HYPERBOLIC AUTOMORPHISMS OF TORI AND PSEUDO-RANDOM SEQUENCES

Calcolo 29 (1992) 213–240

M. Abundo, L. Accardi, A. Auricchio
Centro Matematico V. Volterra e
Dipartimento di Matematica
Universita' "Tor Vergata"
00173 Roma, Italy

Abstract

A method for generating pseudo-random sequences of d-dimensional vectors is considered;it is based on the *ergodic theory of periodic orbits* in the sense of [3] for unstable dynamical systems such as the hyperbolic automorphisms of the d-dimensional Torus. Since they are ergodic, their orbits are dense and *chaotic* in some sense, however the ergodic property holds only for orbits having initial points with irrational coordinates, the remaining ones being periodic. Unfortunately, those orbits are the only ones that a computer is able to generate. Since a pseudo-random sequence in $[0,1]^d$ is a long periodic orbit which has chaotic behaviour similar in some sense to the one of aperiodic orbit, in this note, we shall prove lower and upper bounds for the length of the period of orbits of the hyperbolic automorphisms of the d-dimensional Torus, expressed in terms of the (rational) starting point. The algorithms proposed are free of computational error, since they work in integer arithmetic. Surprisingly the elimination of the round off errors turns out in an *increase* of the length of the period. Statistical testing and the problem of estimating the discrepancy of the obtained sequences are also treated.

1. INTRODUCTION

In this paper we consider an algorithm to generate pseudo-random sequences of vectors in dimension $d \geq 2$.

It is well known that for high dimensional problems, the numerical- statistical methods are more efficient than traditional methods of the numerical calculus and that the problem of generating d-dimensional pseudo-random sequences cannot be reduced to the generation of pseudo-random numbers (this both for theoretical and practical reasons such as the length of execution). Therefore methods to generate directly pseudo-random sequences of

d-dimensional vectors are of practical interest. The notion of *pseudo-random sequence* depends on the apriori choice of a set of statistical tests in a sense that we try to make precise through the following definition.

A family of pseudo-random sequences on a set Ω is given by :
i) an evolution map $S : \Omega \longrightarrow \Omega$;
ii) a subset $\Omega_0 \subset \Omega$, called the set of initial points with the property that $\forall x_0 \in \Omega_0$, the orbit of x_0 (with respect to S) , that is the set

$$\Omega_{x_0} = \{x \in \Omega : x = S^n x_0 \ , n \in N\}$$

is a sequence of points of Ω which passes some standard statistical tests.
A description of the statistical tests used to define pseudo-random sequences can be found e.g. in [9] (see also [14]).

Thus, the theory of the generation of pseudo-random sequences from a set Ω naturally leads to study the statistical properties of endomorphisms $S : \Omega \longrightarrow \Omega$. The pair (Ω, S) is called a (deterministic, discrete) dynamical system.
Frequently, it is also given a measure μ invariant with respect to S :

$$\mu(E) = \mu(S^{-1}E) \quad , \forall \ E \ \mu - measurable \ in \ \Omega$$

and the triple (Ω, S, μ) is called a metric dynamical system.
It is well known that to every metric dynamical system one can canonically associate a stationary Markov chain (X_n) whose point probabilities are given by :

$$Pr\{X_0 \in E_0; X_1 \in E_1; ....X_n \in E_n\} = \mu(E_0 \cap S^{-1}E_1 \cap .... \cap S^{-n}E_n) \ ; E_j \subset \Omega$$

Thus the chaotic hierarchy for stochastic processes (ergodicity,mixing of various order,K-systems,...,Bernoulli systems,...) can be carried over to dynamical systems and one can speak of *chaotic* properties of deterministic dynamical systems.
These considerations suggest that the dynamical systems with strong chaotic properties are natural candidates as generators of pseudo-random sequences. In fact these systems seem to realize precisely the program of generation of pseudo-random sequences, i.e. to construct a deterministically generated sequence which *mimics* the behaviour of a random sequence.

There are however some theoretical obstructions to the naive application of the theory of chaotic dynamical systems to the generation of pseudo-random sequences :
1) The computer is a finite machine, hence it can only generate periodic sequences.
2) The length of the period of a sequence does not guarantee *per se* good statistical (i.e. chaotic) properties of the sequence.
3) All the results of ergodic theory are valid up to sets of measure zero and, for most dynamical systems, the states effectively realizable on a computer fall precisely into the class of zero measure sets, excluded by the results of ergodic theory (see below for an example).
Computer experiments however show that, notwithstanding the above mentioned theoretical obstructions, a large class of chaotic dynamical systems are indeed good generators of pseudo-random sequences. In other terms : it is an experimental fact that the *long periodic orbits of a dynamical system with stocasticity properties exhibit a chaotic behaviour similar to the one of aperiodic orbits.*
This fact suggests a natural generalization of classical ergodic theory in the following direction: while classical ergodic theory studies the conditions under which, for a large class of initial conditions x_0, a relation of ergodic-type holds :

$$lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N} f(S^n x_0) = \int_\Omega f d\mu \quad ,\forall f \in C^1(\Omega) \tag{1.2}$$

for a dynamical metric system (Ω, S, μ), now we are interested to investigate relations such as :

$$\frac{1}{N}\sum_{n=1}^{N} f(S^n x_0) - \int_\Omega f d\mu = O(\frac{1}{N^\alpha}) \tag{1.3}$$

for a large class of initial conditions x_0 belonging to a periodic orbit of lenght N , where N is a large enough, but finite integer, and $\alpha > 0$.

Some results of the type (1.3) have been established for particular dynamical systems (see e.g. [7]).
In the sequel, we refer to the property (1.3) as an *ergodic property of periodic orbits.*
Our aim will be to study the ergodic theory of periodic orbits in the case of automorphisms of the Torus and to apply the results to the problem of generation of pseudo-random vectors in arbitrary dimensions.

We prove, by theoretical arguments based on central limit theorem, that an estimate like (1.3) should hold with $\alpha = \frac{1}{2}$ (section 3.) and show that numerical experiments confirm this prediction (cf. figures 1.,2.).

In the sequel, we will consider a particular class of unstable systems, where $\Omega = T^d$ (d-dimensional Torus) and the evolution is described by the so called hyperbolic automorphisms of Torus.

The choice of the hyperbolic automorphisms of the Tori is easily understood if one remarks that the most famous phisical examples of *random sequences* are obtained by means of unstable systems.

Some of the usual method to generate pseudo-random numbers are based on the theory of Galois fields, and they generate periodic sequences which pass the usual statistical tests; so we can say that they are *chaotic sequences* ,in some sense. However, such generation methods give little information about the link between the length of the period and the fact that the orbits are eventually chaotic.
From our point of view these methods could be considered also as automorphisms of the Torus. However not *metric* automorphisms, in the sense that the Lebesgue measure is not preserved. Thus a theory of quasi-invariant (with respect to the Lebesgue measure) automorphisms of the Tori, would unify the present approach and the one based on Galois fields.

In section 2., we prove some lower and upper bounds on the period of orbits of hyperbolic automorphisms of the d-dimensional Torus, in terms of rational starting points. It is remarkable that our lower estimate improves linearly with the dimension (cf. (2.18)).

In section 4. we describe computer algorithms to construct pseudo-random sequences without computational error, that is in integer arithmetic.

