Konstantin Savvidy

MIXMAX and other RNG in higher dimensions

Athens, July 3, 2018

Part 1, MIXMAX

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

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

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

- So, $x(t) = A^t \; x(0) \quad t = 0, 1, 2, 3, 4, \dots$
- It is defined on a N-dimensional real torus with periodic boundary conditions:

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

Computer Realization

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

- Then, the recursion is equivalent to

$$\vec{x}\,' = A.\vec{x} \mod 1 \iff a'_i = \sum_{j=1}^{N} A_{ij}\, a_j \mod p$$

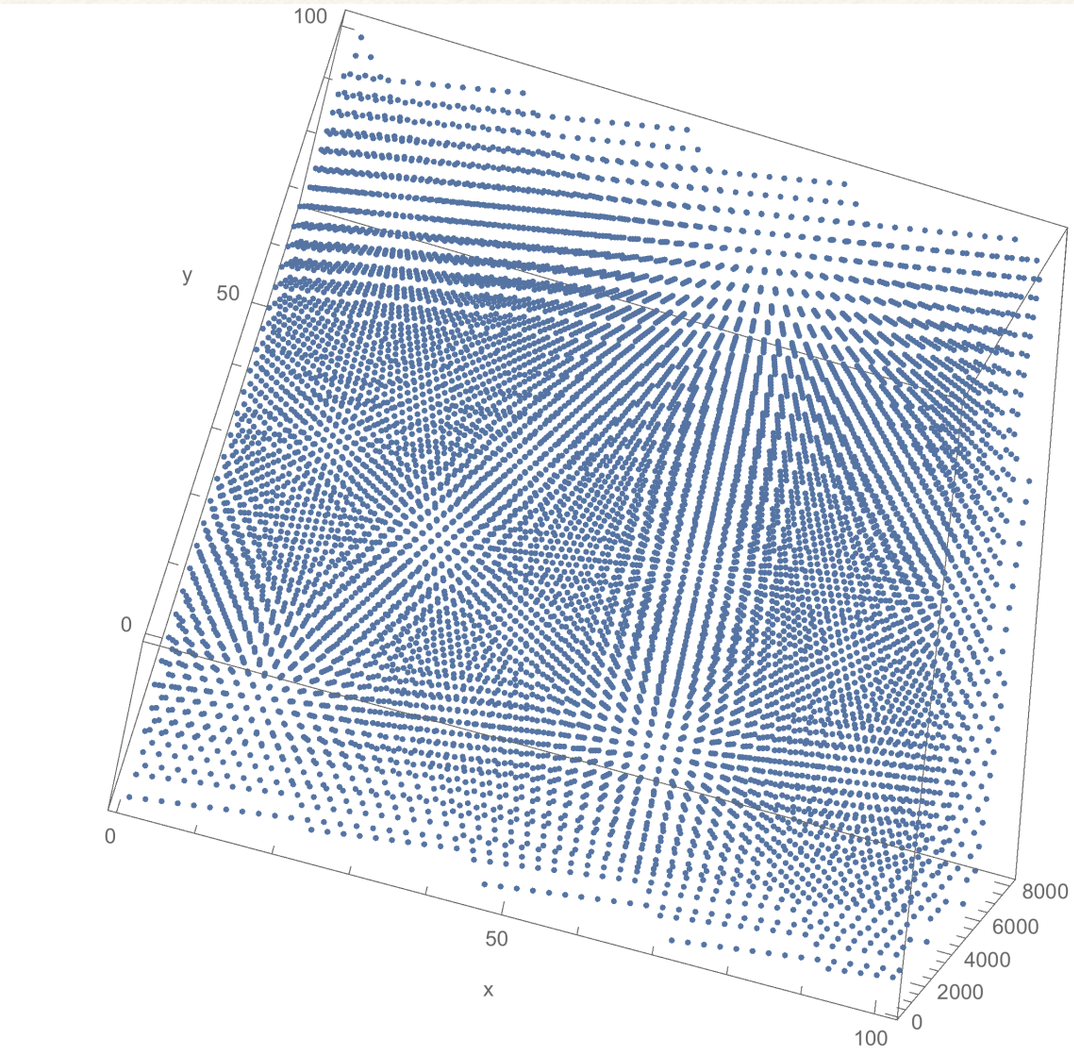
- The computer simulates the periodic, rational trajectories exactly.

