An introduction to Monte Carlo methods

Elena Akhmatskaya and Enrico Scalas

Bilbao, 15-19 April 2013

(Pseudo-)random number generators

Enrico Scalas

Bilbao, 15 April 2013

(Pseudo-)random number generators

Pre-requisites:

- Elementary probability theory
- Random variables
- Discrete distributions (Bernoulli, Binomial, Poisson, …)
- Continuous distributions (Uniform, Normal, Exponential, ...)

(Pseudo-)random number generators

History

The Monte Carlo method was introduced in connection to the development of nuclear weapons, especially to study the trajectory of neutrons through materials interacting with nuclei along the way. Part of the work leading to thermonuclear bombs is still classified. The Monte Carlo method was declassified in the 1950s. (see Harlow and Metropolis 1983).

(Pseudo-)random number generators

Two problems:

1. Generate a sequence of i.i.d. random numbers distributed according to $U[0,1]$;

2. Given an i.i.d. sequence $U_1, U_2, \ldots \sim U[0,1]$ and a target distribution F on $\mathbb{R}^k$ find $m \geq k$ and a deterministic function $h : [0,1]^m \to \mathbb{R}^k$ such that $h(U_1, \ldots, U_m) \sim F$. This means: generate a random variable or vector with distribution F.

(Pseudo-)random number generators

Problem 1 can be further specified.

1a. The relative frequency

$$\frac{N\left(\left\{1 \le i \le n : U_i \in [0,b]\right\}\right)}{n}$$

must converge to b for $n \to \infty$.

1b. The pairs $(U_1, U_2), \ldots, (U_n, U_{n+1}), \ldots$ should be uniformly distributed in $[0,1]^2$.

1c. For every $k \ge 1$, the k-tuples

$$\left\{\left(U_i, U_{i+1}, \ldots, U_{i+k-1}\right)\right\}_{i \ge 1}$$

should be uniformly distributed in $[0,1]^k$.

(Pseudo-)random number generators

Problem 1 can be tackled by means of a deterministic recurrence relation

$$X_{i+1} = f\left(X_i, X_{i-1}, \ldots, X_{i-s}\right), i \geq s, s \geq 0$$

starting from a *seed*

$$\left(X_s, X_{s-1}, \ldots, X_0\right) \in \mathbb{R}^{s+1}.$$

If $0 \leq X_i \leq K, \forall i$, one takes $U_i = X_i / K.$

A *good* pseudo-random rumber generator must satisfy statistical tests of uniformity and independence.

(Pseudo-)random number generators

Example: The midsquare method (by Von Neumann)

Take an integer between 0 and 10000 and square it. The next number consists of the middle four digits of the square. If necessary add zeros to the left of the square, in order to get an 8-digit integer.

$$0 \le X_i \le 10^5, X_0 = 3457, (X_0)^2 = 11950849, X_1 = 9508, U_1 = 9508/10000 = 0.9508$$

$$X_1 = 9508, (X_1)^2 = 90402064, X_2 = 4020, U_2 = 4020/10000 = 0.4020$$

Many problems: 3792 is a fixed point (it has other fixed points). Many seeds lead to convergence to very short cycles. Seeds smaller than 100 converge to 0.

(Pseudo-)random number generators

Example: Fibonacci generators

$$X_{i+1} = (X_i + X_{i-1}) \bmod m \,, m \in \mathbb{N}, m \gg 1$$
$$U_i = X_i / m$$

In this case, one can prove that

$$\Pr(X_i < X_{i+1} < X_i) = 0$$

but this probability should be 1/6 for i.i.d. uniform random variables.

(Pseudo-)random number generators

Example: Linear congruential generators I

The (infamous) IBM RANDU algorithm

$$X_0 : \text{random seed}$$
$$X_{i+1} = 65539\, X_i \bmod 2^{31},$$
$$U_i = X_i / 2^{31}.$$

belongs to this class. In general

$$X_0 : \text{random seed}$$
$$X_{i+1} = (a\, X_i + c) \bmod m,$$
$$a, m \in \mathbb{N}^+, c \in \mathbb{N}$$
$$U_i = X_i / m.$$

These generators cannot have a period larger than *m.*

(Pseudo-)random number generators

Example: Linear congruential generators II

Theorem (Knuth, 1981)
The period of a linear congruential generator is m if and only if the following conditions hold true:

1. c and m are relatively prime,
2. every prime factor of m divides a-1, and
3. if 4 divides m, then 4 divides a-1.

So, if $m = 2^{31}$, to have this period, c must be odd and $a = 4k+1$, for some integer k greater than 1.

