Random walk tests for pseudo-random number generators

Smile Markovski[*], Danilo Gligoroski[†] and Verica Bakeva[‡]

Abstract. *It is well known that there are no perfectly good generators of random number sequences, implying the need of testing the randomness of the sequences produced by such generators. There are many tests for measuring the uniformity of random sequences, and here we propose a few new ones, designed by random walks. The experiments we have made show that our tests discover some discrepancies of random sequences passing many other tests.*

Key words: *random sequence, random walk, PRNG (pseudo-random number generator), normal distribution;* χ^2*-test*

AMS subject classifications: 11K45, 60J15

Received September 24, 2001 Accepted October 18, 2001

1. Introduction

A pseudo-random number generator (PRNG) is a device producing a sequence of numbers $s_1 s_2 \ldots$ with a given distribution which is supposed to be uniform, where $s_1, s_2, \ldots$ are elements of a given set of numbers. In fact, in practice, we cannot design a perfect PRNG, since the way we build the device is not a random one, which affects the uniformity of the produced sequences. That is why the word "pseudo" is used and we have to measure the randomness of the obtained sequences. There are a lot of tests for such measurements and all of them measure the difference between the generated pseudo-random sequences and the theoretically supposed ideal random sequence. We say that a PRNG passes a test if the random sequences produced by that PRNG passes the test with a probability near to 1. We can classify PRNGs depending on the tests they have passed. So, for obtaining a better classification we should have many different tests. Here we propose several new tests based on the random walk in a discrete coordinate plane.

[*] Faculty of the Natural Sciences and Mathematics, Institute of Informatics, P.O.Box 162, 1 000 Skopje, Republic of Macedonia, e-mail: smile@pmf.ukim.edu.mk

[†] Faculty of the Natural Sciences and Mathematics, Institute of Informatics, P.O.Box 162, 1 000 Skopje, Republic of Macedonia, e-mail: danilo@pmf.ukim.edu.mk

[‡] Faculty of the Natural Sciences and Mathematics, Institute of Informatics, P.O.Box 162, 1 000 Skopje, Republic of Macedonia, e-mail: verica@pmf.ukim.edu.mk

Given a (pseudo) random sequence, a random walk can be defined in many different ways. If the random sequence has elements from the set $\{0, 1, 2, 3\}$, then we can use four one-step directions left (0), right (1), up (2) and down (3). But, if the random generator produces real numbers from the interval $[0, 1)$, then the directions can be chosen depending on their belonging to the intervals $[0, 0.25)$, $[0.25, 0.5)$, $[0.5, 0.75)$, $[0.75, 1)$. Of course, for arbitrary number sets, walking can be defined in many other ways, and in what follows we suppose that the considered sequences have members from the set $\{0, 1, 2, 3\}$.

The random walk paradigm can be used for designing many suitable tests for PRNGs. We suppose that in all cases which under consideration each point (x, y) of the discrete plane has weight 0 at the beginning, and we will increase the weights of the points by using suitable definitions of the walk. We consider two kinds of walking described in *Section 2*. According to the type of walk, the tests may be designed differently, depending on the way of dividing the plane in regions. We consider three ways of dividing the plane by using:

1) the coordinate axis - the plane is divided into four quadrants: $\{(x, y)|x \geq 0, y > 0\}$, $\{(x, y)|x < 0, y \geq 0\}$, $\{(x, y)|x \leq 0, y < 0\}$, $\{(x, y)|x > 0, y \leq 0\}$;

2) circles - the plane is divided into rings $\{(x, y) \mid (2i)^2 \leq x^2 + y^2 < (2i + 2)^2\}$ for $i = 0, 1, 2 \ldots$;

3) squares - the plane is divided into bands $\{(x, y) \mid 2i \leq |x| + |y| < 2i + 2\}$ for $i = 0, 1, 2, \ldots$.

In *Section 3* we will present in more detail how the tests are designed according to the division of the plane.

In *Section 4* we present several experiments obtained by the tests given here and in [4], and a comparative analysis for six PRNGs is made as well.

