Konstantin Savvidy

The study of the MIXMAX RNG

CERN, July 4, 2016

Part 1

How it all began?

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 Savvidy 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**

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

Part 2, MIXMAX

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

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

- A is a specific matrix

$$\begin{pmatrix} 2 & 3 & 4 & 5 & \ldots & & N & 1 \\ 1 & 2 & 3 & 4 & \ldots & & N-1 & 1 \\ & & \ldots & & & & & \\ 1 & 1 & 1 & 1 & \ldots & 2 & 3+S & 1 \\ 1 & 1 & 1 & 1 & \ldots & 1 & 2 & 1 \\ 1 & 1 & 1 & 1 & \ldots & 1 & 1 & 1 \end{pmatrix}$$

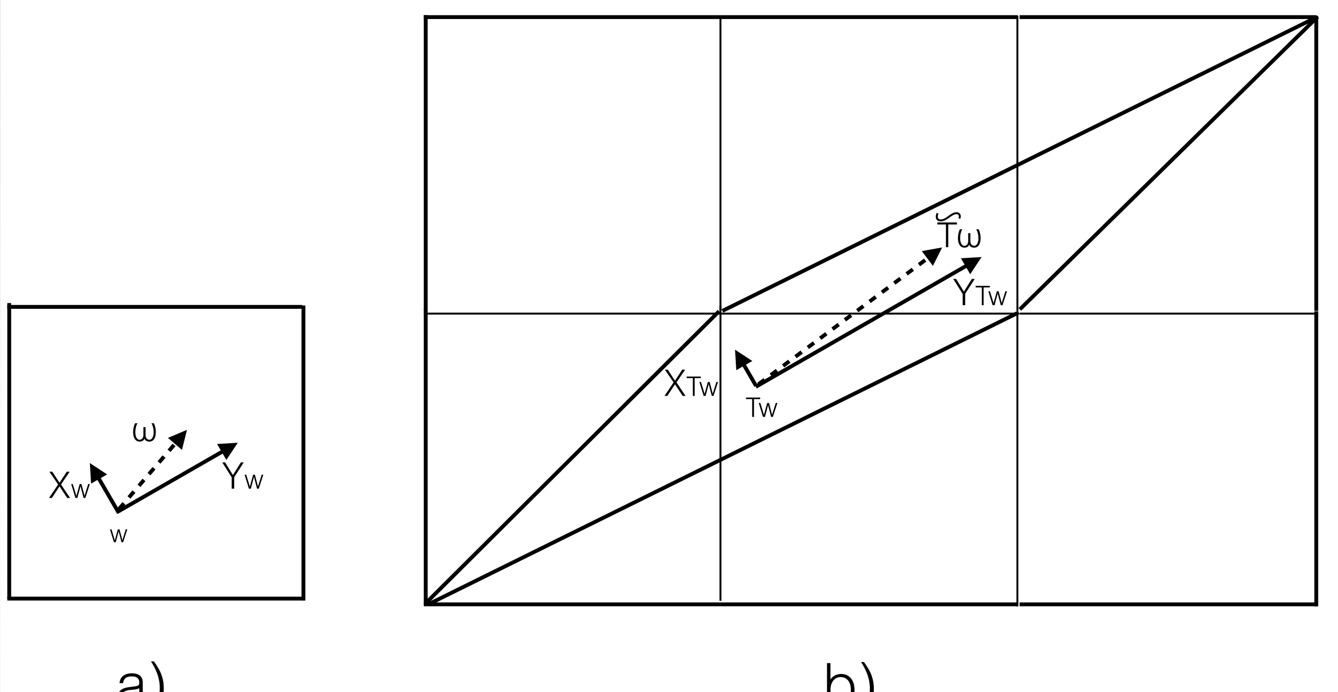
- So, $x(t) = A^t\, x(0) \quad t = 0, 1, 2, 3, 4, \ldots$

