1. Publications

2. Monte Carlo Method

3. Metropolis algorithm

4. Many particle systems $\# 10^{30}$.

5. Kolmogorov discrepancy $D_N \sim c\sqrt{N}$

6. Dynamical Systems $T^t x_0 \Rightarrow x_t$

7. Classification of Dynamical Systems:

K - systems, Entropy.

8. $D_N(T)$; $\tau_0 = 1/h(T)$

9. High Dimensional K-systems

10. Period of Generator on Galois field

$$\tau = p^{\mathcal{N}}-1/p-1.$$

11. Examples

$$p = 2^{61}-1 \quad \mathcal{N} = 256$$

$$\tau \simeq 2^{15000}$$

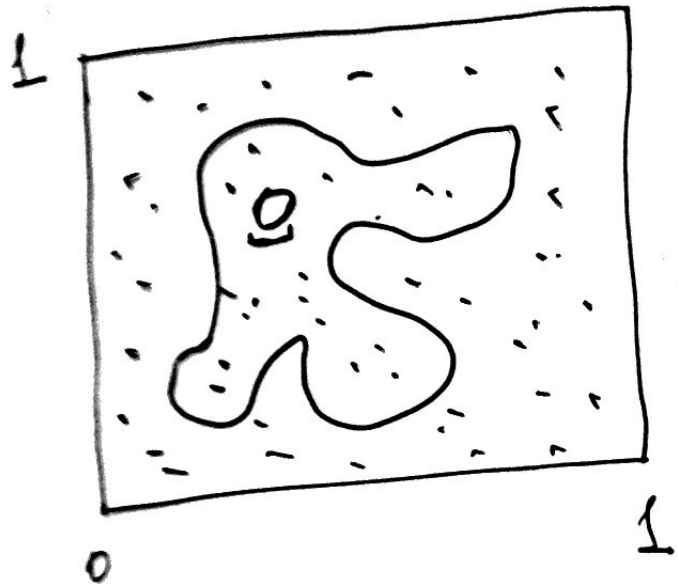
12.

Publications.

1. J. Comp. Phys. 97 (1991) 566; Preprint EPI-1986
2. J. Comp. Phys. 97 (1991) 573; Preprint EPI-1986.
3. Preprint EPI-1986 „ Sinai Billiards as Pseudorandom number generators".
4. Int. J. Mod. Phys. C 7 (1996) 73 „ K-system generators on Galois field".
5. F. James, Chaos, Solitons & Fractals 6 (1995) 221 „ Chaos and Randomness"
6. M. Lüscher „ A portable high-quality random number generator ..." Comp. Phys. Comm. 79 (1994) 100
7. F. James „ RANLUX: A Fortran implementation of RNG" Comp. Phys. Comm 1994

In Yerevan: collaboration was with N. Akopov - at DESY now.

