Logistic map: A possible random-number generator

S. C. Phatak* and S. Suresh Rao†
Institute of Physics, Bhubaneswar-751005, India
(Received 7 September 1993; revised manuscript received 15 July 1994)

The logistic map is one of the simple systems exhibiting order to chaos transition. In this work we have investigated the possibility of using the logistic map in the chaotic regime (LOGMAP) for a pseudorandom-number generator. To this end we have performed certain statistical tests on the series of numbers obtained from the LOGMAP. We find that the LOGMAP passes these tests satisfactorily and therefore it possesses many properties required of a pseudorandom-number generator.

PACS number(s): 05.45.+b, 05.20.−y, 01.50.Ht, 02.70.Lq

I. INTRODUCTION

A sequence of numbers that are chosen at random are useful in many different kinds of applications such as simulation, sampling, numerical analysis, decision making, recreation, etc. A sequence of truly random numbers is unpredictable and hence unreproducible. Such a sequence can only be generated by a physical process, for example, radioactive decay, thermal noise in electronic devices, cosmic ray arrival time, etc. In practice, however, it is very difficult to construct physical generators that are fast enough and at the same time accurate and unbiased. Furthermore, one would like to be able to repeat the calculation at will, for debugging or developing the program. Thus, for most calculational purposes, pseudorandom numbers (PRN) have been introduced. Pseudorandom numbers are numbers computed from a deterministic algorithm (hence, it is called pseudorandom or quasirandom) and therefore reproducible. Obviously, these are not at all random in the mathematical sense, but are supposed to be indistinguishable from a sequence generated truly randomly. A good PRN generator should possess long period, high speed, and randomness.

Over the years, various PRN generators have been developed and can be broadly classified into the following categories [1]: (i) linear recurrence methods, (ii) multiplicative congruential generators, (iii) Tausworthe generators, and (iv) combination generators. All these are bit based generators. These methods have various parameters or inputs and the period and the statistical properties of PRN sequences sensitively depend on these parameters. The first two are known to have periods of about $\sim 10^9$ on a 32-bit machine. In the other two methods one can achieve a much larger period ($\sim 10^{170}$) [1].

It is not easy to invent a foolproof source of random numbers. Generally, a number of tests [2] are performed to test the *randomness* of the numbers generated by PRNs. In spite of these tests, one finds that a PRN that has passed these tests may fail when applied to some physical applications: For example, in a recent study, Ferrenberg, Landau, and Wong [3] have shown that even the high quality PRNs are biased under certain circumstances. Extensive Monte Carlo simulations by this group on an Ising model, for which exact answers are known, have shown that ostensibly high quality random-number generators may lead to subtle, but dramatic, systematic errors for some algorithms, but not others. They traced the discrepancy to the correlations in the random numbers. Another recent study by Vattulainen *et al.* [4] find no such correlations. This only means that what is "random" enough for one application may not be *random* enough for another. The important criterion is that a specific algorithm must be tested together with the random-number generator being used regardless of which tests the generator has passed. This being the scenario, it may be useful to consider PRNs based on algorithms different from conventional algorithms. In the present work, we discuss a PRN generator based on an inherently chaotic (random) algorithm and its statistical properties. Here we have employed the logistic map in the chaotic regime as a PRN generator. We feel that such an effort is useful because it provides an entirely different method of producing PRNs. Also, the algorithm used is very simple, so the generator is quite fast. There have been earlier attempts to use the logistic map as a random-number generator. Ulam and von Neumann [5] studied the logistic map and noted that by appropriate transformation, the numbers from the logistic map can be converted to a sequence of random numbers uniformly distributed in the interval $(0,1)$. Collins *et al.* [6] applied logit transformation on the logistic map and generated a near-Gaussian distribution. Peng *et al.* [7] used the logistic map in the chaotic regime to calculate the properties of a well known random process: the invasion percolation problem. In this study, it was found that the static properties of percolating clusters, except for the percolation threshold, are correctly calculated but the dynamical properties are not. It is not clear from this work if this difference is due to nonuniform nature of the distribution or due to the correlation between successive numbers. The method we are adopting here differs from the earlier calculations in two respects. In the earlier works, the random numbers were drawn from the logistic map, which is

*Electronic address: phatak@iopb.ernet.in
†Electronic address: suresha@iopb.ernet.in

known to have a distribution of $\sim \frac{1}{\sqrt{x(1-x)}}$ and is used in the simulation studies. We use a simple transformation to convert this distribution into a uniform distribution. Also, the earlier calculations make no attempt to either remove or study the effects of the correlations that exist between succesive numbers generated by the logistic map. We have done that. Here we draw the numbers from a uniform distribution (see below) and investigate the statistical properties. Our calculations show that the period of such a generator is of the order of 10^8 (although theoretically infinite) if the computations are done in double precision. This can be enhanced further if the quadruple precision is employed and is certainly larger than 10^9. Our investigation of the distribution properties of this PRN generator show some peculiarities. These can be cured by introducing the τ shift (to be explained below). In the following, we shall first describe the logistic map and discuss the PRN generator in Sec. II. The results of different tests performed on PRNs thus generated are presented in Sec. III, and the conclusions are given in Sec. IV.

II. THE LOGISTIC MAP

Chaos in dynamical systems has been investigated over a long period of time [8]. With the advent of fast computers, the numerical investigations of chaos have increased considerably over the last two decades and by now, a lot is known about chaotic systems. One of the simplest and most transparent systems exhibiting order to chaos transition is the logistic map [9]. The logistic map is a discrete dynamical system defined by

$$x_{i+1} = \mu x_i(1 - x_i), \tag{1}$$

with $0 \leq x_i \leq 1$. Thus, given an initial value (seed) x_0, the series x_i is computed. Here, the subscript i plays the role of discrete time. The behavior of the series as a function of the parameter μ is interesting. A thorough investigation of logistic map has already been done [9]. Here, without going into detailed discussion, we simply note the following.