(Pseudo-)random number generators

Example: Linear congruential generators III

Knuth proved that the period of RANDU is 2^{29} if one starts from an odd seed. But RANDU fails to satisfy condition 1.c.

$$65539 = 2^{16} + 3$$
$$X_{i+1} = \left(2^{16} X_i + 2 X_i + X_i\right) \bmod 2^{31},$$
$$X_{i+2} = \left(6 X_{i+1} - 9 X_i\right) \bmod 2^{31}$$

Therefore $X_{i+2} - 6 X_{i+1} + 9 X_i$ is always divisible by 2^{31}.
Hence, one has $U_{i+2} - 6 U_{i+1} + 9 U_i \in \{-5, -4, \ldots, 9\}$.
The triples (U_i, U_{i+1}, U_{i+2}) lie in one of 15 parallel hyperplanes in $[0,1]^3$.

(Pseudo-)random number generators

Example: Marsaglia's generators

In 1995, Marsaglia suggested *multiply-with carry generators*.

$$X_{i+1} = (a\, X_i + C_i) \bmod m,$$
$$C_{i+i} = \text{floor}\left[(a\, X_i + C_i)/m\right]$$

as well as

$$X_{i+1} = 2^{13}\left(X_i + X_{i-1} + X_{i-2}\right) \bmod \left(2^{32} - 5\right),$$

a generator whose period is approximately 2^{96}.

(Pseudo-)random number generators

Problem 2 can be solved in several ways. Here is a list of strategies:

- Inversion method
- Rejection method
- Special methods
- Markov chain Monte Carlo (MCMC)

(Pseudo-)random number generators

Inversion method I

Suppose we are given a random variable with cumulative distribution function $F_X(x) = \Pr(X \le x)$.
If $U \sim U[0,1]$, setting $X = F_X^{-1}(U)$ solves the problem.

