Random and pseudorandom numbers

Victor Kocheganov

September 12, 2013

Agenda

Monte Carlo

Figure: Monte Carlo city

Stochastic systems modeling and analysis

1. Queueing theory
2. Mathematical finance

Stochastic systems modeling and analysis

1. Queueing theory
2. Mathematical finance
3. Actuarial science

Stochastic systems modeling and analysis

1. Queueing theory
2. Mathematical finance
3. Actuarial science
4. Physics

Stochastic systems modeling and analysis

1. Queueing theory
2. Mathematical finance
3. Actuarial science
4. Physics

Decision theory (matrix games)

		Defender		
		(2,0)	(1,1)	(0,2)
	(2,0)	0	2/3	2/3
Attacker	(1,1)	1/3	0	2/3
	(0,2)	1/3	1/3	0

Decision theory (matrix games)

		Defender (2,0)	Defender (1,1)	Defender (0,2)
Attacker	(2,0)	0	2/3	2/3
Attacker	(1,1)	1/3	0	2/3
Attacker	(0,2)	1/3	1/3	0

Strategy $= (p_1, \quad , p_2, \quad p_3)$

Aesthetics

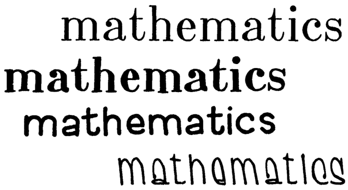

FIGURE 22.
A bit of randomness introduced into various styles of type.

"I think it can be said that the letters in this final example have a warmth and charm which makes it hard to believe that they were really generated by a computer following strict mathematical rules."

D.E. Knuth, Mathematical typography — Bull. Amer. Math. Soc. 1 (1979), 369

Numerical analysis

Denote $f(y) = \sum_{i=1}^{n} y_i^2$. Want to estimate

$$I = \int_0^1 dy_1 \ldots \int_0^1 f(y) dy_n$$

with estimators ($N = M^n$):

$$\tilde{I}_1 = \frac{1}{N} \sum_{j=1}^{N} f(\overline{x}_j),$$

where $\{\overline{x}_j\}_{1 \leqslant j \leqslant N}$ form uniform grid in $[0;1]^n$ cube and

$$\tilde{I}_2 = \frac{1}{N} \sum_{j=1}^{N} f(\overline{x}_j^{\prime}),$$

where $\overline{x}_j^{\prime}$ is uniform random point in j-th subcube.

Numerical analysis

Table: n=1

N	$\lvert I - \tilde{I}_1 \rvert$	$\lvert I - \tilde{I}_2 \rvert$
10^2	$5 * 10^{-3}$	$7 * 10^{-6}$
10^3	$5 * 10^{-4}$	$4 * 10^{-7}$
10^4	$5 * 10^{-5}$	$5 * 10^{-9}$
10^5	$5 * 10^{-6}$	$4 * 10^{-10}$
10^6	$5 * 10^{-7}$	$1 * 10^{-11}$
10^7	$5 * 10^{-8}$	$1 * 10^{-12}$

Table: n=2

N	$\lvert I - \tilde{I}_1 \rvert$	$\lvert I - \tilde{I}_2 \rvert$
10^2	10^{-1}	$6 * 10^{-5}$
10^4	10^{-2}	10^{-6}
10^6	10^{-3}	$5 * 10^{-7}$
10^8	10^{-4}	$3 * 10^{-9}$

Table: n=3

N	$\lvert I - \tilde{I}_1 \rvert$	$\lvert I - \tilde{I}_2 \rvert$
10^3	0.145	$2 * 10^{-3}$
10^6	0.0145	$6 * 10^{-6}$

Numerical analysis

Assume $f(\cdot)$ and $\frac{\partial f}{\partial x_k}$ are continuous and $\left|\frac{\partial f}{\partial x_k}\right| \leqslant L$, $1 \leqslant k \leqslant n$.
Then