Monte Carlo method



Π^2

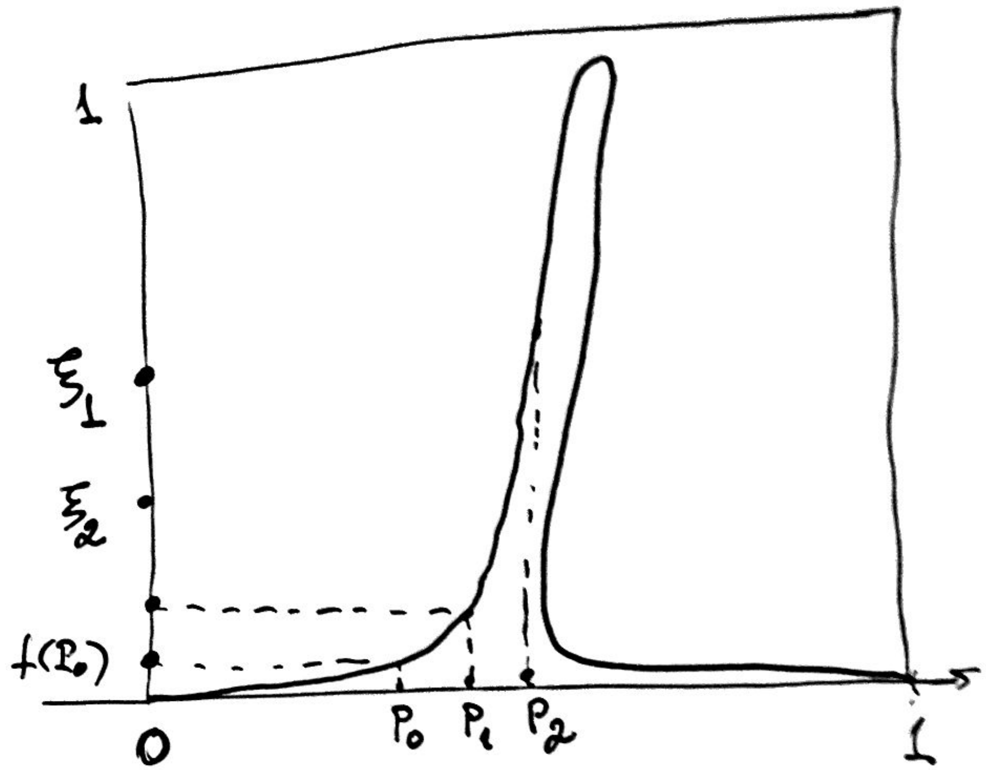
The area of Ω ?

In probability theory:

$\xi \in \Pi^2 \qquad \rho(\xi) = 1$

$$\text{Area } \Omega = \frac{\#\text{ inside } \Omega}{N}$$

Metropolis algorithm.



The area is small

$p \in [0,1]$ $\xi \in [0,1]$

take p_1 and ξ_1 and compear

$f(P_1)$ ξ_1

if $f(P_1) < \xi_1$ then stay at P_0 and generate P_2 ξ_2

if $f(P_2) > \xi_2$ then jump to P_2. and so on

$$\rho(P) = f(P)$$

$$\int_{\Pi} f(P)\, dP = \frac{1}{N}\sum_{i=0}^{N-1} P_i$$

$$\int_{\Pi} f(P)\cdot g(P)\, dP = \frac{1}{N}\sum_{i=0}^{N-1} g(P_i)$$

$$Z(\beta) = \int e^{-\beta V(x_1 \dots x_N)}\, d^D x_1 \dots d^D x_N$$

$D=3 \qquad N = 10^{30}$

$$\rho \equiv e^{-\beta V(x_1, \dots, x_N)}$$

3D Ising 1979 Parisi

1985 Migdal

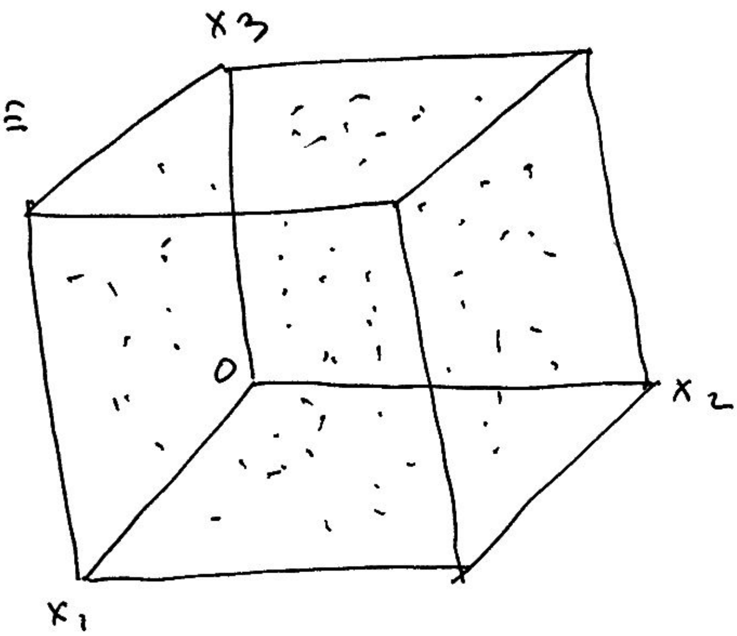
K-system generator of Pseudorandom Numbers.

$$P_0, P_1, P_3, \dots, P_N$$

$$P = (x_1, x_2, \dots, x_d)$$

$$0 \le x_i \le 1.$$

$\Pi^d \equiv$



Quality of pseudorandom numbers?