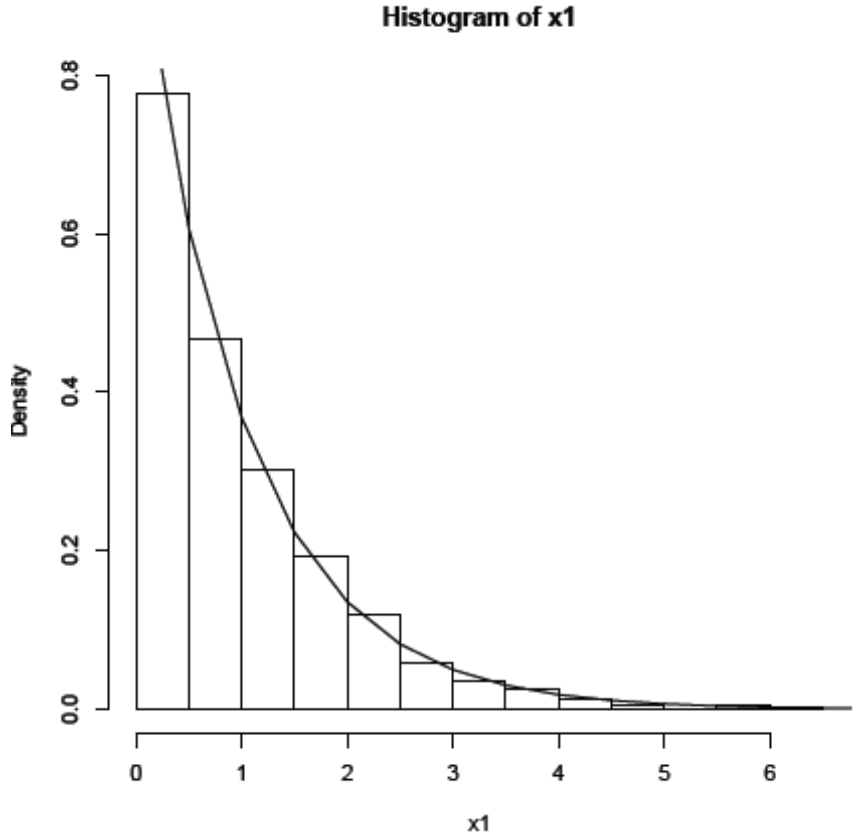
Example: The exponential distribution

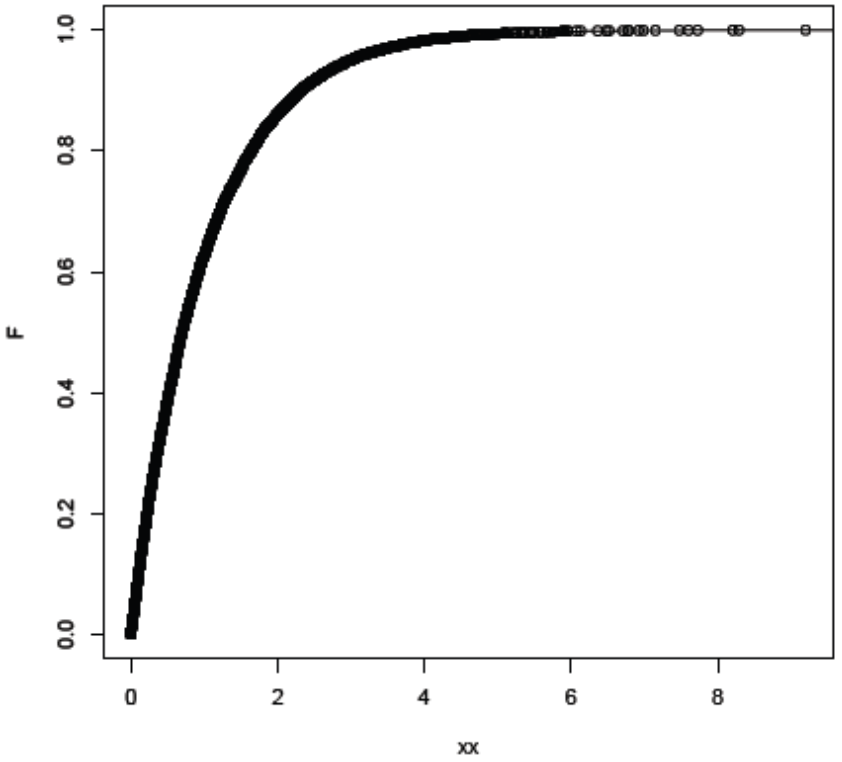
$$F_X(x) = 1 - \exp(-\lambda x), x \ge 0$$
$$F_X^{-1}(u) = \frac{-1}{\lambda} \log(1-u), 0 \le u \le 1$$
$$F_X^{-1}(1-u) = \frac{-1}{\lambda} \log(u)$$

(Pseudo-)random number generators

Inversion method II

Example: The exponential distribution





(Pseudo-)random number generators

Inversion method III

If the inverse cumulative distribution function is not available analytically, one can

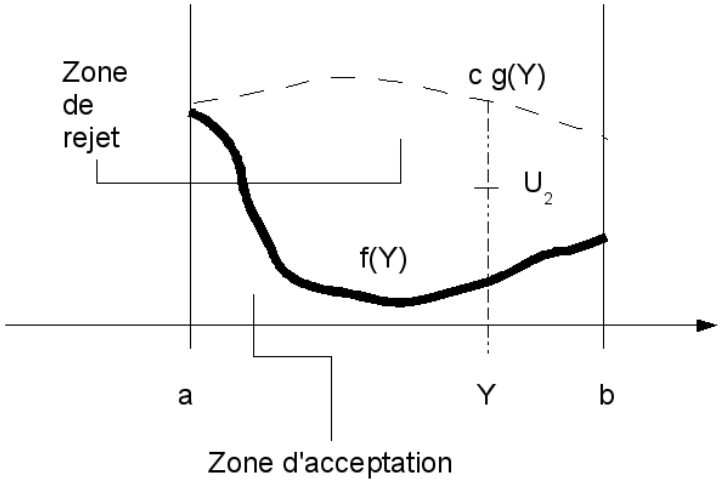
- Try to find a uniform approximant
- Use Newton's inversion method
- Use tables and linear (or other) interpolation

(Pseudo-)random number generators

Rejection method I

It is due to Von Neumann (again). The probability density function is needed.

$$c = \sup\{ f_X(x) : x \in [a, b] \}$$



Step 1: Generate $Y \sim U[a, b]$

Step 2: Generate $P \sim U[0, cg(Y)]$

Step 3: If $P \leq f_X(Y)$ set $X \leftarrow Y$ and stop, otherwise reject and go to Step 1.

(Pseudo-)random number generators

Rejection method II

Example: Wigner semi-circle law

$$f_X(x) = \frac{2}{\pi}\sqrt{1-x^2}, x \in [-1,1]$$

(Pseudo-)random number generators

Special methods I

For several important distributions, one can use special methods based on their properties and their relation with the uniform distribution.