Assertion 1

$$P\left(\left|I - \tilde{I}_2\right| \leqslant (nL/\varepsilon)N^{-1/2-1/n}\right) \geqslant 1 - \varepsilon^2, \quad 0 < \varepsilon < 1$$

and

Assertion 2

$\sup_f \left|I - \tilde{I}_1\right| \leqslant nLN^{-1/n}$

Quick sort

Consider array

$$(a[1], a[2], \dots, a[N])\,.$$

We want to sort it in direct (increasing) order.

```
// begin with QuickSort(a, 1, N)
QuickSort(a, begin, end)
if begin < end
  then q = Partition (a,begin, end);
  QuickSort(a, begin, q-1);
  QuickSort(a, q+1, end);
```

```
Partition(a,begin,end)
 x = a[end];
 i = begin - 1;
 for j = begin to (end - 1)
   if a[j] <= x
     then i = i+1;
     exchange a[i] and a[j]
 exchange a[i+1] and a[end];
 return i + 1;
```

Quick sort

$T(N) = ?$

```
// begin with QuickSort(a, 1, N)
QuickSort(a, begin, end)
if begin < end
  then q = Partition (a,begin, end);  // (end - begin) <= (N - 1) iterations
  QuickSort(a, begin, q-1);           // T(q -  begin) <= T(N - 1) iterations
  QuickSort(a, q+1, end);             // T(end - q) <= T(N - 1) iterations
```

In the worst case

$$T(N) = (N-1) + (N-2) + \ldots + 2 + 1 = \frac{(N-2)*(N-1)}{2} = O\left(N^2\right)$$

iterations when

$$a[1] < a[2] < \ldots < a[N].$$

Quick sort

But! If

$$P\left(a[i_1] < a[i_2] < \ldots < a[i_N]\right) = \frac{1}{N!}$$

for any permutation $(i_1, i_2, \ldots, i_N)$, then

$$\overline{T}(N) = E\left[T(N)\right] = O\left(N \log N\right)!$$

Quick sort

But! If

$$P\left(a[i_1] < a[i_2] < \ldots < a[i_N]\right) = \frac{1}{N!}$$

for any permutation $(i_1, i_2, \ldots, i_N)$, then

$$\overline{T}(N) = E\left[T(N)\right] = O\left(N \log N\right)!$$

And what if instead of $\frac{1}{N!}$ we have arbitrary distribution

$$(p_1, p_2, \ldots, p_{N!})?$$

Quick sort

But! If

$$P\left(a[i_1] < a[i_2] < \ldots < a[i_N]\right) = \frac{1}{N!}$$

for any permutation $(i_1, i_2, \ldots, i_N)$, then

$$\overline{T}(N) = E\left[T(N)\right] = O\left(N \log N\right)!$$

And what if instead of $\frac{1}{N!}$ we have arbitrary distribution

$$(p_1, p_2, \ldots, p_{N!})?$$

Lets use pseudorandom numbers!

$$\overline{T}(N) = O\left(N \log N\right).$$

Matrix equations

A, B and $C \in R^{N \times N}$.

$$A \times B = C? \tag{1}$$

Complexity (determined algorithms): $O\left(N^3\right)$ or $O\left(N^{2.3}\right)$.

Matrix equations

A, B and $C \in R^{N \times N}$.

$$A \times B = C? \tag{1}$$

Complexity (determined algorithms): $O\left(N^3\right)$ or $O\left(N^{2.3}\right)$.

$x \in \{0;1\}^N$ — uniform random vector. Instead of (1) check

$$A \times B \times x = C \times x? \tag{2}$$

Decision rule: if (2) is true (false) then (1) is true (false).

Matrix equations

A, B and $C \in R^{N\times N}$.

$$A \times B = C? \tag{1}$$

Complexity (determined algorithms): $O\left(N^3\right)$ or $O\left(N^{2.3}\right)$.
$x \in \{0;1\}^N$ — uniform random vector. Instead of (1) check

$$A \times B \times x = C \times x? \tag{2}$$

Decision rule: if (2) is true (false) then (1) is true (false).
Complexity: $O\left(N^2\right)$. Error probability:

$$P\left(\text{"false"} | A \times B = C\right) = 0, \quad P\left(\text{"true"} | A \times B \neq C\right) \leqslant \frac{1}{2}$$

Repeat it 20 times and get error probability $< 10^{-6}$.

