Лекция

фрагменты

теории вероятностей и

математической статистики

Генератор псевдослучайных чисел

Генератор псевдослучайных чисел (ГПСЧ, pseudorandom number generator, PRNG) — алгоритм, порождающий последовательность чисел, элементы которой *почти* независимы друг от друга и подчиняются заданному распределению (обычно *равномерному*).

От качества используемых ГПСЧ напрямую зависит качество получаемых результатов. Если выбрать хороший алгоритм, полученная численная последовательность псевдослучайных чисел будет проходить большинство тестов на случайность. Одной из характеристик такой последовательности является период повторения, который должен быть больше рабочего интервала, из которого берутся числа.

Генератор псевдослучайных чисел включён в состав современных процессоров, например, RdRand входит в набор инструкций IA-32.

Никакой детерминированный алгоритм не может генерировать ***абсолютно случайные*** числа, он может только аппроксимировать некоторые их свойства. *Любой* ГПСЧ с ограниченными ресурсами будет зацикливаться (повторяет последовательность чисел)

Генератор псевдослучайных чисел

Линейный конгруэнтный метод был предложен Д.Г.Лемером в 1949 г.
Суть метода заключается в вычислении последовательности чисел X_n

$$X_{n+1} = (a * X_n + c) \ mod \ m$$

m — модуль (натуральное число, относительно которого вычисляют остаток от деления, m > 2)

a — множитель (0< a < m)

c — приращение (0< c < m)

X_0 — начальное значение (X_0 < m)

Такой ряд называется *линейной конгруэнтной последовательностью.*

ЛКП, определенная числами ***m, a, c*** *и* ***X_0,*** периодична с периодом, не превышающим ***m***.

При этом длина периода равна ***m*** тогда и только тогда, когда:

числа ***c*** и ***m*** взаимно простые (т.е. не имеют общих делителей);

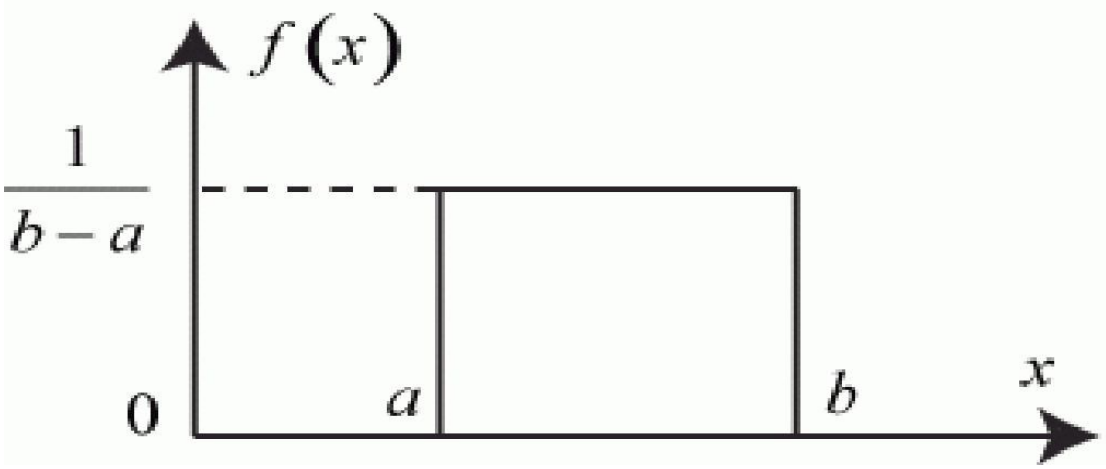
b = a – 1 кратно ***p*** для каждого простого ***p***, являющегося делителем ***m***;

b кратно 4, если ***m*** кратно 4.

Было доказано наличие этого свойства для случая ***m = 2^z***

где ***z*** — число битов в машинном слове (16, 32, 64…)

Равномерное распределение



$$f(x)=\begin{cases}\dfrac{1}{b-a}, a \le x \le b;\\ 0, x \prec a, x \succ b /\end{cases}$$

Плотность вероятности

$$M[\gamma] = \frac{a+b}{2}$$

Мат. ожидание

$$D[\gamma] = \frac{(b-a)^2}{12}$$

Дисперсия

Пример функции равномерного распределения на интервале [0, 1]

```
static long int ax = 1;
double random(void)
{
   int ix = ax * 1220703125;
   if (ix < 0)
      ix = ix + 1073741824 + 1073741824;
   double rnd = ix * 0.4656613 e–9;
   ax = ix;
   return (rnd);
}
```

Датчики на основе линейного конгруэнтного метода сохраняют свою полезность для *некриптографических* приложений, в т.ч. для моделирования. Они в большинстве используемых эмпирических тестов демонстрируют хорошие статистические характеристики.

Пример функции равномерного распределения

Для улучшения статистических свойств числовой последовательности во многих генераторах псевдослучайных чисел используется только часть битов результата. Например, в стандарте ISO/IEC 9899 языка *C* приведен пример функции ***rand***(), принудительно отбрасывающей младшие 16 и один старший разряд.

```
static unsigned long int next = 1;
int rand(void) {
     next = next * 1103515245 + 12345;
     return (unsigned int)(next/65536) % 32767;
}
void setrand(unsigned int seed) {
     next = seed;
}
```

Генератор псевдослучайных чисел

Инверсный конгруэнтный метод был предложен Эйхенауэром и Леном в 1986 году как замена линейному конгруэнтному методу. Данный метод состоит в вычислении последовательности случайных чисел X_n в кольце вычетов по модулю натурального числа n .

Основным отличием ИКМ от линейного метода является использование при генерации нового элемента – числа, обратного к предыдущему элементу, вместо самого предыдущего элемента.
Параметрами генератора являются:
seed — "соль"; **a** — множитель ($0 < a < n$); **c** — приращение ($0 < c < n$).

Инверсные конгруэнтные генераторы обладают неплохой равномерностью. Полученные методом ИКМ последовательности остаются стабильными при изменении параметров, имеют период значительно превышающий период линейных генераторов. Алгоритм ИКМ позволяет добиться прироста производительности при использовании на многоядерных системах.

Пример реализации ИКМ

```
int mod_inv(int b, int n) {
      int  b0 = n, t, q, x0 = 0, x1 = 1;
      if (n == 1) return 1;
      while (b > 1)    {
            q = b / n;   t = n;  n = b % n;  b = t;
            t = x0;  x0 = x1 - q * x0;  x1 = t;
      }
      if (x1 < 0) {x1 += b0;}
      return x1;
}
int ICG(int n, int a, int c, int seed) {
    if (seed == 0)  return c;
    return (a * mod_inv(seed, n) + c) % n;
}
int main(void)  {
      int seed = 1, n = 5, a = 2, c = 3, count = 10; //например
      for (int i = 0; i < count; i++)  {
            cout << seed << endl;    seed = ICG(n, a, c, seed);
      }
      return 0;
}
```

Генератор псевдослучайных чисел

`Вихрь Мерсенна` (Mersenne twister, MT) — ГПСЧ, разработанный в 1997 году японскими учёными Макото Мацумото и Такудзи Нисимура.

`Вихрь Мерсенна` основывается на свойствах простых чисел Мерсенна (имеющими вид 2^p-1) и обеспечивает быструю генерацию высококачественных по критерию случайности псевдослучайных чисел.

`Вихрь Мерсенна` лишён недостатков, присущих ГПСЧ ЛКМ, таких как малый период, легко выявляемые статистические закономерности, предсказуемость.

Для чисел Мерсенна тест на простоту целых намного проще.

Известно много простых чисел Мерсенна (т.е. простых вида 2^p-1) до $p = 43112609$

Генератор псевдослучайных чисел

Алгоритм *Вихрь_Мерсенна* использует регистр сдвига с обобщённой обратной связью (twisted generalised feedback shift register).

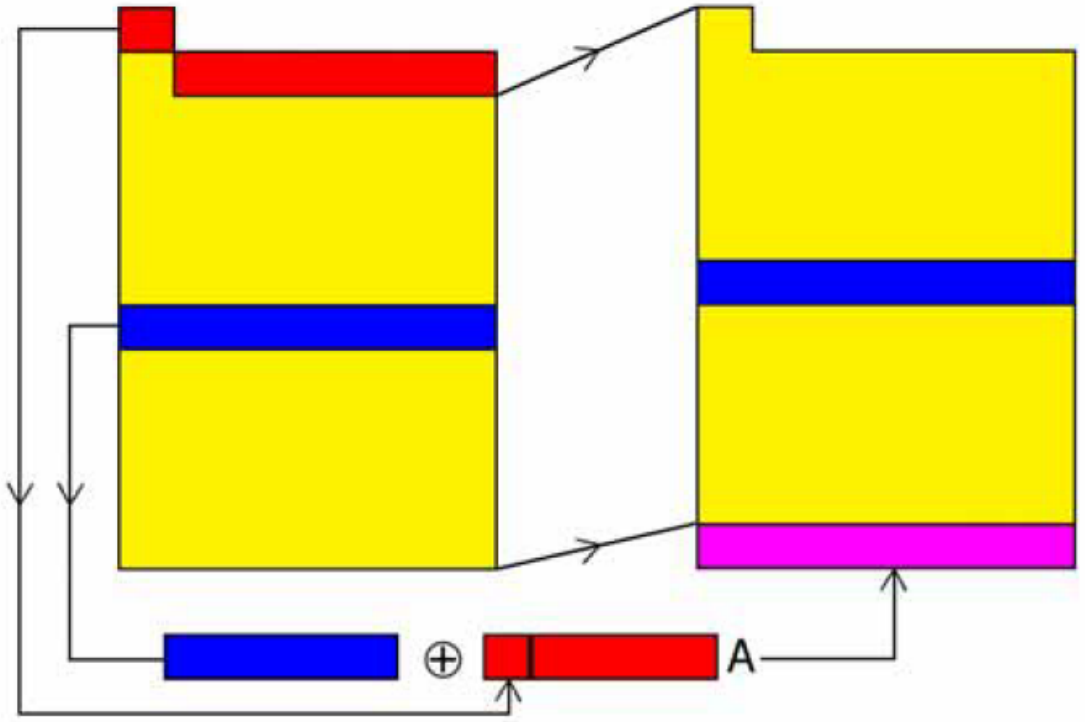
«Вихрь (скрутка)» — это преобразование, которое обеспечивает равномерное распределение генерируемых псевдослучайных чисел в 623 измерениях (для линейных конгруэнтных генераторов оно равно 5 измерениям), поэтому функция корреляции между двумя последовательностями подвыборок в выходной последовательности алгоритма MT пренебрежимо мала.

Псевдослучайная последовательность, порождаемая MT, имеет очень большой период, равный $(2^{19937} - 1)$, что более чем достаточно для многих практических приложений.

Алгоритм MT

Вихрь Мерсенна алгоритмически реализуется двумя основными частями: *рекурсивной* и т.н. *упрочняющей* (закалка).