- It is defined on a N-dimensional real torus with periodic boundary conditions:

$$x \in [0, 1)$$

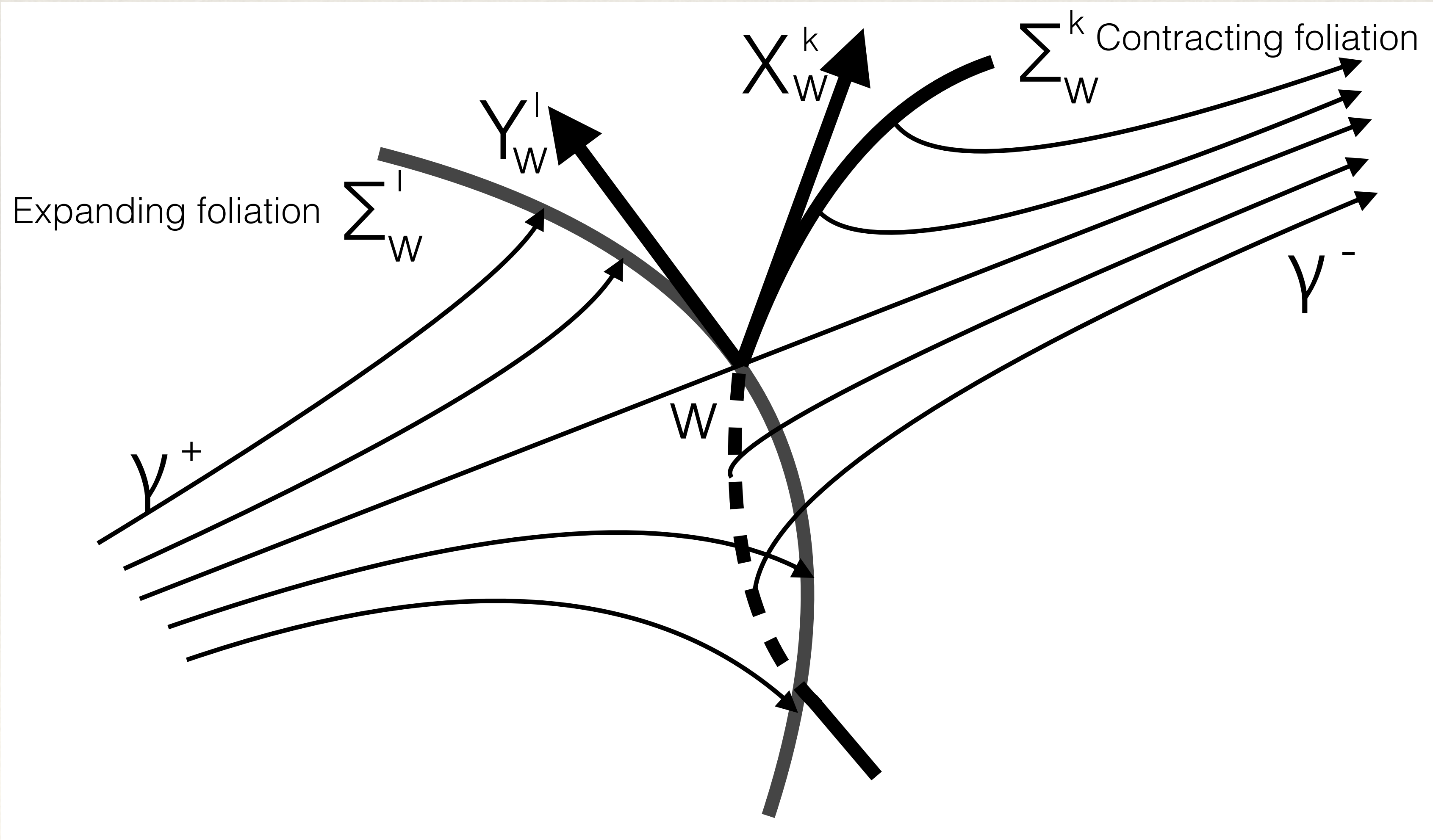
Tangent space

- The tangent space of the torus is simply R^N and the automorphism acts on it as linearly. There are contracting X and expanding Y linear spaces, these are spanned by the eigenvectors of the matrix which correspond respectively to the eigenvalues inside and outside the unit circle.



Contracting and Expanding Foliations

- Roughly speaking, for each trajectory there is a multitude of other trajectories, which infinitely approach it as $T \to +\infty$. These form all together the contracting foliation. It is not invariant under T.



