Anosov C-systems and MIXMAX RNG Generator

George Savvidy

Institute of Nuclear and Particle Physics
Demokritos National Research Center
Athens, Greece

Second MIXMAX Meeting
4 July 2016
CERN

1.G.Savvidy and N. Ter-Arutyunyan,
On the Monte Carlo simulation of physical systems
J.Comput.Phys. **97** (1991) 566; Preprint EFI, 1986

2.K.Savvidy, The MIXMAX random number generator
Comput.Phys.Commun. 196 (2015) 161

3.G. Savvidy, Anosov C-systems and Random Number Generators
Theor.Math.Phys. 2016; arXiv:1507.06348

4.G. G. Athanasiu, E. G. Floratos, G. K. Savvidy
K-system generator of pseudorandom numbers on Galois field,
Int. J. Mod. Phys. C **8** (1997)

5.K.Savvidy and G.Savvidy
Spectrum and Entropy of C-systems. MIXMAX Generator,
Chaos, Solitons and Fractals, 91 (2016) 33-38

Dmitri Anosov, in his fundamental work on *hyperbolic dynamical C-systems* pointed out that the basic property of the geodesic flow on closed Riemannian manifolds V^n of negative curvature is a *uniform instability of all its trajectories*.
In physical terms that means that *in the neighbourhood of every fixed trajectory the trajectories behave similarly to the trajectories in the neighbourhood of a saddle point*.
The hyperbolic instability of the dynamical system $\{T^t\}$ which is defined by the equations $(w \in W^m)$

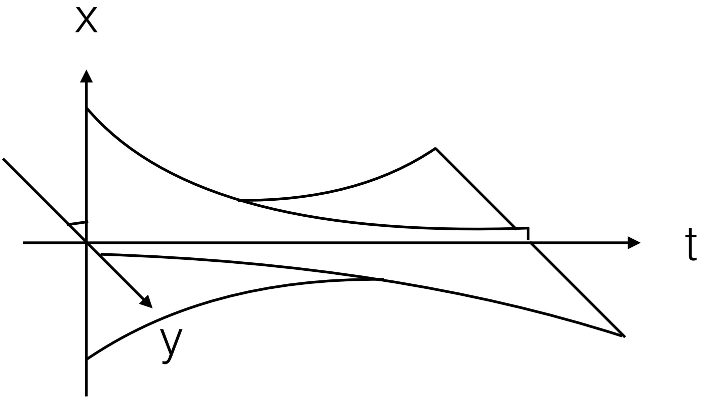
$$\dot{w} = f(w) \tag{1}$$

takes place for all solutions $\delta w \equiv \omega$ of the deviation equation

$$\dot{\omega} = \frac{\partial f}{\partial w}\bigg|_{w(t)=T^t w} \omega \tag{2}$$

in the neighbourhood of each phase trajectory $w(t) = T^t w$.

The Anosov C-systems are genuine hyperbolic systems



the behaviour of all nearby trajectories is exponentially unstable

The C-condition requires that the tangent space R^m_w at each point w of the m-dimensional phase space W^m of the dynamical system $\{T^n\}$ should be decomposable into a direct sum of the two linear spaces X^k_w and Y^l_w with the following properties:

$$C1.$$
$$R^m_w = X^k_w \bigoplus Y^l_w$$
$$and\ they\ are\ such\ that\ \{\tilde{T}^n\}$$
$$C2.$$
$$a)|\tilde{T}^n\xi| \leq\ a|\xi|e^{-cn}\ for\ n \geq 0;\ |\tilde{T}^n\xi| \geq\ b|\xi|e^{-cn}\ for\ n \leq 0,\ \xi \in X^k_w$$
$$b)|\tilde{T}^n\eta| \geq\ b|\eta|e^{cn}\ \ for\ n \geq 0;\ |\tilde{T}^n\eta| \leq\ a|\eta|e^{cn}\ for\ n \leq 0,\ \eta \in Y^l_w,$$

where the constants a,b and c are positive and are the same for all $w \in W^m$ and all $\xi \in X^k_w$, $\eta \in Y^l_w$. The length $|...|$ of the tangent vectors ξ and η is defined by the Riemannian metric ds on W^m.