Integer equations

Let x_1, x_2, ..., $x_N \in Z_+$ and $Q(x_1, x_2, \ldots, x_N)$ be k-degree polinom.

$$Q(x_1, x_2, \ldots, x_N) \equiv 0? \tag{3}$$

No polinomial algorith.

Integer equations

Shwartz Lemm

If $\{x_i\}_{1 \leqslant i \leqslant N}$ are independent uniform random numbers from $\{0, 1, \ldots, n\}$ then

$$P\left(Q\left(x_1, x_2, \ldots, x_N\right) = 0 | Q\left(\cdot, \cdot, \ldots, \cdot\right) \not\equiv 0\right) < \frac{kN}{n}.$$

Let $n = 2kN + 1$ then $P\left(\text{Error}\right) < 1/2$.
Check 100 times => $P\left(\text{Error}\right) < 1/2^{100}$

What does it mean «random numbers»?

Psychological test

$$
\begin{gathered}
10001011101111010000 \\
01111011001101110001
\end{gathered} \tag{4}
$$

Psychological test

$$\begin{matrix} 10001011101111010000 \\ 01111011001101110001 \end{matrix} \tag{4}$$

$$\begin{matrix} 00000000000000000000 \\ 11111111111111111111 \end{matrix} \tag{5}$$

Remarks:

- $P(\xi_i = 1) = P(\xi_i = 0) = \frac{1}{2}$
- Consider only $(\xi_1, \xi_2, \ldots, \xi_N)$, where N is large $(N \to \infty)$

Remarks:

- $P(\xi_i = 1) = P(\xi_i = 0) = \frac{1}{2}$
- Consider only $(\xi_1, \xi_2, \ldots, \xi_N)$, where N is large $(N \to \infty)$

Remarks:

- $P(\xi_i = 1) = P(\xi_i = 0) = \frac{1}{2}$
- Consider only $(\xi_1, \xi_2, \ldots, \xi_N)$, where N is large $(N \to \infty)$

Problem

Denote

$$\Omega = \{0, 1\}^{\infty}.$$

Want to find

$$R \subset \Omega \text{ — set of random sequences.}$$

General approach

Let $L\colon \Omega \to \{0,1\}$ be a characteristic property indicator of sequence $(a_1, a_2, \ldots)$.

$(a_1, a_2, \ldots)$ — random sequence $\Leftrightarrow L\,(a_1, a_2, \ldots) = 1$

General approach

Let $L\colon \Omega \to \{0, 1\}$ be a characteristic property indicator of sequence $(a_1, a_2, \ldots)$.

$(a_1, a_2, \ldots)$ — random sequence $\Leftrightarrow L\,(a_1, a_2, \ldots) = 1$

What L functions can you imagine?

Intuitive assumption

Consider sequence

$$(a_1, \quad a_2, \quad \ldots, \quad a_{N-1}, \quad a_N, \quad a_{N+1}, \ldots).$$

Obviously we want

$$\lim_{N\to\infty} \frac{\nu_N\left("1"\right)}{N} = \frac{1}{2}, \tag{6}$$

where $\nu_N\left("1"\right) = \sum_{i=1}^{N} Indicator \left\{a_i = 1\right\}$.

Intuitive assumption

Consider sequence

$$(a_1, \quad a_2, \quad \ldots, \quad a_{N-1}, \quad a_N, \quad a_{N+1}, \ldots).$$

Obviously we want

$$\lim_{N\to\infty} \frac{\nu_N\left("1"\right)}{N} = \frac{1}{2}, \tag{6}$$

where $\nu_N\left("1"\right) = \sum_{i=1}^{N} Indicator\left\{a_i = 1\right\}$.

What about sequence

$$0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ \ldots?$$

Definition 1

$(a_1, a_2, \dots)$ is random if for any computable functions $F()$ and $G()$:

1. $n(1) = F(\Lambda), n(2) = F(a_{n(1)})$

$$\left(a_{n(1)}, a_{n(2)}, \dots\right) \text{ – mixed}$$

2. Get $a_{n(k)} \Leftrightarrow G\left(a_{n(1)}, a_{n(2)}, \dots, a_{n(k-1)}\right) = 1$

$$(\tilde{a}_1, \tilde{a}_2, \dots) \text{ — result sequense}$$

true following

$$\lim_{N\to\infty} \frac{\nu_N\left("1"\right)}{N} = \frac{1}{2}$$

Intuitive assumption

Let

$$(a_1, a_2, \ldots)$$

be a casino tool, that is gamer tries to predict these numbers.