We shall see two examples

- The Gamma distribution
- The normal distribution

(Pseudo-)random number generators

Special methods II

Example: The Gamma distribution

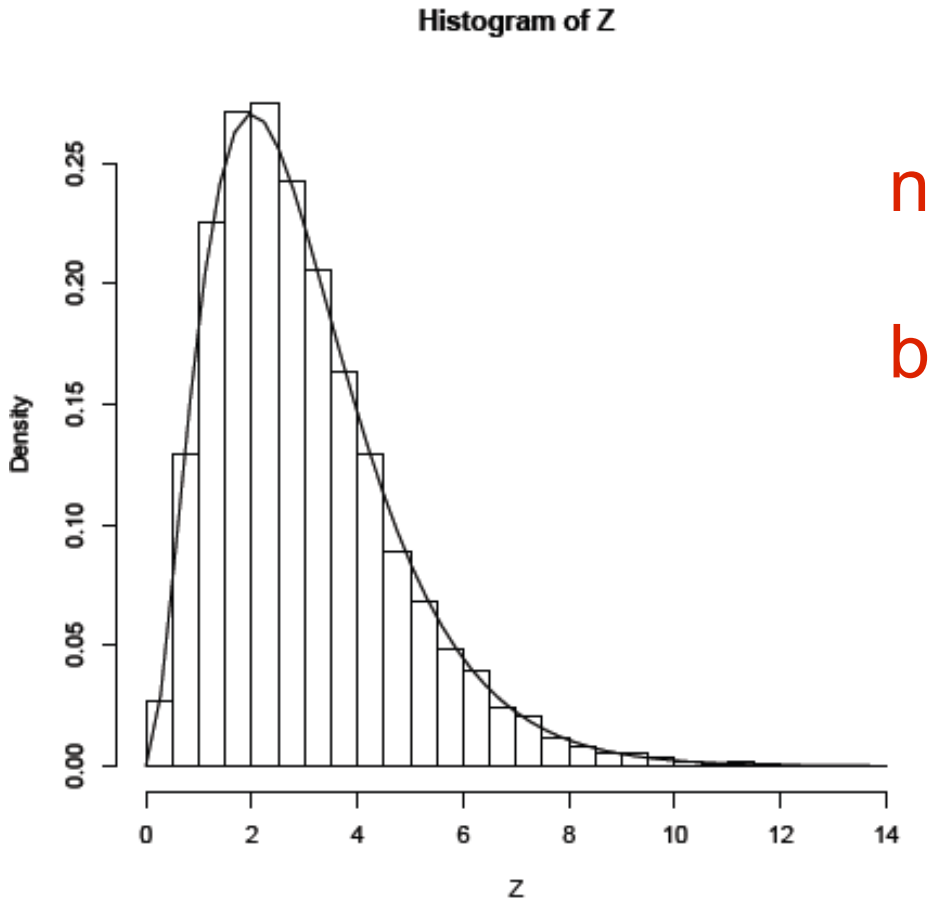
$$X \sim \text{Gamma}(a, b),\ a, b > 0$$
$$f_X(x; a, b) = b^a x^{a-1} \exp(-b x)/\Gamma(a),\ x \geq 0$$
$$f_X(x; n, b) = b^n x^{n-1} \exp(-b x)/(n-1)!,\ x \geq 0,\ n \in \mathbb{N}$$
$$X \sim \text{Gamma}(1, b) \sim \text{Exp}(b)$$

Proposition: Let $X_1, \ldots, X_k$ be a sequence of r.v.s s.t. $X_i \sim \text{Gamma}(a_i, b)$ then $Z = X_1 + \ldots + X_k \sim \text{Gamma}(a_1 + \ldots + a_k, b)$.
If $X_i \sim \text{Exp}(b), \forall i$ then $Z \sim \text{Gamma}(n, b)$.

(Pseudo-)random number generators

Special methods III

Example: The Gamma distribution



n=3

b=1

(Pseudo-)random number generators

Special methods IV

Example: The normal distribution

$$X \sim \mathrm{N}(\mu, \sigma), \sigma > 0$$

$$f_X(x; \mu, \sigma) = \frac{1}{\sqrt{2\pi}\sigma} \exp\left(\frac{-(x-\mu)^2}{2\sigma^2}\right), \; x \in \mathbb{R}$$

$$X \sim \mathrm{N}(0,1)$$

$$f_X(x; \mu, \sigma) = \frac{1}{\sqrt{2\pi}} \exp\left(\frac{-x^2}{2}\right), \; x \in \mathbb{R}$$

Proposition: Assume $X \sim \mathrm{N}(0,1)$ then $X^2 \sim \mathrm{Gamma}(1/2, 1/2)$.