(i) Equation (1) has $x = 0$ and $x = (\mu - 1)/\mu$ as fixed points. That is, if $x_i = 0$ or $(\mu - 1)/\mu$, then $x_{i+1} = x_i$.

(ii) For $\mu < 1$, $x = 0$ is an attractive (stable) fixed point. That is, for any value of the seed x_0 between 0 and 1, x_i approaches 0 exponentially.

(iii) For $1 \leq \mu \leq 3$, $x = (\mu - 1)/\mu$ is an attractive fixed point.

(iv) For $3 < \mu < 4$, the logistic map shows interesting behavior such as repeated period doubling, appearance of odd periods, etc.

(v) For $\mu = 4$ the logistic map is chaotic.

Since the chaotic behavior of the logistic map is of interest to us, we shall discuss the last point in detail. If we choose two seeds x_0 and $y_0 = x_0 + \delta x$, with δx arbitrarily small, x_i and y_i differ by a finite amount for large enough i. For example, if $\delta x = 10^{-12}$, $x_i - y_i \sim 0.1$ for $i \sim 40$. In fact, $x_i - y_i$ grows exponentially with i and this is the definition of chaos. An analytic solution of a logistic map exists for $\mu = 4$. If we choose $x_i = [1 - \cos(\theta_i)]/2$ and $x_{i+1} = [1 - \cos(2\theta_i)]/2$, the logistic map for $\mu = 4$ can then be defined by

$$\theta_{i+1} = \begin{cases} 2\theta_i, & \text{for } \theta_i < \pi/2 \\ 2\pi - 2\theta_i, & \text{for } \theta_i > \pi/2. \end{cases} \tag{2}$$

Clearly, the map in terms of θ_i is given by stretching the line of length π to 2π and folding it. An examination of Eq. (2) shows that one gets periodic series if the seed θ_0 is a rational fraction of π. On the other hand, the series does not have periodicity if θ_0 is an irrational fraction. Also, for any θ_0 which is an irrational fraction of π, the set $\{\theta_i\}$ computed using Eq. (2) is distributed uniformly between 0 and π. It is this property of the logistic map that we intend to exploit for generating uniformly distributed random numbers and to study its statistical behavior.

Consider a set of numbers

$$y_i = \frac{1}{\pi}\cos^{-1}(1 - 2x_i), \tag{3}$$

where

$$x_{i+1} = 4x_i(1 - x_i). \tag{4}$$

From the discussion above, y_i's are expected to be distributed uniformly between 0 and 1, except when $x_i = \frac{1}{4}, \frac{1}{2}, \frac{3}{4}$, or 1. For these special values one gets periodic series. For any other rational fraction x_0 we do not expect any periodicity. Thus, it appears that starting with a rational fraction x_0 we can generate a set of uniformly distributed numbers $\{y_i\}$ using Eqs. (3) and (4). Furthermore, since a small change in x_0 produces large deviations in x_i's (and therefore y_i's), different initial values of x_0 differing by small amount would produce different uncorrelated sets $\{y_i\}$. This seems to be a very good property for a random-number generator to possess.

There are, however, three difficulties to be overcome before we can construct a random-number generator from Eqs. (3) and (4). The first is due to truncation error in computers. We find that when the calculations are done in single precision, x_i becomes 0 after about 5000 iterations. The exact value of i depends on x_0 but it is ususally $\sim$ 5000. The reason for this is as follows. If x_i differs from 1/2 by a small amount ϵ ($x_i = 0.5 + \epsilon$), $x_{i+1} = 1 - \epsilon^2$ and if $\epsilon^2 < 10^{-7}$, x_{i+1} is stored as 1 in the computer. So $x_{i+n} = 0$ for $n \geq 2$. This difficulty is overcome by modifying the algorithm suitably when x_i is close to 0.5.

The second problem is related to the period of random numbers. LOGMAP, such as most of the standard PRN generators, suffers from the problem of periodicity. The periodicity in LOGMAP is essentially introduced by truncation. We have not been able to deduce theoretical estimates of the possible periods and their lengths. We have, therefore, computed the periods occurring in LOGMAP by starting with random seeds x_0 chosen from another PRN generator (RANMAR—the generator proposed by Marsaglia, Zaman, and Tsang [10]). The calculations have been performed with single and double precision. After 5000 calculations in double precision seven distinct periods were found. The longest period has a length larger than 7×10^7 and it occurs with a frequency of 64%. Two smallest periods have lengths smaller than 10^6 and they occur three times and twice. The rest of the periods have lengths larger than 10^6. There may be periods other than the observed ones, but they are extremely rare (frequency $< 2 \times 10^{-4}$). Single precision calculations, which are faster, were repeated 10^5 times and six periods were found. Here also, two smallest periods of lengths 136 and 143 occur with frequencies 7×10^{-4} and 4×10^{-4}, respectively. Thus, these calculations indicate that the periods of LOGMAP are finite in number.

Another interesting point regarding the periodicity is that the seeds x_0 generally do not belong to one of the periodic series. In fact, we find that the LOGMAP enters a periodic loop after 10^7 or more iterations. Furthermore, the number of iterations after which the LOGMAP enters the periodic series is different for different seeds and is not related to the final periodic series. We believe that the numbers belonging to periodic series should be excluded. Thus, for a given seed, we have kept the first 10^7 numbers in our analysis.