1. Gamer knows nothing and he just predicts $(n(1), i(1), v(1))$; casino checks whether $i(1) = a_{n(1)}$; $V(1) = V(0) + / - v(1)$;
2. Gamer knows $a_{n(1)}$ and tries to predict the next number; he says $(n(2), i(2), v(2))$; $V(2) = V(1) + / - v(2)$;
3. $\ldots$

Every time gamer applies some decision function $\Xi()$, named "strategy".

Definition 2

Suppose gamer has $V(0) = 1$ money initially.

Definition

$(a_1, a_2, \ldots)$ is random if there is no computable strategy $\Xi()$, that implies

$$V(k) \xrightarrow[k\to\infty]{} \infty.$$

Theorem

Let U be class of «unpredictable» sequences and S be class of frequency stable sequences. Then

$$U \subset S.$$

Random and pseudorandom numbers

Figure: Random

$$X_{n+1} = (aX_n + c) \mod m$$

Figure: Pseudorandom

Examples

- Flipping a coin or dices, dragging balls from an urn etc;
- making radioactive decay experiments;

Examples

- Flipping a coin or dices, dragging balls from an urn etc;
- making radioactive decay experiments;
- on Linux (v. $\geqslant$ 1.3.30) reading */dev/random* file.

Examples

- Flipping a coin or dices, dragging balls from an urn etc;
- making radioactive decay experiments;
- on Linux (v. $\geqslant 1.3.30$) reading */dev/random* file.

Disadvantages

1. Slowness;
2. lack of replicability;

Disadvantages

1. Slowness;
2. lack of replicability;
3. systematic bias.

Disadvantages

1. Slowness;
2. lack of replicability;
3. systematic bias.

Ways to improve

1. Slowness (prerecorded tables);
2. lack of replicability (prerecorded tables);

Ways to improve

1. Slowness (prerecorded tables);
2. lack of replicability (prerecorded tables);
3. systematic bias (difficult to quantify, no general solution).

Ways to improve

1. Slowness (prerecorded tables);
2. lack of replicability (prerecorded tables);
3. systematic bias (difficult to quantify, no general solution).

Advantages

They are truly random! Nobody can argue with it.

Application: as a seed for pseudorandom numbers.

The first pseudorandom numbers generator

John von Neumann.

Suppose we have X_n. Calculate X_n^2 and get, for example, 10 digits from the middle as X_{n+1}.

Example:

$$X_n = 5772156649 \rightarrow X_n^2 = 33317\textcolor{red}{7923805949}09201$$

$$X_{n+1} = 7923805949$$

The first pseudorandom numbers generator

John von Neumann.

Suppose we have X_n. Calculate X_n^2 and get, for example, 10 digits from the middle as X_{n+1}.

Example:

$$X_n = 5772156649 \to X_n^2 = 33317792380594909201$$

$$X_{n+1} = 7923805949$$

Disadvantage: a few numbers and hard to calculate.

Assertion

20-digits binary number generates at maximum 142 different numbers.

"Random numbers should not be generated with a method chosen at random"

D. E. Knuth "The Art of Computer Programming", 2, page 6

"Random numbers should not be generated with a method chosen at random"

D. E. Knuth "The Art of Computer Programming", 2, page 6

Some theory should be used.

What numbers do we need?

- Every random number U_n uniformly distributed in $[0, 1]$ can be transformated to arbitrary distributed random number.

What numbers do we need?

- Every random number U_n uniformly distributed in $[0, 1]$ can be transformated to arbitrary distributed random number.
- Every number in a computer is represented with only finite accuracy.

What numbers do we need?

- Every random number U_n uniformly distributed in $[0,1]$ can be transformated to arbitrary distributed random number.
- Every number in a computer is represented with only finite accuracy.