Entropy

- Calculating the volume expansion rate on Y, we get:

$$H = \log \prod_{|\lambda_i|>1} \lambda_i = \sum_{|\lambda_i|>1} \log(\lambda_i)$$

- Equally well, on the contracting space X, the volume contraction rate is

$$H = -\log \prod_{|\lambda_i|<1} \lambda_i = -\sum_{|\lambda_i|<1} \log(\lambda_i)$$

- Decay of correlations is also governed by entropy:

$$\tau_0 \leq 1/h$$

Measuring the speed of divergence

- Phase space volume is conserved, $det\, A = 1$
- This means that if we split the tangent space into the C-dimensional contracting space X and the N-C dimensional space Y then the expansion and contraction is equal, but how can we define it?
- The volume on X contract exponentially:

$$V_X(t) = V_X(0) \times e^{-Ht}$$

- The volume on Y expands, also exponentially, and at the same rate:

$$V_Y(t) = V_X(0) \times e^{+Ht}$$

- What is H? It is the entropy!!!
- Under inversion of time, $t \to -t$, X and Y are exchanged.

- There exists periodic and aperiodic trajectories.
- Periodic trajectories of the desired period T can be found by solving the following equation:

$$A^T . x = x + b$$

where b is an integer vector.
- The solution is $x = (A^T - \mathbb{I})^{-1} . b$
- It follows that since A^T - I is nonsingular, the solution exists for all b, and x is typically a vector of rational numbers with the same denominator for each T.
- Also, it immediately proves that ALL irrational vectors lie on aperiodic trajectories.

The period

- If you start with x as a rational vector, it will remain on the same rational sub lattice generated by the p=lcd(x)
- The search for trajectories with provable periods leads to sub lattices where this denominator is a prime number.
- This by itself does not lead to all points on the lattice having the same period.
- Existing mathematical literature also did not seem to have the appropriate criterion ready.

The period

- The conditions turned out to be the following one:
  1) The characteristic polynomial of the matrix should be irreducible in the Galois field $\mathbb{F}[p]$

  2) If and only if 1) is true, then the period of all trajectories on the rational sub lattice will be the same and the period will be some simple fraction of

$$q = \frac{p^N - 1}{p - 1}$$

- I have developed some technology and powerful analytical methods to compute the characteristic polynomial and to check this condition.

Remark: the characteristic polynomial of this system cannot be a primitive polynomial in the field $\mathbb{F}[p^N]$

Computer Realization

- We work with rational numbers: $x_i = a_i/p$

- Then, the recursion is equivalent to

$$\vec{x}\,' = A.\vec{x} \mod 1 \quad \Longleftrightarrow \quad a_i' = \sum_{j=1}^{N} A_{ij}\, a_j \mod p$$

- The computer simulates the periodic, rational trajectories exactly.