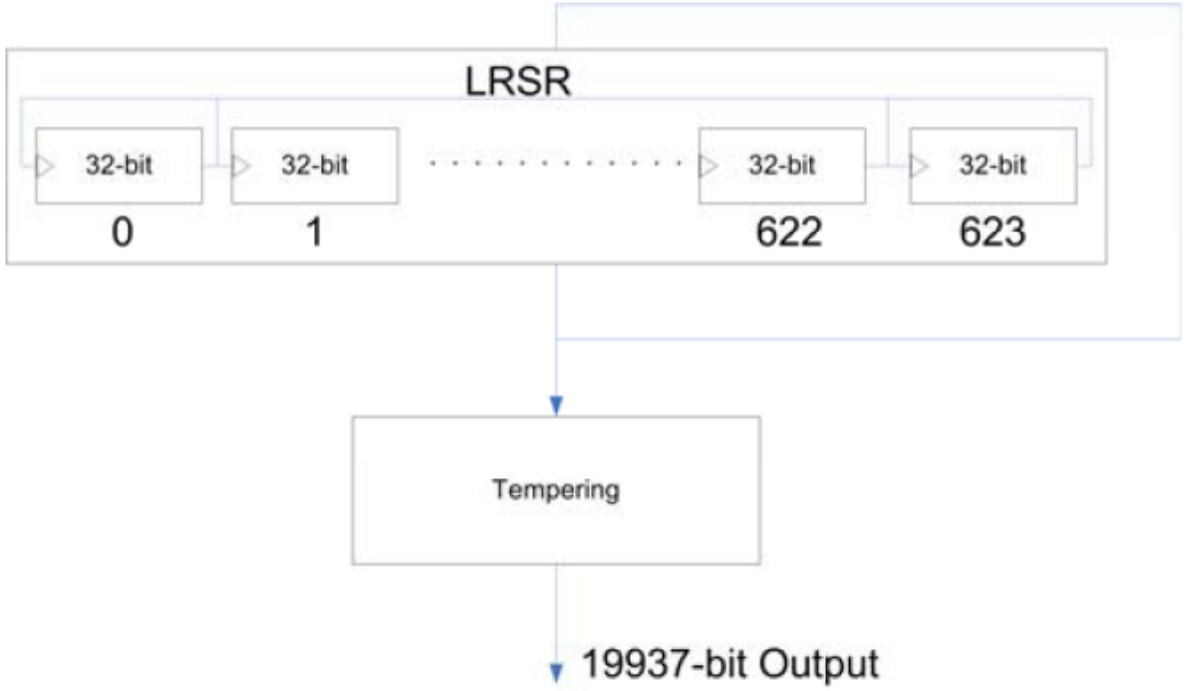
Рекурсивная часть представляет собой регистр сдвига с линейной обратной связью, в котором все биты в его слове определяются рекурсивно; поток выходных битов определяются также рекурсивно функцией битов состояния.



Алгоритм MT

Регистр сдвига состоит из 624 элементов = 19937 бит. Каждый элемент имеет длину 32 бита за исключением первого элемента, который имеет только 1 бит за счет отбрасывания битов.

Процесс генерации начинается с логического умножения на битовую маску, отбрасывающей 31 бит, кроме наиболее значащего



Алгоритм MT

Следующим шагом выполняется инициализация (x0, x1,…, x623) любыми беззнаковыми 32-разрядными целыми числами. Следующие шаги включают в себя объединение и переходные состояния. Пространство состояний имеет 19937 бит (624·32 - 31). Следующее состояние генерируется сдвигом одного слова вертикально вверх и вставкой нового слова в конец. Новое слово вычисляется гаммированием средней части с исключённой частью. Выходная последовательность начинается с x624, x625,…

Алгоритм MT

Параметры *MT* были тщательно подобраны для достижения свойств равномерности. Параметры **n** и **r** выбраны так, что характеристический многочлен был равен числу Мерсенна 19937. Значение **w** эквивалентно размеру слова процессора = 32 бита. Значения n, m, r и w фиксируются, а значение последней строки матрицы A выбирается случайным образом.

Параметры закалки (*tempering*) подобраны так, чтобы получить хорошее равномерное распределение.

n	624
w	32
r	31
m	397
a	$9908B0DF_{16}$
u	11
s	7
t	15
l	18
b	$9D2C5680_{16}$
c	$EFC60000_{16}$

Алгоритм MT

B.4 Текст программы для метода Мерсенна Твистера

Ниже приведен текст программы для метода Мерсенна Твистера на языке Си. Функция genrand () генерирует псевдослучайные числа в виде целого 32-битового числа без знака из интервала от 0 до $(2^{32} – 1)$ включительно. Функция genrand_31 () генерирует псевдослучайные числа в виде целого 31-битового числа без знака из интервала от 0 до $(2^{31} – 1)$ включительно. Функция init_genrand (s) инициализирует начальное число в виде 32-битового целого числа без знака [целое число из интервала от 0 до $(2^{32} – 1)$ включительно]. Перед обращением к genrand () или genrand_31 () необходимо один раз выполнить инициализацию init_genrand (*s*). Различные начальные числа *s* приводят к генерации разных последовательностей случайных чисел. Параметры в этой программе необходимо сохранять.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО 28640— 2012

Статистические методы

ГЕНЕРАЦИЯ СЛУЧАЙНЫХ ЧИСЕЛ

ISO 28640:2010
Random variate generation methods
(IDT)

Разработка модели системы состоит из двух тесно связанных подразделов.

Первый подраздел называют структурным моделированием.

В этом компоненте определяются объекты, местоположения, ресурсы и процессы, которые описывают структуру и функционирование системы.

Результатом является математическое и логическое представление, например, модель системы массового обслуживания, определяющее как работает система.

Второй подраздел называют моделированием данных.

В этом компоненте моделируются описательные данные, необходимые для выполнения разработанной модели.

Модель данных используется для генерации множества потоков случайных величин, представляемых во время моделирования.

Это данные таких параметров как:

- ❖ время между прибытиями объектов,
- ❖ время обслуживания процессов,
- ❖ графики использования ресурсов,
- ❖ частота отказов,
- ❖ время перемещения объектов,
- ❖ другие данные количественного описания работы системы.

Сбор данных для каждого параметра означает сбор выборок из совокупности базовых компонентов данных, представленной распределением из реальной совокупности наблюдений.

В начале исследования предполагают, что данные в выборках независимы и идентично распределены ($I\,I\,D$).

«Независимость» означает, что между последовательными выборками нет взаимосвязи или влияния (корреляции).

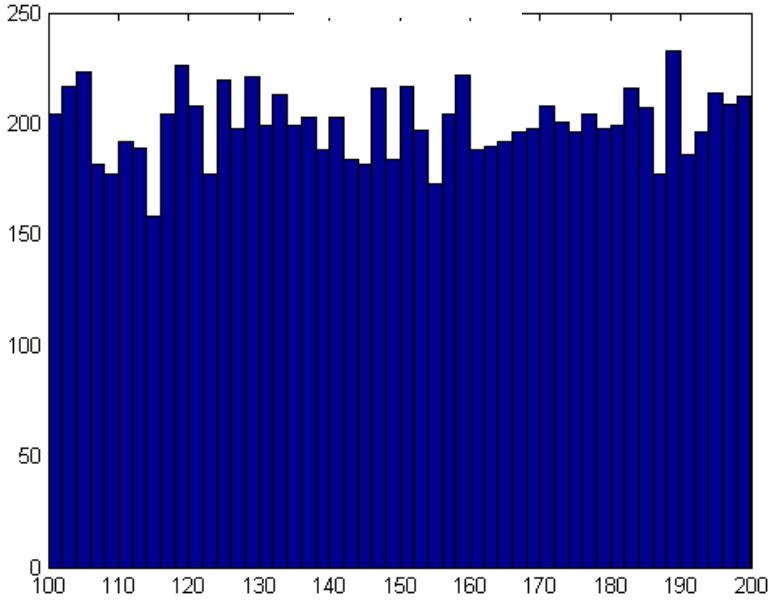
«Идентично распределенный» означает, что каждая выборка поступает из одного и того же базового распределения.

Также предполагают, что базовое распределение является простым (одномодальным) и стационарным (не изменяющимся во времени).

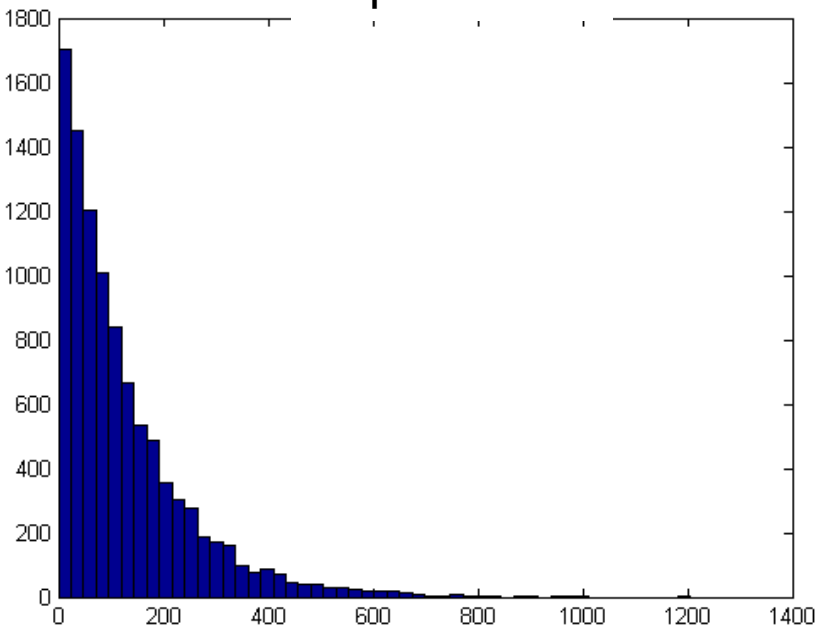
Существует 3 варианта генерации потока случайных величин, необходимого для моделирования:

1) значения выборки могут быть использованы непосредственно для формирования потока случайных величин;
2) набор выборок может быть использован для генерации эмпирического распределения, которое, в свою очередь, может быть использовано для генерации потока случайных величин;
3) может быть идентифицирована теоретическая функция распределения, которая соответствует набору выборок. Это теоретическое распределение может быть использовано для генерации потока случайных величин.

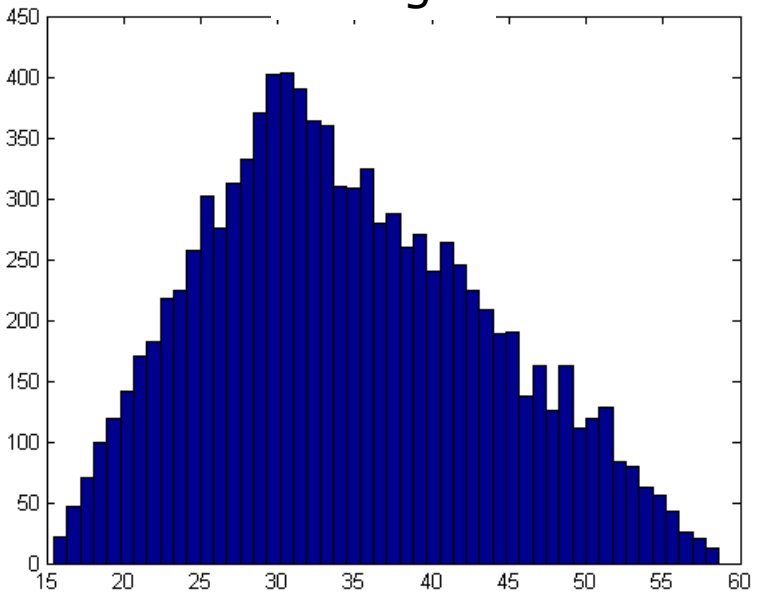
uniform



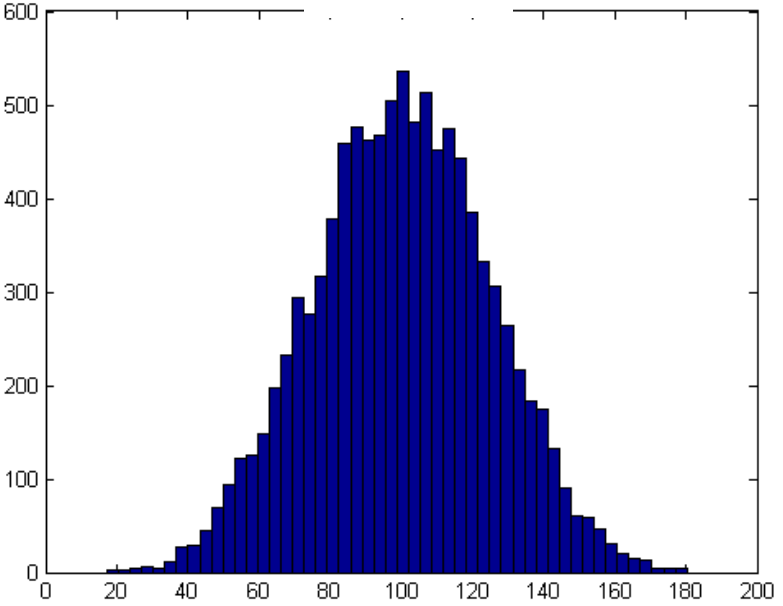
exponential



triangle



normal



Пример функции равномерного распределения на интервале [m-s, m+s]

```
double uniform(double m, double s)
{
   return(m – s + 2 * random() * s);
}
```