-

Three parameter family

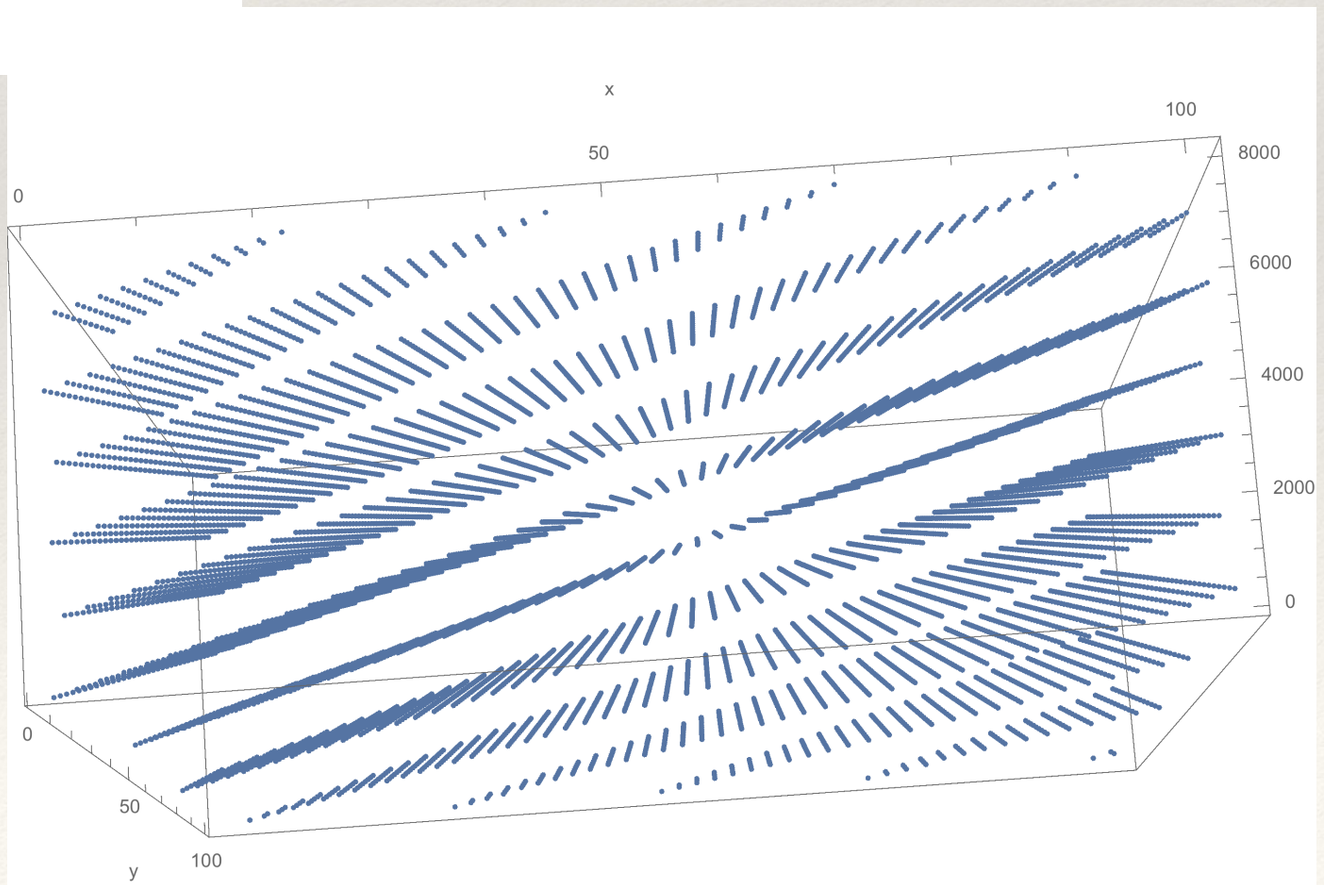
$$A(N,s,m)=\begin{pmatrix}
1 & 1 & 1 & 1 & \dots & 1 & 1\\
1 & 2 & 1 & 1 & \dots & 1 & 1\\
1 & m+2+s & 2 & 1 & \dots & 1 & 1\\
1 & 2m+2 & m+2 & 2 & \dots & 1 & 1\\
1 & 3m+2 & 2m+2 & m+2 & \dots & 1 & 1\\
 & & & \dots & & & \\
1 & (N-2)m+2 & (N-3)m+2 & (N-4)m+2 & \dots & m+2 & 2
\end{pmatrix}$$