Search for generators with largest N and period

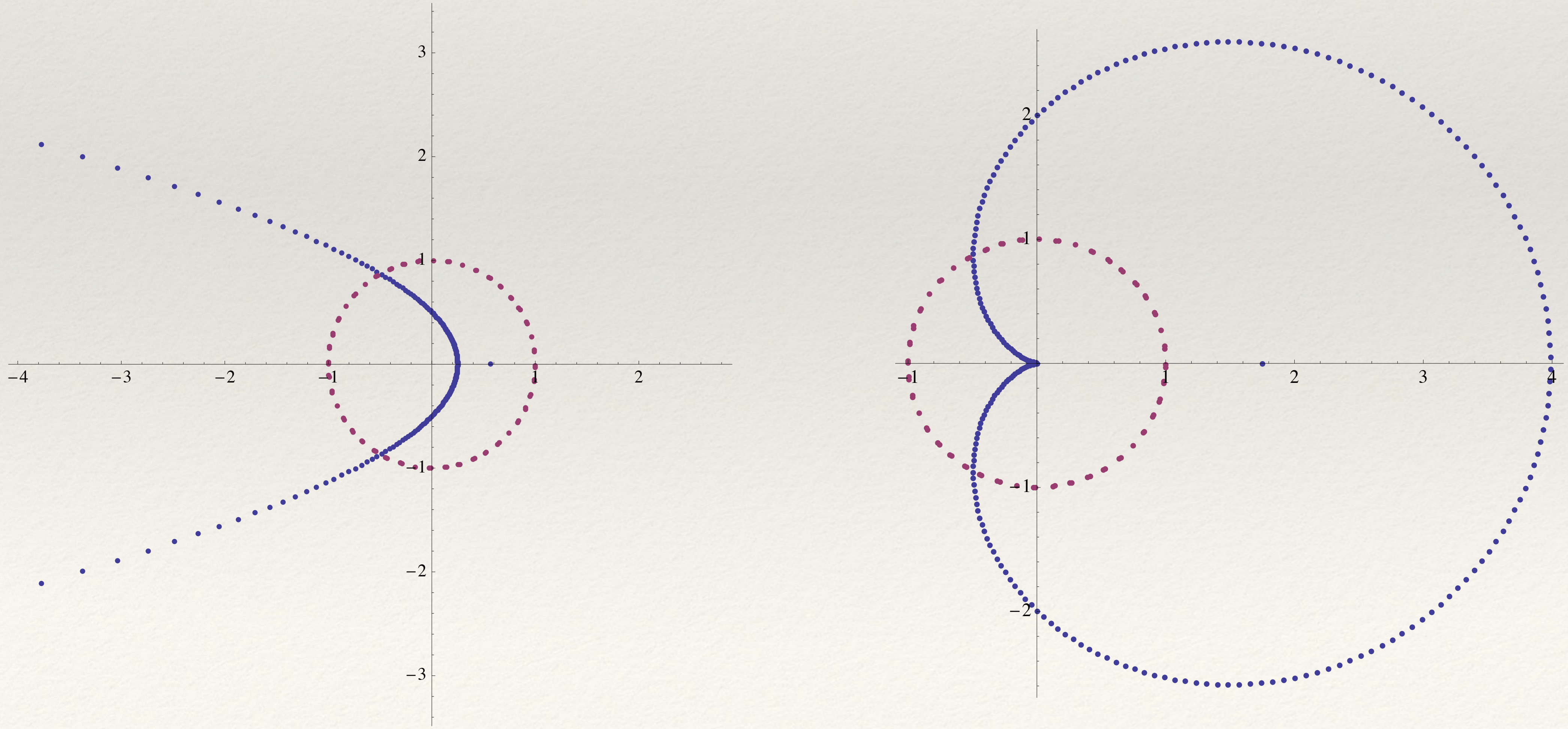
- The search ran in 2015 for several CPU-months and has yielded the following generators:

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 1: Table of properties of generators for large matrix size N. The third column is the value of the Kolmogorov entropy, which needs to be greater than about $h \approx 50$ for the generator to be empirically acceptable. Therefore, it should not be surprising that for all of these generators, the sequence passes all tests in the BigCrush suite [16]. For the largest of them, the period approaches a million digits.

The Spectrum

- Ok, so what is actually the spectrum of the eigenvalues of the MIXMAX matrix?
- It is complex, with many eigenvalues with $|\lambda| \sim 1/4$