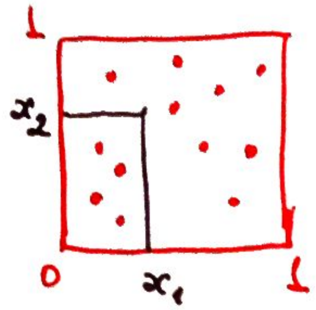
Kolmogorov discrepancy D_N

$$D_N(P_0, \dots P_{N-1}) = \sup_{\{P\}} \left| N \cdot x_1 \cdots x_s - A \right|$$

A - is number of points P_i with coordinates $0 \le x_1^{(i)} \le x_1$; .... ; $0 \le x_s^{(i)} \le x_s$

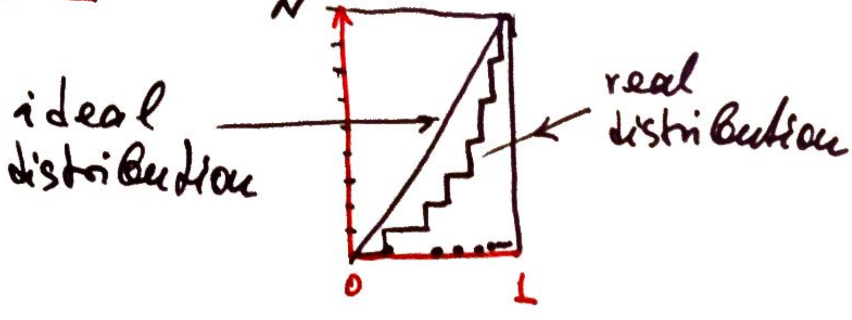
$N x_1 \cdots x_s$ - is the number of points for ideal uniform distribution.

$s = 2$

$\Pi^2 \equiv$ 

$N = 12$
$A = 4$

$s = 1$



<u>Theorem.</u>

$$\left| \frac{1}{N} \sum_{k=0}^{N-1} f(P_k) - \int_{\Pi^s} f(P)\,dP \right| \le \text{Const.} \frac{D_N}{N}$$

D_N - estimates a maximal diviation of real distribution of points from ideal one. $D_N \le N$.

One should generate sequence P_K, so that D_N would grow as slowly as possible.

Dynamical origin of P_K

α) For random quantity ξ, $\rho(\xi) = 1$, then by central limiting theorem

$$D_N(\xi) \approx \sqrt{N}$$

so

$$\left| \frac{1}{N} \sum_{K=0}^{N-1} f(P_K) - \int f(P)\, dP \right| \leq \text{Const} \frac{1}{\sqrt{N}}$$

β) trajectory of dynamical system T

$$P_1 = TP_0 \;, \quad P_2 = TP_1 = T^2 P_0 \;, \ldots, \; P_{N-1} = T^{N-1} P_0$$

and Π^{D} - as the phase space of the dynamical system T, Liouville theorem should holds!

The rate of convergence is provided by the dynamical properties of a system T

$$\left| \frac{1}{N} \sum_{K=0}^{N-1} f(T^K P_0) - \int f(P)\, dP \right| \leq \text{Const.} \frac{D_N(T)}{N}$$

How to get the best rate of convergence? $D_N(T)$

1. Area preserving map of the phase space M

$$M \overset{T^t}{\longmapsto} M \qquad T^t A = A_t$$

$$T^t x_0 = x_t$$

in classical mechanics $x = \binom{q}{p}$.