2. Types of walk

We will consider the following two types of walk in the discrete plane:

2.1. Walking with a fixed number of steps (chess-walk)

Let k be a fixed positive integer. For a given sequence $\alpha = s_1 s_2 \ldots s_d$, beginning from the coordinate centre $(0, 0)$ we make k steps according to the values of the first k elements $s_1 s_2 \ldots s_k$ and we add 1 to the weight of the coordinate (m, n) where the walk stops. After that, beginning again from $(0, 0)$, we continue to walk following the next k elements $s_{k+1} \ldots s_{2k}$ and we increase by 1 the weight of the point where the walk stops, and so on.

For a given pseudo-random sequence, we can count the weights of the points of the plane. Note that the weight of a point is, in fact, the frequency of arrivals at that point. On the other hand, assuming that we have a perfectly uniform random sequence, we can count the weights as a product of the probability of the arrival at the point (m, n) and the number of trials, obtaining in such a way the theoretical frequency of arrivals. Since the walk is in accordance with a random sequence, the points of stops can be described by a random vector (X, Y) and its probability distribution can be determined by the following proposition.

Proposition 1. *Let (m, n) be a point of the discrete plane and let k be a positive integer. Then the probability $P_k(m, n) = P\{X = m, Y = n\}$ that a walk beginning from the coordinate centre $(0, 0)$ will stop at the point (m, n) after k steps is equal to 0 in the case when $|m| + |n| > k$ or the number $|m| + |n| + k$ is odd, and in the opposite case it is equal to*

$$P_k(m,n) = \frac{1}{4^k} \sum_{q=0}^{\frac{k-|m|-|n|}{2}} \binom{k}{|m|+q} \binom{k-|m|-q}{q} \binom{k-|m|-2q}{\frac{k-|m|-|n|-2q}{2}}. \qquad (1)$$

Proof. Let $m > 0,\ n > 0$. (The other cases can be treated in the same manner.) If k and $m + n$ have different parity, then it is not possible to arrive at the point (m, n) beginning from the coordinate centre, and the same is true if $k < m + n$. In the opposite case, for reaching the point (m, n) we need to make at least m steps to the right and at least n steps up. So, if we have $m + q$ $(q \geq 0)$ steps to the right, we have to have q steps to the left and that can be made by $\binom{k}{m+q}\binom{k-m-q}{q}$ ways. The remaining $k - m - 2q$ steps have to be made up or down and if $n + r$ of them are made up, then r steps have to be made down, where $n + 2r = k - m - 2q$, which can be realized by $\binom{k-m-2q}{r}$ ways.

Finally, since there are 4 possible walking directions, the number of all possible ways with the length k starting from $(0, 0)$ is 4^k. □

By *Proposition 1* we have that the density plot of the probability distribution looks like a chess table (see *Figure 1*).

Note that

$$P_k(m,n) = P_k(n,m) = P_k(|m|,|n|) \qquad (2)$$

since equality (1) can be transformed in a form symmetrical in m and n. For instance, when $\frac{k-m-n}{2}$ is an odd number, we have

$$P_k(m,n) = \frac{1}{4^k} \sum_{q=0}^{\left[\frac{k-|m|-|n|}{4}\right]} \binom{k}{\frac{k-|m|-|n|}{2}} \binom{\frac{k-|m|-|n|}{2}}{q} \left(\binom{\frac{k+|m|+|n|}{2}}{|m|+q} + \binom{\frac{k+|m|+|n|}{2}}{|n|+q} \right)$$

where $[a]$ denotes the integer part of a. A similar formula can be derived for the even case.

From the joint distribution of (X, Y), we determine marginal distributions of X and Y, particulary. Using the symmetry of m and n in the equation (2), we can conclude that the random variables (r.v.) X and Y are distributed identically. By the total probability theorem, we have

$$\begin{aligned} P\{X=m\} &= \sum_{n=-(k-|m|)}^{k-|m|} P\{X=m, Y=n\} \\ &= \frac{1}{2^{m+k}} \sum_{p=0}^{\left[\frac{k-|m|}{2}\right]} \binom{k}{|m|+p} \binom{k-|m|-p}{p} \frac{1}{4^p}, \end{aligned}$$

where $m \in \{-k, -k+2, \ldots, k-2, k\}$.

