, *Phys. Rev. Lett.* **73**, 2513 (1994); I. Vattulainen, T. Alla-Nissila, and K. Kankaala, *Phys. Rev.* **E52**, 3205 (1995); P. D. Coddington, *Int. J. Mod. Phys.* **C7**, 295 (1996).
6. S. Kirkpatrick and E. P. Stoll, *J. Comp. Phys.* **40**, 517 (1981).
7. M. Lüscher, *Comp. Phys. Comm.* **79**, 100 (1994).
8. F. James, *Comp. Phys. Comm.* **79**, 111 (1994).
9. G. Marsaglia and A. Zaman, *Ann. of Appl. Prob.* **1**, 462 (1991).
10. L. N. Shchur, J. R. Heringa, and H. W. J. Blöte, *Physica* **A241**, 579 (1997).
11. R. P. Brent, *Math. of Comp.* **63**, 389 (1994).
12. S. W. Golomb, *Shift Register Sequences*, 2nd edition (Aegean Park Press, Laguna Hills, 1982).
13. L. N. Shchur and H. W. J. Blöte, *Phys. Rev.* **E55**, R4905 (1997).
14. A. L. Talapov, H. W. J. Blöte, and L. N. Shchur, *JETP Lett.* **174** (1995).
15. R. M. Ziff, to be published in *Computers in Physics*, 1998.
16. V. I. Arnold, *Geometrical Methods in the Theory of Ordinary Differential Equations, 2nd edition* (Springer, New York, 1988), p. 121–131.
17. M. Tabor, *Chaos and Integrability in Nonlinear Dynamics* (John Wiley and Sons, New York, 1989), p. 167–174.
18. R. S. MacKay, in "Quantum chaos," *Proc. Int. School of Physics* "*Enrico Fermi*," Varenna, August 1991, G. Casati, I. Guarneri, and U. Smilansky (eds.), (North-Holland, 1993).
19. E. S. Nikolaevsky and L. N. Shchur, *JETP* **58**, 1 (1983).
20. G. Orwell, *Animal Farm* (Secker & Warburg, London, 1945).