The preceding discussion clearly shows that the periodicity in LOGMAP arises from truncation errors, although why a particular periodic series occurs and why there are very few periodic series present is not clear. Our conjecture is that truncation errors amount to using μ [of Eq. (1)] slightly different from 4. That is, calculation of x_{i+1} on computer is equivalent to an infinite precision calculation with μ different from 4. Now, this effective value of μ would depend on x_i. It is, however, possible that the effective value of μ in a periodic series is smaller than 4 and for that value of μ the logistic map may be periodic. The logistic map for $\mu < 4$ does exhibit periodicities, but these are not stable. That is, with a small change in μ the periodicity is lost. This would mean that in a computer calculation few periodic series will be present. Also, a periodic series in a computer calculation results when calculated x_i belongs to one of the periodic series. This being somewhat arbitrary, the number of iterations after which the LOGMAP enters the periodic loop are not fixed.

The third difficulty is that of correlation among the successive y_i's. Equations (3) and (4) clearly show that the succesive y_i's are correlated, although a set of y_i's are uniformly distributed in the interval [0,1]. The standard procedure for removing such a correlation is to shuffle the set of numbers obtained from the logistic map [11]. Our calculations show that the correlations have a peculiar effect on the distribution properties and these persist even after shuffling (see below). On the other hand, the correlations between two numbers y_i and $y_{i+\tau}$ reduce as τ is increased from 1. We call these τ-shifted numbers. The statistical tests have been performed on these τ-shifted sets with τ ranging from 1 to 14. The following calculations have been done in double precision.

III. STATISTICAL TESTS

In order to test the PRN generator (LOGMAP) described in Sec. II, we have performed certain tests, for various values of τ, described below. For comparison, we have also done these tests on the PRN generator RAND—available on our machine and RANMAR. These tests are as follows.

(1) Distribution test: here we verify central limit theorem.

(2) Moments calculation: We have calculated $\langle x^n \rangle$ and its variance σ_n.

(3) χ^2 test: in the one-dimensional (1D) case, we have divided the interval $[0,1]$ into n equal bins and calculated χ^2 and its distribution. For the 2D case, we have divided the region $[0,1] \otimes [0,1]$ into n equal blocks and repeated the calculation of χ^2 and its distribution.

In addition, we have also performed other tests [2] such as the run-up test, n-tuple test, etc. Results of these tests will not be presented here. The main reason is that the results of these tests are in concurrence with the above mentioned tests and it will not alter our conclusions. In the following, we report the results for LOGMAP and RANMAR.

A. Distribution test

Suppose that $\{x_i\}$ is a sequence of mutually independent random variables that are governed by the probability density function $P(x)$. Then the central limit theorem asserts that, subject to certain conditions on the moments of $P(x)$ [12], the variable $y_N = \sum_{i=1}^N x_i$, in the limit of large N, is distributed normally, i.e.,

$$P_N(y) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{(y-\mu)^2}{2\sigma^2}\right),$$

where $\mu = N\langle x \rangle$ and $\sigma^2 = N(\langle x^2 \rangle - \langle x \rangle^2)$.

We have obtained the distribution function of the numbers obtained from LOGMAP for $N = 24$ for various τ shifts. In Fig. 1, the solid line indicates the exact distribution and diamond dots indicate the distribution obtained from the LOGMAP with $\tau = 1, 2$, and 3 calculation. From Fig. 1, one can see that for $\tau = 1$ (sequential case), the distribution from the LOGMAP is skewed a little. Although the distribution for $\tau = 2$ agrees better than the sequential case, still it is far from satisfactory. For $\tau = 3$ and greater, the distribution is in excellent agreement with the theoretical one. Thus, this test shows that although the successive numbers are correlated, a set of numbers obtained by picking every alternate or every third number would behave as a set of random numbers [13].

B. Moments

For a given set of τ-shifted N numbers generated from LOGMAP, we calculate the nth moment $\langle x_\tau^n \rangle$ as

$$\langle x_\tau^n \rangle = \frac{1}{N} \sum_{i=1}^{N} x_{i+\tau}^n. \tag{5}$$

We then repeat this test for M such sets and caclulate the global average $\overline{\langle x_\tau^n \rangle}$ and variance σ_n as

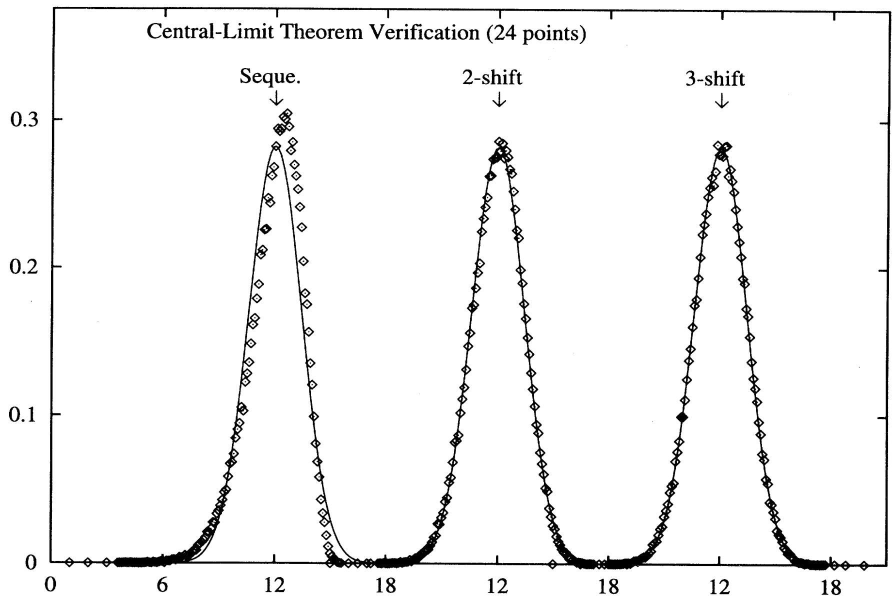

FIG. 1. Central limit theorem verification for 24 numbers. The figure shows the plot of $P_N(y)$ vs y. The solid curve is the exact distribution $P_N(y) = \frac{1}{\sqrt{2\pi N\sigma^2}}\exp\left(-\frac{(y-N_\mu)^2}{2N_\sigma^2}\right)$, where $N = 24$, $\mu = 1/2$, and $\sigma^2 = 1/12$. The diamonds with dot are obtained from the LOGMAP with τ=1, 2, and 3 (as indicated by the label).