General approach

$$X_n \in \{0, 1, \ldots, m-1\} \to U_n = X_n/m \to \textit{ arbitrary distribution}$$

Hence we need $X_n \in \{0, 1, \ldots, m-1\}$.

Definition

Choose four numbers:

- m — the modulus; $0 < m$.
- a — the multiplier; $0 \leqslant a < m$.
- c — the increment; $0 \leqslant c < m$.
- X_0 — the starting value; $0 \leqslant X_0 < m$

Definition

Choose four numbers:

- m — the modulus; $0 < m$.
- a — the multiplier; $0 \leqslant a < m$.
- c — the increment; $0 \leqslant c < m$.
- X_0 — the starting value; $0 \leqslant X_0 < m$

$$X_{n+1} = (aX_n + c) \mod m, \quad n \geqslant 0.$$

Example

For $m = 10$, $X_0 = a = c = 7$ we get

$$7,\ 6,\ 9,\ 0,\ 7,\ 6,\ 9,\ 0,\ \ldots$$

Congruential sequences always get into loop. Unfortunately.

Choise of modulus (m). $X_{n+1} = (aX_n + c) \mod m$

- Period length $< m$.

Choise of modulus (m). $X_{n+1} = (aX_n + c) \mod m$

- Period length $< m$.
- Generation speed.
  Using $m = 2^e$ numbers (e is a computer's word size, e.g.) is faster.

Choise of modulus (m). $X_{n+1} = (aX_n + c) \mod m$

- Period length $< m$.
- Generation speed.
  Using $m = 2^e$ numbers (e is a computer's word size, e.g.) is faster.
- Random properties.
  Suppose $m = 2^e \implies$ the right-hand digits of X_n are much less random than the left-hand digits.

Assertion

If d is divisor of m and if ($Y_n = X_n \mod d$) then

$$Y_{n+1} = (aY_n + c) \mod d.$$

You can use $m = 2^e - 1$ instead.

Choise of multiplier (a) and increment (c).

$X_{n+1} = (aX_n + c) \mod m$

Goal: achieve the longest period (m). Is it possible?

Choise of multiplier (a) and increment (c).

$X_{n+1} = (aX_n + c) \mod m$

Goal: achieve the longest period (m). Is it possible?
Yes:

$$X_{n+1} = (X_n + 1) \mod m.$$

Choise of multiplier (a) and increment (c).

$X_{n+1} = (aX_n + c) \mod m$

Goal: achieve the longest period (m). Is it possible?
Yes:

$$X_{n+1} = (X_n + 1) \mod m.$$

Theorem

The linear congruential sequence defined by m, a, c and X_0 has period length m if and only if

1. c is relatively prime to m;
2. $a - 1$ is a multiple of p, for every prime p dividing m;
3. $a - 1$ is a multiple of 4, if m is a multiple of 4.

Potency. $X_{n+1} = (aX_n + c) \mod m$

Suppose $\{X_n\}$ has maximum period (that is m).

Definition

The least integer s such that

$$(a-1)^s \equiv 0\,(\text{ } modulo \ m)$$

called «potency».

The larger potency $\Longrightarrow$ the more random sequence.

Potency. $X_{n+1} = (aX_n + c) \mod m$

Let $X_0 = 0$ and $b = a - 1$, then

$$X_n = ((a^n - 1)\, c/b) \mod m,$$

after transformations:

$$X_n = c\left(n + \binom{n}{2} b + \ldots + \binom{n}{s} b^{s-1}\right) \mod m.$$

Potency. $X_{n+1} = (aX_n + c) \mod m$

Let $X_0 = 0$ and $b = a - 1$, then

$$X_n = ((a^n - 1)\, c/b) \mod m,$$

after transformations:

$$X_n = c\left(n + \binom{n}{2} b + \ldots + \binom{n}{s} b^{s-1}\right) \mod m.$$

In particular:

$s = 1 \Longrightarrow X_n = cn \mod m;$
$s = 2 \Longrightarrow X_n = cn + c\binom{n}{2} b \mod m \Longrightarrow X_{n+1} - X_n \equiv c + cbn$