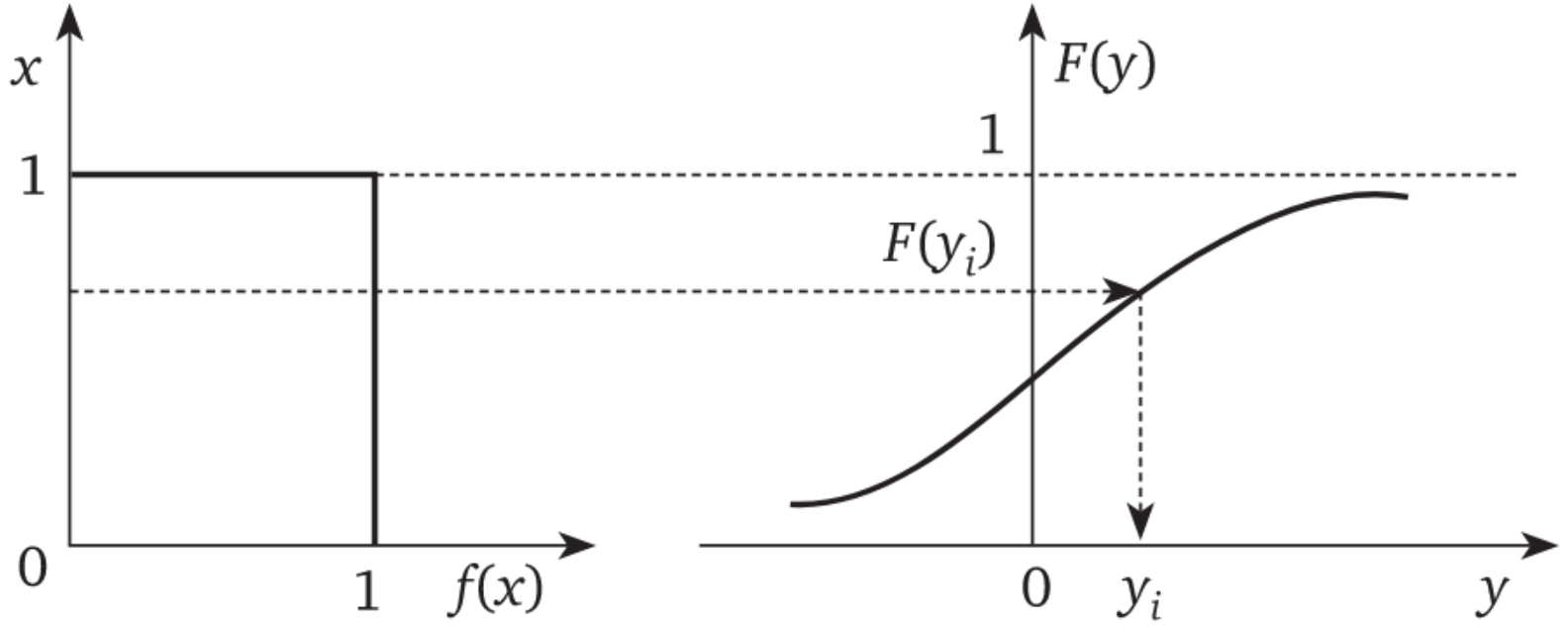
Функция random() – стандартный ГСЧ в интервале [0..1)

Произвольное распределение

Теорема: Если случайная величина ***y*** имеет плотность распределения вероятностей *f(y)*, то распределение случайной величины *F(y)* равномерно в интервале [0,1)

$$F(y) = \int_{-\infty}^{y} f(t)dt$$

$$F(y) \sim uniform[0; 1)$$



$$x_i = \int_{-\infty}^{y_i} f(y)dy$$

$$y_i = F^{-1}(x_i)$$

Произвольное распределение

Метод обратного преобразования (преобразование Н.В. Смирнова) — способ генерации случайных величин с заданной функцией распределения путём модификации работы генератора равномерно распределённых чисел.

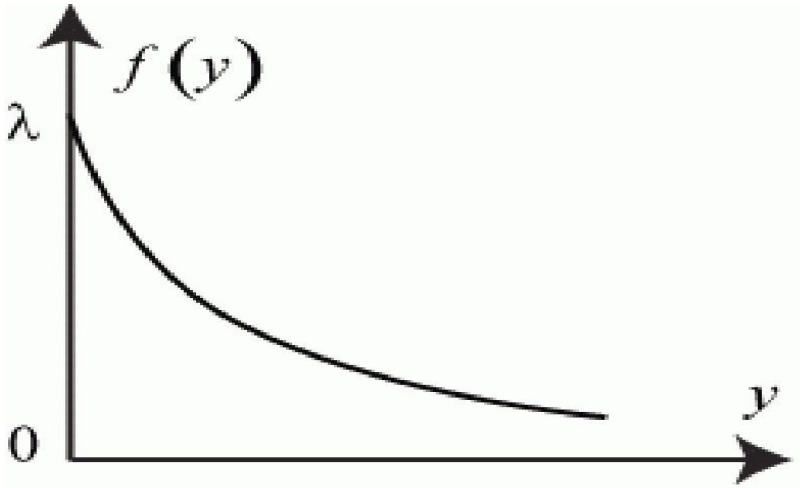
Используя генератор стандартного непрерывного равномерного распределения, можно получить выборку из распределения, задаваемого функцией распределения ***F(x)***.

Если функция **F : R → [0 , 1]** строго возрастает на всей области определения, то она *биективна*, следовательно имеет обратную функцию.

При *биективном* отображении каждому элементу одного множества соответствует ровно один элемент другого множества, при этом определено обратное отображение, которое обладает тем же свойством. Поэтому *биективное* отображение называют **взаимно-однозначным** отображением (соответствием).

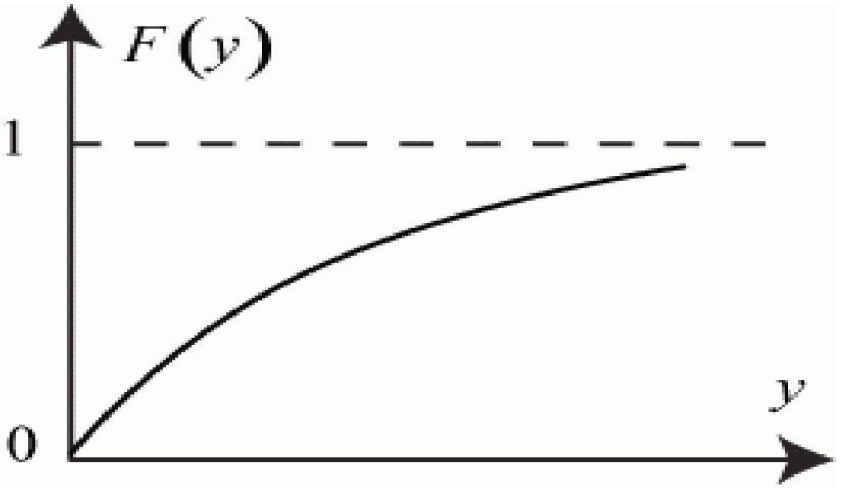
Если между двумя множествами можно установить *биекцию (*взаимно-однозначное соответствие), то такие множества называются ***равномощными.***

Экспоненциальное распределение



$$f(y)=\begin{cases}0 \text{ при } & y \le 0,\\ \lambda e^{-\lambda y} \text{ при } & y \succ 0.\end{cases}$$

Плотность распределения



$$F(y)=\begin{cases}0 \text{ при } & y \le 0,\\ 1-e^{-\lambda y} \text{ при } & y \succ 0.\end{cases}$$

Функция распределения

$$x_i=\int_{-\infty}^{y_i} f(y)dy=\int_{-\infty}^{0} f(y)dy+\int_{0}^{y_i} f(y)dy=\int_{0}^{y_i} f(y)dy=1-e^{-\lambda y_i};$$

$$x_i \in \text{Random}();\ \ e^{-\lambda y_i}=1-x_i;\ -\lambda y_i=\ln(1-x_i);\ y_i=-\frac{1}{\lambda}\ln(1-x_i).$$

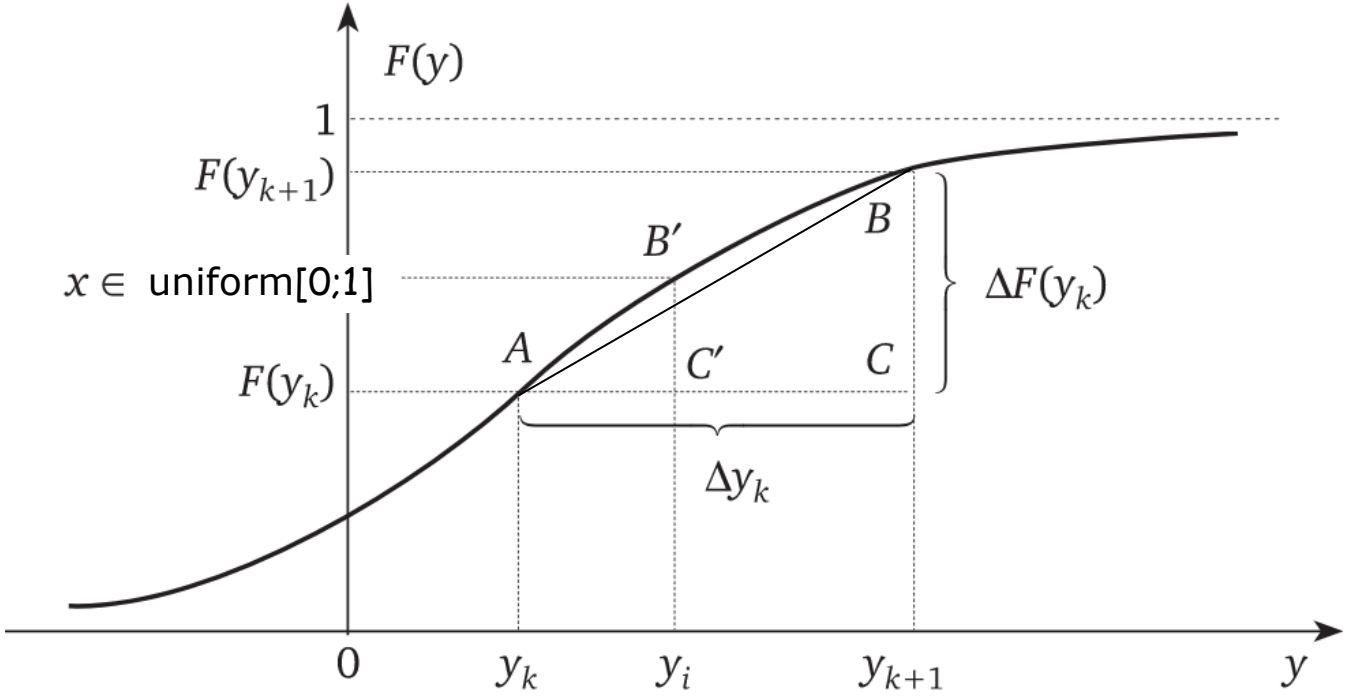
```
y = - Ln(Random) / λ
```

Пример функции экспоненциального распределения

```
double exponential(double la)
{
   double r = log(random());
   return(1.0 / la * (–r));
}
```