$$\overline{\langle x_\tau^n\rangle} = \frac{1}{M}\sum_{j=1}^{M}\langle x_\tau^n\rangle_j, \quad (6)$$

$$\sigma_n(\tau) = \frac{1}{M}\sum_{j=1}^{M}\langle x_\tau^n\rangle_j^2 - \overline{\langle x_\tau^n\rangle}^2. \quad (7)$$

We have varied τ from 1 to 14 for two different values of N—1024 and 8096—and M is held fixed at 4000. For random numbers uniformly distributed between 0 and 1, $\overline{\langle x^n\rangle}^{\text{th}} = \frac{1}{n+1}$ and $\sigma_n^{\text{th}} = \frac{n^2}{(2n+1)(n+1)^2}$. The results for the PRN generator based on the logistic map are shown in Table I.

An inspection of Table I shows that $\overline{\langle x_\tau^n\rangle}$ agrees well with the theoretical values for different n's and τ's. The agreement is comparable with the results of RANMAR. But $\sigma_n(\tau)$ departs significantly from the theoretical value for $\tau = 1$, and the departure systematically increases with the increase in n. The variance is calculated by subtracting two almost equal numbers, so some loss of accuracy is expected. But the departure is much larger. On the other hand, for τ larger than 4, the calculated variances are close to the theoretical values and are comparable with those obtained from RANMAR.

C. χ^2 test

In the 1D χ^2 test, the interval [0,1] is divided into n equal parts and the numbers r_i falling in the ith interval,

TABLE I. $\langle x^n\rangle$ and σ_n for LOGMAP with $\tau = 1,3$, and 6 and RANMAR for $n = 1,2,\ldots,10$. $N = 8196$ and $M = 4000$.

n		$\tau = 1$	$\tau = 3$	$\tau = 6$	RANMAR	Exact
1	$\langle x\rangle$	0.50010	0.50006	0.50000	0.49993	0.50000
	σ_1	0.08400	0.08460	0.08626	0.08155	0.08333
2	$\langle x^1\rangle$	0.33340	0.33341	0.33332	0.33324	0.33333
	σ_2	0.03736	0.08784	0.09102	0.08736	0.08889
3	$\langle x^3\rangle$	0.25004	0.25007	0.24999	0.24991	0.25000
	σ_3	0.01392	0.07828	0.08111	0.07964	0.08036
4	$\langle x^4\rangle$	0.20002	0.20006	0.20000	0.19992	0.20000
	σ_4	0.00518	0.06839	0.07092	0.07086	0.07111
5	$\langle x^5\rangle$	0.16667	0.16672	0.16667	0.16660	0.16667
	σ_5	0.00273	0.06002	0.06240	0.06305	0.06313
6	$\langle x^6\rangle$	0.14285	0.14291	0.14286	0.14280	0.14286
	σ_6	0.00276	0.05318	0.05550	0.05642	0.05651
7	$\langle x^7\rangle$	0.12498	0.12505	0.12500	0.12495	0.12500
	σ_7	0.00363	0.04759	0.04990	0.05087	0.05104
8	$\langle x^8\rangle$	0.11109	0.11115	0.11112	0.11107	0.11111
	σ_8	0.00469	0.04298	0.04528	0.04620	0.04648
9	$\langle x^9\rangle$	0.09997	0.10004	0.10001	0.09997	0.10000
	σ_9	0.00567	0.03913	0.04143	0.04225	0.04263

out of a set of N numbers, are calculated. For a uniform distribution, χ^2 is defined by

$$\chi_n^2 = \frac{1}{N/n} \sum_{i=1}^{n} (r_i - N/n)^2. \tag{8}$$

The test is repeated for M such sets and the distribution of χ_n^2 is obtained. Theoretically, the χ^2 thus obtained should have a χ^2 distribution for $n-1$ degrees of freedom:

$$P_{\text{th}}(\chi_n^2) = \frac{(\chi_n^2)^{\frac{n-3}{2}} e^{-\chi_n^2}}{\int d\chi_n^2 (\chi_n^2)^{\frac{n-3}{2}} e^{-\chi_n^2}}. \tag{9}$$

The calculation is done for $N = 10\,240$, $M = 4000$, n is varied from 2 to 256, and τ is varied from 1 to 14. The results for $n = 4, 64,$ and 256 are displayed in Figs. 2(a), 2(b), and 2(c). The corresponding χ_n^2 for RANMAR is also given for comparison.

Consider $\tau = 1$ or the sequential case first. The calculated χ^2 distribution differs significantly from the theoretical one. This is somewhat surprising, since the set of numbers obtained from the logistic map are uniformly distributed. We have confirmed that shuffling does not mitigate this problem. Thus, the correlations between successive numbers are probably responsible for this behavior.