The contracting and expanding foliations Σ_w^k and Σ_w^l

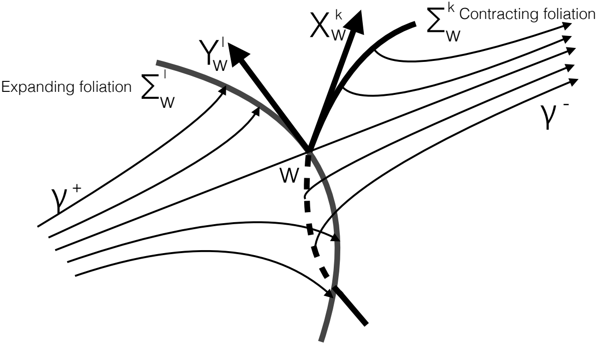


Figure : At each point w of the C-system the tangent space R_w^m is decomposable into a direct sum of two linear spaces Y_w^l and X_w^k. The expanding and contracting geodesic flows are γ^+ and γ^-. The expanding and contracting invariant foliations Σ_w^l and Σ_w^k *are transversal to the geodesic flows* and their corresponding tangent spaces are Y_w^l and X_w^k.

Important Example of C-system: *Torus Automorphisms*
Consider linear automorphisms of the unit hypercube in Euclidean space R^N with coordinates $(u_1, ..., u_N)$ where $u \in [0, 1)$

$$u_i^{(k+1)} = \sum_{j=1}^{N} A_{ij}\, u_j^{(k)}, \qquad mod\ 1, \quad k = 0, 1, 2...... \tag{6}$$

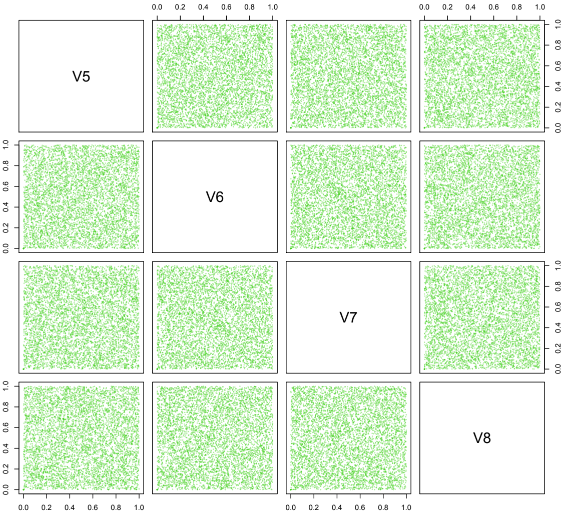
- The dynamical system defined by the integer matrix A has determinant equal to one $DetA = 1$.

Important Example of C-system: *Torus Automorphisms*
Consider linear automorphisms of the unit hypercube in Euclidean space R^N with coordinates $(u_1, ..., u_N)$ where $u \in [0, 1)$

$$u_i^{(k+1)} = \sum_{j=1}^{N} A_{ij}\, u_j^{(k)}, \quad mod\ 1, \quad k = 0, 1, 2...... \tag{6}$$

- The dynamical system defined by the integer matrix A has determinant equal to one $Det A = 1$.
- The Anosov hyperbolicity C-condition: the matrix A has no eigenvalues on the unit circle. Thus the spectrum $\Lambda = \lambda_1, ..., \lambda_N$ fulfils the two conditions:

$$1)\ Det A = \lambda_1 \lambda_2 .... \lambda_N = 1, \qquad 2)\ \ |\lambda_i| \neq 1. \tag{7}$$


V5
V6
V7
V8
0.0
0.2
0.4
0.6
0.8
1.0

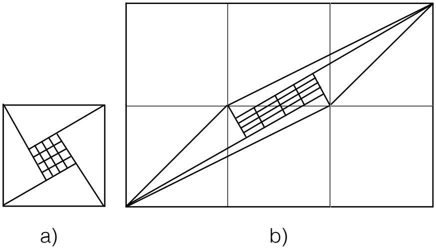
- The eigenvalues of the matrix A are divided into the two sets $\{\lambda_\alpha\}$ and $\{\lambda_\beta\}$ with modulus smaller and larger than one:

$$0 < |\lambda_\alpha| < 1 < |\lambda_\beta|. \tag{8}$$

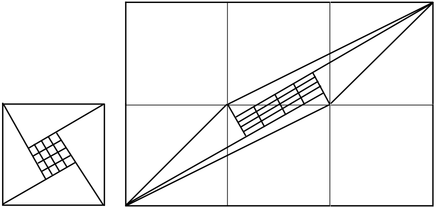
- The eigenvalues of the matrix A are divided into the two sets $\{\lambda_\alpha\}$ and $\{\lambda_\beta\}$ with modulus smaller and larger than one:

$$0 < |\lambda_\alpha| < 1 < |\lambda_\beta|. \quad (8)$$

- There exist two families of planes
$X = \{X_\alpha\}$ and $Y = \{Y_\beta\}$
which are parallel to the corresponding eigenvectors
$\{e_\alpha\}$ and $\{e_\beta\}$.

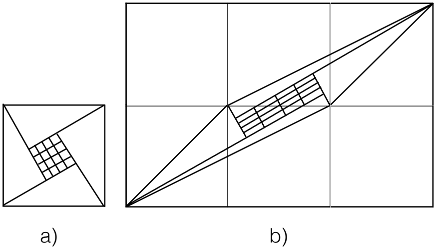


- The eigenvectors of the matrix A $\{e_\alpha\}$ and $\{e_\beta\}$ define two families of parallel planes $\{X_\alpha\}$ and $\{Y_\beta\}$



a) b)

- The eigenvectors of the matrix A $\{e_\alpha\}$ and $\{e_\beta\}$ define two families of parallel planes $\{X_\alpha\}$ and $\{Y_\beta\}$
- The automorphism A is contracting the points on the planes $\{X_\alpha\}$ and expanding points on the planes $\{Y_\beta\}$.



- The eigenvectors of the matrix A $\{e_\alpha\}$ and $\{e_\beta\}$ define two families of parallel planes $\{X_\alpha\}$ and $\{Y_\beta\}$
- The automorphism A is contracting the points on the planes $\{X_\alpha\}$ and expanding points on the planes $\{Y_\beta\}$.
- The a) depicts the parallel planes of the sets $\{X_\alpha\}$ and $\{Y_\beta\}$ and b) depicts their positions after the action of the automorphism A.

Periodic Trajectories of Anosov C-systems

All trajectories with rational coordinates $(w_1, ..., w_m)$*, and only they, are periodic trajectories of the automorphisms of the torus.*

Let us fix the integer number p, then the points on a torus with the coordinates having a denominator p form a finite set $\{a_1/p, ..., a_m/p\}$. The automorphism with integer entries transform this set of points into itself, therefore all these points belong to periodic trajectories.

Let $w = (w_1, ..., w_m)$ be a point of a trajectory with the period $n > 1$ then

$$T^n w = w + q, \tag{9}$$

where q is an integer vector. The above equation with respect to w has nonzero determinant, therefore the components of w are *rational*.

- The Kolmogorov entropy of a Anosov C-system is:

$$h(A) = \sum_{|\lambda_\beta|>1} \ln |\lambda_\beta|. \tag{10}$$

The entropy h(A) depends on the spectrum of the operator A.

- The Kolmogorov entropy of a Anosov C-system is:

$$h(A) = \sum_{|\lambda_\beta|>1} \ln|\lambda_\beta|. \tag{10}$$

The entropy h(A) depends on the spectrum of the operator A.

- *This allows to characterise and compare the chaotic properties of dynamical C-systems quantitatively →*

  computing and comparing their entropies.

- The variety and richness of the periodic trajectories of the C-systems essentially depends on entropy, the number of periodic trajectories $\pi(T)$ of a period T has the form

$$\pi(T) \sim e^{T\ h(A)}/T \tag{11}$$

- The variety and richness of the periodic trajectories of the C-systems essentially depends on entropy, the number of periodic trajectories $\pi(T)$ of a period T has the form

$$\pi(T) \sim e^{T\ h(A)}/T \tag{11}$$

- A system with larger entropy $h(A)$ is more densely populated by the periodic trajectories of the period T.

