Random Walk Tests for Pseudo Random Number Generators

Smile Markovski, Danilo Gligoroski and Verica Bakeva

University "St. Cyril and Methodius",
Faculty of Natural Sciences and Mathematics,
Institute of Informatics, P. O. Box 162,
Skopje, Republic of Macedonia
e-mail: {smile,danilo,verica}@pmf.ukim.edu.mk
fax: +389-91-232-078

It is well known that there are no perfectly well generators of random sequences of numbers, implying the need of testing the randomness of the sequences produced by such generators. There are many tests for measuring the uniformity of the 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 the random sequences passing many other tests.

1 Introduction

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 random number generator, since the way we are building the device is not a random one, which affects the uniformity of the produced sequences. That is why we use the word "pseudo" and we have to measure the randomness of the obtained sequences. There are a lot of tests for such measurements and all of them are measuring the difference between the obtained pseudo-random sequences by a PRNG and the theoretically supposed ideal random sequence. We say that a PRNG is passing a test if the random sequences produced by that PRNG are passing the test with a probability near to 1. We can classify PRNGs depending of 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 on a discrete coordinate plane.

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 the 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 of 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, the movements 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 walks can be used for designing many suitable tests for PRNGs. We suppose that in all cases which we are considering each point (x, y) of the discrete plane has a weight 0 at the beginning, and we increase

the weights of the points by using suitable definitions of the movements. We consider two kind of movements described in Section 2. According to these movements, the tests may be designed differently, depending of the way of dividing of the plane in regions. We consider three ways of dividing of the plane by using:

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

In Section 3 we will present in more details how the tests will be designed according to the movements and the divisions of the plane.

In Section 4 we present several experiments obtained by the tests given here and in [1], and a comparative analysis for six PRNGs is made as well.

2 Movements

We will consider the following two kinds of movements.

2.1 Movements with fixed number of steps (chess-movements)

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 movement stopped. After that, beginning again from $(0,0)$, we continue the movement following the next k elements $s_{k+1} \ldots s_{2k}$ and we increase the weight of the point where the movements stopped, 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 movements are following 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 movement 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 $m \geq 0$, $n \geq 0$. (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 at the right, we have to have q steps at 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 the probability of moving left, right, up, down is $1/4$, the probability of making k steps is $\frac{1}{4^k}$. □

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

Note that

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

since the equality (1) can be transformed in a form symmetrical on 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 the 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 identically distributed. 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 $m \in \{-k, -k+2, \ldots, k-2, k\}$.

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 movement 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 we make a step at left, $X_i = 1$ if we make a step at right and $X_i = 0$ if we make a step up or down. The mean and the variance of X_i are $EX_i = 0$ and $DX_i = 1/2$ which imply that $EX = 0$ and $DX = k/2$. By the central limit theorem we have:

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

2.2 Movements with random number of steps (sun-movements)

The difference between chess-movements and sun-movements is only in choosing the number of steps before stops. Namely, now at first we fixed an integer $l > 1$ and read the members $s_1, s_2, \ldots, s_l$ of the sequence $\alpha = s_1 s_2 \ldots s_d$ and after that beginning from (0,0) we make k_1 steps following the sequence $s_{l+1} \ldots s_{l+k_1}$, where the number $k_1 = s_1 s_2 \ldots s_l$ is being represented in 4-base

system. After that we choose the next l members $s_{k_1+l+1}, \ldots, s_{k_1+2l}$ and beginning again from (0,0) we make $k_2 (= s_{k_1+l+1} \ldots s_{k_1+2l})$ steps following the sequence $s_{k_1+2l+1} \ldots s_{k_1+2l+k_2}$, and so on. Note that $0 \leq k_i \leq 4^l - 1$ for each $i = 1, 2, \ldots$ So, the number of steps k_i can be considered as a random variable K with set of values $\{0, 1, \ldots, 4^l - 1\}$.

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 movement 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-movements. Also, in this case, K has the uniform distribution on the set $\{0, 1, \ldots, 4^l - 1\}$ and so $P\{K = k\} = \frac{1}{4^l}$ as well. 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 Appendix).