As τ is increased, the agreement between calculated and theoretical distributions improves. From Fig. 2(a), we find that for $n = 4$, the $\tau = 2$ distribution already agrees reasonably well with the theoretical distribution. On the other hand, for $n = 256$, one gets a good agreement for $\tau \sim 6$ or larger. This clearly shows that in order

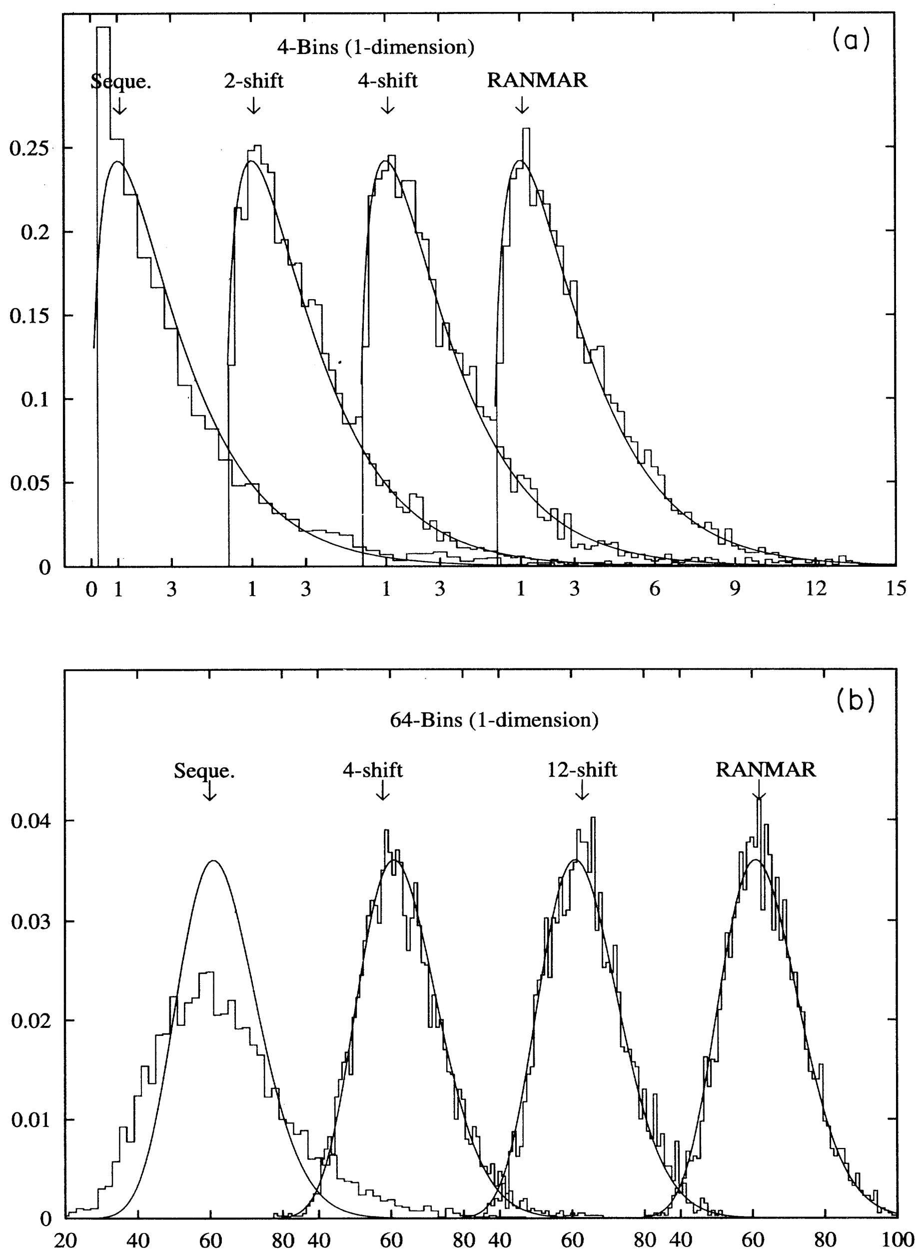

FIG. 2. Plot of the χ^2 distribution, $P(\chi^2)$ vs χ^2 for the one-dimensional case. The smooth curve is obtained from the exact distribution, Eq. (9), and the histogram is obtained from the LOGMAP and RANMAR, labeled appropriately. (a) For 4 bins, (b) for 64 bins, and (c) for 256 bins.

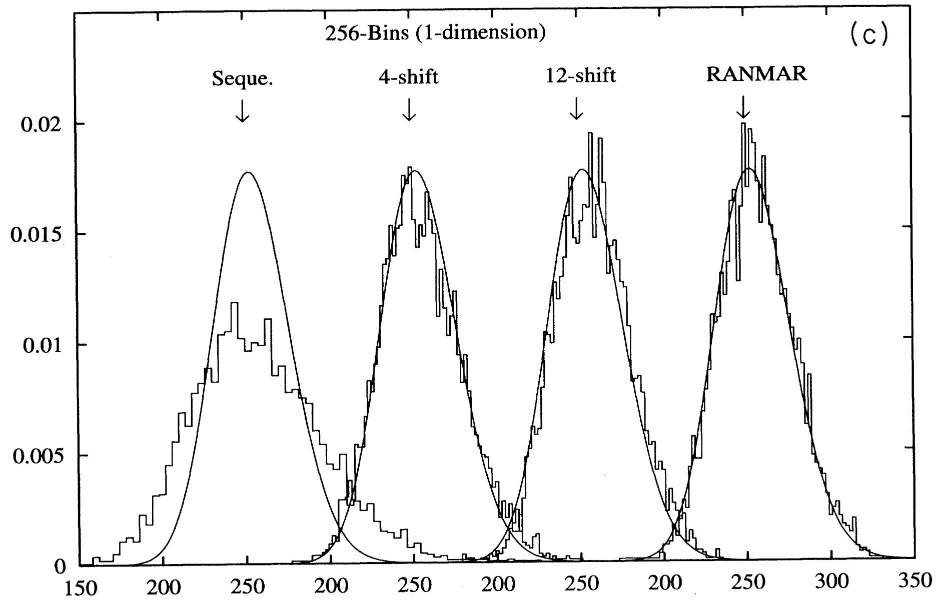

FIG. 2 *(Continued)*.

to have "randomness" on a finer scale (corresponding to smaller bin size, or larger n), the τ shift must be larger.

