Spectral Test of the MIXMAX Random Number Generators

Narek Martirosyan

A.I. Alikhanyan National Science Laboratory
Yerevan, Armenia

MIXMAX Workshop,
Athens, Greece, 03-04 July 2018

in Collaboration with:

Konstantin Savvidy and George Savvidy

arXiv:1806.05243

Uniform random variable

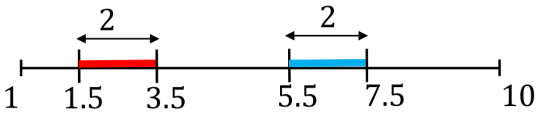
Random variable u is said to be uniformly distributed if it has constant probability distribution

$$f(u) = \begin{cases} c & \text{if } u \in [a, b] \\ 0 & \text{otherwise} \end{cases}$$

$$\int_{-\infty}^{\infty} f(u)du = \int_a^b f(u)du = 1 \implies c = \frac{1}{b-a}$$

$$Prob(u \in [c, d]) = \int_a^d \frac{1}{b-a}du - \int_a^c \frac{1}{b-a}du = \frac{d-c}{b-a}$$

intervals in $[a, b]$ are equally likely



Random number generator

Monte Carlo calculations require a sequence of numbers in $[0, 1]$ that are drawn from uniform distribution.

A random number generator (RNG) is aimed to produce a sequence of numbers that imitates independent observations of uniformly distributed random variable.

The oldest and the most used technique:
Linear congruential generators (LCG)

$$
\begin{aligned}
x_i = a(x_{i-1} + c) \mod p, \\
x_i \in \{0, 1, \dots, p-1\}, \\
u_i = \frac{x_i}{p} \in [0, 1)
\end{aligned}
$$

Desirable properties

- good statistical properties
- good underlying theory
- sufficiently long period
- lack of predictability
- fast performance
- cryptographic security

Uniformity measures: Kolmogorov-Smirnov test

$$u \sim U[0,1)$$

Cumulative Distribution Function(CDF)

$$F(x) \equiv Prob(u \leq x) = \int_0^x 1 du = x$$

Suppose you have a sequence of n numbers from RNG:

$$u_1, u_2, u_3, \ldots, u_n$$

Empirical Cumulative Distribution Function(ECDF)

$$F_n(x) = \frac{1}{n}(number\ of\ u_i \leq x)$$

If numbers were indeed drawn from $U[0,1)$ then

$$F_n(x) \to F(x), \quad \forall x$$

Uniformity measures: Kolmogorov-Smirnov test

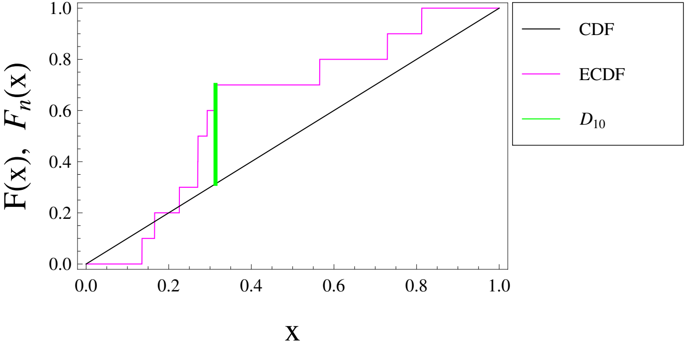
Glivenko-Canteli theorem

$$Prob(\lim_{n\to\infty} sup_x |F_n(x) - F(x)| = 0) = 1$$

$$D_n = sup_x |F_n(x) - F(x)|$$

Example:

0.271, 0.135, 0.293, 0.812, 0.729, 0.270, 0.225, 0.313, 0.565, 0.165



Uniformity measures: TestU01

"TestU01: a C library for empirical testing of random number generators",
L'Ecuyer and Simard, 2007.

Many empirical statistical tests are implemented in TestU01, including K-S test, random walks and many others.

Uniformity measures: TestU01

"TestU01: a C library for empirical testing of random number generators",
L'Ecuyer and Simard, 2007.

Many empirical statistical tests are implemented in TestU01, including K-S test, random walks and many others.

The outcome of TestU01 BigCrush suite applied on MIXMAX, Mersenne Twister using 64-bit computer with *Intel Core i*3 -4150 processor of clock speed 3.50×4 *GHz*.