- The variety and richness of the periodic trajectories of the C-systems essentially depends on entropy, the number of periodic trajectories $\pi(T)$ of a period T has the form

$$\pi(T) \sim e^{T\ h(A)}/T \qquad (11)$$

- A system with larger entropy $h(A)$ is more densely populated by the periodic trajectories of the period T.
- The relaxation time $\tau(A)$ can be associated with the dynamical system

$$\tau(A) = 1/h(A) \qquad (12)$$

and it should be smaller that the correlation time τ of the system under investigation

$$\tau(A) \leq \tau \qquad (13)$$

A strong instability of trajectories of a dynamical C-system leads to the apperance of statistical properties in its behaviour. As a result the time average of the function $g(w)$ on W^m

$$\frac{1}{N}\sum_{n=0}^{N-1} g(T^n w) \tag{14}$$

behaves as a superposition of quantities which are statistically weakly dependent. Therefore for the C-systems on a torus it was demonstrated by Leonov that the *deviation of the time averages (14) from the phase space averages*

$$\int_{W^m} g(w)dw \tag{15}$$

multiplied by $\sqrt{N}$ have at large $N \to \infty$ the Gaussian distribution:

$$\lim_{N\to\infty} \mu\left\{w : \sqrt{N}\left(\frac{1}{N}\sum_{n=0}^{N-1} g(T^n w) - \int_{W^m} g(v)dv\right) < z\right\} =$$
$$= \frac{1}{\sqrt{2\pi}\sigma_g}\int_{-\infty}^{z} e^{-\frac{y^2}{2\sigma_g^2}} dy.$$

The importance of the multiplication by the factor $\sqrt{N}$ can be understood as follows. The difference in the bracket has an upper bound in terms of the Kolmogorov discrepancy $D_N(T)$:

$$\left|\frac{1}{N}\sum_{n=0}^{N-1} g(T^n w) - \int_{W^m} g(v)dv\right| \leq C\,\frac{D_N(T)}{N}, \qquad (16)$$

where C is a constant and $D_N(T)$ grows as $\sqrt{N}$. Therefore after multiplication of the quantity in the bracket by $\sqrt{N}$ it is bound by a constant.

The mportant result of the Bowen theorem states that

$$\int_{W^m} f(w) d\mu(w) = \lim_{n \to \infty} \frac{1}{N_n} \sum_{w \in \Gamma_n} f(w), \qquad (17)$$

where Γ_n is a set of all points on the trajectories of period n. The total number of points in the set Γ_n we defined earlier as N_n.

- The Anosov C-systems have very strong chaotic properties:
  the exponential instability of all trajectories
  in fact the instability is as strong as it can be in principle.

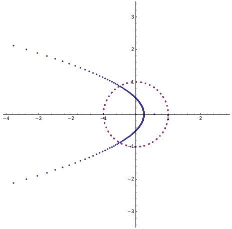
- The Anosov C-systems have very strong chaotic properties: the exponential instability of all trajectories in fact the instability is as strong as it can be in principle.

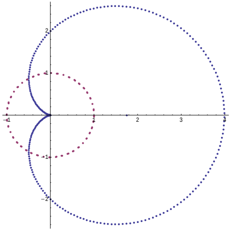
- Our aim is to study these characteristics of the C-systems and develop our earlier suggestion to use the Anosov C-systems as random number generator for Monte-Carlo simulations

Family of operators A(N,s) parametrised by the integers N and s

$$A(N,s) = \begin{pmatrix} 1 & 1 & 1 & 1 & ... & 1 & 1 \\ 1 & 2 & 1 & 1 & ... & 1 & 1 \\ 1 & 3+s & 2 & 1 & ... & 1 & 1 \\ 1 & 4 & 3 & 2 & ... & 1 & 1 \\ & & & ... & & & \\ 1 & N & N-1 & N-2 & ... & 3 & 2 \end{pmatrix} \quad (18)$$

The matrix is of the size $N \times N$
Its entries are all integers $A_{ij} \in \mathbb{Z}$
Det A $=1$
The spectrum and the value of the Kolmogorov entropy?





Eigenvalue Distribution of A(N,s) and of $A^{-1}(N,s)$
all of them are lying outside of the unit circle

Size N	Magic s	Entropy	Period $\approx \log_{10}(q)$
256	-1	164.5	4682
256	487013230256099064	193.6	4682

Table : Properties of operators A(N,s) for different special s.

Size N	Magic s	Entropy (lower bound)	Period $\approx \log_{10}(q)$
7307	0	4502.1	134158
20693	0	12749.5	379963
25087	0	15456.9	460649
28883	1	17795.7	530355
40045	-3	24673.0	735321
44851	-3	27634.1	823572

Table : Table of properties of the operator $A(N,s)$ for large matrix size N. The third column is the value of the Kolmogorov entropy. All these generators passes tests in the BigCrush suite. For the largest of them the period approaches a *million digits*.