2. Classification of the map.

i) <u>ergodic if</u>

$$\lim_{t\to\infty} \frac{1}{t}\int dt\, \mu[T^t A \cap B] = \mu[A]\cdot\mu[B].$$

ii) <u>mixing if</u>

$$\lim_{t\to\infty} \mu[T^t A \cap B] = \mu[A]\cdot\mu[B]$$

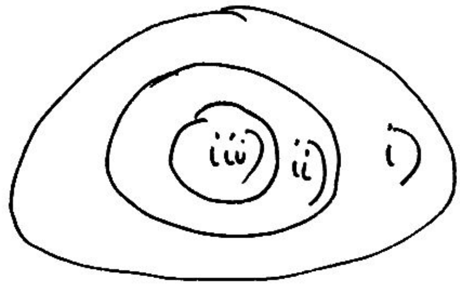
iii) <u>n-fold mixing</u>

$$\lim_{t_1 \ldots t_n\to\infty} \mu[A_0 \cap T^{t_1} A_1 \cap T^{t_2+t_1} A_2 \cap \cdots T^{t_n+\ldots t_1} A_n]$$

$$= \mu[A_1] \cdots \mu[A_n].$$

There is hierarchy of systems

iii) $\supset$ ii) $\supset$ i)



iv) $n \to \infty$ mixing of any multiplicity

v) K-systems

Split-up $\xi = \{C\}$: $\bigcup_{\xi \in C} C = M$, $C' \cap C'' = \phi$

α) $\bigvee_{-\infty}^{+\infty} T^t \xi = \epsilon$ split-up into separate points of M

β) $\bigwedge_{-\infty}^{+\infty} T^t \xi = \nu$ split-up consisting of M

v) $\supset$ iv) $\supset$ iii) $\supset$ ii) $\supset$ i)

K-systems have mixing of any multiplicity n –

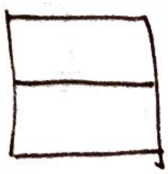
The best statistical property among all dynamical systems!

$h(T)$ – called the Kolmogorov entropy

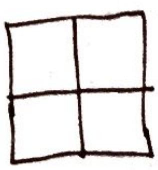
$$0 \le h(T) \le \infty$$

the entropy of $\xi = \{C\}$ is $H(\xi)$

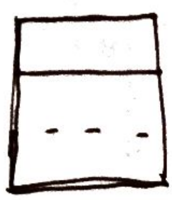
$$H = -\sum_{C\in\xi} \mu[C] \ln \mu[C]$$



$$H = -\frac{1}{2}\ln\frac{1}{2} - \frac{1}{2}\ln\frac{1}{2} = -\ln\frac{1}{2} = \ln 2$$



$$H = -\frac{1}{4}\ln\frac{1}{4} - \frac{1}{4}\ln\frac{1}{4} \cdots = -\ln\frac{1}{4} = 2\ln 2$$



$$H = -\frac{1}{3}\ln\frac{1}{3} - \frac{2}{3}\ln\frac{2}{3} = -\ln\frac{1}{3} - \frac{2}{3}\ln 2 =$$
$$= \ln 3 - \frac{2}{3}\ln 2$$

if many splits $\xi_1, \dots \xi_\alpha, \dots$

$$H\left(\bigvee_\alpha \xi_\alpha\right) = -\sum \mu\left[\bigcap_\alpha C_\alpha\right] \ln \mu\left[\bigcap_\alpha C_\alpha\right]$$

$$T^{t=1} = T$$

$$\xi \;,\; T\xi \;,\; T^2\xi \;, \ldots\ldots$$

$$H_n(T,\xi) = H(\xi \vee T\xi \vee T^2\xi \ldots \vee T^n\xi)$$

$$h(T) = \sup_{\xi} \lim_{n\to\infty} \frac{1}{n} H(\xi \vee T\xi \vee \ldots \vee T^n\xi)$$

$H_n(T,\xi)$ – quantity of information during the time $t = n$.

$h(T,\xi)$ – information per unit time.