Potency. $X_{n+1} = (aX_n + c) \mod m$

Let $X_0 = 0$ and $b = a - 1$, then

$$X_n = ((a^n - 1)\, c/b) \mod m,$$

after transformations:

$$X_n = c\left(n + \binom{n}{2} b + \ldots + \binom{n}{s} b^{s-1}\right) \mod m.$$

In particular:

$s = 1 \Longrightarrow X_n = cn \mod m$;

$s = 2 \Longrightarrow X_n = cn + c\binom{n}{2} b \mod m \Longrightarrow X_{n+1} - X_n \equiv c + cbn$

denoting ($d = cb \mod m$) we have $(X_n, X_{n+1}, X_{n+2}) \in$

$$x - 2y + z = d + m, \qquad x - 2y + z = d - m,$$
$$x - 2y + z = d, \qquad x - 2y + z = d - 2m.$$

Potency. $X_{n+1} = (aX_n + c) \mod m$

Examples:

1. Let $m = 2^e$; it is divisible by high powers of prime 2. Choosing $a = 2^k + 1$, have relatevely big potency.

Potency. $X_{n+1} = (aX_n + c) \mod m$

Examples:

1. Let $m = 2^e$; it is divisible by high powers of prime 2. Choosing $a = 2^k + 1$, have relatevely big potency.
2. Let $m = 2^e - 1$; commonly it is not divisible by high powers of primes $\Longrightarrow$. There could not be a big potency.

"Chi-square" test. Experiment

Throw two "true" dices.
s — sum of the result numbers.

value of s =	2	3	4	5	6	7	8	9	10	11	12
probability, p_s =	$\frac{1}{36}$	$\frac{1}{18}$	$\frac{1}{12}$	$\frac{1}{9}$	$\frac{5}{36}$	$\frac{1}{6}$	$\frac{5}{36}$	$\frac{1}{9}$	$\frac{1}{12}$	$\frac{1}{18}$	$\frac{1}{36}$

"Chi-square" test. Experiment

Throw two "true" dices.
s — sum of the result numbers.

value of s =	2	3	4	5	6	7	8	9	10	11	12
probability, p_s =	$\frac{1}{36}$	$\frac{1}{18}$	$\frac{1}{12}$	$\frac{1}{9}$	$\frac{5}{36}$	$\frac{1}{6}$	$\frac{5}{36}$	$\frac{1}{9}$	$\frac{1}{12}$	$\frac{1}{18}$	$\frac{1}{36}$

Repeat $n = 144$ times:

value of s =	2	3	4	5	6	7	8	9	10	11	12
observed number, Y_s =	2	4	10	12	22	29	21	15	14	9	6
probability, p_s =	$\frac{1}{36}$	$\frac{1}{18}$	$\frac{1}{12}$	$\frac{1}{9}$	$\frac{5}{36}$	$\frac{1}{6}$	$\frac{5}{36}$	$\frac{1}{9}$	$\frac{1}{12}$	$\frac{1}{18}$	$\frac{1}{36}$

"Chi-square" test. Statisctic

$$V = (Y_2 - np_2)^2 + (Y_3 - np_3)^2 + \ldots + (Y_{12} - np_{12})^2 \,. \tag{7}$$

"Chi-square" test. Statisctic

$$V = (Y_2 - np_2)^2 + (Y_3 - np_3)^2 + \ldots + (Y_{12} - np_{12})^2 . \qquad (7)$$

Better to analyse:

$$V = \frac{(Y_2 - np_2)^2}{np_2} + \frac{(Y_3 - np_3)^2}{np_3} + \ldots + \frac{(Y_{12} - np_{12})^2}{np_{12}}. \qquad (8)$$

"Chi-square" test. Statisctic

$$V = (Y_2 - np_2)^2 + (Y_3 - np_3)^2 + \ldots + (Y_{12} - np_{12})^2. \qquad (7)$$

Better to analyse:

$$V = \frac{(Y_2 - np_2)^2}{np_2} + \frac{(Y_3 - np_3)^2}{np_3} + \ldots + \frac{(Y_{12} - np_{12})^2}{np_{12}}. \qquad (8)$$

In our example:

$$V = \frac{(2-4)^2}{4} + \frac{(4-8)^2}{8} + \ldots + \frac{(9-8)^2}{8} + \frac{(6-4)^2}{4} = 7\frac{7}{48}. \qquad (9)$$