(Pseudo-)random number generators

Special methods V

Example: Box-Muller method

$$X_1 \perp X_2, X_1, X_2 \sim \mathrm{N}(0,1),$$

$$f_{X_1, X_2}(x_1, x_2) = \frac{1}{2\pi} \exp\left(\frac{-(x_1^2 + x_2^2)}{2}\right), x_1, x_2 \in \mathbb{R}$$

$$R = \sqrt{X_1^2 + X_2^2}, \Theta = \widehat{(X_1, X_2)}$$

$$g_{R,\Theta}(r, \theta) = \frac{1}{2\pi} r \exp\left(\frac{-r^2}{2}\right), r > 0, \theta \in [0, 2\pi)$$

$$R^2 = X_1^2 + X_2^2 \sim \mathrm{Gamma}(1, 1/2), \Theta \sim U[0, 2\pi]$$

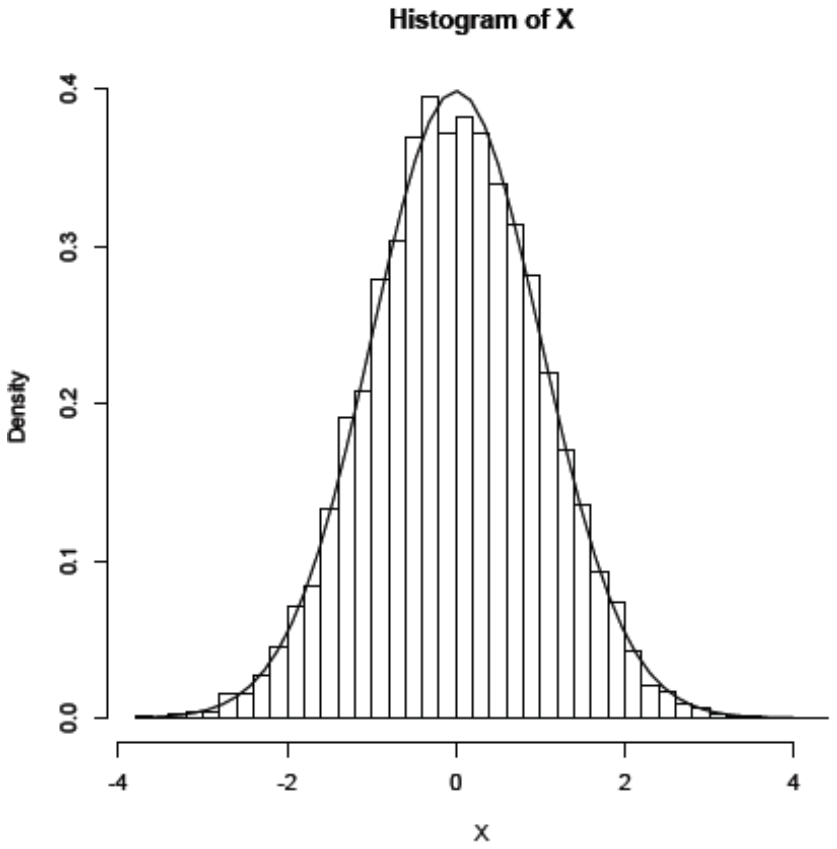
$$R \leftarrow \sqrt{-2 \log U_1}, \Theta \leftarrow 2\pi U_2$$

$$X_1 \leftarrow \sqrt{-2 \log U_1} \cos(2\pi U_2), X_2 \leftarrow \sqrt{-2 \log U_1} \sin(2\pi U_2).$$

(Pseudo-)random number generators

Special methods VI

Example: Box-Muller method



(Pseudo-)random number generators

Conclusions

The basic ingredients for Monte-Carlo simulations are

- A *good* pseudo-random number generator for uniform deviates in the interval [0,1];
- Efficient methods to generate deviates for any distribution of interest.

Both problems are still open to new research contributions

Exercise: What about discrete distributions?

(Pseudo-)random number generators

References

Devroye L (1986) Non-Uniform Random Variate Generation, Springer, New York NY.

Harlow F H, Metropolis N (1983) Computing & computers, weapons simulation leads to the computer era, Los Alamos Science **7**:132-141.

Kemeny J G, Laurie Snell J (1960) Finite Markov Chains, Van Nostrand, Princeton NJ.

Knuth D E (1981) The Art of Computer Programming, Volume 2: Seminumerical Algorithms, Addison Wesley, Reading MA.

Madras N (2002) Lectures on Monte Carlo Methods,Fields Institute Monographs, American mathematical Society, Providence RI.

Marsaglia G (1995) The Marsaglia Random Number CDROM including the Diehard Battery of Tests of Randomness: http://www.stat.fsu.edu/pub/diehard/.

Nahin P J (2008) Digital Dice, Princeton University Press, Princeton NJ.