Konstantin Savvidy

The MIXMAX RNG

CERN, July 3, 2015

How it all began?

Part 1

Infrared Instability of the Vacuum State of Gauge Theories and Asymptotic Freedom

G.K. Savvidy (Yerevan Phys. Inst.). Jan 1977. 8 pp.
Published in **Phys.Lett. B71 (1977) 133**
EFI-214-6-77-YEREVAN
DOI: 10.1016/0370-2693(77)90759-6

Classical Solutions of Yang-Mills

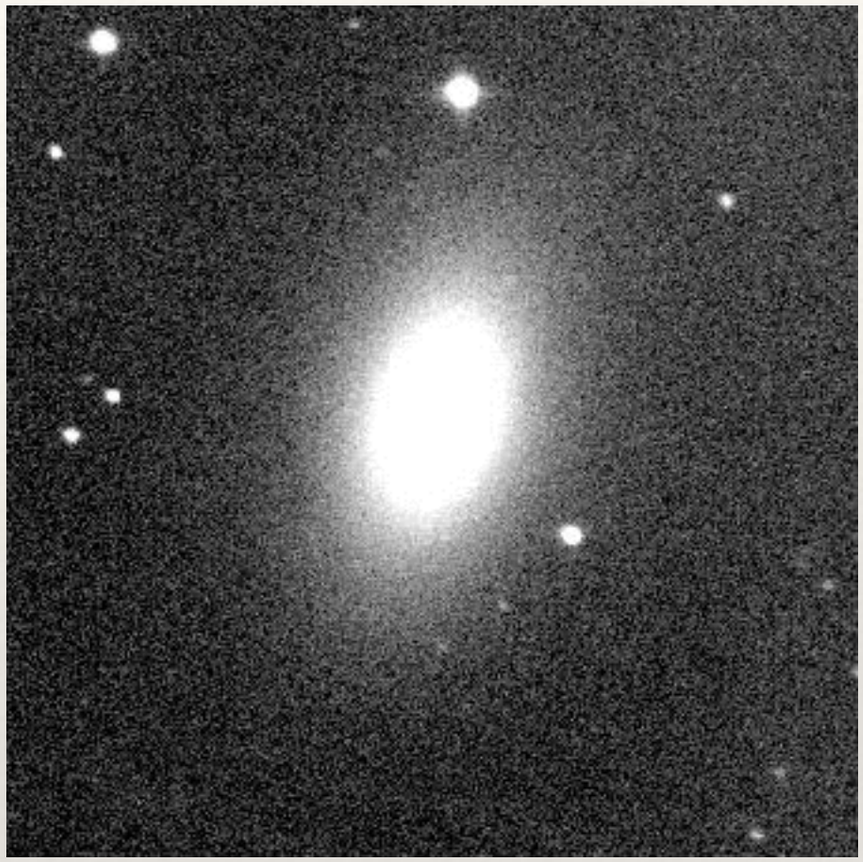
- Plane wave ansatz: $A^a_\nu(k_\mu\, x^\mu)$
- There are massive solutions! $k^2 > 0$
- Further simplification with $A^1_1 = x, A^2_2 = y$ produces the Hamiltonian: $H = p_x^2/2 + p_y^2/2 + x^2 y^2$
- This system was studied experimentally by Natalia starting in 1981 on a PDP-9

Classical Yang-mills Mechanics. Nonlinear Color Oscillations
Sergei G. Matinyan, G.K. Savvidy, N.G. Ter-Arutunian Savvidy (Yerevan Phys. Inst.). 1981.
Published in **Sov.Phys.JETP 53 (1981) 421-425, Zh.Eksp.Teor.Fiz. 80 (1981) 830-838**

Yang-mills Classical Mechanics As A Kolmogorov K System
G.K. Savvidy (Yerevan Phys. Inst.). Dec 1982. 14 pp.
Published in **Phys.Lett. B130 (1983) 303**

Stellar Relaxation

- Elliptical Galaxy is a beehive of 10^10 stars in a settled, steady but completely chaotic state.
- Relaxation or mixing time calculated naively from binary encounters is far too long.



- The problem is formulated as geodesic motion on the 3N dimensional configuration manifold. Chaotic behavior is due to the negative curvature.