In section 5. we deal with statistical tests for the obtained sequences of random vectors.**2.**

An hyperbolic automorphism of the Torus T^d is defined by a map :

$$S : T^d \longrightarrow T^d \tag{2.1}$$

such that, if $\phi \in T^d$

$$\phi \longrightarrow A\phi \ (mod 1) \doteq S\phi \ ,$$

where A is a symmetric matrix of order d with integer entries such that $\mid detA \mid = 1$ and its eigenvalues do not belong to the unit circle.

As it is easy to see, the normalized Lebesgue measure on the Torus is invariant under the evolution of S. The hyperbolic automorphisms of the Torus have been widely studied in the literature (see e.g. [Arn 68, Bow 75] and the references quoted in section 3.), and many results have been shown about their property of ergodicity and mixing (that is *chaoticity* of the orbits, in some sense). However, the ergodic properties of the map S are guaranteed only for the orbits which have initial point with irrational coordinates, while, as we shall see below, the orbits obtained starting from rational points are periodic and those orbits are the only ones that a computer is able to generate.

If $\phi = (\phi_1, ...\phi_d) \in T^d$,we have:

$$S(\phi) = A\phi - [A\phi] = \{A\phi\} \tag{2.2}$$

where [ ] and { } denote , respectively, the integer and fractionary part of the vector $A\phi \in T^d \cong [0,1]^d$. The map defined in (2.1) , (2.2) is the more general hyperbolic automorphism of the Torus T^d . If λ_i , $i = 1, ..r$ are the (real) eigenvalues of the matrix A, we have

$$\mid \lambda_1 \cdot \lambda_2 \cdot \cdots \lambda_r \mid = \mid detA \mid = 1.$$

Since $\mid \lambda_i \mid \neq 1, \forall i$, we can divide the eigenvalues of A into two groups : the ones with absolute value less than 1 and the ones with absolute value greater than 1. So, the matrix A is "contracting" along the directions of the eigenvectors corresponding to the eigenvalues of the first group, while it is "expanding" along the directions of the eigenvectors corresponding to the eigenvalues of the second group. This property is referred as the hyperbolic property of the matrix A. So, through any point of T^d two local manifolds exist, the so called stable and unstable manifold, such that the map S is contracting along the first manifold and it is expanding along the second one.
Moreover generically the eigenvalues will be irrational numbers,hence even if always working with integers,in approriate coordinates one is effectively doing irrational rotations of the Torus.

A famous example in dimension $d = 2$ is obtained taking :

$$A = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \tag{2.3}$$

We have $\lambda_1 \doteq \lambda = \frac{1+\sqrt{5}}{2}$, $\lambda_2 = \lambda^{-1}$; if v_1 and v_2 are the respective eigenvectors (they are irrational!) the matrix A is contracting along the direction of v_2 and expanding along the direction of v_1 .

To construct examples of hyperbolic automorphisms of Tori , one can proceed as follows.
Take two symmetric matrices $A = (a_{ij})$, $B = (b_{hk})$ of order $d > 1$ with integer entries such that $\mid detA \mid = \mid detB \mid = 1$. Then, we consider the symmetric matrix $C = A \otimes B = (a_{ij}b_{hk})$ obtained as the the tensor product of the matrices A and B .As it is easy to see by means of spectral decomposition, the eigenvalues of C are given by $\{\lambda_i\mu_j\}_{i,j=1,..d}$, where $\{\lambda_i\}, \{\mu_j\}$ are the (real) eigenvalues of A and B , respectively.
We set $S(\phi) = C\phi \ (mod\ 1)$; then, since $detC = (detA) \cdot (detB)$, in order to obtain that S is an hyperbolic automorphism of the Torus, it is enough to impose that $\mid \lambda_i\mu_j \mid \neq 1$, $\forall i, j = 1, .., d$.
In this way we can obtain hyperbolic automorphisms of arbitrary high dimensions,by means of lower dimensional ones.

Another symple way to obtain hyperbolic automorphisms of Tori is the following. Consider two symmetric matrices T_1 , T_2 of order d with integer entries satisfying the hyperbolic property (for example, T_i may be diagonal or block matrices). Then, $T = T_2T_1T_2$ is an hyperbolic matrix , if its eigenvalues do not belong to the unit circle.
This last property is generic, in the sense that the pairs T_1, T_2 such that $T_2T_1T_2$ has an eigenvalues with absolute values 1 are very rare. However at the moment there are no simple criteria which allow to exclude the occurrence of eigenvalues with absolute values equal to 1. Such criteria would be of practical relevance for the construction of hyperbolic automorphisms of Tori of arbitrary large dimensions.

Example 1
Put

$$T_1 = \begin{pmatrix} 5 & 0 & 2 \\ 0 & 1 & 0 \\ 2 & 0 & 1 \end{pmatrix} \ , \ T_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

Then :

$$T = T_2T_1T_2 = \begin{pmatrix} 5 & 2 & 2 \\ 2 & 5 & 3 \\ 2 & 3 & 2 \end{pmatrix}.$$

Example 2

Put

$$T_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 13 & 8 \\ 0 & 8 & 5 \end{pmatrix} \ , \ T_2 = \begin{pmatrix} 2 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}.$$

Then :

$$T = T_2 T_1 T_2 = \begin{pmatrix} 9 & 8 & 7 \\ 8 & 13 & 8 \\ 7 & 8 & 6 \end{pmatrix}.$$

Example 3

Put

$$T_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 5 & 2 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \ , \ T_2 = \begin{pmatrix} 2 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

Then :

$$T = T_2 T_1 T_2 = \begin{pmatrix} 9 & 7 & 4 & 2 \\ 7 & 6 & 4 & 2 \\ 4 & 4 & 5 & 3 \\ 2 & 2 & 3 & 2 \end{pmatrix}.$$

As it is easily seen, the eigenvalues of these matrices T have modulus different from 1.

It is well known that the normalized Lebesgue measure on the Torus is invariant under S and its is not only ergodic (that is (1.2) holds), but also mixing (see e.g. [4]) .

As it is easy to prove by induction, we have :

$$S^k = A^k \phi \ \ (mod 1) \ , \forall \phi \in T^d \ , \forall k \in N \qquad (2.4).$$

Now we state the following :

Proposition 2.1

If the initial point $\phi \neq 0$ has rational coordinates, that is :

$$\phi = (\phi_1, \phi_2, ...\phi_d) \in [0,1]^d \ , \phi_i \in Q \ , i = 1, ..d,$$

then the S-orbit of ϕ , $\Omega_\phi = \{S^k \phi, k \in N\}$, is periodic. **Proof.**

Trivially, if $\phi = 0$, we have $S^k \phi = 0 \ , \forall k$.

If $\phi \neq 0$, let be $\phi_i = \frac{p_i}{q_i}$, $i = 1, ..d$, where p_i and q_i are relatively prime integer numbers.