Произвольное распределение

Метод кусочно-линейной аппроксимации
функции распределения случайной величины



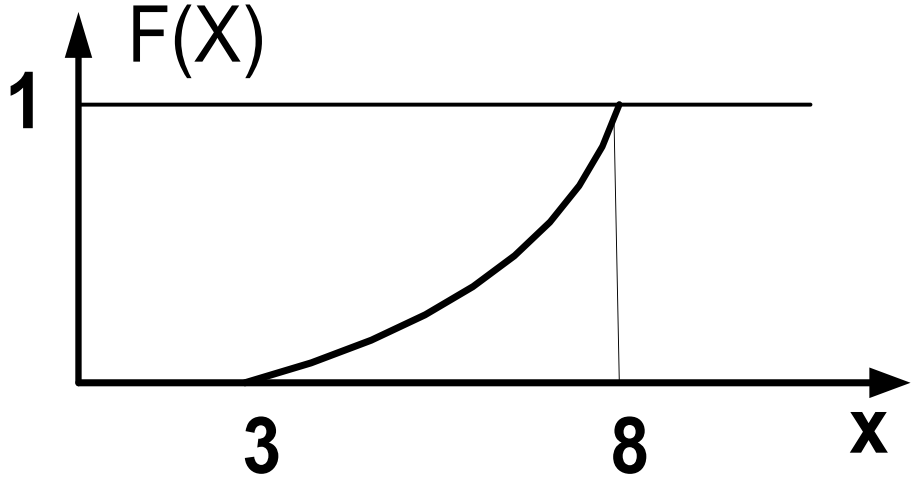
1. Генерируется случайное число x
   из uniform[0;1]
2. Сравнивается x со значениями $F(y)_k$, k=1,n
3. При совпадении - выдается y_k
4. Иначе случайное число y_k вычисляется из подобия треугольников ABC и AB'C'

$$\frac{\Delta F(y_k)}{\Delta y_k} = \frac{x_i - F(y_k)}{y_i - y_k}.$$

В случае функции распределения общего вида чаще всего необходимо численно находить точную нижнюю грань (что может быть достаточно трудоёмко)

Пример произвольного распределения

Метод обратной функции : задача



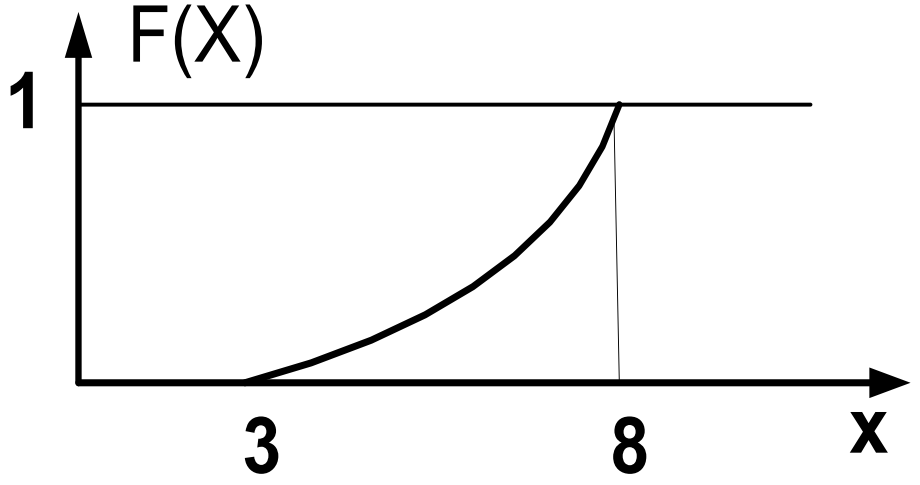
$$F(x) = b\,(x - a)^2$$

1. Найти коэффициенты **a** и **b**

2. Вывести формулу для получения случайной величины X с заданной функцией распределения F(x), имея в распоряжении случайную величину Rand ~ *uniform* [0;1]

Пример произвольного распределения

Метод обратной функции : задача



$$F(x) = b\,(x - a)^2$$

1. Найти коэффициенты **a** и **b** **=> (a=3; b= 1/25)**

2. Вывести формулу для получения случайной величины X :

x = 5 * sqrt (Rand) + 3

Нормальное распределение

Центральная предельная теорема:

Если исход случайного события определяется большим числом случайных факторов и влияние каждого фактора мало, то такой случайный исход хорошо аппроксимируется нормальным распределением.

$$\eta = \frac{\sum_{i=1}^{N} x_i - NM(x)}{\sqrt{ND(x)}}$$

Теорема Леви-Линдеберга:

Случайная величина η, где x_i – случайные числа одного и того же распределения с матем.ожиданием M[x] и дисперсией D[x] при $N \to \infty$ асимптотически стремится к нормальному распределению с $M[\eta]=0$ и $D[\eta]=1$

При N=6

$$y_i = \frac{\sum_{i=1}^{N} x_i - 3}{\sqrt{0.5}} = \sqrt{2}\left(\sum_{i=1}^{6} x_i - 3\right)$$

При N=12

$$y_i = \frac{\sum_{i=1}^{N} x_i - 6}{\sqrt{1}} = \sum_{i=1}^{12} x_i - 6$$

Пример функции нормального распределения

$p(x)$ - нормальное распределение с мат.ожиданием **m** и среднеквадратичным отклонением **s**

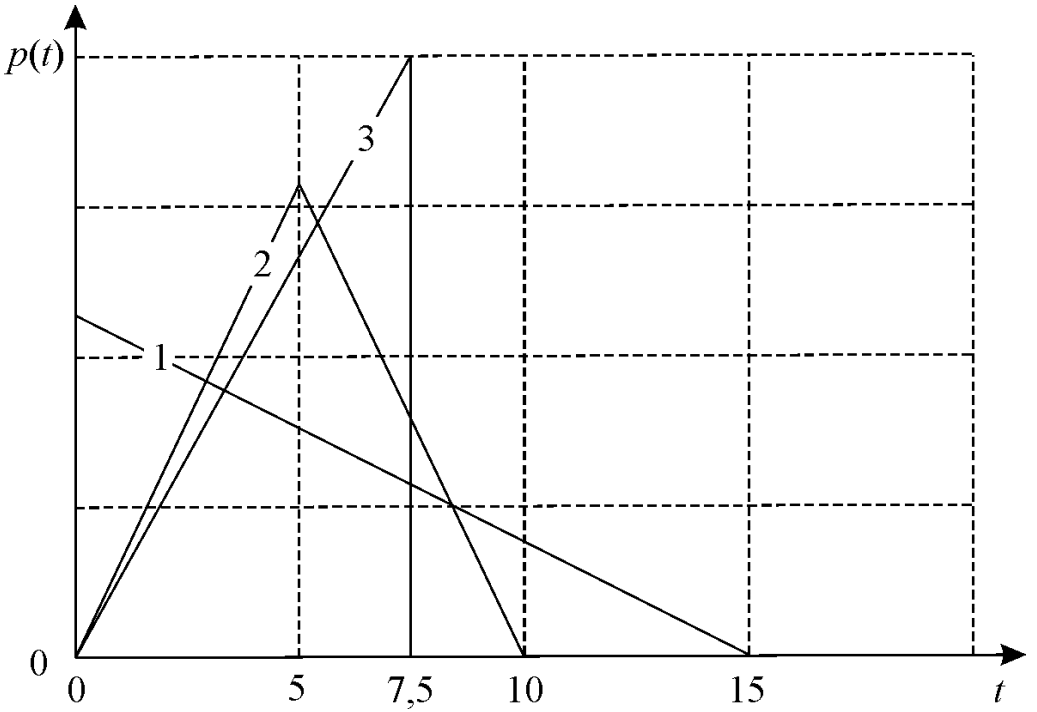
$$p(x) = \frac{1}{s\sqrt{2\pi}} \exp\left[-\frac{1}{2}\left(\frac{x-m}{s}\right)^2\right]$$

```
double normal(double mo, double sd)
{    // почти нормальное распределение
     // по методу Леви-Линдеберга
   double a = 0.0;
   for (int i = 0; i < 12; i++)
      a += random();

   return (mo + (a – 6.0) * sd);
}
```

Пример функции нормального распределения

```
double Normal (double mo, double sd) {
// нормальное распределение
// по методу Бокса-Мюллера

double r =sqrt(-2.0 *log(1.0 -random())) * sd;

double phi =2.0 * PI * random();

return (mo + r * cos(phi));

}
```

Пример функции треугольного распределения




```
double triangle
    (double a,
     double m,
     double b)
{
    double x, r;
    r = random();
    if( r <= (m–a)/(b–a) )
        x = a + sqrt( r*(m–a)*(b–a) );
    else
        x = b – sqrt( (1.0–r)*(b–m)*(b–a) );
    return (x);
}
```

Основные задачи математической статистики

А) оценивание параметров :
разделяется на *точечное* оценивание и *интервальное* оценивание параметров распределения. Чаще всего по результатам наблюдений требуется получить точечные оценки *математического ожидания* и *дисперсии* исследуемой случайной величины.
В случае, когда нужно получить интервал, в который с заданной вероятностью попадает исследуемый параметр - это задача интервального оценивания.

Б) статистическая проверка гипотез:
заключается в том, что делается *предположение* о распределении вероятностей случайной величины, например, о значении параметров функции распределения, и решается вопрос о его согласовании с полученными результатами наблюдений.

В качестве гипотез выступают предположения о законе распределения, о параметрах исследуемой случайной величины, о корреляционной зависимости между случайными величинами и др.

После обработки результатов выборки делается предположение (*гипотеза*) о законе распределения или о каком-то параметре случайной величины.

Гипотезы о *параметрах* законов распределений случайных величин называются *параметрическими*. Гипотезы о *законе распределения* случайных величин называются *непараметрическими*.

Статистическим критерием называется правило, согласно которому для каждой реализации выборки гипотеза отвергается или не отвергается.

Для построения критерия используется некоторая *случайная* величина - *статистика критерия* – с известным законом распределения, когда проверяемая гипотеза верна.

Проверяемую гипотезу обозначают *H*0 и называют *основной (нулевой*) гипотезой. *Альтернативная* с *H*0 гипотеза обычно обозначается *H1*.

Ошибкой первого рода α называется не принятие **верной** гипотезы *H0*.

$$P(|T| < T\alpha \mid H0) = \alpha$$

Величину Tα называют критической границей, или критическим уровнем, а вероятность α — уровнем значимости критерия.

Вероятность допустить ошибку первого рода равна уровню значимости α.

Ошибкой второго рода β называется *принятие* **неверной** гипотезы *H0*.

Мощностью критерия называется *вероятность* не совершения ошибки второго рода (1 – β).

Критерий согласия и вид критической области подбираются так, чтобы мощность критерия была наибольшей.

Тестирование псевдослучайности

Тесты Д.Кнута основаны на статистическом критерии χ^2 (хи^2) Пирсона.

