THE BEAUTY AND UTILITY OF PSEUDO-RANDOM NUMBERS:

Computer Art or Computer Science?

L. Yaroslavsky

Tampere, TICSP, July, 2000
Standard way for generating uniformly distributed pseudo-random numbers


\[ I_k = (C_1 I_{k-1} + C_2) \mod C_3 \]

The selection of $C_1$, $C_2$ and $C_3$ is a sort of an art
Metal links

(sqrt(13), pi, 7.9, pi)
Rainy day

(\pi, \sqrt{17}, 5, 3)
See waves

(sqrt(13), pi, 8, 3)
Rhapsody in blue

$\sqrt{13}, \pi, 14.82, 3$
Autumn

\[ C_1 = 7^5 = 16807; \ C_2 = 0; \ C_3 = 2^{31} - 1 = 2147483647 \]

**Period:** \( 2^{31} - 2 \approx 2,1 \cdot 10^9 \)

P. L’Ecuer, 1988, Communications of ACM, vol. 31, pp. 742-774:

Combining two different sequences with different periods:

\[
I_k = (I_k^1 + I_k^2) \mod (C_3^{\text{or}2}) ;
\]

\[
I_k^2 = (C_1^1 I_1^1 + C_2^1) \mod C_3^1 ;
\]

\[
I_k^2 = (C_1^2 I_1^2 + C_2^2) \mod C_3^2
\]

\[
C_3^1 = 2 \times 3 \times 7 \times 631 \times 81031 + 1 ;
\]

\[
C_3^2 = 2 \times 19 \times 31 \times 1019 \times 1789 + 1
\]

**Period:** \( \approx 2.3 \times 10^{18} \)

Press et al: We will pay $1000 to the first reader who will find a statistical test that this generator fails in nontrivial way.
One dollar
Results of test of histogram and correlations of Matlab’s rand.m
Color image (R=rand(128), G=rand(128), B=rand(128))

Pseudo-color display of R=rand(128) (colormap “prism”)
Side lobes of autocorrelation function (5 times smoothed by ones(3)) of Matlab’s rand.m
Generating pseudo-random numbers with Gaussian distribution: Transformation method


Pseudo-random numbers \( \{\xi\} \) with known distribution density \( p(\xi) \) can be converted into numbers \( \{\eta\} \) with distribution density \( p(\eta) \) by nonlinear transformation \( \eta = F(\xi) \) that is defined by differential equation:

\[
\frac{dF}{d\xi} = \frac{p(\xi)}{p(\eta)}
\]

Features:
- accuracy of output distribution depends on the accuracy of the input distribution
- if there are correlations in input numbers they propagate to the output
- additional computations are required if one needs to generate correlated p/r numbers
Convergence of variance of Matlab’s randn.m with increasing size of the array: several tests
Foggy twilight
Generating pseudo-random numbers with Gaussian distribution: FFT method


Generating p/r numbers with arbitrary distribution

Point wise multiplication by weight coefficients defined by the required correlation function

FFT

\[
\eta_l = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} w_k (\xi_k^r + i \xi_k^i) \exp \left( i 2\pi \frac{kl}{N} \right); \quad w_k = w_{N-k}.
\]

\[
\langle \eta_l^r \eta_m^r \rangle = \langle \eta_l^i \eta_m^i \rangle = \frac{1}{N} \sum_{k=0}^{N-1} w_k^2 \exp \left( i 2\pi \frac{k(l-m)}{N} \right)
\]
FFT method features:

- Output distribution tends to Gaussian with the increase of N however input distribution is
- Obtaining necessary correlation function in one step
- Low computational complexity (O(logN) per number)
- Input correlations do not propagate to output
Matlab randn.m and FFT method

Matlab randn 128x128

FFT method 128x128
Supernova
Clouds in the night
J. J. Heine, S. R. Deans, D. Gangadharan, L. P. Clarke, Multiresolution analysis of two-dimensional 1/f processes: approximation methods for random variable transformations, Optical Engineering, 38(9), 1505-1516 (Sept. 1999): “The intriguing aspect of the study is that a stationary stochastic process is used as the input to a linear filtering operation, and the output can be very irregular with a multimodal gray value histogram for certain values of “beta”. Wrong!!!
64*128*128 fract+pf(beta=1.5) images and their histogram displayed in normal plot.
CONCLUSION

• Generating pseudo-random numbers is a sort of an art
• Pseudo-random number generators are capable of providing nice looking images
• Pseudo-random number generators are capable of sometimes fooling people