We have , $\forall i = 1, ..d; \forall k \in N$:

$$(A^k\phi)_i = \sum_{j=1}^{d} A_{ij}^k \phi_j = \sum_{j=1}^{d} A_{ij}^k \frac{p_j}{q_j} =$$

$$= \frac{1}{q_1 \cdot q_2 \cdot \cdot q_d} \cdot [a_{i1}^k p_1 \prod_{j\neq 1} q_j + a_{i2}^k p_2 \prod_{j\neq 2} q_j + ... + a_{id}^k p_d \prod_{j\neq d} q_j] =$$

$$= \frac{N_i}{Q},$$

where $Q = \prod_{k=1}^{d} q_k$, N_i an integer .
Passing to the map S :

$$(S^k\phi)_i = \{\frac{N_i}{Q}\} = \frac{\alpha_i}{Q}, \tag{2.5}$$

where α_i is an integer less than Q.
Than, $\forall i = 1, ..d$ there are at most Q possible choices of the numerator α_i in (2.5) which give distinct point in T^d . So, the S-orbit with initial point ϕ has to be periodic. From the above proposition, it follows that, if we denote $per(\phi)$ the period of the orbit having rational initial point $\phi = (\phi_1, ...\phi_d), \phi_i = \frac{p_i}{q_i}$, we have :

$$per(\phi) \leq (\prod_{i=1}^{d} q_i)^d. \tag{2.6}$$

The inequality (2.6) gives an upper bound to the period of an orbit with initial point having rational coordinates. We observe that (2.6) is only a rather *crude* estimate to $per(\phi)$.
Our aim is to find (rational) initial points ϕ's such that $per(\phi)$ assumes *very large* values. In this way, we should have a *very long* periodic orbit which simulates a chaotic aperiodic orbit, in the sense discussed in section 1.

Let us consider a rational initial point $\phi \neq 0$ which is very close to 0 , that is the denominators q_i , $i = 1, ..d$ are large and the numerators p_i are small.Then, the point ϕ, under iteration of the matrix A , remains in $(0, 1)^d$ for a large number of iterations, say L.

The first part $\{\phi, S\phi, S^2\phi, ...S^L\phi\}$ of the orbit of ϕ corresponds to the tract where S is a linear map (that is $S = A$) .Due to the hyperbolic property of the matrix A, the points $\{S^k\phi\}_{k=0,..L}$ are all distinct and approach the boundary of $(0,1)^d$ when k increases.Hence, $per(\phi) \geq L$.

However, the above remark is useless for our purposes because the orbit, although long, is not uniformly distributed in T^d. Indeed, we observe that the point ϕ after a certain number of iterations follows a path close to the direction of the eigenvector corresponding to the largest eigenvalue of A until it reaches a boundary of $(0,1)^d$ and reemerges from the opposite side.

The above consideration shows that the choice of the initial point ϕ has to be more accurate, if we wish to obtain a long periodic orbit which well simulates a chaotic orbit.
Our next step will be to look for initial points ϕ for which $per(\phi)$ is large enough, and S does not behave as a linear map along the first part of the orbit.

Proposition 2.2
Let $\phi \in T^d$ and $l \in N$ be such that $S^l\phi = \phi$, with $\phi = (\phi_1, ..\phi_d), \phi_i = \frac{p_i}{q_i}, p_i, q_i$ relatively prime integers , $i = 1, 2, ..d$.

Then, for every $i = 1, 2, ..d$, q_i divides the integer number $\Delta_l = det(A^l - I)$, where I is the identity matrix of order d.

Proof.
By the hypothesis , $A^l\phi = \phi + M_l$, where M_l denotes a d-dimensional vector with integer components ; so, we have :

$$(A^l - I)\phi = M_l. \tag{2.7}$$

Since A is an hyperbolic matrix, the matrix $\hat{A} = A^l - I$ is invertible ; then there exists a matrix $\bar{A}$ with integer entries such that $\hat{A}^{-1} = \frac{1}{\Delta_l}\bar{A}$.

Hence :

$$\phi = \frac{1}{\Delta_l}\bar{A}M_l. \tag{2.8}$$

From (2.8) , by separation of the components, it follows that :

$$\frac{p_i}{q_i} = \frac{a_i}{\Delta_l}, \tag{2.9}$$

for a certain $a_i \in Z$, and so :

$$a_i = \frac{\Delta_l p_i}{q_i}. \tag{2.10}$$

Since p_i and q_i are relatively prime, (2.10) implies that q_i divides Δ_l and this completes the proof .

From the Proposition 2.2 , it easily follows :

Corollary 2.3 If , for some $\phi = (\frac{p_i}{q_i})$,and $l \in N$ $S^l\phi = \phi$, then

$$\mid det(A^l - I) \mid \geq q_1 \cdot q_2 \cdots q_d \tag{2.11}$$

We notice that :

$$\mid det(A^l - I) \mid = \prod_{i=1}^{r} \mid \lambda_i^l - 1 \mid \tag{2.12}$$,

where $\lambda_1, \lambda_2, ...\lambda_r$ denote the eigenvalues of the matrix A . We can divide the spectrum Λ_A of A into 4 groups:

$\Lambda_1 = \{\lambda \in \Lambda_A : \lambda > 1\}$, $\Lambda_2 = \{\lambda \in \Lambda_A : 0 < \lambda < 1\}$

$\Lambda_3 = \{\lambda \in \Lambda_A : -1 < \lambda < 0\}$, $\Lambda_4 = \{\lambda \in \Lambda_A : \lambda < -1\}$.

Denote $n_i = card(\Lambda_i)$, $i = 1, ..4$; $M_{\Lambda_i} = max\{\lambda \in \Lambda_i\}$, $m_{\Lambda_i} = min\{\lambda \in \Lambda_i\}$ and split the product in (2.12) into 4 factors :

$$i) \quad \prod_{\lambda \in \Lambda_1} \mid \lambda^l - 1 \mid = \prod_{\lambda \in \Lambda_1} (\lambda^l - 1) \leq {M_{\Lambda_1}}^{ln_1},$$

$$ii) \quad \prod_{\lambda \in \Lambda_2} \mid \lambda^l - 1 \mid = \prod_{\lambda \in \Lambda_2} (1 - \lambda^l) \leq \prod_{\lambda \in \Lambda_2} (1 - {m_{\Lambda_2}}^l) = (1 - {m_{\Lambda_2}}^l)^{n_2} \leq 1,$$

iii) We have :

$$\prod_{\lambda \in \Lambda_3} \mid \lambda^l - 1 \mid \leq \prod_{\lambda \in \Lambda_3} (1 - {m_{\Lambda_3}}^l) = (1 - {m_{\Lambda_3}}^l)^{n_3};$$

moreover $m_{\Lambda_3}^l \geq m_{\Lambda_3}$, which implies $(1 - m_{\Lambda_3}^l) \leq (1 - m_{\Lambda_3})$;

Then :

$$\prod_{\lambda \in \Lambda_3} \mid \lambda^l - 1 \mid \leq \prod_{\lambda \in \Lambda_3} (1 - m_{\Lambda_3}) = (1 - m_{\Lambda_3})^{n_3}.$$

iv) We have :

$$\prod_{\lambda \in \Lambda_4} \mid \lambda^l - 1 \mid \leq \prod_{\lambda \in \Lambda_4} (1 - m_{\Lambda_4}^l) = (1 - m_{\Lambda_4}^l)^{n_4} \tag{2.13}$$

Notice that , if $x < -1$, :

$$(1 - x^l) \leq (1 - x)^l. \tag{2.14}$$

Indeed, as it is easily seen by using the binomial formula, (2.14) is equivalent to the following inequality:

$$-x^l \leq (-1)^l x^l + \sum_{k=1}^{l-1} \begin{pmatrix} l \\ k \end{pmatrix} x^{l-k}(-1)^{l-k}, \tag{2.15}$$

where , $\forall k$, $x^{l-k}(-1)^{l-k} > 0$; so , if l is even (2.15) holds, since $-x^l \leq x^l$ and , if l is odd it also holds, since $(-1)^l x^l = -x^l$.