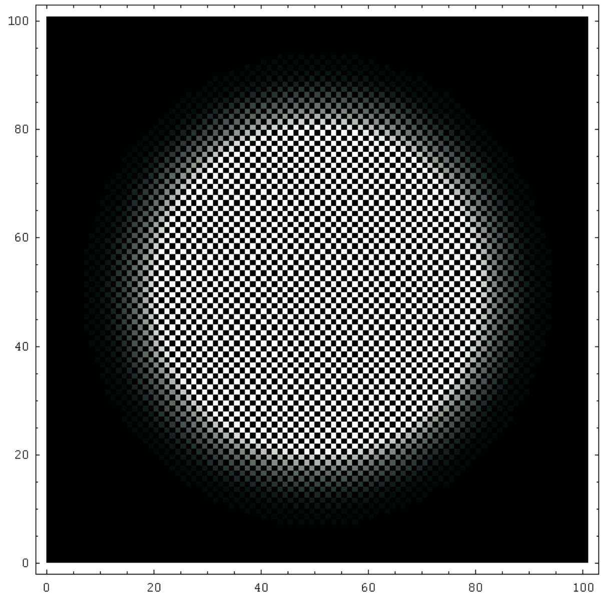

Figure 1. *Density plot of chess-movement. Brighter parts have a higher probability to be visited, whereas the darker ones have less. The black ones are not visited at all.*

The r.v. X (or Y) can be presented as a sum $X = \sum_{i=1}^{k} X_i$, where X_i is a r.v. denoting the walking in the i-th step and

$$X_i : \begin{pmatrix} -1 & 0 & 1 \\ 1/4 & 1/2 & 1/4 \end{pmatrix}. \tag{3}$$

Namely, $X_i = -1$ if the step is to the left, $X_i = 1$ if the step is to the right and $X_i = 0$ if the step is up or down. The mean and the variance of X_i are $EX_i = 0$ and $DX_i = 1/2$ which implies that $EX = 0$ and $DX = k/2$. By the central limit theorem we have:

Proposition 2. *The distribution of the random variable X converges to the normal $N(0, k/2)$ distribution for large enough k.*

2.2. Walking with a random number of steps (sun-walk)

The difference between chess-walk and sun-walk is only in choosing a different number of steps before stopping. Namely, now at first we fix an integer $l > 1$. Then we read numbers $s_1, s_2, \dots, s_l$ of the sequence $\alpha = s_1 s_2 \dots s_d$ and after that beginning from $(0,0)$ we make k_1 steps following the sequence $s_{l+1} \dots s_{l+k_1}$, where the number $k_1 = 4^{l-1} \cdot s_1 + 4^{l-2} \cdot s_2 + \dots + 4 \cdot s_{l-1} + s_l$ (i.e. we consider that the sequence $(s_1 s_2 \dots s_l)_4$ is the notation of k_1 in the 4-base system). We increase by 1 the weight of the point (m,n) where the walk stops. After that we choose the next l members $s_{k_1+l+1}, \dots, s_{k_1+2l}$ and beginning again from $(0,0)$ we make $k_2 = (s_{k_1+l+1} \dots s_{k_1+2l})_4$ steps following the sequence $s_{k_1+2l+1} \dots s_{k_1+2l+k_2}$, and so on. Note that $0 \le k_i \le 4^l - 1$ for each $i = 1, 2, \dots$ So, the number of steps k_i can be considered as a random variable K with a set of values $\{0, 1, \dots 4^l - 1\}$.

Consider the case of a perfectly uniform random sequence. Then using the total probability theorem, the probability $P(m,n) = P\{X = m, Y = n\}$ that a walk beginning from the coordinate centre $(0,0)$ will stop at the point (m,n) is given by $P(m,n) = \sum_{k=0}^{4^l-1} P_k(m,n) P\{K = k\}$, where $P_k(m,n)$ is defined as for chess-walk. Also, in this case, K has the uniform distribution on the set $\{0, 1, \dots 4^l - 1\}$ and so $P\{K = k\} = \dfrac{1}{4^l}$. Thus, we have proved

Proposition 3.

$$P(m,n) = \frac{1}{4^l} \sum_{k=0}^{4^l-1} P_k(m,n). \tag{4}$$

By *Proposition 3* we have that the density plot of the probability distribution looks like a sun (see *Figure 2*).