The same arguments as for chess-movements give rise the description of the r.v. $X = \sum_{i=1}^{K} X_i$, where X_i are defined as in (3). From $EX^j = E(E(X^j|K))$, $j = 1, 2$, we have determined 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 side, 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 three members of their Maclaurin's series. □

3 Tests

Using the three ways of dividing of the discrete plane on regions (described in Section 1) and the two kinds of movements (Section 2), we will design six tests as well. In each of them, we compare the 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 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 a 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 satisfy the condition $P\{\chi^2 > \chi^2_{h-1,p}\} = p$, for given p. (In our experiments, we take $p = 0.05$.) In 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) [4] For this test we use the chess-movements. The discrete plane is divided by the coordinate axis on 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 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 s stops i.e. the sum of the weights of all points in the plane to be s, we will have $E_0 = E_1 = E_2 = E_3 = \frac{s}{4}$. (Clearly, $s = [\frac{d}{k}]$.)

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

Chess-Circle Test (CCT) Here we consider the chess-movements and we divide the plane on 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 finite number of rings. Namely, for a given number k of steps 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

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

where s denotes the number of stops.

Sun-Circle Test (SCT) This test is similar to CCT, but here we consider sun-movements instead of chess-movements. Consequently, the difference between the CCT and 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 sequence with average of d members, as in SQT.

Chess-Square Test (CST) There is no big difference between CCT and CST except of the division of the plane. We consider the chess-movements and we divide the plane on 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 choosed 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 a same manner as CST where chess-movements are replaced by sun-movements instead. Everything else is as in SCT.

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

4 Experiments

We have checked several PRNGs presented in [1] with our tests. The obtained results are given in Table 1 below. In our experiments we wanted to have about $s = 10^6$ 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-movements were used, and $l = 4$ for the sun-movements (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 CQT and SQT we used the whole discrete plane and we took (following [4]) that a pseudo-random sequence was passing 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 limited by $|x| \leq 50,\ |y| \leq 50$. (We should note that in all of the experiments we have made, the stops were in this part of the plane with probability near to 1.)

In such a way for CCT and SCT we took $h = 26$ and we divided the plane on 26 regions consisting of the rings $R_0, \ldots, R_{24}$ 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 CST and SST is a little more complicated. Namely, because of our limitation $|x| \leq 50,\ |y| \leq 50$, we divided the plane on 36 regions, i.e. on 25 bands $B_i = \{(x, y) \mid 2i \leq |x| + |y| < 2i + 2\}$ for $i = 0, 1, 2, \ldots, 24$, 10 "semi-bands" $B_i = \{(x, y) \mid 2i \leq |x| + |y| < 2i + 2,\ |x| \leq 50,\ |y| \leq 50\}$ for $i = 25, \ldots, 34$ 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.

Further, we present a few PRNGs we were checking with our tests, all of them from [1]:

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

- KISS is defined by

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

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

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

- RAN2 is from Numerical Recipes [3].

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

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 the 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-movements, and it seems that MSRAN is better then RAN2 according to our tests. Depending on the choosing of the parameters of CG, quite different values of χ^2-statistics were obtained, i.e. we can conclude that CG is a kind of 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 a random walk. The experiments we have made showed that they can separate the PRNGs on 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 be aware that a PRNG produces really good random sequences, one have to test it with as many different tests as it is possible. Those we have proposed here can be used for that task as well.

References

[1] ftp://stat.fsu.edu/pub/diehard

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

[3] Press and Teukolsky: *Portable Random Number Generators*, Computers in Physics, Vol. 6, No. 2, 1992, 522-524

[4] I.Vattulainen and T.Ala-Nissila: *Mission Impossible: Find a Random Pseudorandom Number Generator*, Computers in Physics, Vol.9, No. 5, 1995, 500-504