Then , from (2.13), (2.14) , we have :

$$\prod_{\lambda \in \Lambda_4} \mid \lambda^l - 1 \mid \leq (1 - m_{\Lambda_4})^{n_4 l}.$$

Therefore , from i), ii), iii), iv) , we get :

$$\mid \Delta_l \mid = \prod_{\lambda \in \Lambda_A} \mid \lambda^l - 1 \mid \leq M_{\Lambda_1}^{n_1 l}(1 - m_{\Lambda_3})^{n_3}(1 - m_{\Lambda_4})^{n_4 l}. \tag{2.16}$$

Thus :

$$l \geq \frac{log \mid \Delta_l \mid + n_3 log(1 - m_{\Lambda_3})}{n_4 log(1 - m_{\Lambda_4}) + n_1 log M_{\Lambda_1}}.$$

Finally, by using (2.11), (2.12) , we obtain : **Proposition 2.4**

In the hypotheses of Proposition 2.2 , the following inequality holds :

$$l \geq \frac{log(q_1 \cdot \cdot q_d) + n_3 log(1 - m_{\Lambda_3})}{n_4 log(1 - m_{\Lambda_4}) + n_1 log M_{\Lambda_1}}. \tag{2.17}$$

Example (d=2)
If $A = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$, and $S^l \phi = \phi$, we have: $n_{\Lambda_1} = 1, n_{\Lambda_3} = n_{\Lambda_4} = 0, M_{\Lambda_1} = \frac{1+\sqrt{5}}{2} = \lambda, m_{\Lambda_2} = \lambda^{-1}$, and from (2.17) we obtain : $l \geq \frac{log(|\Delta_l|)}{log\lambda}$ that is $\lambda^l \geq \mid det(A^l - I) \mid$ which is almost obvious, since λ is the largest eigenvalue of A . By Proposition 2.1 and Proposition 2.4, we get the following :

Theorem 2.4
Let $\phi = (\frac{p_1}{q_1}, ...\frac{p_d}{q_d}) \in T^d$ with p_i and q_i relatively prime , i=1, ...d , and let S be an hyperbolic automorphism of the Torus T^d .

Then, if Ω_ϕ is a periodic orbit with initial point $\phi \in T^d$, we have :

$$\frac{log(\prod_{i=1}^{d} q_i) + n_{\Lambda_3} log(1 - m_{\Lambda_3})}{n_{\Lambda_4} log(1 - m_{\Lambda_4}) + n_{\Lambda_1} log M_{\Lambda_1}} \leq per(\phi) \leq (\prod_{i=1}^{d} q_i)^{d} . \tag{2.18}$$

Remark 2.1
Theorem 2.4 furnishes lower and upper bounds to the period of an orbit having initial point with rational coordinates.
The left hand size of (2.18) is particularly meaningful in the case when the dimension d is large ;if , for istance, we choose $q_i = q$, i=1, ...d , q being a large integer number, we obtain for $per(\phi)$ a lower bound of order $\frac{d \cdot logq}{const.}$, which implies that the period is very large.Now, we are concerned with the problem of determinating a point $\phi \in T^d$ and an integer l such that :

$$S^l \phi = \phi \tag{2.19}$$

$$S^k \phi \neq \phi \ \forall k < l. \tag{2.20}$$

If ϕ has coordinates $\frac{p_i}{q_i}, i = 1, ..d$, then condition (2.19) follows from the fact that q_i divides the coefficients of the i^{th} column of the matrix $(A^l - I)$, as it is easy to see.
Then, the choices of ϕ and l have to be done in such a way that there exist almost one column of the matrix $A^l - I$ for which the greatest common divisor of the elements on that column is different by 1. This one is only a sufficient condition, but it is not necessary, as we can see by the following counterexample:

$$A = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} , l = 2 , \phi = \begin{pmatrix} 1/5 \\ 2/5 \end{pmatrix};$$

then :

$$S\phi = \begin{pmatrix} 4/5 \\ 3/5 \end{pmatrix} , S^2\phi = \begin{pmatrix} 1/5 \\ 2/5 \end{pmatrix} = \phi.$$

Note that the matrix $A^2 - I = \begin{pmatrix} 4 & 3 \\ 3 & 1 \end{pmatrix}$ and the coefficients on the columns are not divisible by 5 . Obviously, the fact that the condition (2.19) holds does not imply that also condition (2.20) is satisfied.
Example

$$A = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} , l = 6 ; \phi = \begin{pmatrix} 1/2 \\ 1/2 \end{pmatrix} ;$$

we have $S^6\phi = \phi$, but also $S^3\phi = \phi$ .So, in order to obtain a proper periodic orbit of period l, some further conditions have to be required.

Proposition 2.5

Let l be a prime integer number and let $\phi \in T^d$ be a vector with rational components such that :

$$S^l\phi = \phi \tag{2.21}$$

$$S\phi \neq \phi \tag{2.22}$$

Then :

$$S^k\phi \neq \phi \ , \forall k < l.$$

Proof

Let us suppose that there exists an integer $k < l$ such that $S^k\phi = \phi$. From algebra follows that there exist integer numbers n and m such that

$$nk + ml = the\ greatest\ common\ divisor\ of\ k\ and\ l.$$

Since l is prime, we have : $nk + ml = 1$.
Then : $S^{nk+ml}\phi = S\phi \neq \phi$ (from (2.22)) .
On the other hand : $S^{nk+ml}\phi = S^{nk}(S^{ml}\phi) = S^{nk}\phi = \phi$, and we obtain a contradiction. This completes the proof of the Proposition 2.5 .**Proposition 2.6**

Let $q_1, ...q_d$ and $p_1, ...p_d$ be relatively prime integers and consider the vectors in T^d :

$\phi = (\frac{p_1}{q_1}, ...\frac{p_d}{q_d})$, $\phi^{(i)} = (0, ...\frac{p_i}{q_i}, ...0)$, $0 \leq p_i < q_i$, $i = 1, ..d$

where only the i-th component of $\phi^{(i)}$ is non-zero.
Denote $k_i = per(\phi^{(i)})$, $i = 1, ...d$,so that $S^{k_i}\phi^{(i)} = \phi^{(i)}$, and $K = the\ least\ common\ multiple$ of the integers $k_1, ...k_d$. Then :
i) $S^K\phi = \phi$. Moreover : ii) $K = per(\phi)$.

Proof

First, notice that, as easily seen, for any integer l

$$S^l\phi = \sum_{j=1}^{d} S^l\phi^{(j)}. \tag{2.24}$$

Since K is the $l.c.m.$ of $k_1, ...k_d$ and $S^{k_j}\phi^{(j)} = \phi^{(j)}$, then $S^K\phi^{(j)} = \phi^{(j)}$, $j = 1, ...d$ and so $S^K\phi = \sum_{j=1}^{d} S^K\phi^{(j)} = \sum_{j=1}^{d} \phi^{(j)} = \phi$ which proves the part i) .