Collective Relaxation Of Stellar Systems
V.G. Gurzadian, G.K. Savvidy (Yerevan Phys. Inst.). Jun 1983. 33 pp.
Published in **Astrophys.J. 160 (1986) 203-210**

PRNG

- In the course of this research the idea came about that if there was any system which was provably chaotic in all of the phase space, then such a system could be used as a source of good quality pseudo-random numbers.

Sinai Billiards As A Pseudorandom Number Generator
R.O. Abramian, N.Z. Akopov, G.K. Savvidy, N.G. Ter-Arutunian Savvidy (Yerevan Phys. Inst.). Jul 1986. 8 pp.
EFI-922-73-86-YEREVAN

On The Problem Of Monte Carlo Modeling Of Physical Systems
G.K. Savvidy, N.G. Ter-Arutunian Savvidy (Yerevan Phys. Inst.). Jan 1986. 13 pp.
EFI-865-16-86-YEREVAN, EFI-865(16)-86

After this, there were many other splendid works in the 1980's, 90's and 2000' and 2010' but I will not tell you about it today.

Part 2, MIXMAX

- Mixmax is a specific matrix realization of a chaotic dynamical matrix-recursive system:

$$\vec{x}' = A.\vec{x} \mod 1$$

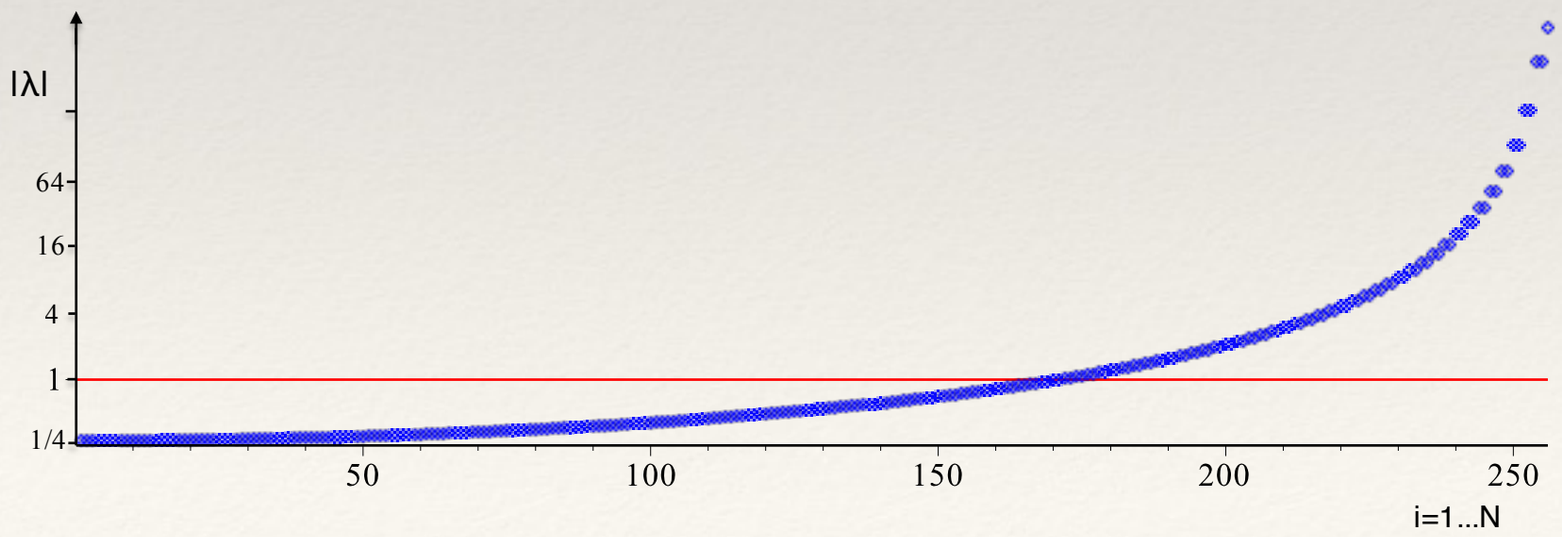
$$\begin{pmatrix} 2 & 3 & 4 & 5 & \dots & N & 1 \\ 1 & 2 & 3 & 4 & \dots & N-1 & 1 \\ & & \dots & & & & \\ 1 & 1 & 1 & 1 & \dots & 2 & 3 & 1 \\ 1 & 1 & 1 & 1 & \dots & 1 & 2 & 1 \\ 1 & 1 & 1 & 1 & \dots & 1 & 1 & 1 \end{pmatrix}$$