Вычисляемое значение статистики χ^2 сравнивается с табличными результатами, и в зависимости от вероятности появления такой статистики делается вывод о её качестве.

Большинство тестов используют метод проверки гипотезы о случайности последовательности с использованием статистического распределения.

Мерой расхождения теоретического и эмпирического распределений является *взвешенная сумма квадратов отклонений*.

$$U = \sum_{i=1}^{k} \frac{(n_i - n \cdot p_i)^2}{n \cdot p_i} = \chi^2,$$

Тестирование выборок

Рекомендуется иметь в каждом из ***k*** интервалов

разбиения (bins, pockets) измерений ***ni* > 5**.

$$U = \sum_{i=1}^{k} \frac{(n_i - n \cdot p_i)^2}{n \cdot p_i} = \chi^2,$$

pi - вероятность появления

значения из ***i***-го интервала

Формирование гипотезы о типе закона распределения происходит после построения частотной гистограммы для выборки.
Формы гистограмм нормального, показательного и равномерного законов распределения принципиально различные.

Например, для проверки в Excel используют функцию ХИ2.ОБР.ПХ()

Если χ^2 наблюд < χ^2 критич - гипотеза о законе распределения принимается

Если χ^2 наблюд > χ^2 критич - гипотеза о законе распределения отвергается

Вычислительные тесты Д. Кнута

Проверка несцепленных серий -- Последовательность разбивается на **m** непересекающихся серий и строится распределение χ^2 для частот появления каждой возможной серии.

Проверка интервалов -- Данный тест проверяет равномерность распределения символов в исследуемой последовательности, анализируя длины подпоследовательностей, все элементы которых принадлежат определённому числовому интервалу.

Проверка комбинаций -- Последовательность разбивается на подпоследовательности определённой длины, и исследуются серии, состоящие из различных комбинаций чисел.

Проверка перестановок -- Данный тест проверяет равномерность распределения символов в исследуемой последовательности, анализируя взаимное расположение чисел в подпоследовательностях.

Проверка на монотонность -- Служит для определения равномерности исходя из анализа невозрастающих и неубывающих подпоследовательностей.

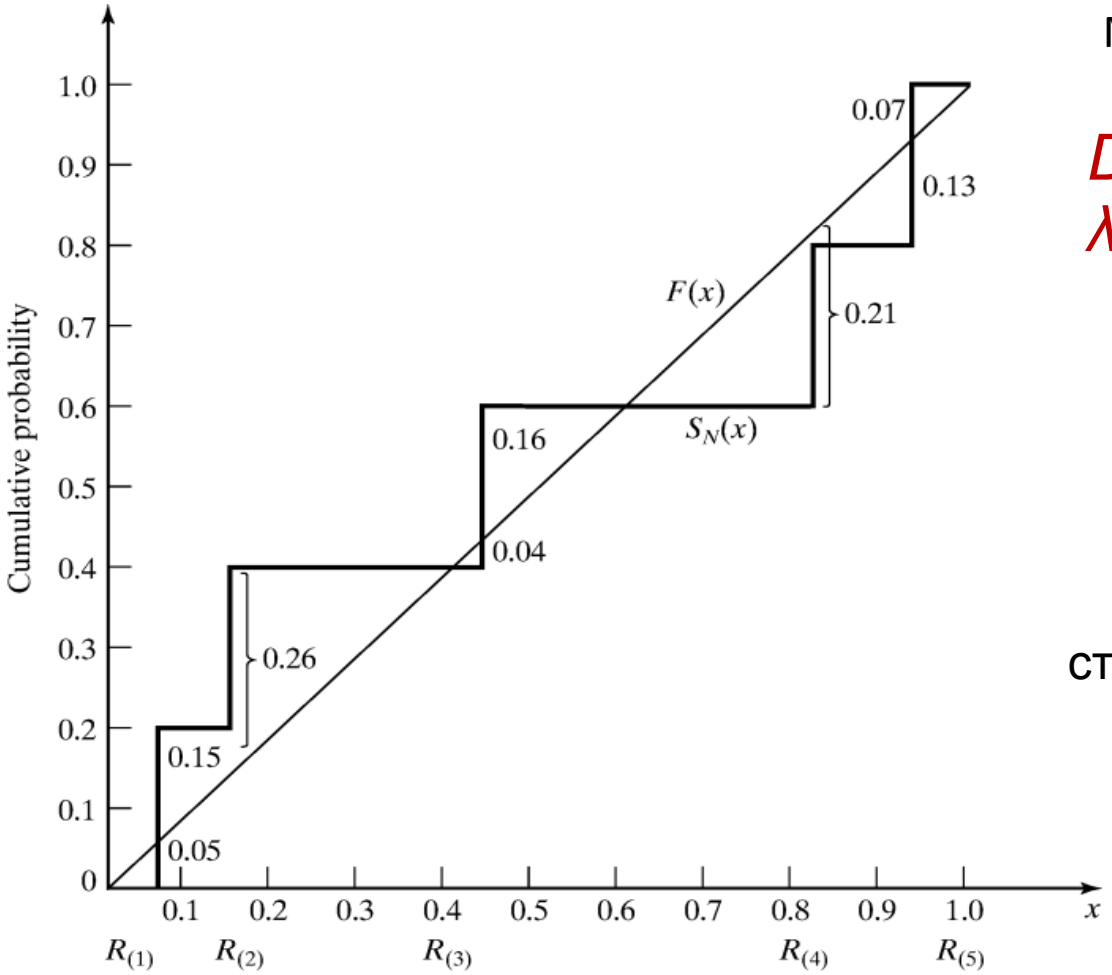
Проверка корреляции -- Данный тест проверяет взаимонезависимость элементов последовательности.

Проверка распределения

на равномерность по критерию согласия Колмогорова-Смирнова

необходимо построить функции распределения F(x) для теоретического и эмпирического распределений, определить максимум **d** модуля разности между ними и найти **λ**, затем найти критическую вероятность P(*λ*)

i	*1*	*2*	*3*	*4*	*5*
R(i)	*0.05*	*0.14*	*0.44*	*0.81*	*0.93*
i/N	*0.20*	*0.40*	*0.60*	*0.80*	*1.00*
i/N -R(i)	*0.15*	*0.26*	*0.16*	*-*	*0.07*
R(i)-(i-1)/N	*0.05*	*-*	*0.04*	*0.21*	*0.13*



Малое P значит неприемлемость гипотезы!

$D = max(D+, D-) = 0.26$

$\lambda^* \approx \sqrt{N} D \rightarrow \lambda^* \approx 2.236 * 0.26 \approx 0.581$

λ	0,4	0,6	0,8	1,0	1,5
P(λ)	0,997	0,864	0,544	0,27	0,022

при $n \rightarrow \infty$ вероятность $d\sqrt{n} \geq \lambda$

стремится к пределу $P(\lambda) = 1 - \sum_{k=-\infty}^{\infty} (-1)^k e^{-2k^2\lambda^2}$.

$\lambda = \sqrt{N} D + 1 / (6\sqrt{N})$

критерий с поправкой Большева

Графические тесты

К этой категории относятся тесты, результаты которых отображаются в виде графиков, характеризующих свойства исследуемой последовательности :

гистограмма распределения элементов последовательности -- позволяет оценить равномерность распределения чисел в под-интервалах и определить частоту повторения каждого под-интервала;

распределение на плоскости -- предназначено для определения зависимости между элементами последовательности;

проверка серий -- позволяет определить равномерность отдельных символов в последовательности, а также равномерность распределения серий из К бит;

проверка на монотонность -- служит для определения равномерности исходя из анализа невозрастающих и неубывающих подпоследовательностей;

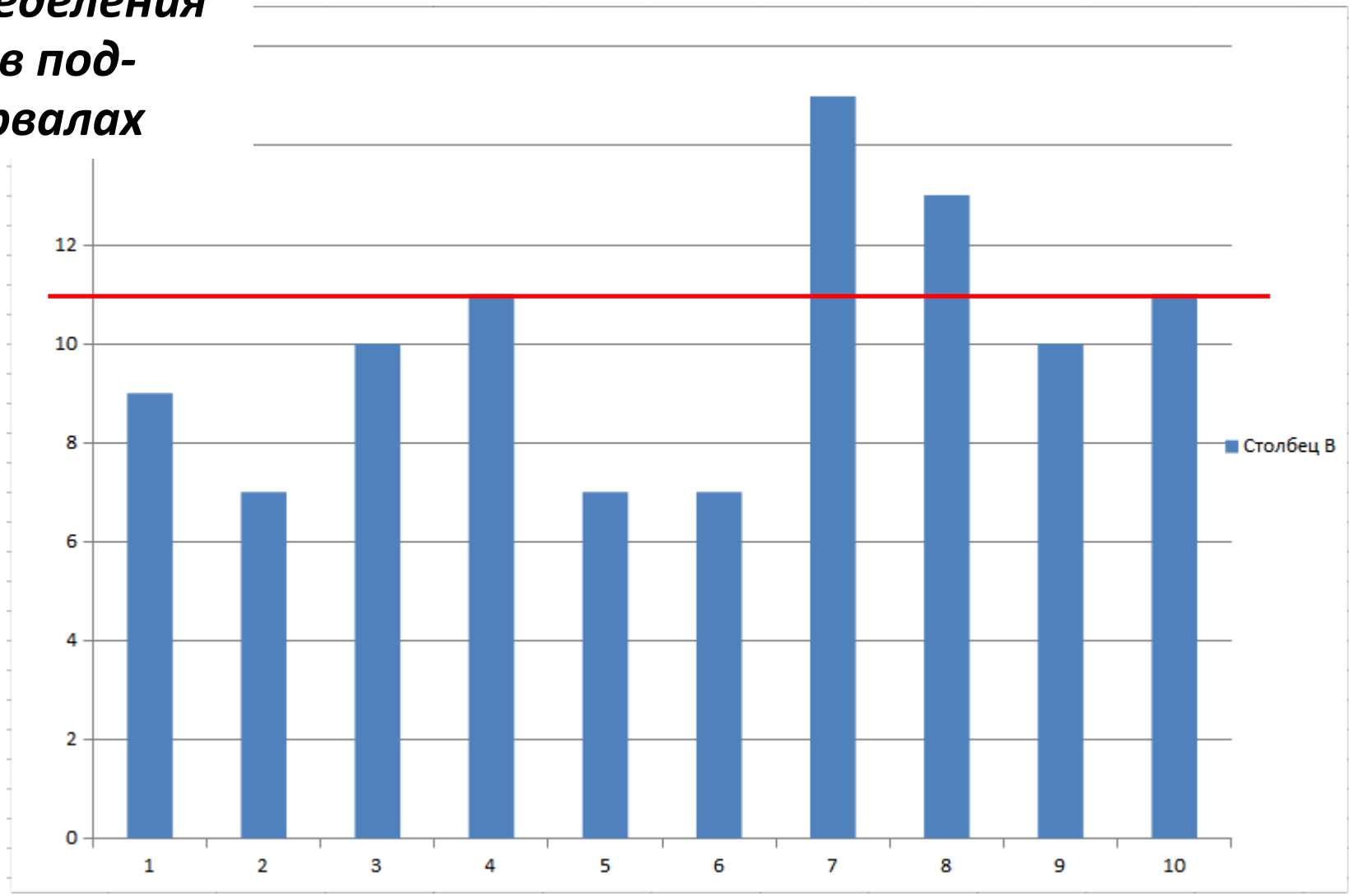
автокорреляционная функция -- предназначена для оценки корреляции между сдвинутыми копиями последовательностей и отдельных выборок;

профиль линейной сложности -- тест оценивает зависимость линейной сложности последовательности от её длины;

