K-systems

K-systems are the continuous many-dimensional Hamiltonian classical dynamical systems we have defined often in these meetings.

They have the property of K-mixing which we have seen means that the coordinates of any point on a given trajectory will be independent of the coordinates of other points on the trajectory provided all the points are taken sufficiently far apart. [The definition of mixing is given below.]

The random number generators (RNG's) Ranlux and Mixmax are not K-systems because discrete systems cannot have all the properties of the corresponding continuous system.

The main goal of this talk is to show how to determine whether a discrete RNG has the mixing properties of the corresponding continuous system.

Mixing and K-Mixing

1. Zero-mixing is the same as ergodic motion. It means that the system will asymptotically come arbitrarily close to any point in the available space.
2. One-mixing means that the coverage will be uniform, in the sense that asymptotically, the probability of finding the system in any given volume of state space is proportional to the volume.
3. Two-mixing means that the probability of the system being in one volume of state space at one time, and another volume at another faraway time, is proportional to the product of the two volumes.
4. N-mixing means that the probability of finding the system in N different volumes at N different faraway times is proportional to the product of the N volumes.
5. K-mixing is N-mixing for arbitrarily large N.

Mixing in Sinai's billiards

Another way of looking at chaos in classical dynamical systems is the trajectory of a ball on a frictionless billiard table, studied extensively by Ya. G. Sinai.

On a standard rectangular table, it can be shown that the motion is almost always ergodic (almost all trajectories will cover the whole table asymptotically), but there is no mixing, so these systems are not K-systems.

If the edges of the table are curved outward, there is a focussing effect, and the motion is not even sure to be ergodic. On an elliptical table, for example, the system is integrable, and not chaotic.

But if the edges of the table are curved inward, they defocus nearby trajectories, leading in most cases to K-mixing.

Divergence of Nearby Trajectories

K-systems diverge exponentially, in the following sense:
If a K-system is initiated from two different but arbitrarily close initial states, the distance between the two trajectories will increase exponentially as the two trajectories advance in time.

There are two quantities often used to measure the speed of divergence.
One is the Lyapunov Exponent, which is proportional to the logarithm of the modulus of the largest eigenvalue of the underlying matrix.
The other is the Kolmogorov Entropy which depends on the logarithms of all the eigenvalues greater than one.
The theory of K-mixing being an asymptotic theory, it says only that to have K-mixing asymptotically, both these quantities must be > 0.
Unfortunately it does not tell us how to use either quantity to determine when the mixing becomes effective. This is not surprising, since the 'critical value' must depend on the precision of the trajectories, which is infinite for the continuous systems.

Neighbouring Trajectories for the Discrete Case

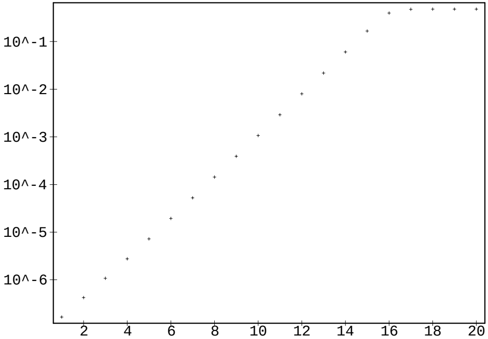
Fortunately, the behaviour of nearby trajectories is one of the properties that should be the same for the discrete and continuous systems, in the limit of high density of the discrete points.

The main difference is that in the continuous system, the two trajectories can start arbitrarily close together, whereas the discrete trajectories must be initially at least one bit apart. That is the precision of the trajectories in the discrete system.

K-mixing in dynamical systems implies an exponential divergence of nearby trajectories. If we now consider a discrete RNG and wish to know if it has the mixing properties of a continuous K-system, it should be sufficient to observe the evolution of two trajectories of the discrete RNG initially one bit apart as a function of time. If the divergence is exponential, we can say it has the mixing properties of a K-system.

Neighbouring Trajectories in Ranlux and Mixmax

RANLUX:



MIXMAX (small *s* and *m*):

Lorenzo Moneta has made the corresponding plot for Mixmax. The points for Mixmax(256) also follow a straight line, and reach 1/2 after only 3 iterations for 53-bit precision.

The Ranlux Matrix reverse-engineered from Marsaglia's SWB contains only zeroes and ones. The eigenvalues are $\neq 1$ but close.

The Savvidy Matrix has much larger and smaller eigenvalues.

$$\begin{array}{ccccccccc}
1 & 1 & 1 & 1 & 1 & 1 & \ldots & 1 & 1 \\
1 & 2 & 1 & 1 & 1 & 1 & \ldots & 1 & 1 \\
1 & 3+s & 2 & 1 & 1 & 1 & \ldots & 1 & 1 \\
1 & 4 & 3 & 2 & 1 & 1 & \ldots & 1 & 1 \\
1 & 5 & 4 & 3 & 2 & 1 & \ldots & 1 & 1 \\
 & \ldots & & & & & & & \\
 & \ldots & & & & & & & \\
1 & N & N-1 & N-2 & & \ldots & & 3 & 2
\end{array}$$

The extended Savvidy Matrix uses (very) large values of s, and the numbers larger than 1 are multiplied by a (very) large integer m.

Martin Luscher's comment on large *m* and *s*

The algorithm with large values of m and/or s can no longer be regarded as a discrete approximation to a classical dynamical system that smoothly maps the N-dimensional torus onto itself. Continuity at distances much larger than the "lattice spacing" [equal to $1/p = 1/(2^{61} - 1)$] is in fact lost when the "modulo" operation is applied after multiplication of the random numbers by the large coefficients of the matrix A.

As a consequence, the relevance of the classical mathematical theory of Anosov C systems is not obvious to me anymore. The "nearby-trajectories" tests, for example, become quite meaningless.

For large m and/or s, the algorithm is a kind of hybrid of an Anosov dynamical system and a linear-congruential algorithm with a large multiplier. Maybe this is better than mixmax with small m and s, but I would not know how to analyse such generators theoretically, because they are neither a discrete approximation to a classical dynamical system nor a linear-congruential generator.