Limiting entropy

- We have been able to prove the following limiting formula as

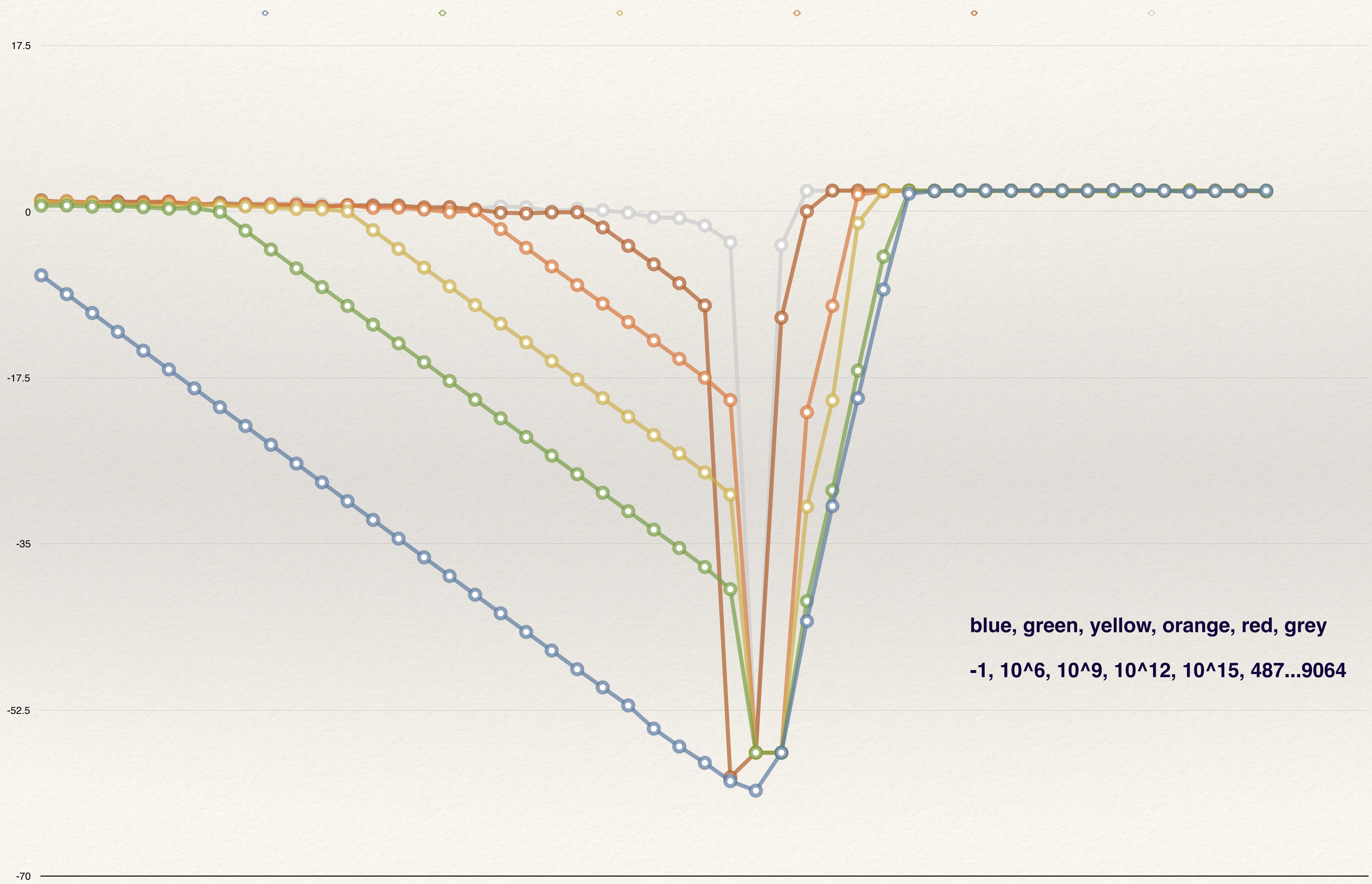
$$N \to \infty$$

$$r(\phi) = 4\ \cos^2(\phi/2)$$

- Such a curve is called a "cardiod" and its inverse is simply a parabola.
- This allows to calculate the limiting value of the entropy as well:

$$H \to \frac{2}{\pi} N$$

Dependence of the SPECIAL on nearby trajectories



New Family of generators

- Increasing N leads to linearly-increasing entropy, but can we make generators with good mixing properties for small N?
- We have proposed a generalized, three- and four-parameter matrixes in the same family which have much larger entropy, much bigger maximum eigenvalues and much smaller small eigenvalues.