Another definition $\quad f \in L_2(M)$

$$U^t f(x) = f(T^t x)$$

U^t as one parameter unitary operator, all $|\lambda_i| = 1$.

i) ii) … v) – are spectral properties.

countable-multiple Lebesgue

Mixing, n-fold mixing and K-systems

$$\begin{pmatrix}\text{property} \\ \text{of} \\ \text{relaxation}\end{pmatrix} \longrightarrow \begin{pmatrix}\text{to uniform} \\ \text{distribution}\end{pmatrix}$$

Relaxation of K-systems is most rapid because of their exponential instability.

$$\begin{pmatrix}\text{Slow growth of} \\ \text{the discrepancy} \\ D_N(T)\end{pmatrix} \equiv \begin{pmatrix}\text{quick relaxation} \\ \text{of dynamical} \\ \text{system } T\end{pmatrix}$$

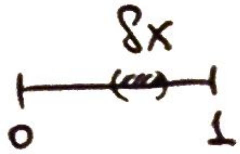
Exp. $\qquad P_K = r\, P_{K-1} \mod 1$

$$R_N = \frac{\langle (P^{L+N} - \langle P^{L+N}\rangle)(P^L - \langle P^L\rangle)\rangle}{\langle (P^L - \langle P^L\rangle)^2\rangle} \sim e^{-N \ln r}$$

Scale of correlation splitting

$$\tau_0 = \frac{1}{\ln r}$$

$$\begin{pmatrix}\text{time of uniform fill} \\ \text{of } [0,1] \text{ from } \delta x\end{pmatrix} = \tau_0 \ln (1/\delta x)$$



Exp. Anosov K- systems.

$$P_k = T P_{k-1} \qquad T = \| a_{kl} \|$$

α) $\det \| a_{kl} \| = 1$

β) $|\lambda_k| \neq 1$

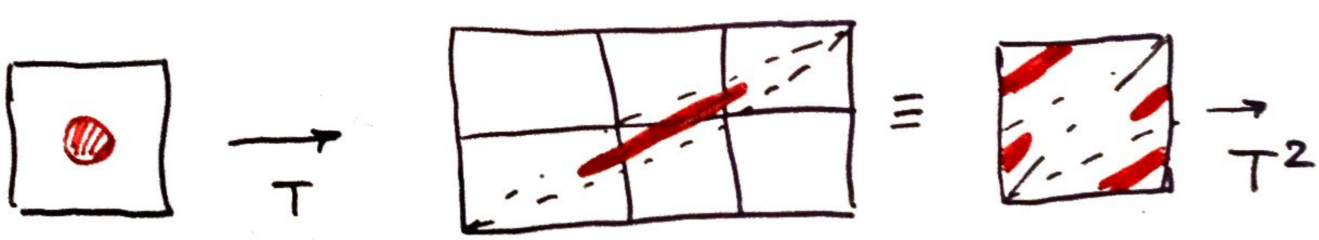
entropy $\quad h(T) = \sum\limits_{|\lambda|>1} \ln |\lambda_k|$

correlation splitting time

$$\tau_0 = \frac{1}{h(T)} = \frac{1}{\sum\limits_{|\lambda|>1} \ln |\lambda_k|}$$

$D = 2$

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}_k = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}_{k-1}$$



$$\lambda_{1,2} = \frac{3 \pm \sqrt{5}}{2} \qquad h(T) = \ln \frac{3+\sqrt{5}}{2}$$

High dimensional K-systems.

$$T_2 = \begin{vmatrix} 2 & 1 \\ 1 & 1 \end{vmatrix} \qquad T_3 = \begin{vmatrix} 2 & 2 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 1 \end{vmatrix}$$

$$T_4 = \begin{vmatrix} 2 & 3 & 4 & 1 \\ 1 & 2 & 2 & 1 \\ 1 & 1 & 2 & 1 \\ 1 & 1 & 1 & 1 \end{vmatrix} \quad \cdots \quad T_d = \begin{vmatrix} 2 & 3 & 4 & \cdots & d & 1 \\ 1 & 2 & 3 & \cdots & d-1 & 1 \\ 1 & 1 & 2 & \cdots & d-2 & 1 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & 1 & 1 & & 2 & 1 \\ 1 & 1 & 1 & & 1 & 1 \end{vmatrix}$$

T_{170} $\qquad \lambda_{max} \simeq 1539.9 \qquad h(T) = 108.9$

N	1	2	....	10	$\times 10^5$
$D_N/\sqrt{N}$	1.714	- -	- .	3,302	
$D_N/\sqrt{N}$	1.233	- - -	.	1,102	