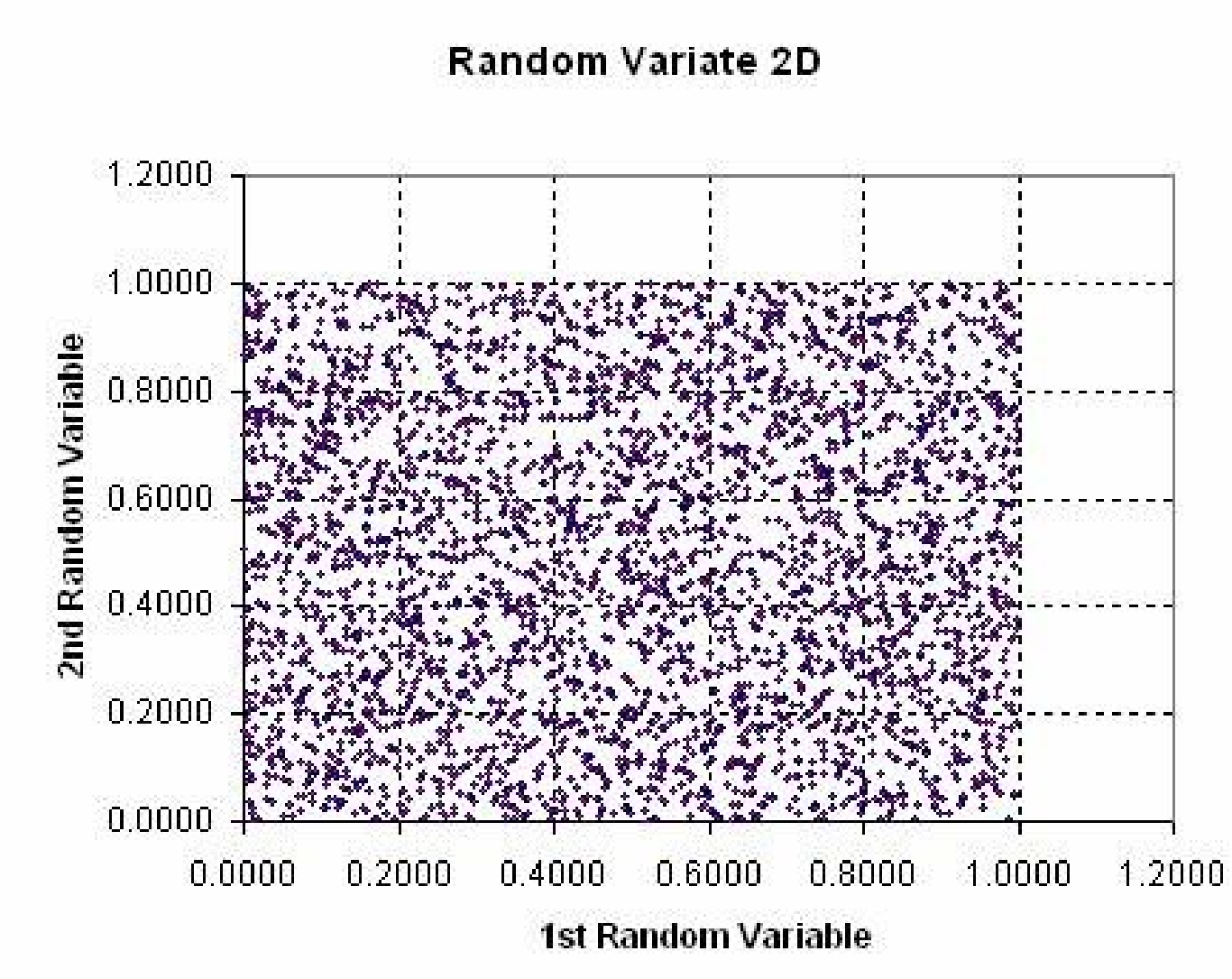
графический спектральный тест -- позволяет оценить равномерность *распределения бит последовательности* на основании анализа размаха выбросов (преобразование Фурье).

Проверка качества равномерности

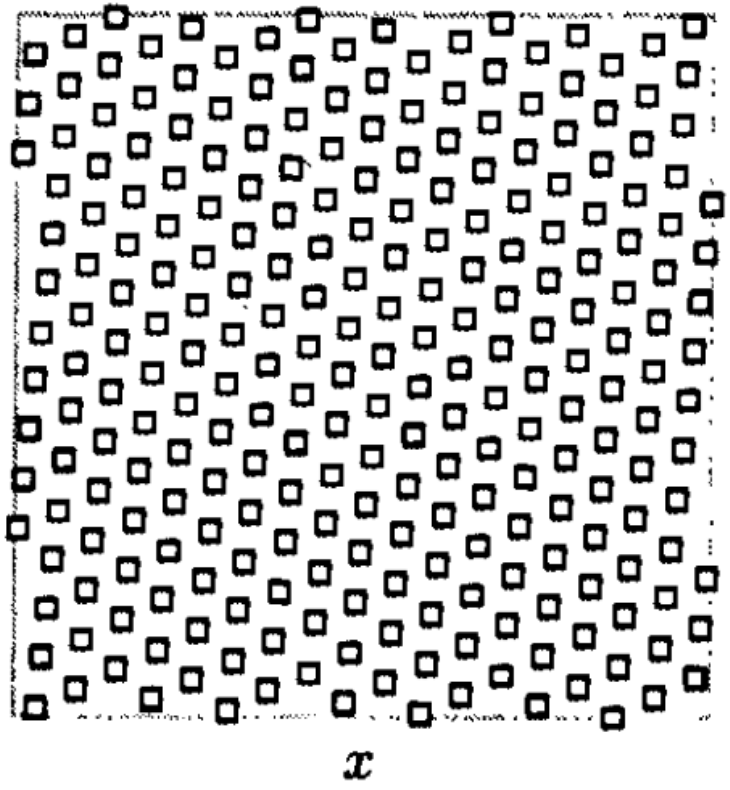
Гистограмма ***распределения чисел в под-интервалах***



Распределение на плоскости

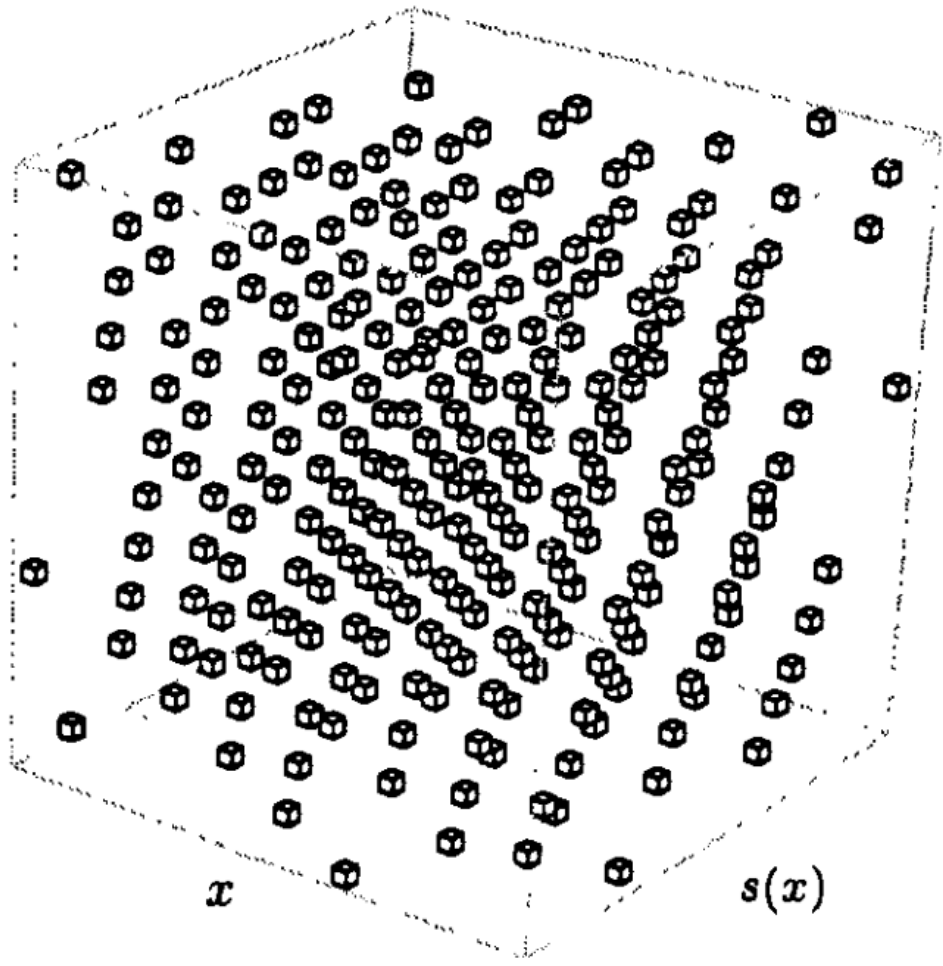


Распределение в пространстве



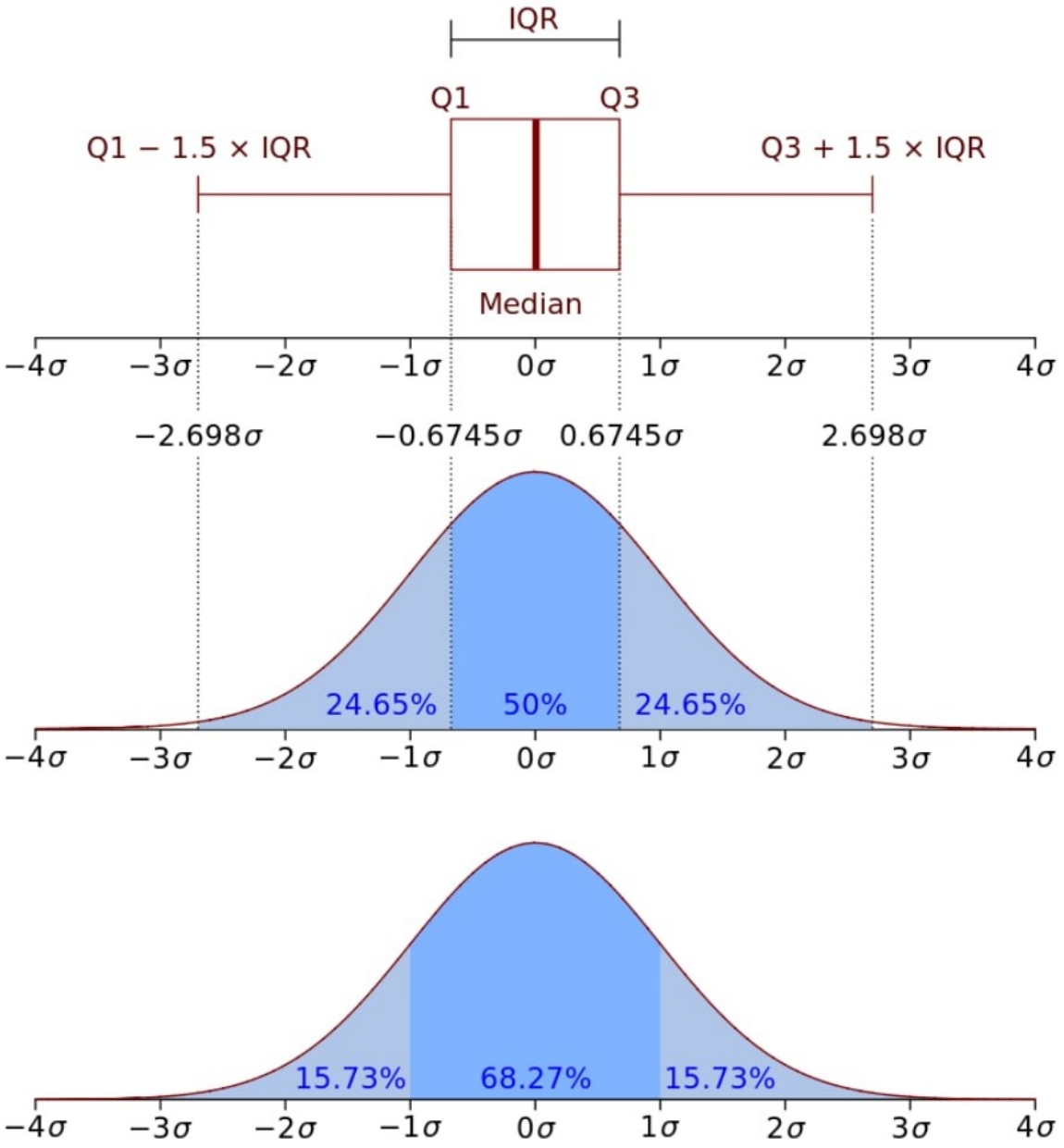
(a) Двумерная решетка, образованная всеми парами последовательных точек (X_n, X_{n+1}), где $X_{n+1} = (137X_n + 187) \bmod 256$.