Three parameter family

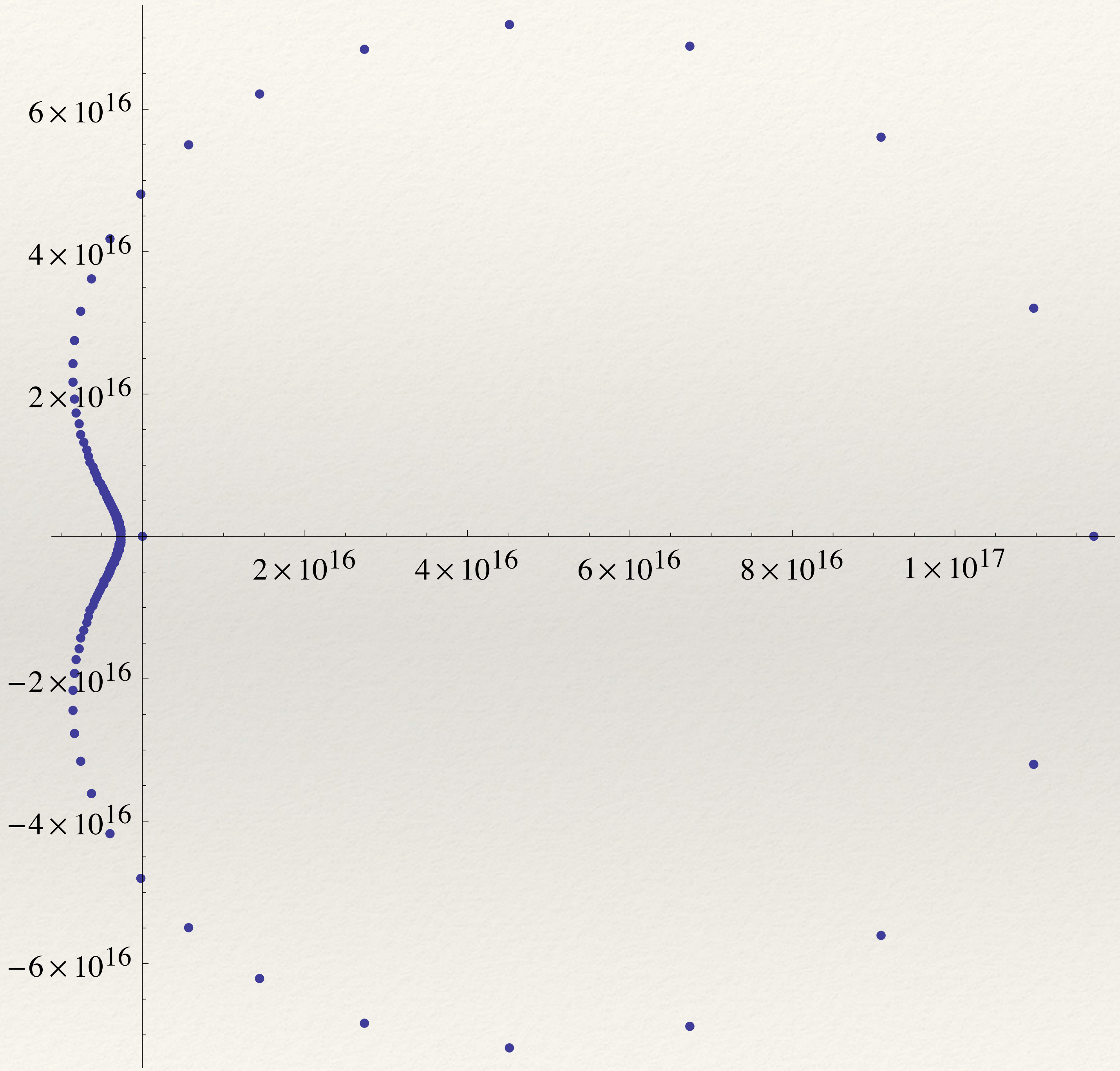
$$A(N,s,m) = \begin{pmatrix} 1 & 1 & 1 & 1 & \dots & 1 & 1 \\ 1 & 2 & 1 & 1 & \dots & 1 & 1 \\ 1 & m+2+s & 2 & 1 & \dots & 1 & 1 \\ 1 & 2m+2 & m+2 & 2 & \dots & 1 & 1 \\ 1 & 3m+2 & 2m+2 & m+2 & \dots & 1 & 1 \\ & & & \dots & & & \\ 1 & (N-2)m+2 & (N-3)m+2 & (N-4)m+2 & \dots & m+2 & 2 \end{pmatrix}$$

- For m=1 it reduces to the old matrix
- It is still of the almost-band form
- The progression of the integers is arithmetic
- The correspondence between the discrete and continuous system is exact and unambiguous if $(N - 2)*m + 2 < p$

Some specific members of the three-parameter family

Size	Magic	Magic	Entropy	Log of the period q
N	m	s		$\approx \log_{10}(q)$
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	8679.2	4389