- A is a specific matrix
- So, $x(t) = A^t \; x(0) \quad t = 0, 1, 2, 3, 4, \dots$
- But it is also defined for non-integer t: $x(t) = e^{t \; \ln A} \; x(0)$
  So the Hamiltonian is H = ln A !

Entropy

- One must study the spectrum of eigenvalues and none of the eigenvalues should be on the unit circle
- Entropy is equal to $h = \sum_{|\lambda|>1} \ln \lambda$
- Decay of correlations is governed by entropy:

$$\tau_0 \leq 1/h$$



Eigenvalues

- I have this approximate formula for the eigenvalues

$$\log(\lambda_k) \lesssim \log(4)\left(-1+\left(\frac{3}{2N}\right)^2 k^2\right) \quad \text{for } k = 1 \ldots \frac{2N}{3}$$

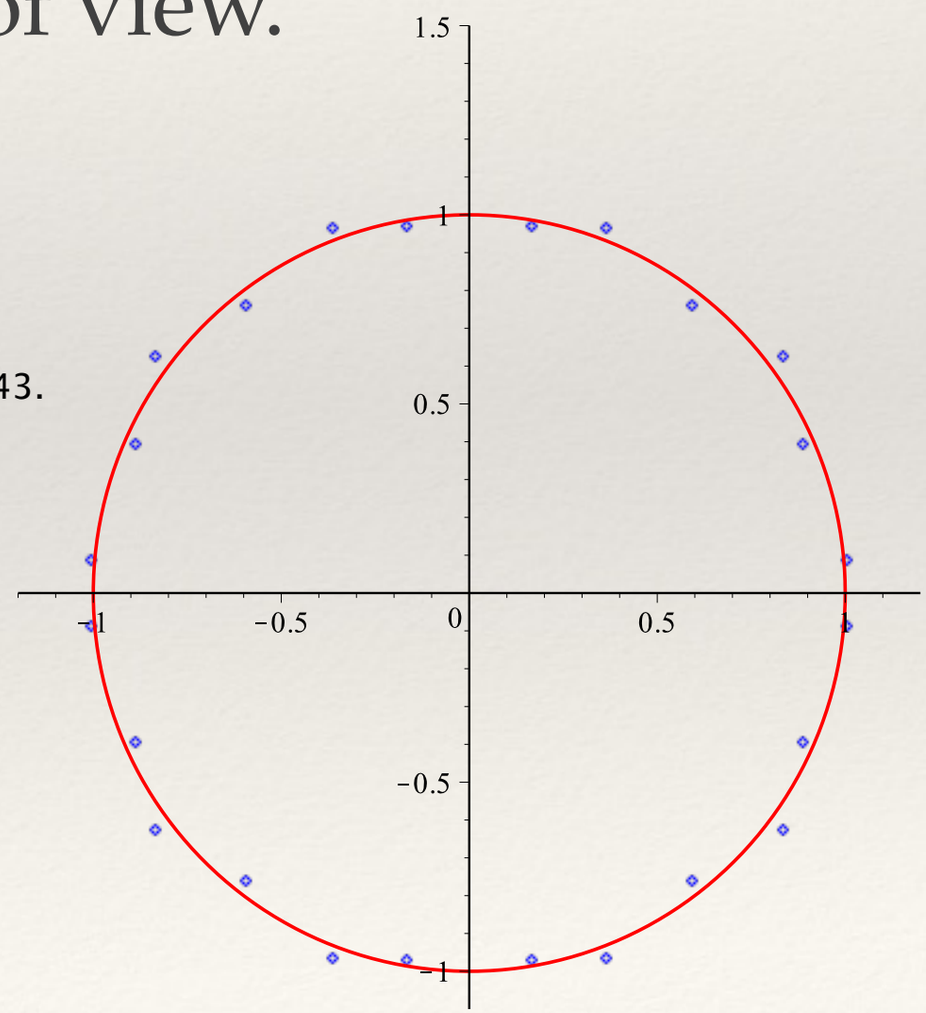
- Which allow to estimate the entropy

$$N\log(4) > h \gtrsim 4/9\, N\, \log(4)$$

Other generators

- RCARRY was an LCG crafted by Marsaglia to be fast, but has a bad multiplier. Luscher studied the system from dynamical systems point of view.