PRNG	Total CPU time	BigCrush	p-value of fail
MIXMAX	$2h\,43m\,51s$	*passed*	—
MT	$3h\,19m\,27s$	3	$0.9990, 1-10^{-15}$

Uniformity distributed points

But we want to have also uniformly distributed tuples

$$(u_i, u_{i+1}, \ldots, u_{i+d-1}) \sim U[0,1)^d, \quad i = 1, 2, \ldots$$

$d = 2$

$$u_1, u_2, u_3, \ldots \implies (u_1, u_2), (u_2, u_3), \ldots$$

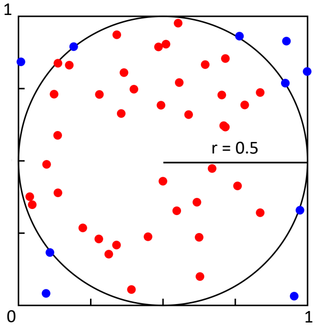
Uniformity distributed points

But we want to have also uniformly distributed tuples

$$(u_i, u_{i+1}, \dots, u_{i+d-1}) \sim U[0,1)^d, \quad i = 1, 2, \dots$$

$d = 2$:

$$u_1, u_2, u_3, \dots \implies (u_1, u_2), (u_2, u_3), \dots$$



$$\frac{S_{circle}}{S_{square}} = \frac{\pi r^2}{1} = \frac{\pi}{4}$$

$$\frac{S_{circle}}{S_{square}} \approx \frac{N_{circle}}{N_{total}} \implies \pi \approx 4\frac{N_{circle}}{N_{total}}$$

Lattice structure

"Random numbers fall mainly in the planes",
George Marsaglia, 1968.

$\pi_1 = (u_1, \ldots, u_d),\ \pi_2 = (u_2, \ldots, u_{d+1}),\ \pi_3 = (u_2, \ldots, u_{d+2}), \ldots$
All points lie in the set of parallel hyperplanes defined by

$$c_1 x_1 + c_2 x_2 + \ldots c_d x_d = 0, \pm 1, \pm 2, \ldots$$

where

$$c_1 + c_2 a + \ldots c_d a^{d-1} \equiv 0 \text{ } \mathit{modulo} \text{ } p$$

and there are at most

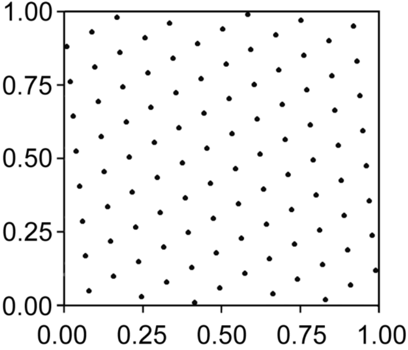
$$|c_1| + |c_2| + \ldots + |c_d|$$

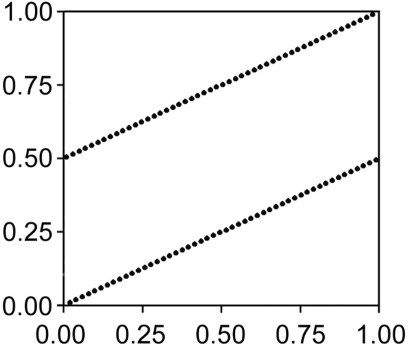
hyperplanes which intersect the unit d-dimensional hypercube.

Lattice structure

$d = 2$: all points (u_i, u_{i+1}) generated by LCGs:

$$x_i = 89x_{i-1}(mod\ 101) \qquad x_i = 51x_{i-1}(mod\ 101);$$
$$u_i = x_i/101$$





Quality of RNGs

- The big distance between hyperplanes (planes in 3d, lines in 2d) implies that the unit hypercube is mainly empty, hence the points are not uniformly distributed.
- The distance between adjacent hyperplanes can be used for the assessment of the quality of uniformity of d-dimensional points.
- But points can be covered by parallel hyperplanes in various ways, hence all possible coverings have to be considered.
- The spectral test determines the maximum distance between adjacent parallel hyperplanes over all possible coverings. The shorter the distance is, the better is the uniformity.

Lattice

A lattice is the set of all points (vectors) constructed as follows

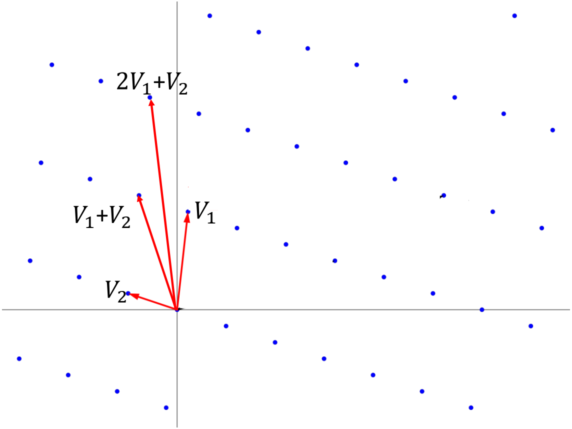
$$\wedge = \left\{ \mathbf{g} \in R^d \;\middle|\; \mathbf{g} = \sum_{i=1}^{m} z_i \mathbf{v}_i, \quad z_i \in Z \right\},$$

where $\mathbf{v}_1, \mathbf{v}_2 \ldots, \mathbf{v}_m \in R^d$ are m linearly independent vectors