Appendix

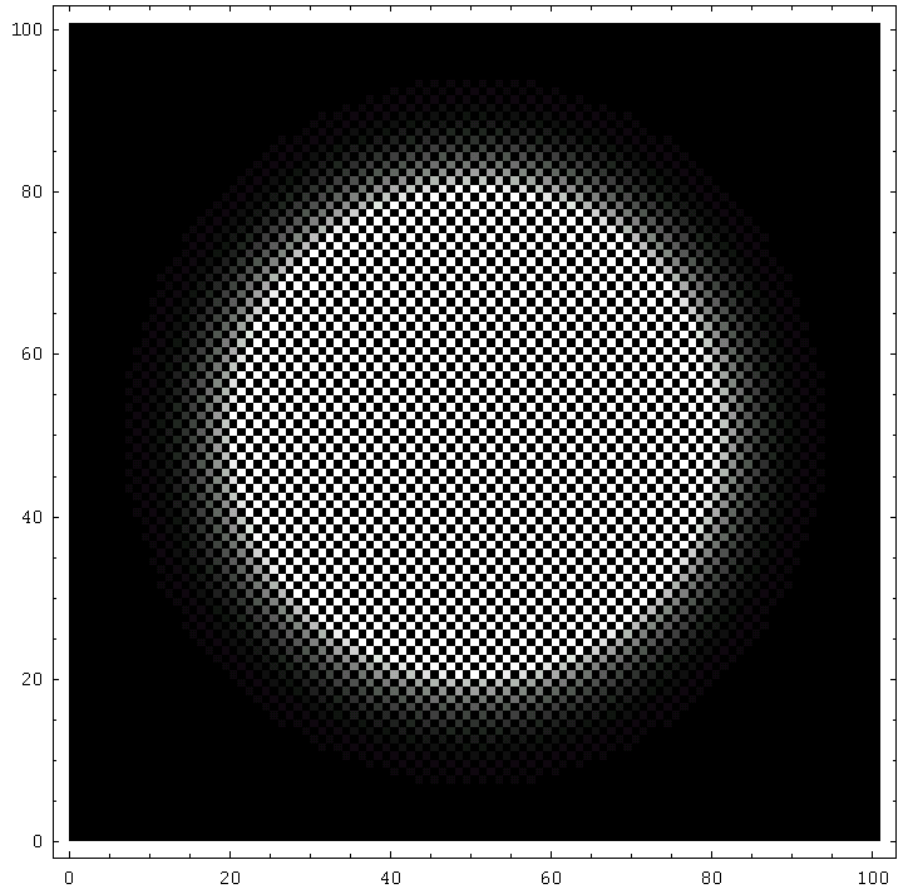

Figure 1: Density plot of chess-movement. The brighter parts have higher probability to be visited, while the darker parts have less. The black ones are not visited at all.

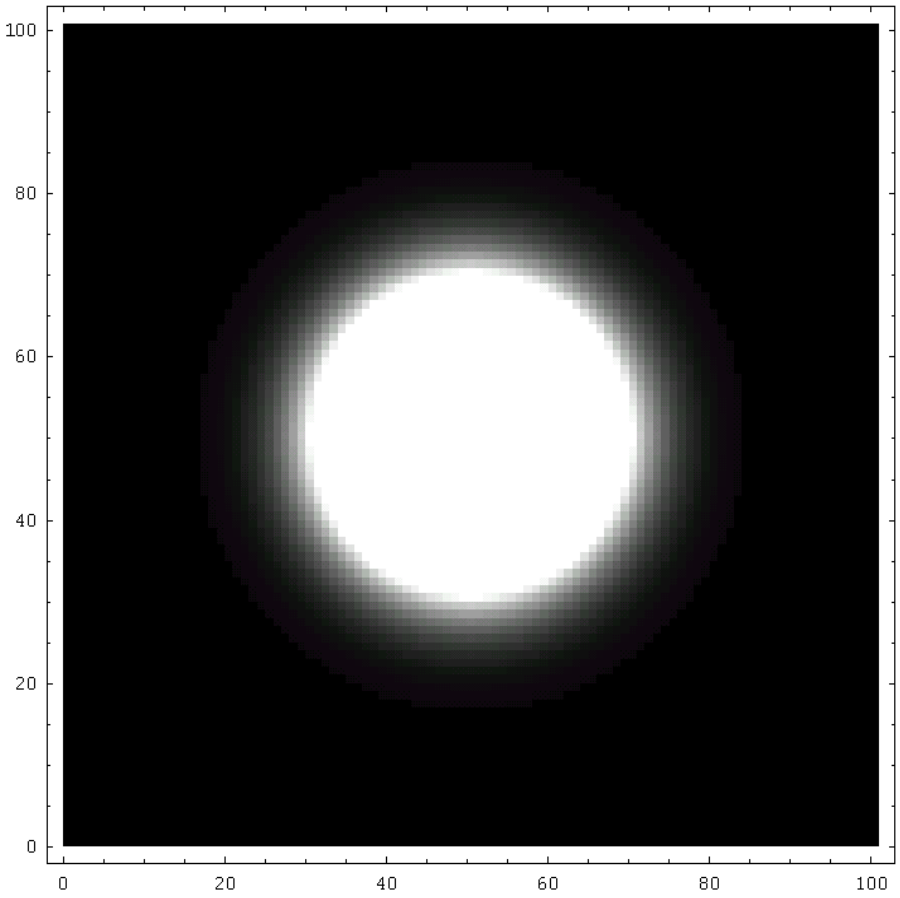

Figure 2: Density plot of sun-movement. The brighter parts have higher probability to be visited, while the darker parts have less.