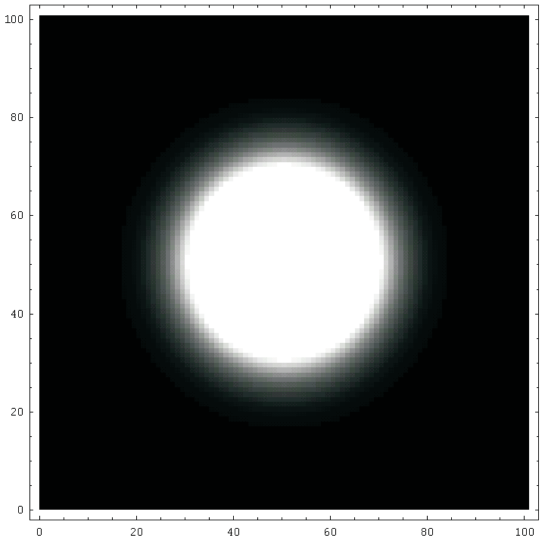

Figure 2. *Density plot of sun-movement. Brighter parts have a higher probability to be visited, whereas the darker ones have less.*

The same arguments as for chess-walk can be used for the description of the r.v. $X = \sum_{i=1}^{K} X_i$, where X_i are defined as in (3). From $EX^j = E(E(X^j|K))$, $j = 1, 2, \ldots$, we can determine that:

$$EX = 0, \qquad DX = EX^2 = \frac{4^l - 1}{4}.$$

Proposition 4. *The distribution of the random variable X can be approximated by the normal $N\left(0, \frac{4^l-1}{4}\right)$ distribution.*

Proof. The characteristic function of the r.v. X is $\varphi_X(t) = \frac{1}{4^l}\sum_{j=0}^{4^l-1}\left(\cos\frac{t}{2}\right)^{2j}$ and its Maclaurin's serie is $\varphi_X(t) = 1 - \frac{4^l-1}{8}t^2 + O(t^4)$. On the other hand, the characteristic function of the normal $N\left(0, \frac{4^l-1}{4}\right)$ distribution is $\varphi(t) = \exp\left(-\frac{4^l-1}{8}t^2\right)$ and both functions have the same first three members of their Maclaurin's series. □

3. Tests

Using the three ways of dividing the discrete plane in regions (described in *Section 1*) and the two types of walking (*Section 2*), we will design six tests as well. In each of them, we will compare random sequences obtained by PRNGs with the supposed theoretical ones by using the Pearson χ^2-test, where the test statistics is given by $\chi^2 = \sum_{i=0}^{h-1}\frac{(O_i - E_i)^2}{E_i}$, and it has χ^2 distribution with $h-1$ degrees of freedom. In this formula h denotes the number of classes (regions of division of the plane), O_i denotes the number of arrivals at the i-th class from a random sequence obtained by a PRNG and E_i is the theoretically obtained (expected) frequency. We accept the assumption that the random sequence generated by PRNG is uniformly distributed if $\chi^2 \leq \chi^2_{h-1,p}$, where $\chi^2_{h-1,p}$ is a number which satisfies the condition $P\{\chi^2 > \chi^2_{h-1,p}\} = p$, for given p. (In our experiments, we take $p = 0.05$.) In the opposite case, we reject the assumption of uniformity. Note that the statistics will be relevant only if we have enough large sequences.

Chess-Quadrant Test (CQT) [3]. For this test we use the chess-walk. The discrete plane is divided by the coordinate axis in four regions (quadrants) and for a given pseudo-random sequence $\alpha = s_1 s_2 \ldots s_d$ let $O_0,\ O_1,\ O_2,\ O_3$ be the numbers of arrivals in the corresponding regions. The weight of the origin $(0,0)$ is divided by 4 and then added to each of the regions. Theoretically, if α is really a random sequence, and if we want to have altogether r stops i.e. the sum of the weights of all points in the plane to be r, we should have $E_0 = E_1 = E_2 = E_3 = \frac{r}{4}$. (Clearly, $r = [\frac{d}{k}]$.)

Sun-Quadrant Test (SQT). This test is of the same kind as the CQT, but here we consider sun-walk instead of chess-walk and we have again $E_0 = E_1 = E_2 = E_3 = \frac{r}{4}$. Since we have r stops, we should test sequences with an average of $d = r(l + EK)$ members, where $k = EK = (4^l - 1)/2$ is the mean of the r.v. K.

