10. Generating random numbers

Recap:	method	physics
1.	$\int dx$, $\frac{d}{dx}$, ODEs	classical mechanics
2.	roots $\rightsquigarrow$ iteration	bifurcation & chaos
3.	eigenvalue problems	quantum mechanics
we are here 4.	random numbers ↳ Monte-Carlos sim.	} statististical physics
5.	Partial Diff. Equations	field theory

10.1. Random vs. pseudo-random

Computer is deterministic $\rightsquigarrow$ no real random numbers
BUT we encountered deterministic chaos, i.e. in logistic map.
"real" random processes only in QM
→ Hardware Random Number Generators use thermal noise in semiconductors or radio active decays.

10.2. Pseudo RNG = PRNG

- Generate sequence of equally distributed numbers r_n from initial value called seed
- same seed same sequence ⟶ reproducible
- repeat after the period length
  ↳ For cryptography it has to be hard to predict r_{n+1} from r_n.

10.2.1. linear congruential generator (LCG)

Iteration of $\boxed{r_{n+1} = (a r_n + c) \bmod m}$

for $a, c, m \in \mathbb{N}$ remainder after /m

- period lenght $\leq m$
- $a(m-1) < 2^{32}$ or 2^{64} to avoid overflow

example $a = 7^5 = 16807$, $c = 0$ and $m = 2^{32} - 1$

subclass called multiplicative LCG

Quality criteria : - speed :-)
- period length $(2^{32} - 2) \sim 10^9$:-|
- no correlation between :-C

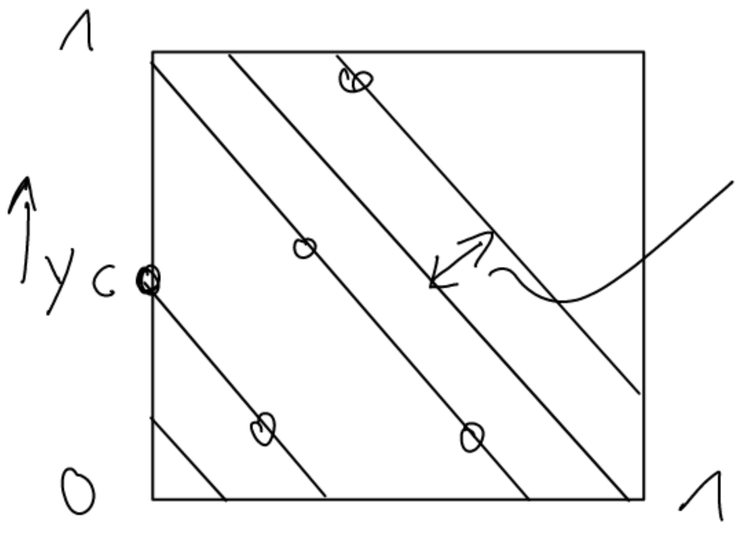
Marsaglia-effect $(r_n, \ldots, r_{n+k-1})$, normalized to the interval $[0,1]$ by

$r'_n = \frac{r_n}{m-1}$ are located on Hyperplanes in the k-dim. unit cube $[0,1]^k$.

↳ at $k = 2$ without mod on line

$(x, y) = x(1, a) + (0, c)$

$(r_n, r_{n+1}) = r_n(1, a) + (0, c) + k_n m (0, 1)$



max. distance between planes

⇒ define $v_k = 1 / d_k$ (larger is better)

Upper bound $\boxed{\vartheta_k < m^{1/k}}$, in diffused points in k-cube

but usually much worse.

Trick: combine multiple LCGs ⇝ Wichmann-Hill gen.

$$x_n = [171\, x_{n-1}] \bmod 30296$$
$$y_n = [172\, y_{n-1}] \bmod 30307$$
$$z_n = [170\, z_{n-1}] \bmod 30323$$
$$u_n = \left[\frac{x_n}{30269} + \frac{y_n}{30307} + \frac{z_n}{30323}\right] \bmod 1$$

10.2.2. Xor-shift generator

- Xor $(a \oplus b)$ =

b \ a	0	1
0	0	1
1	1	0

(apply bitwise)

- shift

example xor shift 32

even better, combination of different PRNGs

i.e. output of $PRNG_1$ as seed for $PRNG_2$

10.3. Different probability distributions

Output of PRNG is equally distributed, i.e. in $[0,1)$

$$p(x) = \begin{cases} 1 & \text{for } 0 \leq x < 1 \\ 0 & \text{otherwise} \end{cases}$$

How to get Gauss, ..., distribution?

10.3.1. Transformation and inversion method

Apply function $f(x) = y$. The

$$|\tilde{p}(y)\,dy| = |p(x)\,dx| \quad \text{or} \quad \boxed{\tilde{p}(y) = p(x)\left|\frac{dx}{dy}\right|}$$

examples: • $y = -\frac{1}{\lambda}\ln x \rightsquigarrow x = e^{-\lambda y}$

$\tilde{p}(y) = \lambda e^{-\lambda y}$ exponential distribution

10.3.2. Gauss distribution

1-dim. transformation meth. does not work

$\rightsquigarrow$ 2-dim. $\tilde{p}(y_1, y_2) = p(x_1, x_2)\left|\frac{\partial(x_1, x_2)}{\partial(y_1, y_2)}\right|$

with

$$\left|\frac{\partial(x_1, x_2)}{\partial(y_1, y_2)}\right| = \left(\frac{1}{\sqrt{2\pi}} e^{-y_1^2/2}\right)\left(\frac{1}{\sqrt{2\pi}} e^{-y_2^2/2}\right)$$

$\rightsquigarrow$

$$\boxed{\begin{aligned} y_1 &= \sqrt{-2\ln x_1}\cos(2\pi x_2) \\ y_2 &= \sqrt{-2\ln x_1}\sin(2\pi x_2) \end{aligned}}$$