"Chi-square" test. Test

$$V = \sum_{s=1}^{k} \frac{\left(Y_s - np_s\right)^2}{np_s} \xrightarrow{d} \chi^2\left(k-1\right)$$

"Chi-square" test. Test

$$V = \sum_{s=1}^{k} \frac{(Y_s - np_s)^2}{np_s} \xrightarrow{d} \chi^2 (k-1)$$

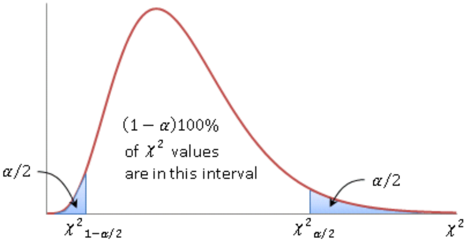

Figure: $\chi^2 (k-1)$ density

$$P\Big(\chi^2_{1-\alpha/2}(k-1) \leqslant \\ \leqslant V(Y_1, Y_2, \dots, Y_k) \leqslant \\ \leqslant \chi^2_{\alpha/2}(k-1) \,|\, V \in \chi^2(k-1)\Big) = \\ = 1-\alpha$$

"Chi-square" test. Pseudorandom numbers generators app

Consider

$$A = \{0, 1, \ldots, m-1\}.$$

"Chi-square" test. Pseudorandom numbers generators app

Consider

$$A = \{0, 1, \ldots, m-1\}.$$

Split A into k subsets (of size $\frac{m}{k}$, e.g.):

$$A = \left\{0, 1, \ldots, \frac{m}{k} - 1\right\} \cup \left\{\frac{m}{k}, \frac{m}{k} + 1, \ldots, 2\frac{m}{k} - 1\right\} \cup \ldots$$
$$\ldots \cup \left\{m - \frac{m}{k}, m - \frac{m}{k} + 1, \ldots, m - 1\right\}.$$

"Chi-square" test. Pseudorandom numbers generators app

Consider

$$A = \{0, 1, \ldots, m-1\}.$$

Split A into k subsets (of size $\frac{m}{k}$, e.g.):

$$A = \left\{0, 1, \ldots, \frac{m}{k} - 1\right\} \cup \left\{\frac{m}{k}, \frac{m}{k} + 1, \ldots, 2\frac{m}{k} - 1\right\} \cup \ldots$$
$$\ldots \cup \left\{m - \frac{m}{k}, m - \frac{m}{k} + 1, \ldots, m - 1\right\}.$$

Generate n random numbers. n should satisfy

$$np_s = \frac{n}{k} \geqslant 5$$

"Chi-square" test. Pseudorandom numbers generators app

Consider

$$A = \{0, 1, \dots, m-1\}.$$

Split A into k subsets (of size $\frac{m}{k}$, e.g.):

$$A = \left\{0, 1, \dots, \frac{m}{k} - 1\right\} \cup \left\{\frac{m}{k}, \frac{m}{k} + 1, \dots, 2\frac{m}{k} - 1\right\} \cup \dots$$
$$\dots \cup \left\{m - \frac{m}{k}, m - \frac{m}{k} + 1, \dots, m - 1\right\}.$$

Generate n random numbers. n should satisfy

$$np_s = \frac{n}{k} \geqslant 5, \quad \text{better} \quad \geqslant 8$$

"Chi-square" test. Pseudorandom numbers generators app

Consider

$$A = \{0, 1, \dots, m-1\}.$$

Split A into k subsets (of size $\frac{m}{k}$, e.g.):

$$A = \left\{0, 1, \dots, \frac{m}{k} - 1\right\} \cup \left\{\frac{m}{k}, \frac{m}{k} + 1, \dots, 2\frac{m}{k} - 1\right\} \cup \dots$$
$$\dots \cup \left\{m - \frac{m}{k}, m - \frac{m}{k} + 1, \dots, m - 1\right\}.$$

Generate n random numbers. n should satisfy

$$np_s = \frac{n}{k} \geqslant 5 \quad \text{better} \quad \geqslant 8 \quad \text{better} \quad \geqslant 10$$