Chess-Circle Test (CCT). Here we consider the chess-walk and we divide the plane in rings $R_i = \{(x, y) \mid (2i)^2 \leq x^2 + y^2 < (2i + 2)^2\}$ for $i = 0, 1, 2 \ldots$. We should consider only a finite number of rings. Namely, for a given number of steps k before stop, the points in the rings R_i, for $2i > k$, have a weight equal to 0. But, since the probability of a stop in a ring R_i is decreasing when i is increasing, it is enough to consider only the rings $R_0, R_1 \ldots, R_{h-2}$ for some h much smaller than k and the region $R_{h-1} = \{(x, y) \mid x^2 + y^2 \geq (2h - 2)^2\}$. For a theoretical case, according to (1), we can count the frequency of arriving at the region R_i by

$$E_i = r \sum_{(m,n)\in R_i} P_k(m, n),\ i = 0, \ldots, h - 2, \qquad E_{h-1} = r - \sum_{i=0}^{h-2} E_i \tag{5}$$

where r denotes the number of stops.

Sun-Circle Test (SCT). This test is similar to the CCT, but here we consider sun-walk instead of chess-walk. Consequently, the difference between the CCT and the SCT appears only in (5) where the probabilities $P_k(m, n)$ should be replaced by $P(m, n)$ (given in (4)), in order to obtain the SCT. Also, we should test sequences with an average of d members, as in the SQT.

Chess-Square Test (CST). There is no big difference between the CCT and the CST except for the division of the plane. We consider the chess-walk and we divide the plane in bands $B_i = \{(x, y) \mid 2i \leq |x|+|y| < 2i+2\}$ for $i = 0, 1, 2, \ldots, h-2$ and the region $B_{h-1} = \{(x, y) \mid |x| + |y| \geq 2h - 2\}$, where h can be chosen much smaller than k. The values E_i are obtained as in (5) by replacing B_i instead of R_i.

Sun-Square Test (SST). The SST is obtained in the same manner as the CST where chess-walk is replaced by sun-walk. Everything else is the same as in the SCT.

Remark 1. *We have divided the discrete plane in circles because of the normal distribution (*Propositions 2 *and* 4*). On the other hand, the limitations $|m|+|n| \leq k$ in* Proposition 1 *suggested the division of the discrete plane by squares.*

4. Experiments

We have checked several PRNGs presented in [4] by using our tests. The obtained results are given in *Table 1* below. In our experiments we wanted to have about $r = 10^6$ stops, i.e. the weight of the plane to be about 10^6. We took $k = 256$ (and then d is about 256×10^6) when chess-walk was used, and $l = 4$ for the sun-walk (in which case the number of steps before stops is between 0 and 255, and the average value of d is about 130×10^6).

For the CQT and the SQT we used the whole discrete plane and we took (following [3]) that a pseudo-random sequence passed the χ^2-test if $\chi^2 < 7.815262$ with significance level $p = 0.05$ and three degrees of freedom.

For making computer programs for the tests CCT, SCT, CST and SST we considered only a part of the discrete plane, i.e. the square limited by $|x| \leq 50$, $|y| \leq 50$. (We should note that in all experiments, the stops were in the defined square with probability near to 1.)

In such a way for the CCT and the SCT we took $h = 26$ and divided the plane in 26 regions consisting of the rings $R_0, \dots, R_{24}$ and of the region $R_{25} = \{(x, y) \mid x^2 + y^2 \geq 2500\}$. A pseudo-random sequence passes the χ^2-test if $\chi^2 < 37.658$ with significance level $p = 0.05$ and 25 degrees of freedom.

The situation with the CST and the SST is a little bit more complicated. Namely, because of our limitation $|x| \leq 50$, $|y| \leq 50$, we divide the plane in 36 regions, i.e. in 25 bands $B_i = \{(x, y) \mid 2i \leq |x| + |y| < 2i + 2\}$ for $i = 0, 1, 2, \dots, 24$, 10 "semi-bands" $B_i = \{(x, y) \mid 2i \leq |x| + |y| < 2i + 2,\ |x| \leq 50,\ |y| \leq 50\}$ for $i = 25, \dots, 34$ and the rest $B_{35} = \{(x, y) \mid |x| + |y| \geq 70\}$. In this case we took that a pseudo-random sequence passes the χ^2-test if $\chi^2 < 49.8102$ with significance level $p = 0.05$ and 35 degrees of freedom.