For the 2D χ^2 test, we choose a pair of successive numbers (x and y coordinates) and determine how they are distributed in n equal-area blocks covering a square of unit side. The χ^2 distributions are calculated as discussed in the 1D case and the results for $n = 4, 64$, and 256 are presented in Figs. 3(a), 3(b), and 3(c). These results follow the same pattern as that of the 1D case with one difference. For $\tau = 1$, the calculated χ^2 distribution is nowhere near the theoretical distribution for $n > 4$. This is simply because the succesive numbers are highly correlated. This can be explained as follows. For the sequential case, when the unit square is divided into four equal blocks, each block would have some number of points. Hence, for $n = 4$, one does not expect any abnormal behavior in the χ^2 distribution. However, this is not the situation when the unit area is divided into more than 2×2 blocks; it would happen that some of the blocks do not contain any points at all. The contribution of these blocks to the χ^2 [see Eq. (3.4)] would be N/n, thus pushing the value of χ^2 higher. However, with a τ shift of 4 or larger, these correlations are more or less wiped out and one gets reasonably good agreement between calculated and theoretical distributions.

IV. DISCUSSION

The results of the tests performed in the preceding section show an interesting dependence on τ shift. This dependence can be understood in terms of the correlations between successive numbers obtained by LOGMAP. These numbers [y_i's of Eq. (3)] are distributed uniformly in $(0,1)$. However, the successive numbers are correlated. Furthermore, these correlations are diluted by introducing the τ shift. To illustrate the dependence of these correlations, let us consider these correlations in more detail [14]. In particular, we shall consider the x_i's of Eq. (4) instead of the y_i's, to simplify the analysis. Let us choose two seeds, x_0 and $x_0 + \delta x_0$. Using the logistic map [Eq. (1) with $\mu = 4$], we can show that for small enough δx_i,

$$|\delta x_{i+1}| \approx 4|\delta x_i| \; |(1 - 2x_i)|. \tag{10}$$

Thus, $|\delta x_{i+1}|/|\delta x_i|$ varies between 0 (for $x_i = 0.5$) and 4 (for $x_i = 0, 1$). Or, on the average, $|\delta x_i| = 2^i |\delta x_0| = |\delta x_0| e^{i \ln 2}$. In other words, as is well known, the Lyapunov exponent of LOGMAP is $\ln 2$. This is illustrated graphically in Fig. 4, where the average of δx_i for 1000 randomly chosen x_0's is plotted against i. The slope for small i gives the Lyapunov exponent and it is found to be 0.301 073 which is very close to $\log 2$. Furthermore, for large i, $|\delta x_i|$ becomes independent of i. This happens when $i \geq -\ln|\delta x_0|/\ln 2$. The value of δx_0 is 10^{-7} and the calculations were done in single precision. As can be seen from the graph, at about $i \sim 23$ onward, the $|\delta x_i|$'s become independent of i. Similar behavior has been observed for for $|\delta y_i|$ also. When the whole exercise has been repeated for $\delta x_0 = 10^{-14}$ and calculations were done in double precision, similar behavior has been observed, with $|\delta x_i|$'s becoming independent of i at about $i \sim 50$ onward.

It is now clear that, depending on the given value of δx_0, if we choose $\tau \geq -\ln|\delta x_0|/\ln 2$, the correlations between successive τ-shifted numbers are completely lost. Thus, if we choose $|\delta x_0| \sim 10^{-3}$, $\tau \sim 10$ would suffice. This can be further illustrated by considering the χ^2 test with four bins of equal size. Consider a sample of N numbers obtained from LOGMAP distributed into these bins with numbers in each bin being n_i ($\sum n_i = N$). Now, if a number x_i lies in the first bin ($0 < x_i < 0.25$), it is clear from Eq. (1) that x_{i+1} lies in the first or second bin. Similarly, if x_i is in the fourth bin, x_{i+1} is in the first or second bin. So, if we ignore the end points, the numbers in bins 1 and 4 ($n_1 + n_4$) must equal the numbers in 1 and 2 $(n_1 + n_2)$, or $n_2 = n_4$. In other words, the n_i's are correlated and calculated χ^2 distribution differs from the theoretical distribution. On the other hand, if we choose $\tau = 2$, the correlations between successive numbers (on the scale of the bin size of 0.25) are completely lost. This is clearly seen in Fig. 4.

The preceeding discussion demonstrates that because of positive Lyapunov exponent of the LOGMAP, the correlations between the successive numbers is diluted if τ shifted numbers are used. Furthermore, the correlations are completely washed away if τ is large enough. For single precision numbers, this would happen when $\tau \sim 23$. However, our tests seem to indicate that smaller values of τ are reasonably good.

V. SUMMARY AND CONCLUSIONS

Various tests on the series of numbers obtained from the LOGMAP have been performed in this work. These tests bring out certain peculiarities which have not been noted before. We notice the following.

(1) The distribution test does not satisfy the central limit theorem for $\tau = 1$. The correlations between suc-