- For m=1 it reduces to the old matrix
- It is still of the almost-band form
- The progression of the integers is arithmetic



Seems OK

but actually



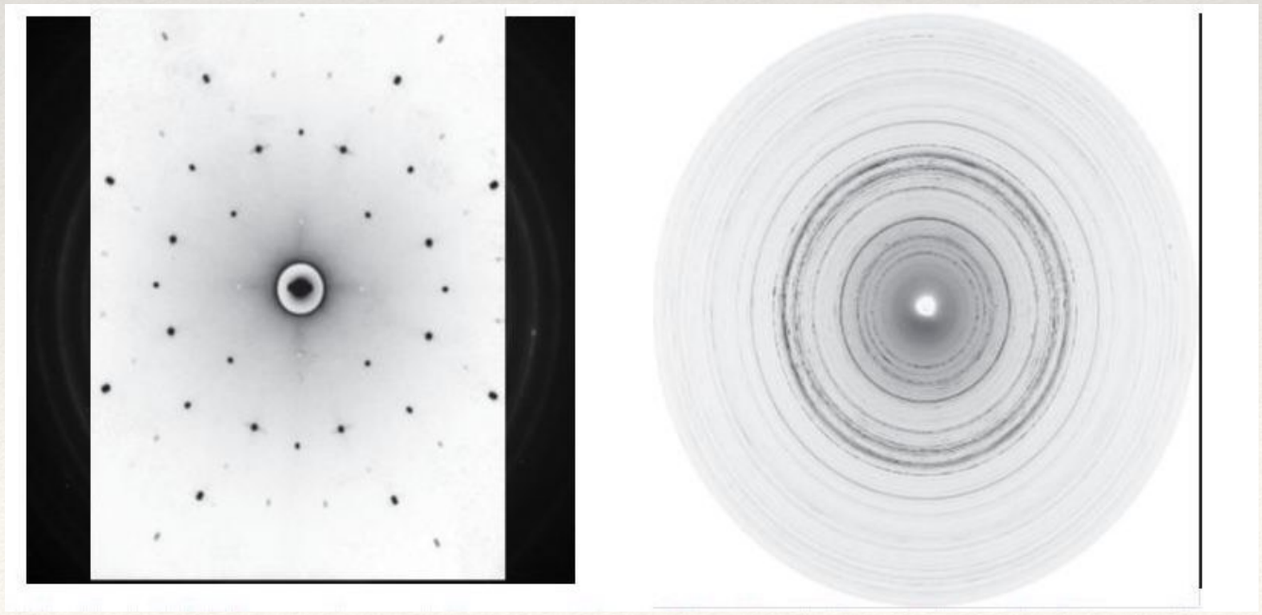
Dual Lattice

- In the lattice formed by RNG output vectors we are interested in the largest distance between planes.
- This is equivalent to searching the shortest vector in the dual lattice defined by

$$\wedge^{\star} = \left\{ \mathbf{y} \in R^{*d} \;\middle|\; \mathbf{y} \cdot \mathbf{g} = n \in Z, \quad \mathbf{g} \in \wedge \right\}.$$

- In x-ray or electron beam crystallography the Laue condition for the reflected beam reads:

$$\triangle \mathbf{k} \cdot \mathbf{x} = n, \;\; n \in Z$$



regular lattice

or maybe some special
irregular arrangement?

Best packings in higher dimensions

- The answer is known in 8 dimensions:
  - (Maryna Viazovska, 2016)

$$\Gamma_8 = \left\{(x_i) \in \mathbb{Z}^8 : \sum_i x_i \equiv 0 \pmod 4\right\}$$

- and in 24 dimensions, Leech lattice

$$\Gamma_{24} = \frac{1}{\sqrt{8}}(\mp 3, \pm 1^{23})$$

- Each ball touches 196,560 others!!!
  Conway (1968) determined the automorphism group of this lattice and discovered three new sporadic simple groups.