(b)



Трехмерная решетка трехмерных строк (X_n, X_{n+1}, X_{n+2})

Проверка нормального распределения



Признаки:

Mean =

Median =

Mode

Skewness =0

(скошенность)

Kurtosis =0

(эксцесс)

IQR – межквартильный интервал

Основные тесты СП

1 – На равномерность, например, по критерию согласия или с помощью частотной гистограммы

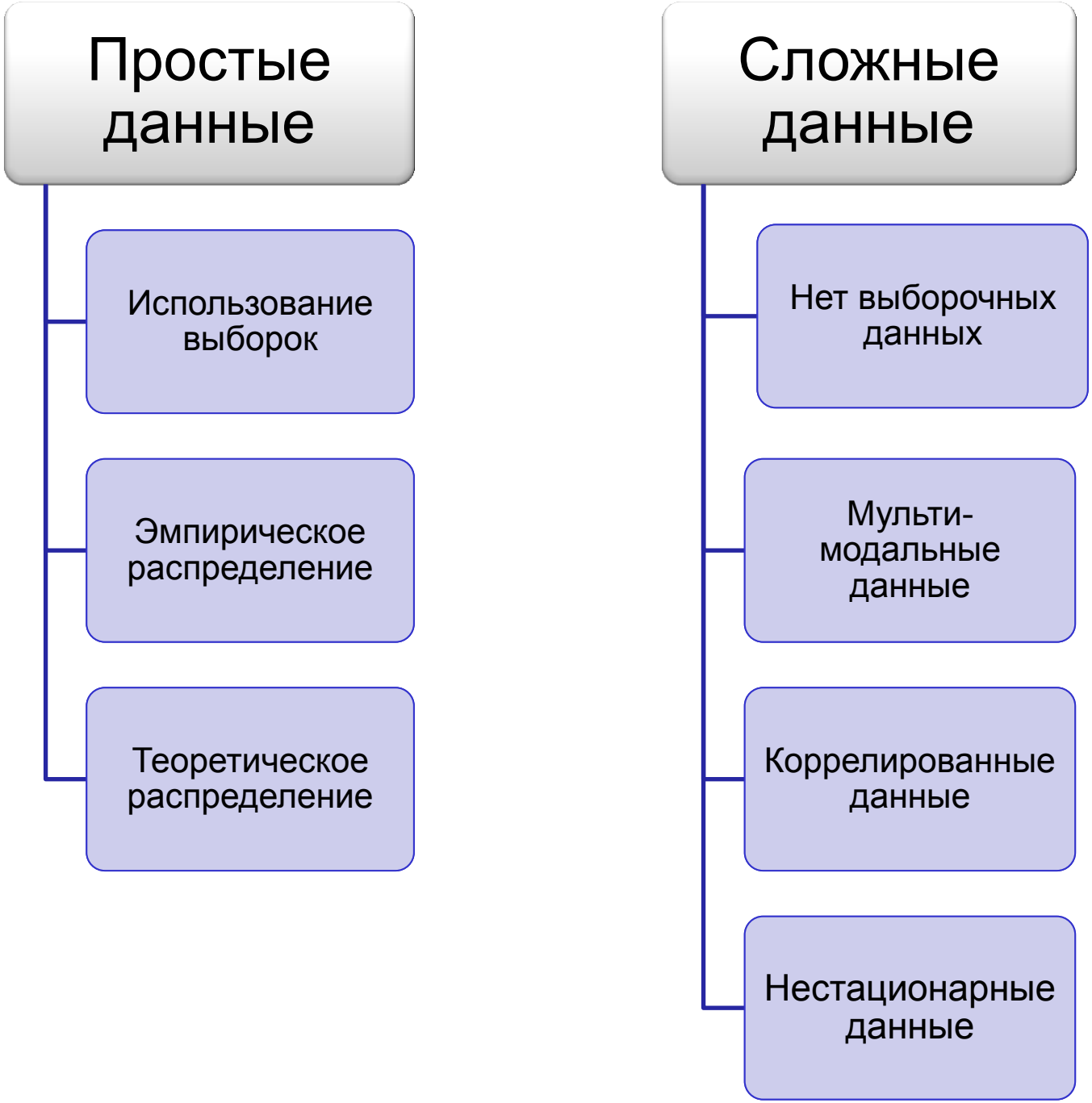
$H_0: Ri \sim U[0,1]$
$H_1: Ri \not\sim U[0,1]$

2 – На независимость (автокорреляцию), например, по критерию автокорреляции или с помощью матрицы корреляции (спектральный тест)

$H_0: Ri \sim independently$
$H_1: Ri \not\sim independently$

Следует помнить, что есть ошибки 1-го рода и 2-го рода.
Если проверяемая *гипотеза* не была отклонена, это еще не означает, что она справедлива.
Организуя процедуру проверки и зная, какие альтернативы *H0 - H1* должны различаться, необходимо выбирать такие *объемы выборок*, чтобы вероятность ошибки 2-го рода оказалась не меньше β.

Для многих проектов моделирования задача разработки хороших моделей входных данных может быть значительно *более сложной*.



Путь к пониманию стохастических процессов:

от **случайных событий**

Случайная переменная СП

(random variable - RV)

переходим от логики к числам

\+ **случайные переменные**

добавляем взаимосвязь между двумя СП

\+ **комбинация двух случайных переменных**

рассматриваем свойства нескольких СП

\+ **последовательность случайных переменных**

привязываем появление СП к моментам времени

= **стохастический (случайный) процесс**

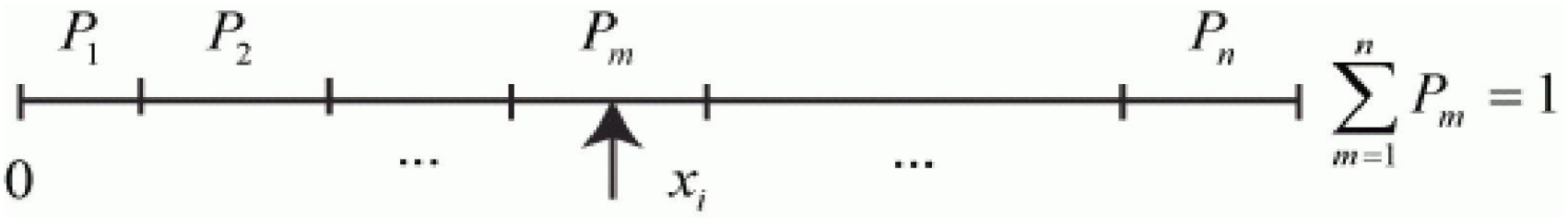
Моделирование событий

Теорема:

В полной группе несовместных событий моделью свершения события *Am*, происходящего с вероятностью *Pm*, является попадание значения x_i в отрезок, равный *Pm* числовой шкалы --

где *n* -число несовместных событий

$$\sum_{m=1}^{n} \mathbb{P}_m = 1$$



Способ определения исходов по жребию

Пример: линия связи может быть в одном из 4 состояний {A}.
Выпало случайное число 0,56. Какое состояние **A - ?**

Состояние	**A1**	**A2**	**A3**	**A4**
Вероятность состояния	**0,15**	**0,4**	**0,25**	**0,2**
Суммарная вероятность	**0,15**	**0,55**	**0,8**	**1,0**

Моделирование событий

Совместные независимые события в модели сводятся к ***одному сложному*** событию.

Пусть независимые события A и B происходят с вероятностями P(A) и P(B) соответственно.
Возможные исходы совместного события *Qi* и его вероятностей *Pi* :

Q_i	AB	$\overline{A}B$	$A\overline{B}$	$\overline{AB}$
P_i	$P_1 = P(A)P(B)$	$P_2 = (1 - P(A))P(B)$	$P_3 = P(A)(1 - P(B))$	$P_4 = 1 - P_1$
l_r	$l_1 = P(A)P(B)$	$l_2 = l_1 + (1 - P(A))P(B)$	$l_3 = l_2 + P(A)(1 - P(B))$	1

Проверку свершения каждого из совместных событий надо осуществлять разными случайными числами, т.к. события независимые

Важнейшим свойством случайного процесса является свойство ***эргодичности***.

Свойство ***эргодичности*** заключается в том, что все реализации случайного процесса имеют одинаковые статистические характеристики. Отсюда следует, что одна реализация случайного процесса характеризует весь случайный процесс, т.е. для определения основных статистических характеристик процесса достаточно выполнить одну реализацию.

Обычно рассматривают свойство эргодичности *по* отношению к одной какой-либо характеристике случайного процесса.

