Quasi-random number generator

Ines Meršak
Mentor: doc. dr. Dejan Velušček

21. 4. 2017

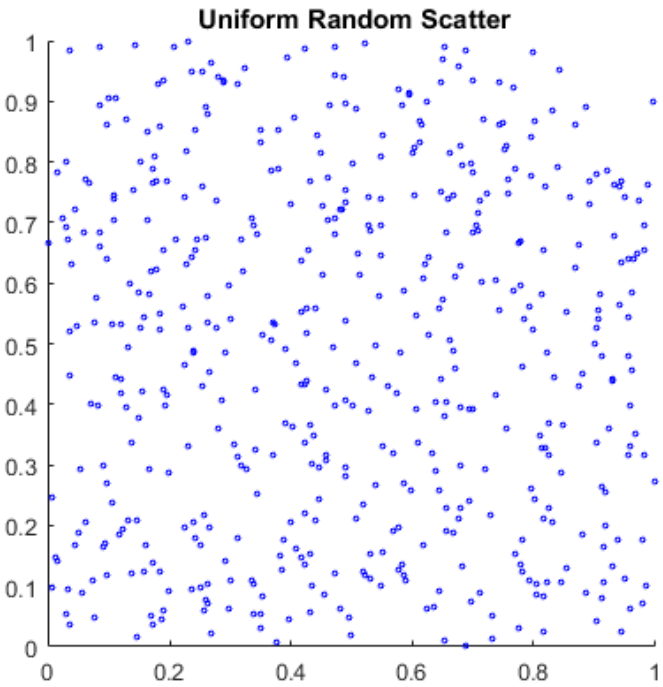
Pseudo-random vs. quasi-random

Pseudo-random number

- computer-generated number
- appears to be random
- generated by an entirely deterministic process

Quasi-random number

- low-discrepancy number
- taking previous draws into account



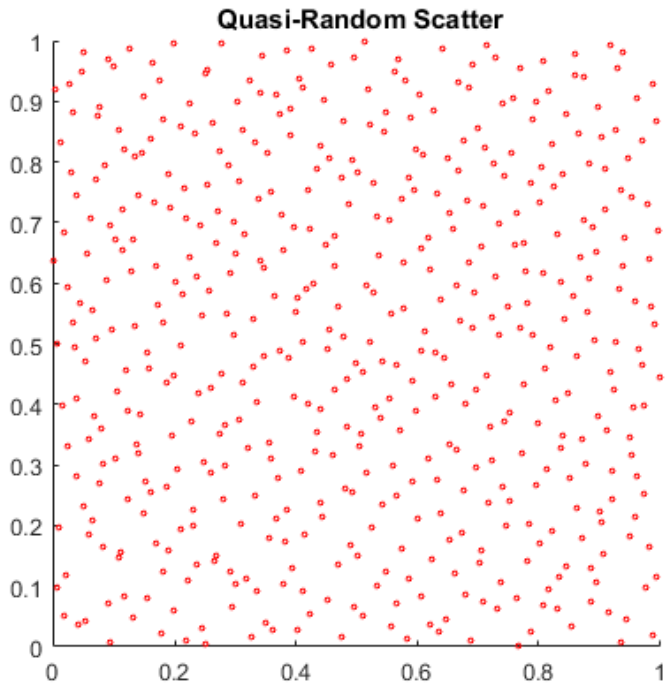


Figure: The comparison between pseudo- (left) and quasi-random numbers. (Source: `www.mathworks.com`.)

Usage

- useful in computational problems
- popular for financial Monte Carlo calculations
- asymptotic convergence is faster than when using pseudo-random numbers

Sobol' numbers

- a new unique generating integer $\gamma(n)$ for each new draw
- the generation is carried out on a set of integers in the interval $[1, 2^b - 1]$
- x_{nk} is the nth draw of Sobol' integer in dimension k
- a set of b direction integers for each dimension k
- for each dimension: select a primitive polynomial modulo two and calculate the direction integers using the coefficients of the polynomial and binary addition
- depending on which bits in the binary representation of $\gamma(n)$ are set, the direction integers are XORed to produce the Sobol' integer x_{nk}

Project timeline

Work done so far:

- reading the source material
- getting familiar with C++

Plan for the rest of the project:

- implement Sobol' number generator with Gray code (end of April)
- test the generator with quasi-Monte Carlo integration (first week of May)
- compare results with the parallel version (first week of May)