To prove ii), let us suppose that an integer $\bar{K} < K$ exists such that $S^{\bar{K}}\phi = \phi$. We fix i and set $\phi = \phi^{(i)} + \bar{\phi}^{(i)}$, where $\bar{\phi}^{(i)} = (\frac{p_1}{q_1}, ...\frac{p_{i-1}}{q_{i-1}}, 0, \frac{p_{i+1}}{q_{i+1}}, ...\frac{p_n}{q_n})$. Then, $S^{\bar{K}}\phi = \phi \Rightarrow$

$(A^{\bar{K}} - I)(\phi^{(i)} + \bar{\phi}^{(i)}) =$ an integer vector . , that is

$(A^{\bar{K}} - I)\phi^{(i)} = (\prod_{j\neq i} q_j)^{-1}(A^{\bar{K}} - I)M$, where $M \in Z^d$ .From this follows that $(\prod_{j\neq i} q_j)(A^{\bar{K}} - I)\phi^{(i)} =$ an integer vector , that is $\prod_{j\neq i} q_j \frac{p_i}{q_i}(A^{\bar{K}} - I)e_i =$ an integer vector , where $e_i = (0, 0, ..0, 1, 0, ...0)$. The last equality implies that q_i has to divide the i-th column of $(A^{\bar{K}} - I)$, then $S^{\bar{K}}\phi^{(i)} = \phi^{(i)}$ and $\bar{K}$ is a multiple of k_i. Since this argument can be repeated for any fixed $i \in \{1, ...d\}$, a contradiction follows.This completes the proof of the Proposition 2.6 .

Remark 2.2

The above proposition is very useful to construct periodic orbits with large period. Infact, if one knows periodic orbits with initial points $\phi^{(i)}$ having *long* periods k_i , the orbit starting from ϕ has a much larger period. This fact permits to save a lot of computer time, when searching long periodic orbits by means of a machine. **Remark 2.3**

The theory developed in this section allows us to construct periodic sequences (that is orbits) of d-dimensional vectors with large period, by using the properties of hyperbolic automorphisms of the d- dimensional Torus .Moreover, it suggests how the initial point ϕ (with rational coordinates) has to be choosen so that the period of the orbit results *very long* .

Then, the ergodic and mixing properties of hyperbolic automorphisms of Tori (see e.g. [4]) entitle us to believe that the orbit are chaotic.

Indeed, the chaos property, the uniform distribution, the indipendent distribution of the components, for the obtained sequences of d-dimensional vectors have to be tested numerically, by means of statistical techniques.

3. DISCREPANCY OF THE PSEUDO-RANDOM SEQUENCES

In Monte Carlo integration one is interested to compute the integral $\int_{T^d} f(x)d\lambda$, where $f : T^d \longrightarrow R$ is a continuous function and $d\lambda$ is the normalized Lebesgue measure on T^d .
If $\{x_n\}_{n\in N}$ is a uniformly distributed sequence on T^d,that is the measure $\mu_N = \frac{1}{N}\sum_{i=1}^{N}\delta_{x_i}$ converges narrowly to the Lebesgue measure $d\lambda$, in the sense that we have the approximation :

$$\int_{T^d} f(x)d\mu_N \to \int_{T^d} f(x)d\lambda \quad (as\ N \to \infty) \tag{3.1}$$

that is :

$$\int_{T^d} f(x)d\lambda \approx \frac{1}{N}\sum_{n=1}^{N} f(x_n)\ ,\ N\ large. \tag{3.2}$$

The speed of convergence in (3.1) is particularly important, in order to obtain fast integration. To give a "measure" of the speed of convergence, we introduce the so called **discrepancy** (see e.g. [16]) .

Let $\{x_n\}$ be a sequence of points in T^d and E a subset of T^d . Then , the quantity $S_N(E) = \sum_{n=1}^{N}\chi_E(x_n)$ counts the number of n , $1 \leq n \leq N$, with $x_n \in E$. **Definition 3.1**

The discrepancy D_N of a sequence $\{x_n\} \subset T^d$ is defined by :

$$D_N = \sup_J \mid \frac{1}{N}S_N(J) - \lambda(J) \mid \tag{3.3}$$

where J runs through all subsets of T^d .
For an infinite sequence of points in T^d we have that $\lim_{N\to\infty} D_N = 0$ is equivalent to say that the sequence is uniformly distributed in T^d (cfr [16]).

Many estimates have been obtained by several authors for the quantity :

$$\mid \frac{1}{N}\sum_{n=1}^{N} f(x_n) - \int_{T^d} f(x)d\lambda \mid \tag{3.4}$$

as a function of the discrepancy D_N , f being a function of bounded variation (see e.g. [16] for a review) .

The discrepancy of an average sequence of points in T^d is under control thanks to the law of the iterated logarithm (see [Chu 49, Kie 61]) from which we obtain (see also [16]) :

$$D_N = O(N^{-\frac{1}{2}}(loglogN)^{\frac{1}{2}}) \tag{3.5}$$

almost surely.

Really, *ad hoc* sequences can be constructed in such a way they behave much better than the average sequence ; some authors considered examples of finite sequences for which $D_N = O(N^{-1}(logN)^a)$ (see [16]) . Our aim is to obtain an estimate for the discrepancy of the sequence $\{x_n\}$ of points in T^d obtained under iteration of the hyperbolic automorphism S , that is :

$$x_n = S^n x \ , \ x \in T^d. \tag{3.6}$$

Altough the dynamical system $(T^d, S, d\lambda)$ is not only ergodic, but also mixing (see e.g. [4]) , it is very difficult to obtain explicit estimates of the speed of convergence in the ergodic theorem:

$$\lim_{N\to\infty} \frac{1}{N} \sum_{k=0}^{N-1} f(S^k x) = \int_{T^d} f(x) d\lambda.$$

In general, no positive ergodic theoretic result is possible in this direction ; for instance, Krengel [15] has shown in a certain case that the speeed of convergence can be arbitrarly slow ; on the other hand, Halasz [11] proved that in some cases the convergence can be arbitrarly fast, that is close to the order N^{-1} .
In our case, although the Lebesgue measure λ is mixing at an exponential rate , we are not able to find an explicit estimate for the speed of convergence in the ergodic theorem. It turns out to be useful the following central limit theorem.**Theorem 3.2**

Let $S : T^d \longrightarrow T^d$ be an hyperbolic automorphism of the torus T^d and let $f : T^d \longrightarrow R$ be an Hölder-continuous function with $\int_{T^d} f d\lambda = 0$.
Then, almost for all $x \in T^d$ the limit exists :

$$D_f = \lim_{N\to\infty} \frac{1}{\sqrt{N}} [\int (\sum_{k=0}^{N-1} f(S^k x))^2 d\lambda]^{\frac{1}{2}}$$

and D_f^2 is equal to the sum of the absolutely convergent series :

$$\int f^2 d\lambda + 2 \sum_{k=1}^{\infty} \int f(foS^k) d\lambda.$$

Moreover, if $D_f \neq 0$, $\forall z \in R$, we have :

$$\lim_{N\to\infty} \lambda\{x \in T^d : \frac{\sum_{k=0}^{N-1} f(S^k x)}{D_f\sqrt{N}} < z\} = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{z} exp(\frac{-u^2}{2})du.$$

For the proof of this theorem see e.g. [18].