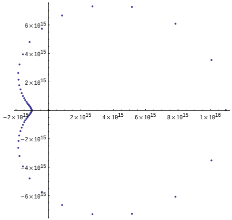
A(N,s,m)

A three-parameter family of C-operators $A(N,s,m)$, where m is some integer:

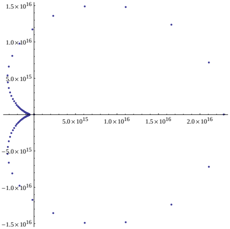
$$\begin{pmatrix}
1 & 1 & 1 & 1 & ... & 1 & 1 \\
1 & 2 & 1 & 1 & ... & 1 & 1 \\
1 & m+2+s & 2 & 1 & ... & 1 & 1 \\
1 & 2m+2 & m+2 & 2 & ... & 1 & 1 \\
1 & 3m+2 & 2m+2 & m+2 & ... & 1 & 1 \\
 & & & ... & & & \\
1 & (N-2)m+2 & (N-3)m+2 & (N-4)m+2 & ... & m+2 & 2
\end{pmatrix}$$

Size N	Magic m	Magic s	Entropy	Period $\approx \log_{10}(q)$
8	$m = 2^{53} + 1$	s=0	220.4	129
17	$m = 2^{36} + 1$	s=0	374.3	294
40	$m = 2^{42} + 1$	s=0	1106.3	716
60	$m = 2^{52} + 1$	s=0	2090.5	1083
96	$m = 2^{55} + 1$	s=0	3583.6	1745
120	$m = 2^{51} + 1$	s=1	4171.4	2185
240	$m = 2^{51} + 1$	s=487013230256099140	8418.8	4389

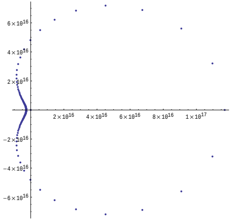
Table : Table of three-parameter MIXMAX generators A(N,s,m). These generators have an advantage of having a very high quality sequence for moderate and small N. In particular, the smallest generator we tested, $N = 8$, passes all tests in the BigCrush suite.



The distribution of the eigenvalues of the $A(N, s, m)$ for $N = 60, s = 0, m = 2^{52} + 1$. The spectrum represents a leaf of a large radius proportional to $\lambda_{max} \approx m$ and a very small eigenvalue at the origin $\lambda_{min} \approx m^{-N+1}$.



The distribution of the eigenvalues of the $A(N,s,m)$ for $N = 120, s = 1, m = 2^{51} + 1$.



The distribution of the eigenvalues of the $A(N, s, m)$ for
$N = 240, s = 487013230256099140, \quad m = 2^{51} + 1.$

- HEPFORGE.ORG, http://mixmax.hepforge.org; http://www.inp.demokritos.gr/ savvidy/mixmax.php

- HEPFORGE.ORG, http://mixmax.hepforge.org; http://www.inp.demokritos.gr/ savvidy/mixmax.php

- ROOT, Release 6.04/06 on 2015-10-13, `https://root.cern.ch/doc/master/mixmax_8h_source.html`

- HEPFORGE.ORG, http://mixmax.hepforge.org; http://www.inp.demokritos.gr/ savvidy/mixmax.php

- ROOT, Release 6.04/06 on 2015-10-13, `https://root.cern.ch/doc/master/mixmax_8h_source.html`

- CLHEP, Release 2.3.1.1, on November 10th, 2015 `http://proj-clhep.web.cern.ch/proj-clhep/`

Conclusion

Use MIXMAX for your Monte-Carlo simulations !

$$\left| \frac{1}{N} \sum_{i=0}^{N-1} f(A^i P_0) - \int_{\Pi^{\mathfrak{D}}} f(P)\, dP \right| \leq Const \frac{D_N(A)}{N} \tag{19}$$

$$D_N(A) \sim \sqrt{N}$$

it will provide a fast convergence!

This work was supported in part by the European Union's Horizon 2020 research and innovation programme under the Marie Skĺodowska-Curie Grant Agreement No 644121.

Thank you!