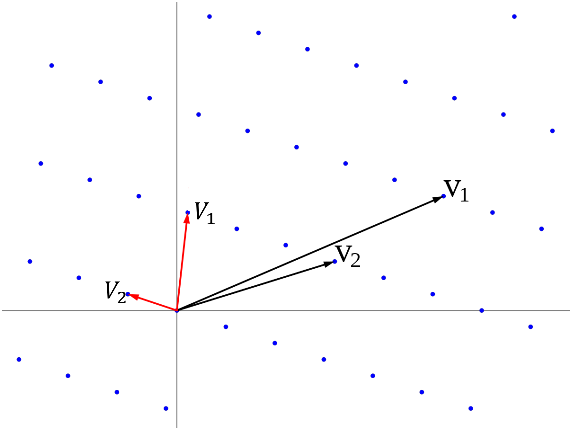
$$\mathbf{V} = \{\mathbf{v}_1, \mathbf{v}_2 \ldots, \mathbf{v}_m\} = \begin{pmatrix} v_1^{(1)} & v_2^{(1)} & \cdots & \cdots & \cdots & v_{m-1}^{(1)} & v_m^{(1)} \\ v_1^{(2)} & v_2^{(2)} & \cdots & \cdots & \cdots & v_{m-1}^{(2)} & v_m^{(2)} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ & & & \cdots & & & \\ v_1^{(d)} & v_2^{(d)} & \cdots & \cdots & \cdots & v_{m-1}^{(d)} & v_m^{(d)} \end{pmatrix}$$

Lattice

$$\wedge = \left\{ \mathbf{g} \in R^2 \;\middle|\; \mathbf{g} = z_1 \mathbf{v}_1 + z_2 \mathbf{v}_2, \quad z_1, z_2 \in Z \right\},$$



Lattice



$\mathbf{V}_1, \mathbf{V}_2 \in R^{d \times m}$ generate the same lattice if

$$\mathbf{V}_1 = \mathbf{V}_2 \mathbf{U}, \quad \mathbf{U} \in Z^{m \times m}, \quad det(\mathbf{U}) = \pm 1.$$

Dual lattice and distances between adjacent hyperplanes

The dual (or reciprocal) lattice $\wedge^\star$ is the set of vectors which have integer scalar product with any of the vector $\mathbf{g} \in R^d$ in $\wedge$:

$$\wedge^\star = \left\{ \mathbf{y} \in R^{*d} \;\mid\; \mathbf{y} \cdot \mathbf{g} = n \in Z, \;\; \mathbf{g} \in \wedge \right\}.$$

The dual lattice basis

$$\mathbf{V}^\star = \mathbf{V}(\mathbf{V}^T\mathbf{V})^{-1} \in R^{*d \times m},$$

If $\mathbf{V}$ is a square matrix (full rank lattices) then $\mathbf{V}^\star = (\mathbf{V}^T)^{-1}$.

The shortest vector in dual lattice

Each dual vector $\mathbf{y}$ defines a set of equally spaced parallel hyperplanes of the original lattice which are orthogonal to $\mathbf{y}$. The distance between adjacent hyperplanes is

$$l = \frac{1}{|\mathbf{y}|}$$

The spectral test reduces to the finding of the shortest vector $\lambda(\wedge^\star)$ in the dual lattice.

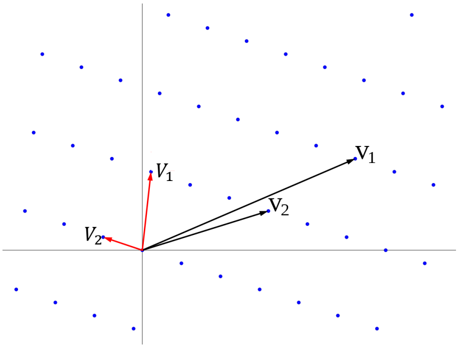
Construct the dual basis $\mathbf{V}^\star$ with $\mathbf{V}^\star = (\mathbf{V}^T)^{-1}$ and find the shortest vector in the dual space:

$$l = \frac{1}{\lambda_{min}}, \quad \text{where} \quad \lambda_{min} = \min_{\mathbf{y} \in \wedge^\star \setminus \{\mathbf{0}\}} |\mathbf{y}|.$$

TThe shortest vector problem (SVP)

"Factoring polynomials with rational coefficients",
A. K. Lenstra, H. W. Lenstra, Jr. and L. Lovász, 1982

The LLL algorithm makes basis vectors as orthogonal as possible with efficient way.