Indeed, for an hyperbolic automorphism of the torus a Markov partition $\{\mathcal{Q}_0, \mathcal{Q}_1, ...\mathcal{Q}_p\}$ exists (see [6]) consisting of subsets having arbitrarily small diameter.
If one consider the symbolic dynamics , i.e. the labeled process on $\hat{\Omega} = \{0, ...p\}^Z$ defined by $\sigma = (\sigma)_k$, with $\sigma_k = \sigma$ if $S^k x \in \mathcal{Q}_\sigma$, $\sigma \in \{0, ...p\}$, $k \in Z$, $x \in T^d$, the S-invariant Lebesgue measure on the torus is codified into a Gibbs measure on Z with a suitable potential Φ on the space of symbols Ω such that $|| \Phi ||= \sum_{R\ni 0}(diamR) \mid \Phi(R) |< \infty$.
Moreover, the labeled process is isomorphic to a Bernoulli process .Hence, ergodicity, mixing,
K property, positive entropy, the exponential decay of correlations follow again ; also the central limit theorem follows (see also [1] , [2] , [10], [12], [17]) .From the central limit theorem we obtain an estimate in probability

for the speed of convergence in the ergodic theorem, or, equivalently, for the discrepancy.
Indeed, if $f : T^d \longrightarrow R$ is an Hölder-continuous function (not necessairly with $\bar{f} = \int f d\lambda =$
$= 0$) , putting $g = f - \bar{f}$ in theorem 3.2 , we obtain the asymptotic approximation of the process $\frac{1}{\sqrt{N}}[\sum_j f(S^j x) - \bar{f}]$ to the Gaussian distribution $\mathcal{N}(\bar{f}, D_f)$, that is , $\forall z \in R$ the inequality

$$\mid \frac{\sum_k f(S^k x) - \bar{f}}{\sqrt{N}} \mid< z$$

holds with probability approximately equal to

$$\frac{1}{D_f\sqrt{2\pi}} \int_{-z}^{z} exp(-\frac{u^2}{2D_f^2})du \ = P_z \ \ , \ N \ large.$$

Then $\mid \frac{1}{N}\sum_k f(S^k x) - \bar{f} \mid< \frac{z}{\sqrt{N}}$ with probability P_z , which can be made arbitrarily close to 1 , by taking a positive large enough value of z .

Therefore, with a large probability, we have :

$$\mid \frac{1}{N} \sum_{k} f(S^k x) - \bar{f} \mid = O(\frac{1}{\sqrt{N}}),$$

f being an Hölder-continuous function, and the discrepancy of our sequence results $D_N = O(\frac{1}{\sqrt{N}})$, with a large probability.
Altough the result does not provide an almost surely estimate, it is perhaps the better theoretic estimate that one can obtain. Moreover, the $N^{-\frac{1}{2}}$ order is confirmed by numerical results obtained by samples of sequences $\{x_n\}$ (see the graphs below) .

4.
The program for the generation of pseudo-random sequences on the torus has been realized exclusively by using variables of integer type. This because, only if integer variables are used the sequences generated by the computer do not differ by the theoretic ones (in the sense that computation errors are not introduced). However, the disadvantage that we have by using numerical data of integer type is given by the fact that these data have a bounded range. Indeed, if a computer with 32 bits registers is used, the integer range consists of the finite interval $[-2^{31}+1, 2^{31}-1]$.
Then, it is clear that to avoid overflow problems we have to make use of integer valued variables with absolute value less than 2^{31}.
This constraint can be partially weakened, as we will see when the description of algorithms for the generation of the pseudo-random sequence will be given in detail.The algorithm stops when the point ϕ_j , under iteration of the map

S, returns to the initial value $\tilde{\phi}_0 = \phi$.Then, the final value of j represents the period of the sequence.

Now, we describe the algorithm, step by step.

(1)
In this step the initial vector $\phi_0 = \phi \in T^d$ is assigned . It is of the form : $\phi = (\frac{p_1}{q_1}, ...\frac{p_d}{q_d}) \in T^d$, where $p_i, q_i, i = 1, ...d$ are integer numbers such that :

a) $p_i < q_i \ \forall i = 1, ...d$;

b) q_i is prime

c) $q_j \neq q_i \ \forall i \neq j$.

Then the vector ϕ is trasformed into another vector $\tilde{\phi}$ given by : $\tilde{\phi} = (\frac{\tilde{p}_1}{Q}.....\frac{\tilde{p}_d}{D})$, where $\tilde{p}_i = \prod_{j=1, j\neq i}^{d} p_i q_j$, $Q = \prod_{i=1}^{d} q_i$.
Of course , $Q > \tilde{p}_i$, $\forall i = 1, ...d$.
The first condition to avoid overflow is

$$Q < 2^{31} - 1 \quad i.e. \ \prod_{i=1}^{d} q_i < 2^{31} - 1. \qquad (C1)$$

The reasons why the vector ϕ has been transformed into the vector $\tilde{\phi}$ will be clarified in the following point (4) . Moreover, we shall see that the condition (C1) is only one of the possible conditions which one might introduce to avoid overflow problems. Indeed, the condition (C1) alone is not sufficient to guarantee that such problems do not arise.

(2)
In this step, the entries of the matrix T are recorded. Also these data are of integer type.
(3)
The integer variable j counts the number of iterations ;its final value contains the number of iterations needed to reach the condition $\phi_j = \tilde{\phi}$ (that is j is equal to the value of the period of the orbit with initial vector ϕ).
(4)
The present step is certainly the most important one in the whole algorithm . It is concerned with the realization of the transformation S , to generate the sequence of pseudo-random vectors.

The j-th vector of the sequence is defined by :

$$(*) \quad \phi_j = S^j\phi \; ; \phi = \tilde{\phi} \; , where \; S\phi = T\phi - [T\phi]$$

As it is easy to see, every vector ϕ_j has the following form :
$\phi_j = (\frac{\alpha_1}{Q}, ...\frac{\alpha_d}{Q}) \; , where \; \alpha_i < Q, \forall i = 1, ..d$
Denoting $\hat{\phi}_{j-1}$the vector whose coordinates are the numerators of the coordinates of the vector ϕ_{j-1}, the relation $(*)$ can be written in the following way :

$$(**) \quad \hat{\phi}_j = T\hat{\phi}_{j-1} \; (mod \; Q).$$

If we put $\hat{\phi}_{j-1} = (\bar{p}_1, ...\bar{p}_d)$, the transformation given by $(**)$ can be written as :

$$\hat{\phi}_j = \begin{pmatrix} (t_{11}\bar{p}_1 + ... + t_{1d}\bar{p}_d) \\ \vdots \\ (t_{d1}\bar{p}_1 + ...t_{dd}\bar{p}_d) \end{pmatrix} \; (mod \; Q)$$

where $(T)_{ij} = t_{ij} \; , \; i, j = 1, ...d.$

Turning back to the problem considered in step (1) , we have to impose the technical conditions :

$$\sum_{j=1}^{d} t_{ij}\bar{p}_j < 2^{31} - 1 \quad , \forall i = 1, ...d.$$

In order that these conditions are satisfied, it is enough to suppose that:

$$d\bar{t}_{ij}Q < 2^{31} - 1, \qquad (C2)$$

where $\bar{t}_{ij} = \max_{i,j=1,..d}\{t_{ij}\}$.
This because each addendum in the sum is less or equal to $\bar{t}_{ij}Q$. Thus , the pair of conditions (C1) and (C2) is sufficient to guarantee that overflow problems do not arise.

Indeed, now we shall describe an alternative algorithm for which sufficient conditions to avoid overflow are weaker than conditions (C1) and (C2).