The eigenvalues closest to the circle have $|\lambda| \approx 1.0085$, the farthest $|\lambda| \approx 1.043$.

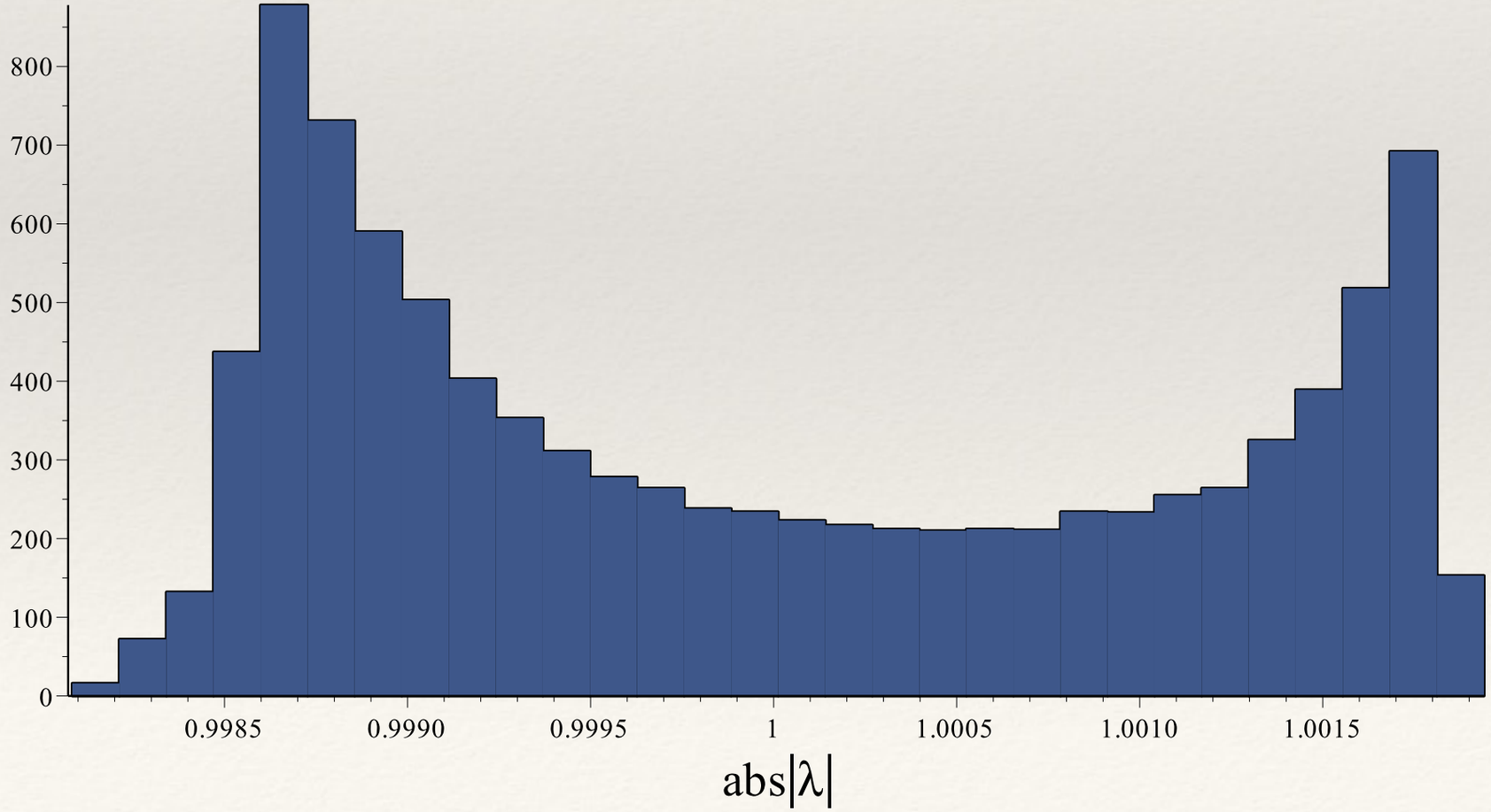


The trouble is related to the fact that the characteristic polynomial of the system is space:

$$x^{24} - x^{14} + 1 = 0$$

Mersenne Twister

- The situation is even worse for the Mersenne Twister. It is a generator with N=19937 and p=2, and with a very space matrix and polynomial.