Finally, we present a few PRNGs we were checking by our tests, all of them from [4]:

- MWC (multiply-with-carry) generator $x_n = a \cdot x_{n-1} + carry \mod 2^{32}$ where the multiplier a is chosen from a predefined list.

- KISS is defined by

$$\begin{aligned} x_n &= a x_{n-1} + 1 \bmod 2^{32}, \\ y_n &= y_{n-1}(I + L^{13})(I + R^{17})(I + L^5), \\ z_n &= 2z_{n-1} + z_{n-2} + carry \bmod 2^{32} \end{aligned}$$

  where the y's are a shift register sequence and the z's are a simple multiply-with-carry sequence.

- ULTRA combines a Fibonacci generator $x_n = x_{n-99} x_{n-33} \bmod 2^{32}$, x's odd, with the multiply-with-carry generator $y_n = 30903 y_{n-1} + carry \bmod 2^{16}$, returning $x_n + y_n \bmod 2^{32}$.

- CG (congruential generator) is defined by $x_n = a x_{n-1} + b \bmod m$, where a, b and m are positive integers.

- RAN2 is from Numerical Recipes [2].

- MSRAN is the system generator in Microsoft Fortran. It is the congruential generator $x_n = 48271 x_{n-1} \bmod (2^{31} - 1)$.

The values of χ^2-test statistics for the above PRNGs are presented in *Table 1.* For each PRNG we have made two experiments, and the bold numbers denote the cases when the PRNG did not pass the corresponding test.

	CQT	SQT	CCT	SCT	CST	SST
MWC	3.6507	1.1157	28.2029	31.0619	30.1743	**51.8553**
	1.9320	5.2171	29.1727	15.4776	28.3449	27.2860
KISS	7.6002	0.4745	**39.5095**	16.6549	**50.3437**	26.7905
	5.1371	4.4888	**41.9264**	17.6388	**64.0689**	23.4839
ULTRA	7.4117	2.9033	17.3133	20.9626	34.0260	25.2775
	1.8869	**10.2128**	24.4770	18.8330	34.1187	25.2625
CG	**42.0610**	**11.8853**	**596.0693**	**161.7642**	**536.1579**	**156.8406**
	646.3155	**389.4645**	26.2560	35.5271	41.2609	28.1710
RAN2	**16.5810**	**31.7990**	25.5687	**517.5578**	29.4951	**554.2418**
	11.3912	**13.3155**	27.8888	**551.4363**	28.9031	**606.0271**
MSRAN	5.0328	**9.9846**	19.7406	**444.5602**	31.1509	**508.2729**
	4.4327	**8.3007**	32.1389	**447.7816**	43.5622	**521.6509**

Table 1. *The values of χ^2-test statistics*

It can be seen from *Table 1* that we can classify different PRNGs. So, MWC and ULTRA passed the tests quite well, KISS passed the tests relatively well, while RAN2 and MSRAN did not pass the tests designed by sun-walk (and it seems that MSRAN is better than RAN2 according to these tests). Depending on the parameters of CG, we obtained quite different values of χ^2-statistics, i.e. we can conclude that CG is a kind of an unstable PRNG.

5. Conclusion

We have defined six different tests for measuring the uniformity of the random sequences generated by PRNGs by using the idea of random walks. The experiments we have made showed that they can separate the PRNGs in different classes, so they can be used for checking the usefulness of PRNGs. The results we have obtained correspond to those obtained by other tests, but not completely. Since it is important to know if a PRNG produces really good random sequences, one has to test it with as many different tests as possible. The tests we have proposed here can be used for that task.

References

[1] D. E. Knuth, *The Art of Computer Programming: Seminumerical Algorithms*, 2nd ed., Vol.2, Addison-Wesley, Reading, MA, 1981.

[2] W. H. Press, S. A. Teukolsky *Portable random number generators*, Computers in Physics **6**(1992), 522–524 .

[3] I. Vattulainen, T. Ala-Nissila, *Mission impossible: Find a random pseudo-random number generator*, Computers in Physics. **9**(1995) 500–504.

[4] `ftp://stat.fsu.edu/pub/diehard`