As seen in the proposition 2.6 , the transformation S^k can be written in the form:

$$S^k\phi = \sum_{i=1}^{d} S^k\phi^{(i)},$$

where $\phi = (\frac{p_1}{d_1}, ...\frac{p_d}{d_d})$ and $\phi^{(i)} = (0, ...\frac{p_i}{d_i}, ...0)$ (see prop. 2.6) .
To determine the iterates of the vector $\phi^{(i)}$ under the transformation S , we can alternatively solve the following system of congruences :

$$S\phi^{(i)} = \begin{pmatrix} t_{11}p_1^{(i)} + ... + t_{1d}p_d^{(i)} \\ \vdots \\ t_{d1}p_1^{(i)} + ... + t_{dd}p_d^{(i)} \end{pmatrix} \ (mod\ q_i)$$

where the quantities $p_j^{(i)}$, $j = 1, ...d$ denote the numerators of the coordinates of the vector obtained after the application of the transformation S to the vector $\phi^{(i)}$, $i = 1, ...d$.
In this way, sufficient conditions to avoid overflow became :

$$\bar{q}_i < 2^{31} - 1 \qquad (C1')$$

$$\bar{q}_i\bar{t}_{ij}d < 2^{31} - 1 \qquad (C2')$$

where $\bar{q}_i = \max_{i=1,..d}\{q_i\}$ and $\bar{t}_{ij} = \max_{i,j=1,..d}\{t_{ij}\}$.
Then, we have d vectors of numerators belonging to Z^d , which have to be divided for the corresponding denumerators and to be taken modulus 1. We clarify all this with the following example. Example

Let us consider

$$T = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \ , \ \phi_0 = (\frac{1}{2}, \frac{1}{3}).$$

We have

$$p^{(1)} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \ , \ p^{(2)} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

these vectors of denominator forming the initial matrix (of the denominators) :

$$P_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Then :
I)

$$T\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \ (mod 2)\ and\ T\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \ (mod 3)\ give\ the\ matrix\ P_1 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

II)

$$T\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \ (mod 2)\ and\ T\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 \\ 2 \end{pmatrix} \ (mod 3)\ give\ the\ matrix\ P_2 = \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix}.$$

III)

$$T\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \ (mod 2)\ and\ T\begin{pmatrix} 0 \\ 2 \end{pmatrix} = \begin{pmatrix} 2 \\ 2 \end{pmatrix} \ (mod 3)\ give\ the\ matrix\ P_3 = \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix}.$$

Iterating this procedure, we obtain at the 12^{th} step the matrix

$$P_{12} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = P_0.$$

Since $P_{12} = P_0$, the algorithm stops and the lenght of the period for the orbit with initial value $(\frac{1}{2}, \frac{1}{3})$ is 12 .
To obtain explicitly the orbit, we have to divide each of the coefficients of the j^{th} columnn of the matrix P_k for the denominator q_j (in this case $q_1 = 2$, $q_2 = 3$).Finally , we have to sum (mod 1) all the entries of the i^{th} row of P_k , to obtain the coordinates of the vector $S^k\phi$, in decimal expansion. Note that , only in the final step, we have used the floating point representation, while before we used integer arithmetic.
Here, the columns of the matrices at the right of each row represent the vectors $S^k\phi^{(i)}$.

We observe that the conditions (C1') and (C2') represent constraints very much weaker than (C1) and (C2) ; indeed, if the dimension d is large, it easily may occur that $Q = \prod q_i$ is greater than $2^{31} - 1$, since we have to choose q_i large enough, owing to the theory developed in section 2. Thus, in some sense, the last algorithm results better than the former one , altough this is to the prejudice of the velocity of execution.

5. STATISTICAL TESTS

In this section we are concerned with statistical tests applied to the pseudo-random sequences of vectors in $[0,1]^d$ obtained as described before .

5.1 χ^2 TEST

This is a test for checking the uniform distribution of the sequences, alternatively to the estimation of the discrepancy (see section 3).

Let us consider a sequence $(x_1, ...x_N)$, $x_i = S^i x$, $i = 1, ..N$ and let $\Delta_1, ...\Delta_k$ be subsets of $[0,1]^d$ such that $\cup_{i=1}^k \Delta_i = [0,1]^d$, $\Delta_i \cap \Delta_j = 0$, $\forall i \neq j$, with $\lambda(\Delta_i) = \frac{1}{k}$, $i = 1, ...k$.

Put $p_i = \frac{1}{k}$;the quantities $N_{p_1}, ...N_{p_k}$ represent the theoretical frequences, that is $N_{p_i} = \frac{N}{k}$, $\forall i = 1, ...k$.

Put $n_i = card\{x_j : x_j \in \Delta_i\}$;these quantities represent the "empirical frequences" . We define the index :

$$T_{N,k} = \sum_{i=1}^{k} \frac{(N_{p_i} - n_i)^2}{N_{p_i}}.$$

In our case :

$$T_{N,k} = \frac{k}{N} \sum_{i=1}^{k} (\frac{N}{k} - n_i)^2.$$

We compare $T_{N,k}$ with the values of the χ^2-variable with (k-1) degrees of freeedom (see e.g. [14]).**Some examples .**

(I)

We considered the matrix

$$T = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$$

and the corresponding sequence $\{S^k x\}_{k=1,N}$ with $N = 10000$;the square $[0,1]^2$ has been partitioned into 9 squares of size $\frac{1}{3}$.

The χ^2-test has been executed relatively to several choices of initial vectors. In the worst case, we obtained $\chi^2 = 2.57$; from the table of χ_8^2 we obtain $Pr\{\chi_8^2 \geq 2.57\} \geq 0.95$, so the sequences passed the test satisfactorily.

(II)

We considered the matrix

$$T = \begin{pmatrix} 5 & 2 & 2 \\ 2 & 5 & 3 \\ 2 & 3 & 2 \end{pmatrix}$$

and the corresponding sequence $\{S^k x\}_{k=1,N}$ with $N = 100000$;the square $[0,1]^3$ has been partitioned into 27 squares of size $\frac{1}{3}$.
Also in this case , relatively to several choices of initial vectors, we obtained $\chi^2 = 16.75$, in the worst case.From the table of χ^2_{26} we obtain $Pr\{\chi^2_{26} \geq 16.75\} \geq 0.90$.

5.2 RUN ALOW - BELOW TEST

Let us consider a partition of $[0,1]^d$ into two regions R_1 and R_2, such that $\lambda(R_i) = \frac{1}{2}$. Of course, an infinite number of such partition exists ;we suppose , for the sake of simplicity, that R_i are regular, connected subsets.

If N is the lenght of the sequence, we put N_i = the number of points which belong to R_i , $i = 1, 2$, while r counts the number of times in which the sequence jumps from a region to another.

Then, the statistic Z :

$$Z = \frac{r - \mu + 1/2}{\sigma}$$

where

$$\sigma^2 = \frac{2N_1N_2(2N_1N_2 - N_1 - N_2)}{N^2(N_1 + N_2 - 1)} \ , \ \mu = \frac{2N_1N_2}{N} + 1$$

is a standard Gaussian variable (see e.g. [9]). The sequence is retained to pass the test if at least the 90% of its points generates values of $z \in [\alpha, \beta]$, where α , β are such that $Pr\{z \in [\alpha, \beta]\} = 0.9$ (z having a standard normal distribution, we have $\alpha = -1.645$ and $\beta = 1.645$).In this way, we eliminate the possibility to obtain suspect values as the ones assumed by the tails of the normal distribution.

Some examples for the run alow test.

(I)

We considered the matrix

$$\begin{pmatrix} 5 & 2 & 2 \\ 2 & 5 & 3 \\ 2 & 3 & 2 \end{pmatrix}$$

and the corresponding sequences, with N=10000 .