The entroopy $h(\tau)$ defines the number $\pi(\tau)$ of periodic trajectoories with period less or equal τ

$$\pi(\tau) \longrightarrow \frac{e^{h \cdot \tau}}{h \cdot \tau}$$

in T_{170}

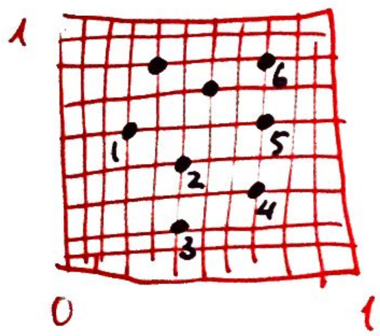
$$\pi(\tau) \longrightarrow \frac{e^{109 \cdot \tau}}{109 \cdot \tau} \quad !$$

Only periodic trajectories can be simulated on a computer.

The periodic trajectories of K-system.

If $P_0 = \left(\frac{q_1}{p_1}; \frac{q_2}{p_2}; \cdots \frac{q_D}{p_D}\right)$ $\quad T = \| a_{ik} \|$

$\| a_{ik}$ - are integer and q_i, p_i also then $P_0 = T^{\tau} P_0$ is periodic trajectory with period τ.



rational sublattice

If $P_0 = \left(\frac{q_1}{p}; \frac{q_2}{p}; \cdots \frac{q_D}{p}\right)$

$0 \leq q_i \leq p$

then trajectory will stay on the same sublattice.

The period τ_p - on sublattice $\leq p^D$

$$\frac{q_i^{(k+1)}}{p} = \sum_j a_{ij} \frac{q_j^{(k)}}{p} \quad \text{mod } 1$$

is equivalent to

$$q_i^{(k+1)} = \sum_j a_{ij} q_j^{(k)} \quad \text{mod } p$$

If p - is prime number then

q_i - belongs to Galois field $GF[p]$
$\{0, 1, \dots, p-1\}$

$GF[3]$ $\{0, 1, 2\}$ $g = 2$ $p = 3$

$g=2$ $g^2 = 4 = 1$

$GF[5]$ $\{0, 1, 2, 3, 4\}$ $g = 3$ $p = 5$

$g=3$ $g^2 = 9 = 4$ $g^3 = 2$ $g^4 = 1$

---

g - is a primitive element of $GF[p]$

$$g^{p-1} = 1 \mod p.$$

i) If eigenvalue λ of $\|a_{ik}\|$ coincides with primitive element g then maximal period $\tau_p = p-1$.

ii) If eigenvalue λ coincides with primitive element of quadratic expension $GF[\sqrt{p}]$, then maximal period $\tau_p = p^2-1$

$GF[\sqrt{3}]$ $\qquad g = 2 \qquad h = \sqrt{2}$

$a + b \cdot h \qquad a, b \in GF[3]$

$w = 1 + \sqrt{2}$

$w^2 = 2\sqrt{2}$

$w^3 = 1 + 2\sqrt{2}$

$w^4 = 2$

$w^5 = 2 + 2\sqrt{2}$

$w^6 = \sqrt{2}$

$w^7 = 2 + 2\sqrt{2}$

$w^8 = 1$

$\tau_3 = 3^2 - 1 = 9$

$x^2 - 2 = 0$

$x = \sqrt{2}$

---

iii) If λ coinside with D-dim. expension of Galois field $GF[\sqrt[D]{p}]$ then the $\tau_p = p^D - 1$

the elements of $GF[\sqrt[D]{p}]$ have the form

$$a + bh + \dots + e h^{D-1}$$

$$a, b, \dots e, \in GF[p]$$

h - is primitive element of $GF[\sqrt[D]{p}]$.

The period is:

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

If one use the largest Mersenne number

$$p = 2^{61} - 1$$

and dimension of the generator $N = 256$

one can get:

$$\tau \approx 2^{61 \cdot 255} = 2^{15555}$$

In 2013 the largest known prime number is:

$$p = 2^{57.885.161} - 1$$

by „Great Internet Mersenne Prime Search"