MIXMAX

The computer implementation of MIXMAX is of the form

$$\mathbf{x}_i = A\mathbf{x}_{i-1} \mod p$$

The generator produces N-dimensional vectors at each step i,

$$\mathbf{x}_i = (x_{i\ 1}, \ldots, x_{i\ N})$$

$$\mathbf{u}_i = \mathbf{x}_i / p$$

$$1)\ A = \lambda_1 \lambda_2 ... \lambda_N = 1, \qquad 2)\ \ |\lambda_i| \neq 1, \quad \forall\ \ i.$$

MIXMAX

"Spectrum and Entropy of C-systems. MIXMAX random number generator",
K. Savvidy and G. Savvidy, 2016

$$
\begin{pmatrix}
1 & 1 & 1 & 1 & \ldots & 1 & 1 \\
1 & 2 & 1 & 1 & \ldots & 1 & 1 \\
1 & m+2+s & 2 & 1 & \ldots & 1 & 1 \\
1 & 2m+2 & m+2 & 2 & \ldots & 1 & 1 \\
1 & 3m+2 & 2m+2 & m+2 & \ldots & 1 & 1 \\
 & & & \ldots & & & \\
1 & (N-2)m+2 & (N-3)m+2 & (N-4)m+2 & \ldots & m+2 & 2
\end{pmatrix}
$$

$N = 8,\ m = 2^{53} + 1,\ s = 0$
$N = 17,\ m = 2^{36} + 1,\ s = 0$
$N = 240,\ m = 2^{51} + 1,\ s = 487013230256099140$

What we study

The MXIMAX generator produces N-dimensional vectors at each step i, and in dimension $d = N$ it has resolution $\approx 2^{-61}$

$d > N$

$$\mathbf{g}_i = (\mathbf{u}_i, \mathbf{u}_{i+1}, \ldots, \mathbf{u}_{i+r-1}) \equiv (g_1, g_2, \ldots, g_{rN}) \in [0,1)^{rN}$$

Lattice basis of matrix LCGs

"The lattice structure of pseudo-random vectors generated by matrix generators",
L. Afflerbach and H. Grothe, 1988.

$$\mathbf{x}_i = A\mathbf{x}_{i-1} \mod p$$

$$\mathbf{g}_i = (\mathbf{u}_i, \mathbf{u}_{i+1}, \ldots, \mathbf{u}_{i+r-1})$$

$$\mathbf{V} = \begin{pmatrix} I/p & \mathbf{0} & \cdots & \mathbf{0} \\ A/p & I & \cdots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ A^{r-1}/p & \mathbf{0} & \cdots & I \end{pmatrix},$$

Lattice structure of MIXMAX

Having the basis we can learn everything about lattice structure of MIXMAX in dimensions $d > N$.

"Spectral Analysis of the MIXMAX Random Number Generators", P. L'Ecuyer, P. Wambergue, E. Bourceret, 2017.

Independently of the parameters N and s of the operator $A(N, s)$ three-parameter $A(N, s, m)$ family of operators, the shortest vector in the reduced dual lattice is $\sqrt{3}$, hence the spectral index is $l_{rN} = 1/\sqrt{3}$.

"A Priori Tests for the MIXMAX Random Number Generator"; S. Konitopoulos and K.G. Savvidy, 2018.

Lattice structure of MIXMAX

The lattice structure results from the relationships between certain coordinates of rN-dimensional points.

For example dual vector of length $\sqrt{3}$ corresponds to the relationship (L'Ecuyer et. al.)

$$g_i^{(2)} + g_i^{(N+1)} - g_i^{(N+2)} = \begin{cases} 0 \\ 1 \end{cases}$$

The relationship is absent if the first component of each generated MIXMAX vector is skipped.

Lattice structure of MIXMAX

Consider the parameters $N = 17$, $m = 2^{36} + 1$ and $s = 0$.

Taking $r = 2$ and skipping only the first coordinate of each output gives the lattice with spectral index

$$l_{2(N-1)} = 1.49 \cdot 10^{-8}.$$

$N = 240$, $m = 2^{32} + 1$ and $s = 271828282$.

$$l_{2(N-1)} = 7.6 \cdot 10^{-10}.$$