Partitioning the cube $[0,1]^3$ by means of the plane $x = \frac{1}{2}$, we obtained the following table

$n_1 = 3$	$\Delta_1 = (-\infty, -1.645)$	$p_1 = 0.05$
$n_2 = 95$	$\Delta_2 = (-1.645, 1.645)$	$p_2 = 0.9$
$n_3 = 2$	$\Delta_3 = (1.645, +\infty)$	$p_3 = 0.05$

Partitioning the unit cube by means of the plane $y = \frac{1}{2}$, we obtained the following table:

$n_1 = 6$	$\Delta_1 = (-\infty, -1.645)$	$p_1 = 0.05$
$n_2 = 91$	$\Delta_2 = (-1.645, 1.645)$	$p_2 = 0.9$
$n_3 = 3$	$\Delta_3 = (1.645, +\infty)$	$p_3 = 0.05$

Partitioning the unit cube by means of the plane $z = \frac{1}{2}$, we obtained the following table:

$n_1 = 3$	$\Delta_1 = (-\infty, -1.645)$	$p_1 = 0.05$
$n_2 = 93$	$\Delta_2 = (-1.645, 1.645)$	$p_2 = 0.9$
$n_3 = 4$	$\Delta_3 = (1.645, +\infty)$	$p_3 = 0.05$

Thus, from these numerical data, we shall conclude that the sequences generated by means of the matrix T pass the test satisfactorily.
(II)
We considered the matrix

$$T = \begin{pmatrix} 5 & 2 \\ 2 & 1 \end{pmatrix}$$

and the corresponding sequence with N=10000.
Partitioning the square $[0, 1]^2$ by means of the line $x = \frac{1}{2}$, we obtained the following table:

$n_1 = 7$	$\Delta_1 = (-\infty, -1.645)$	$p_1 = 0.05$
$n_2 = 91$	$\Delta_2 = (-1.645, 1.645)$	$p_2 = 0.9$
$n_3 = 2$	$\Delta_3 = (1.645, +\infty)$	$p_3 = 0.05$

Partitioning the unit square by means of the line $y = \frac{1}{2}$, we obtained the following table:

$n_1 = 3$	$\Delta_1 = (-\infty, -1.645)$	$p_1 = 0.05$
$n_2 = 91$	$\Delta_2 = (-1.645, 1.645)$	$p_2 = 0.9$
$n_3 = 6$	$\Delta_3 = (1.645, +\infty)$	$p_3 = 0.05$

Also in this case, the test has been passed satisfactorily.

5.3 CORRELATIONS TEST

This test evidentiates possible correlations between the consecutive elements of the generated sequence.
If x_i^j denotes the j-th coordinate of the vector x_i of the sequence, we put $y_i = x_i^j - \tilde{x}$, where $\tilde{x} = 0.5$.Then, set :

$$R = \frac{\sum_{i=2}^{N} y_{i-1} y_i}{\sum_{i=1}^{N} y_i^2}$$

where N is the length of the sequence.
It is well known that , for large N, $z = \sqrt{N}R$ is approximately normally distributed (see e.g. [9]). Then, we can proceed to applying the test in analogous way, as done in subsection 5.3.Example

$$T = \begin{pmatrix} 5 & 2 & 2 \\ 2 & 5 & 3 \\ 2 & 3 & 2 \end{pmatrix}$$

with N=10000.
Relatively to the first coordinate, one obtains the following table:

$n_1 = 6$	$\Delta_1 = (-\infty, -1.645)$	$p_1 = 0.05$
$n_2 = 89$	$\Delta_2 = (-1.645, 1.645)$	$p_2 = 0.9$
$n_3 = 5$	$\Delta_3 = (1.645, +\infty)$	$p_3 = 0.05$

Relatively to the second coordinate, one obtains the following table :

$n_1 = 2$	$\Delta_1 = (-\infty, -1.645)$	$p_1 = 0.05$
$n_2 = 93$	$\Delta_2 = (-1.645, 1.645)$	$p_2 = 0.9$
$n_3 = 5$	$\Delta_3 = (1.645, +\infty)$	$p_3 = 0.05$

Relatively to the third coordinate, one obtains the following table:

$n_1 = 6$	$\Delta_1 = (-\infty, -1.645)$	$p_1 = 0.05$
$n_2 = 90$	$\Delta_2 = (-1.645, 1.645)$	$p_2 = 0.9$
$n_3 = 4$	$\Delta_3 = (1.645, +\infty)$	$p_3 = 0.05$

From these numerical data one can conclude that the matrix T generates sequences of vectors having weakly correlated coordinates.

References

[1] : D.V. Anosov :"Geodesic flows on closed Riemann manifolds with negative curvature. Tr. Mat. Inst. Steklov 90, (in Russian) . English transl.: Proc. Steklov Inst. Math. 90, 235 p , 1967.

[2] : D.V. Anosov , Ya.G. Sinai :"Some smooth ergodic systems" Usp. Mat. Nauk 22, No.5, 107-172 (in Russian), 1967.

[3] : L.Accardi, F. De Tisi, A: Di Libero :"Sistemi Dinamici Instabili E Generazione Di Successioni Pseudo-casuali" C.N.R. Rassegna di Metodi Statistici ed Applicazioni , Cagliari Giugno 1981.

[4] : V.I. Arnold, A.Avez :"Ergodic problems of Classical Mechanics" Benjamin, New York, 1968.

[5] : R.L. Adler, B. Weiss :"Similarity of automorphisms of the torus" Mem. Am. Math. Soc. vol 98, 1968. Benjamin, New York, 1968.

[6] : R. Bowen :"Markov partitions for axiom A diffeomorphisms". Am. J. Math. n.92 , 725-747 , 1970.

[7] : R.Bowen :"Equilibrium states and the ergodic theory of Anosov diffeomorphisms" , Springer LNM , n. 470 , 1975

[8] : K.L. Chung :" An estimate concerning the Kolmogoroff limit distribution" Trans. Amer. Math. Soc. 67, 36-50 , 1949.

[9] : M.Cugiani :" Metodi Numerico statistici" , 1980

[10] : G. Gallavotti :"Aspetti della teoria ergodica, qualitativa e statistica del moto" Quaderno UMI No 21, Pitagora Bologna, 1981.

[11] : G. Halasz :"Remarks on the remainder in Birkhoff's ergodic theorem" Acta math. Acad. Sci. Hungar. 28 , 389-395 , 1976.

[12] : I.A. Ibragimov, Y.V. Linnik :"Independent and stationary sequences of random variables" Groningen: Wolters-Noordhoff , 1971.

[13] : J. Kiefer :"On large deviations of the empiric d.f. of vector chance variables and a law of the iterated logarithm" Pacific J. Math., 11 , 649-660 , 1961.

[14] : D.E. Knuth :"The Art of Computer Programming" vol.II . Addison-Wesley, 1981.

[15] : U. Krengel :"On the speed of convergence in the ergodic theorem" Monatsh. M. 86, 3-6, 1978.

[16] : H. Niederreiter :"Quasi-Monte Carlo methods and pseudo-random numbers" Bull. Am. Math. Soc. 84, No 6 , 957-1041, 1978.

[17] : Ya.B. Pesin, Ya.G. Sinai :"Gibbs measures for partially hyperbolic attractors." Ergodic Theory Dyn. Syst. 2, 417-438, 1982.

[18] : Ya.G. Sinai (Ed.) : "Dynamical systems. Encyclopaedia of Mathematical Sciences" vol II, Springer-Verlag, 1989.