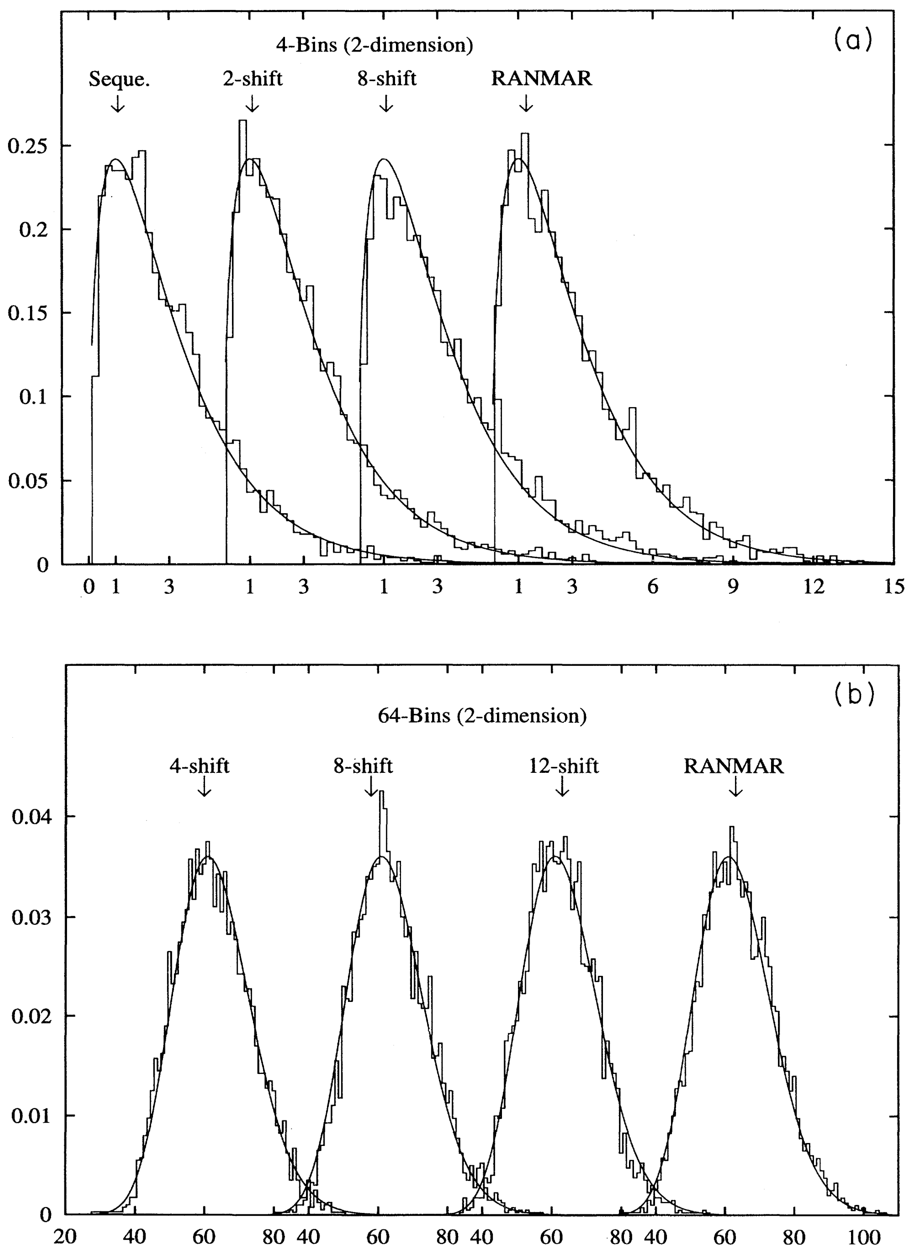

FIG. 3. The plot of the χ^2 distribution, $P(\chi^2)$ vs χ^2 for the two-dimensional case. The smooth curve is obtained from the exact distribution, Eq. (9), and the histogram is obtained from the LOGMAP and RANMAR, labeled appropriately. (a) For 4 bins, (b) for 64 bins, and (c) for 256 bins.

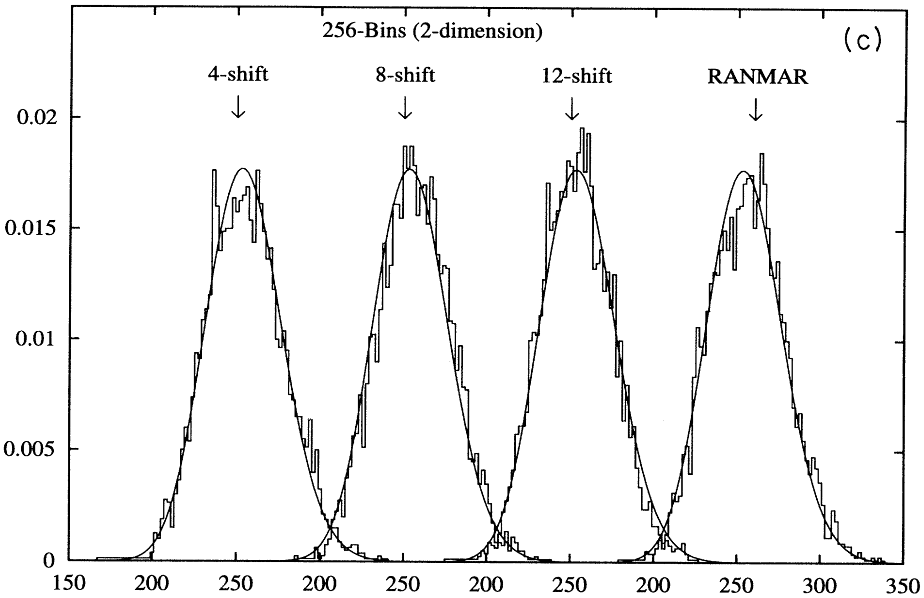

FIG. 3 *(Continued)*.

cesive numbers, which are known to exist, are probably responsible for this. But for $\tau > 2$, the agreement with the central limit theorem is excellent.

(2) The moment calculation confirms the result of the distribution test. That is, the calculated moments agree with their theoretical values, even for $\tau = 1$. The variances of these moments disagree with their theoretical values for $\tau = 1$. However, for $\tau > 4$, the moments as well as variances agree with the theoretical values. This shows that the correlations between successive numbers play a subtle role in moment calculation and removal of these correlations (by τ shifting) is essential.