Computer Realization

- There can only be discrete trajectories, so we work with rational numbers: $x_i = a_i/p$
- Then, the recursion is $$a'_i = \sum_{j=1}^{N} A_{ij}\, a_j \mod p$$
- If and only if the characteristic polynomial is irreducible, then

$$A^q = \mathbb{I} \quad \text{for} \quad q = \frac{p^N - 1}{p - 1}$$

This allows to find the period, and typically it is q.

Implementation

First, we present the formula which allows the efficient calculation of the recursion. Given the vector a with components a_i, $i = 1...N$, a vector of partial sums b is formed according to

$$\begin{aligned} b_1 &= 0 \,, \\ b_i &= b_{i-1} + a_i \quad \text{for } i = 2...N \,. \end{aligned} \tag{8}$$

Then, the new vector is calculated:

$$\begin{aligned} a'_1 &\leftarrow a_1 + b_N \,, \\ a'_i &\leftarrow a_{i-1} + b_i \quad \text{for } i = 2...N \,. \end{aligned} \tag{9}$$

Finally, the correction due to the magic value is applied

$$a'_3 \leftarrow a'_3 + s\, a_2$$

Some particular realizations of MIXMAX

Size N	Magic s	Entropy (lower bound)	Period τ/q	$\approx \log_{10}(q)$	q is fully factored	BigCrush
10	-1	6.2	1/4	165	Yes	33
16	6	9.9	1/32	275	Yes	> 13
40	1	24.6	1/4	716	Yes	3
44	0	27.1	1/4	789	No	4
60	4	37.0	1	1083	Yes	2
64	6	39.4	1/8	1156	No	1 (?)
88	1	54.2	1/2	1597	No	Pass
256	-1	157.7	1	4682	No	Pass
508	5	313.0	1	9309	No	Pass
720	1	443.6	1	13202	No	Pass
1000	0	616.1	1/20	18344	No	Pass
1260	15	776.3	1/2	23118	No	Pass
3150	-11	1940.8	1/12	57824	No	Pass

Table 1: Table of properties of generators for different matrix size N and special magic value s. For each N that we investigated, the period τ is given as a fraction of $q = (p^N - 1)/(p-1)$. For cases where the full integer factorization of q is known, unconditional guarantee can be given about the period of the sequence. In all cases the characteristic polynomial was proved to be irreducible by Pari/GP [20]. The last column indicates whether the generator for that N and special value s passes the BigCrush suite of tests, and if not how many tests are failed. The case of $N = 60$ uses a doubly special matrix which has two entries modified: $a_{32} = a_{54} = 3 + s$. It is seen that the generator gets uniformly better with N until it passes all tests. The most discriminative test for this family of generators appears to be the classic Gap test. On this test alone, the improvement with N is also evident, with progressively better p-values as N is increased, e.g. for N=64 the value of $\chi^2 \approx 372$ for 232 degrees of freedom with $\chi^2/dof \approx 1.6$ indicates only a marginal failure. For all $N > 64$ which we have tested, the generator passes all tests.

Skipping

- Skipping is possible because different powers of A commute, and so we can precalculate and store the power-of-two characteristic polynomial and then it is magic!

$$a(t+m) = A^m \,.\, a(t) = E(A) \,.\, a(t) = \sum_{i=0}^{N-1} e_i \, A^i \,.\, a(t) = \sum_{i=0}^{N-1} e_i \, a(t+i)$$

- Needs an algorithm to calculate the characteristic polynomial without using the explicit matrix.

MIXMAX is currently the fastest and best motivated PRNG on the market.

–Thank you!