Spectrum of the three-parameter family



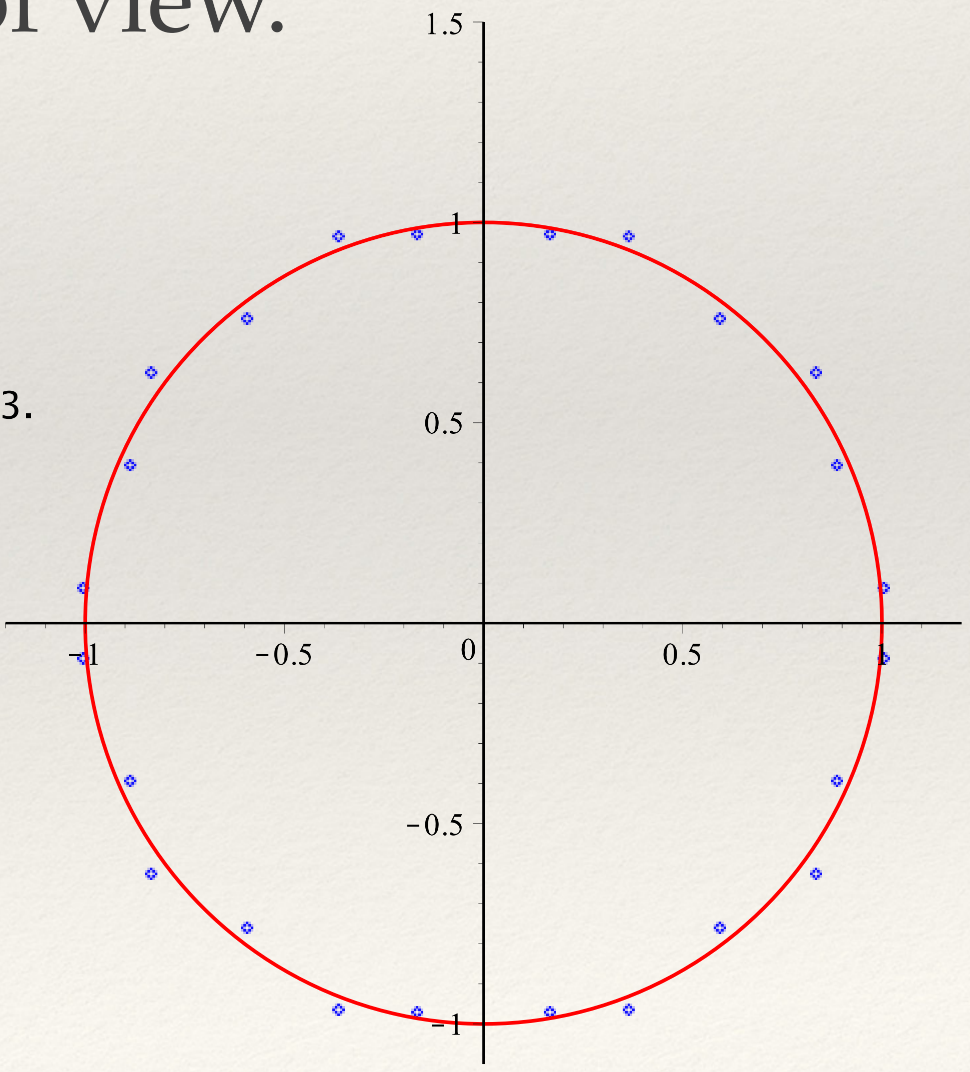
–Thank you!

Overflow slides follow

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 |λ| ≈ 1.0085, the farthest |λ| ≈ 1.043.