(3) The χ^2 tests show that for $\tau = 1$ the χ^2 distributions systematically differ from the theoretical distribution. The agreement between calculated and theoretical distributions is improved by increasing τ. Thus, one must use τ-shifted numbers (with larger value of τ for smaller interval size) to obtain acceptable χ^2 distribution.

We have not presented the results for other tests here. However, these follow the same pattern as far as the τ dependence is concerned. The τ dependence of these results can be understood as follows. The numbers obtained from LOGMAP are uniformly distributed in the interval $(0,1)$. Therefore, averages calculated using these numbers [e.g., moments in case (2) above] agree with the theoretical values. But the quantities that depend on the correlations between successive numbers (slope of the curves in distribution test, variance of moments, χ^2 distribution, etc.) do not agree with the theoretical predictions. As discussed in the preceding section, the correlations between successive τ-shifted numbers are reduced because of a positive Lyapunov exponent of LOGMAP. In particular, in Fig. 4 for single precision accuracy, the correlations are completely lost if $\tau \geq 23$. Our calculations, on the other hand, show that $\tau \sim 10$ already yields reasonable results for distribution tests.

As for computer time, the LOGMAP is, for example, slower than RANMAR. However, in the calculations where PRNs are used, a relatively small fraction of time is spent generating random numbers. Therefore, the relative slowness of the LOGMAP is not a big handicap. The periodicity of LOGMAP introduces severe limitations concerning its applicability. One could overcome these by starting with large number of seeds x_0's. An advantage with this procedure is that correlations between successive numbers are automatically removed, as a result of the positive Lyapunov exponent of LOGMAP. Thus, even if one begins with a large number of x_0's close to each other, within a few tens of iterations, the correlations between x_i's are lost. Also, this procedure is particularly useful for vector and/or parallel processing machines.

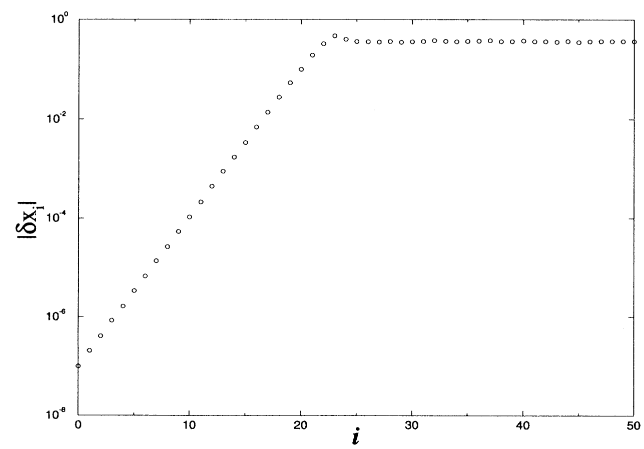

FIG. 4. Average distance $|\delta x_i|$ between neighboring points as a function of the iteration i.

To conclude, we note that the τ-shifted LOGMAP satisfies some of the elementary tests a pseudorandom-number generator must pass. The LOGMAP being based on a physically chaotic process, with calculations where randomness, as opposed to computer time, is important, it is advantageous to use LOGMAP.

ACKNOWLEDGMENTS

We gratefully acknowledge many useful discussions with Professor R. E. Amritkar, Professor S. M. Bhattacharjee, Professor A. M. Jayannavar, and Professor A. Khare.

[1] For a recent review on random-number generators, see, e.g., F. James, Comput. Phys. Commun. **60**, 329 (1990); G. Marsaglia, B. Narasimhan, and A. Zaman, *ibid.* **60**, 345 (1990).
[2] D. E. Knuth, *The Art of Computer Programming Vol. 2: Seminumerical Algorithms*, 2nd ed. (Addison Wesley, Reading, 1981).
[3] A. M. Ferrenberg, D. P. Landau, and Y. J. Wong, Phys. Rev. Lett. **69**, 3382 (1992).
[4] I. Vattulainen, K. Kankaala, J. Saarinen, and T. Ala-Nissila, Helsinki University Report No. HU-TFT-01-93S, 1993 (unpublished).
[5] S. M. Ulam and J. von Neumann, Bull. Am. Math. Soc. **53**, 1120 (1947); P. R. Stein and S. M. Ulam, Rozpr. Mat. **39**, 1 (1964).
[6] J. J. Collins *et al.*, Comput. Phys. **6** (6), 630 (1992).
[7] S. Prakash, C. K. Peng, and P. Alstrøm, Phys. Rev. A **43**, 6564 (1991); C. K. Peng, S. Prakash, H. J. Herrmann, and H. E. Stanley, *ibid.* **42**, 4537 (1990).
[8] E. N. Lorentz, J. Atmos. Sci. **20**, 130 (1993); A. Khare, Phys. Ed. (India) **10**, 30 (1993); M. Taboor, *Chaos and Integrability in Nonlinear Dynamics* (John Wiley and Sons, New York, 1989).
[9] M. J. Feigenbaum, J. Stat. Phys. **19**, 25 (1978).
[10] G. Marsaglia, A. Zaman, and W. W. Tsang, Stat. Prob. Lett. **9**, 35 (1990); see also Ref. [1].
[11] William H. Press *et al.*, *Numerical Recipes in Fortran: The Art of Scientific Computing*, 2nd ed. (Cambridge University Press, Cambridge, 1992).
[12] See, e.g., the appendix of A. I. Khinchin, *Mathematical Foundations of Statistical Mechanics* (Dover, New York, 1949), translated from the Russian edition by G. Gamow, for details.
[13] We find that for the $\tau = 1$ and with shuffling, the agreement with the theoretical distribution is very good. This indicates that the departure for the $\tau = 1$ case is due to the correlation between successive numbers. However, the shuffling does not improve the results for moments and χ^2 tests.
[14] M. Lüscher, Comput. Phys. Commun. **79**, 100 (1994).