The short lattice vector problem

- There does NOT exist polynomial algorithm for finding the shortest lattice vector in a general lattice.
- Finding some short vector within some constant factor of the absolute shortest is possible, but the factor is 2^D
- There is a Gram-Schmidt type algorithm available by Lenstra–Lenstra–Lovász (LLL,1982), which is polynomial-time and OK performance.
- Another algorithm, with excellent results in dimensions up to a few hundred, is called Block Korkine Zolotarev (BKZ).

Linear relations in MIXMAX

- Generally, in the three parameter family:

$$x_i^{(j)} - 2\,x_i^{(j+1)} + x_i^{(j+2)} - x_i^{(j+N+2)} - (m-1)\,x_i^{(j+N+1)} = 0 \mod 1.$$

- For the N = 17, m = 2^36+ 1 and s = 0, this produces a spectral index of ~ 10^-8 in dimensions between N and 2N.
- Is 10^-8 good or not good enough?

Apply hammer to the nail

- For L'Ecuyers combined MRG called MRG32k3a we have the short vector in the dual lattice:
  y = {-1, -1, 0, 0, 0, 3, 0, 0, 1, -2, 2, 0, -1, -2, -1, 2, 0, 1, 0, 1, -1, 1, 0, -3, 0, -2, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, -2, 1, 0, -1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 3, 0, 0, 0, 1, 0, 1, 0, -1, 0, -1, 1, 0, 0, -1, -1, 0, 0, 2, 2, 0, -2, -1, 0, 0, 1, 1, 0, 1, 0, -1, 1, -2, 1, 2, 1, 1, -1, 0, 0, 0, 0, 0, 0, 1, 0, -2, -1, 0, 0, 1, 1, 0, 0, 1, -1, 1, 0, 0, 2, 0, 1, -1, 0, 1, -1, 0, 0, -1};
- MRG32k3a will produce incorrect results when integrating the function f = cos(2π **y.x**) where x is the consecutive output of 121 state iterations.

Monte-Carlo integration

- The **c** are Fourier coefficients in the expansion

$$f(\mathbf{u}) = \sum_{\mathbf{h}\in\mathbb{Z}^{\mathbf{s}}} c_{\mathbf{h}} \ \exp(i\,2\pi\,\mathbf{h}\cdot\mathbf{u})$$

- Monte-Carlo integration:
  we throw random vectors and evaluate the integral of a function in R^D by the sum

$$\frac{1}{n}\sum_{i=1\ldots n} f(\mathbf{x}_i) \to c_0 + \sum_{\mathbf{y}\in\wedge^*} c_{\mathbf{y}}$$

- On the right-hand-side we have c0 (the correct result) plus a sum over all vectors on the dual lattice.

Bounds on accuracy

- For a function which has all partial derivatives up to k times bounded by a common constant A,

$$|f^{(k)}| < A$$

- we have

$$|c_{\mathbf{y}}| < \frac{A}{|\mathbf{y}|^k} < A\ l^k$$

- and in fact in the average case the exponent is D*k.

—Thank you!

Apply hammer to the nail

- For full-luxury RANLUX, a run of LLL and BKZ lattice reductions gives the shortest vector:
  y=[3, -7, 7, -3, 0, -7, 7, 23, -4, 11, -7, 11, 5, 10, 17, -4, 7, 3, -4, 4, -14, -3, -2, 8, 14, 0, -11, -12, 15, 10, -7, -16, -2, -10, -10, -12, 8, -7, 0, 22, 10, 6, 8, 6, -19, -2, -4, -13, 4, -1, 16, -5, -3, 1, 4, -3, -9, -4, -14, 9, -17, 0, -1, 4, 4, 14, -9, -3, -3, 0, 13, -8, 11, 14, -19, -13, -1, 6, 0, -3, -2, 4, 6, -6, -1, -2, 1, -18, 5, 12, 16, -22, -12, -7, -12, -15, 7, 6, -14, -9, -8, -7, 2, 1, -1, 2, -2, -4, 0, -9, -14, 1, 22, 7, 4, -3, -12, -7, 5, 4]
  in D=120 with length ~ 102.9, so that the spectral index is ~0.01

- RANLUX will produce incorrect results when integrating the function f = cos(2π **y.x**) where x is any or all of components of the RANLUX state in 120 consecutive iterations.