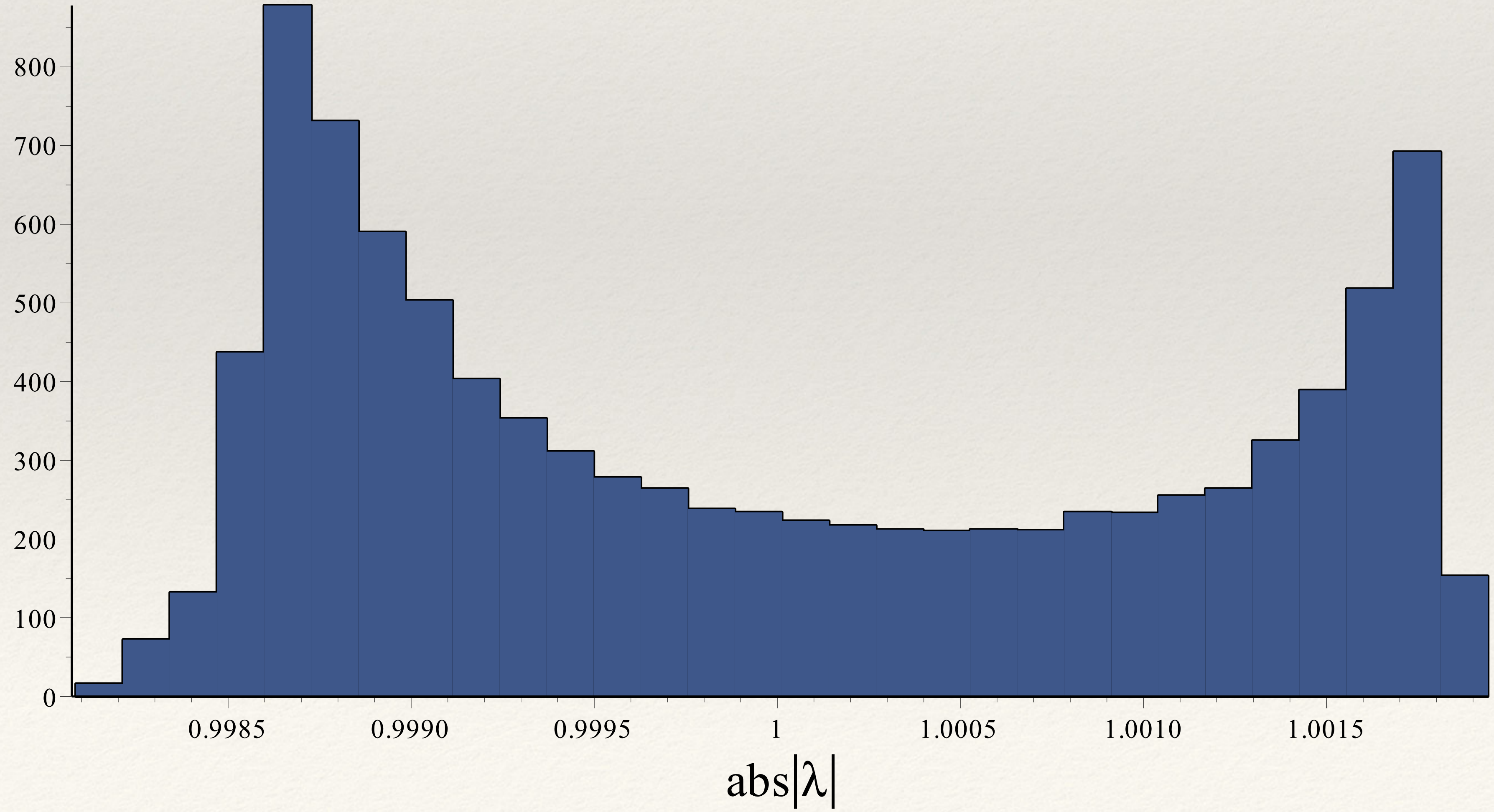


The trouble is related to the fact that the characteristic polynomial of the system is space:

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

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 sparse matrix and polynomial.



RCARRY and RANLUX

- r:=24;
- s:=10;
- b:=2^24;
- m := b^r - b^s +1;
- m = (binary)
111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
111111111111111111111111111111111111111000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000001
- a:=m - (m-1)/b;
111111111111111111111110111111111111111111111111111111111111111111111111111111111111111111111111111
111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
111111111111111111111111111111111111111000000000000000000000001000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000001
- luxa := a^(389) mod m;
110111110000001100000000000000000000000000000010111011100000000000010000000000000000000000000000101
110010010010000101111111111111111111111111101111101100110000001001111111111111111111111111110010010
101011000101100000000000000000000000000000110110010010101010110000000000000000000000000001111010010
011111100101111111111111111111111111111010110010011110011111111111111111111111111111011100111001000
101001101111111111111111111111111110010100100101011101000000000000000000000000000010110000111000100
101100000000000000000000000000010111011001010110010010000000000000000000000000

x` = a*x mod m

x[i+389] = luxa * x[i] mod m

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.