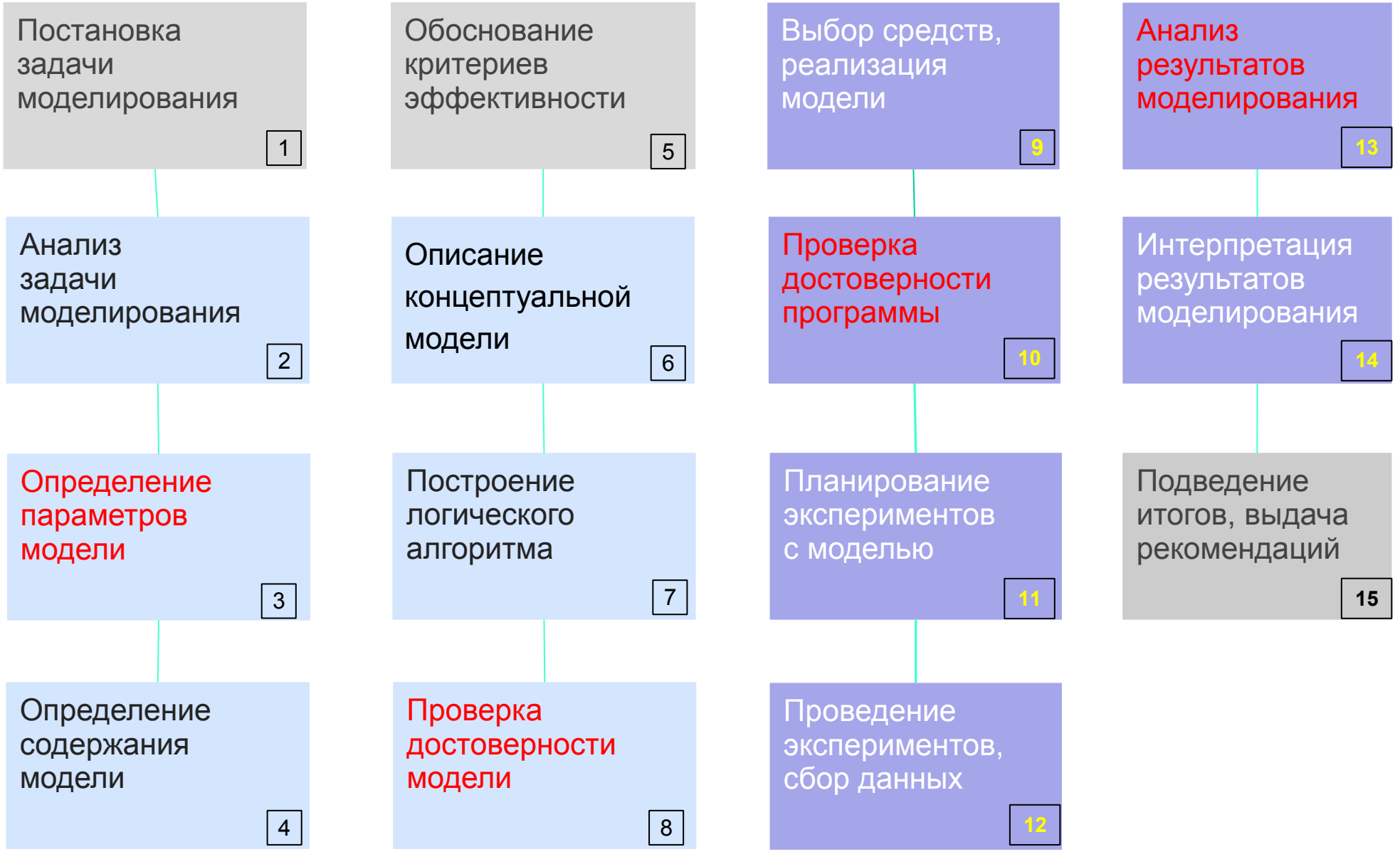
Относительно оценки матожидания свойство ***эргодичности*** формально выглядит так:

$$\frac{1}{N}\sum_{i=1}^{N} x_i(t_j) = \frac{1}{M}\sum_{j=1}^{M} x_i(t_j)$$

Случайный процесс $X(t)$ называется ***эргодическим,*** если его основные характеристики $M[x]$ и $D[x]$ могут быть получены не только усреднением по множеству реализаций, но и усреднением по времени одной реализации.

Например, при изучении флуктуационного шума радиоприемников, представляющего собой стационарный случайный процесс, достаточно ограничиться измерением значений в течение заданного времени Т в одном конкретном образце, и результаты, полученные при обработке данных измерений, могут быть распространены на все идентичные радиоприемники.

Этапы проекта моделирования



Оценка адекватности имитационной модели объекту-оригиналу

Оценка состоит в сравнении статистических характеристик реальной и модельной систем (РС и ИМ) на основе использования методов математической статистики.

Процедура статистического оценивания средних значений выходных статистик ИМ и объекта-оригинала осуществляется как проверка гипотезы о близости средних значений каждой *k*-й компоненты откликов модели *Yk*, известным средним значениям *k*-й компоненты откликов реальной системы *Yk*.

Для этого проводят *N1* опытов на реальной системе и *N2* опытов на ИМ (обычно *N2 > N1*). Для РС и ИМ определяют значения математического ожидания и дисперсии.

Оценка адекватности имитационной модели объекту-оригиналу

Гипотезу *о равенстве средних значений* проверяют при помощи параметрического критерия *z-теста* или по *t-критерию* Стьюдента.

Адекватность модели можно проверить с использованием гипотезы о *равенстве дисперсий отклонений* откликов модели от среднего значения выходных статистик системы. Сравнение дисперсий производится с помощью F-критерия Фишера.

Тестирование гипотезы о *согласованности* распределений откликов реальной системы и откликов ИМ для размера выборки более 100 наблюдений проводят на основе критерия χ^2 .

Для выборок среднего объема ($30 < N < 100$) используют критерий Колмогорова - Смирнова. При малых выборках – критерий Крамерса–фон Мизеса или Колмогорова с поправкой Большева.

Верификация имитационной модели

Верификация - это доказательство утверждения о том, что алгоритм имитационного моделирования, заложенный в разработанную ИМ, отражает замысел исследователя (аналитика).

Процедура верификации заключается в выполнении следующих шагов:

1) проверка работоспособности компонентов системы с проверкой адекватности модельных результатов;
2) осуществление имитационного эксперимента на натурном потоке данных. При этом прогон осуществляется в два этапа:

- управляющие переменные изменяются по всему диапазону значений, а контролируются значения результатов модели;
- проверка соответствия выходных характеристик системы, если ее параметры достигают максимума и минимума.

Верификация имитационной модели

3) проверка на ожидаемость. На этом шаге можно заменить элементы модели стохастические на детерминированные и анализируют результат моделирования. Формальные процедуры верификации связаны с проверкой верности исходных предпосылок.

Алгоритм верификации модели состоит из таких действий:

- анализ компонентов разработанной модели, сопоставление их с аналогичными компонентами объекта-оригинала и обоснование их наличия в ИМ;
- покомпонентное тестирование выходных потоков;
- формулирование и проверка статистических гипотез.

Валидация имитационной модели

Валидация — это проверка согласованности результатов, полученных в ходе реализации имитационной модели, и ожидаемых значений величин, характеризующих реальные процессы и системы, для описания которых создавалась имитационная модель.

Валидация результатов моделирования производится после проведения процедуры верификации модели и проверки логико-математической схемы построения имитационной модели.

Процедура валидации состоит в проверке выходных данных после проведения имитационного эксперимента и сопоставления их с имеющимися статистическими сведениями о моделируемой системе (процессе).

Статистические дескрипторы делятся на три категории:

(1) дескрипторы, которые помогают определить центр распределения, например, среднее значение;

(2) дескрипторы, которые измеряют разброс распределения, например, дисперсия;

(3) дескрипторы, которые указывают на относительное положение в генеральной совокупности, такие как вероятность возникновения или местоположение в квартиле.

Стохастические характеристики:

- математическое ожидание (expectation)
- медиана (median)
- мода (mode)
- дисперсия (variance)

Характеристики случайных переменных

определяются моментами случайных переменных

Оценки

Имитационная модель строится для определения характеристик некоторых случайных величин. Такими случайными величинами могут быть:

- *время обслуживания заявки в системе*;
- *расход сырья*;
- *количество выполненных работ*;
- *время наработки на отказ технического устройства*…

Из характеристик случайных величин наиболее интересуют*:*

матем.ожидание, дисперсия, коэффициент корреляции.

Приближенное значение называют ***оценка*** *характеристики:*

оценка матем.ожидания, оценка дисперсии, оценка коэффициента корреляции.

Оценки

В общем случае модель может служить для достижения двух целей:

описательной — для объяснения или лучшего понимания объекта;

предписывающей — для предсказания и/или воспроизведения характеристик объекта, определяющих его поведение.

Предписывающие модели являются и описательными,
но не наоборот.

Предписывающие модели явно предпочтительнее по своим возможностям, но сложнее по реализации,
поэтому их построение не всегда возможно.

Оценки точности

Точностью характеристики $\overline{\Theta}$ называют величину ε в отношении

$$\left|\overline{\Theta} - \quad M\left[\Theta\right] \right| \leq \varepsilon$$

где $M[\Theta]$ - матем.ожидание случайной величины.

Достоверностью (доверительной вероятностью или надежностью) оценки характеристики $\overline{\Theta}$ называют вероятность α того, что заданная точность достигается:

$$P\left(\left|\overline{\Theta} - M\left[\overline{\Theta}\right]\right| < \varepsilon\right) = \alpha$$

Доверительным называется интервал (*confidence interval*), в который попадают измеренные в эксперименте значения, соответствующие доверительной вероятности.

В доверительном интервале значение точности оценки определяется шириной доверительного интервала: чем меньше доверительный интервал, тем выше точность оценки.

Надежность относится к вероятности того, что оценка верна. Надежность зависит от выбора параметра **α**, используемого при расчете.

Оценка доверительного интервала включает информацию, касающуюся как точности, так и надежности оценки.

Это важные фрагменты информации при принятии решения о значимости оценки.

Точность и надежность - конкурирующие величины: чем больше точность, тем меньше надёжность.

Цель состоит в том, чтобы получить оценку, обладающую приемлемой надежностью и точностью.

Оценка количества реализаций

Связь точности ε и достоверности α с количеством реализаций N модели, когда целью эксперимента является определение оценки матем.ожидания некоторой случайной величины b.

В качестве оценки матем.ожидания возьмём выборочное среднее -

$$\bar{b} = \frac{\sum_{i=1}^{N} b_i}{N}$$ с параметрами $$M\left[\bar{b}\right] = M\left[b\right], \ldots \sigma^2 = \frac{\sigma_b^2}{N}$$

$$P\left(\left|\bar{a} - M\left[b\right]\right| < t_\alpha \sigma_{\bar{b}}\right) = \Phi^*(t_\alpha) = 2\Phi(t_\alpha)$$

Оценка количества реализаций

Связь точности ε и достоверности α с количеством реализаций *N* модели, когда целью эксперимента является определение оценки матем.ожидания некоторой случайной величины ***b***.

$$\varepsilon = t_\alpha \frac{\sigma_b}{\sqrt{N}} \qquad N = t_\alpha^2 \frac{\sigma_b^2}{\varepsilon^2} \qquad S_b^2 = \frac{\sum_{i=1}^{N} (b_i - \bar{b})^2}{N^* - 1}$$

Фрагмент таблицы функции Лапласа

α	***0.8***	***0.9***	***0.95***	***0.99***	***0.995***	***0.997***	***0.999***
$t\alpha$	1.28	1.65	1.96	2.58	2.81	3.0	3.30

$t\alpha$ - двухстронняя квантиль станд.норм.распред. для $P|b - \mu| <= \varepsilon$

Связь точности ε и достоверности α с количеством реализаций ***N*** модели при малом числе степеней свободы k **= N-1** *(при N<100)* :

- для оценки матожидания :

$$N = \frac{\sigma_\alpha^2}{\varepsilon^2(1-\alpha)} \Rightarrow \varepsilon = \sqrt{\frac{\sigma_\alpha^2}{N(1-\alpha)}}$$

- для оценки дисперсии :

$$N = t_\alpha^2 \frac{2S^4}{\varepsilon^2};\ \varepsilon = t_\alpha \frac{S^2\sqrt{2}}{\sqrt{N}}$$

Фрагмент таблицы распределения Стьюдента

p=(1-α)	*0.8*	*0.9*	*0.95*	*0.99*	*0.995*	*0.999*	k
t_α*	**1.28**	**1.66**	**1.98**	**2.62**	**2.86**	**3.37**	120
	1.30	**1.67**	**2.0**	**2.66**	**2.91**	**3.46**	60
	1.31	**1.7**	**2.04**	**2.75**	**3.03**	**3.65**	30
	1.37	**1.81**	**2.23**	**3.17**	**3.58**	**4.59**	10

Оценка количества реализаций

Связь точности ε и достоверности α с количеством реализаций N измерений, когда в качестве показателя эффективности выступает **вероятность** свершения какого-либо события.

В качестве оценки вероятности события выступает частота его свершения:

$$\bar{P} = m / N$$

где N - число реализаций модели;
m - число свершений данного события.

$$P(| \bar{P} — P|) < \varepsilon) = \alpha$$

$$\overline{P} = \frac{\sum_{i=1}^{N} x_i}{N}$$

частота свершения события
(оценка искомой вероятности)

Оценка количества реализаций

Связь точности ε, достоверности α с количеством реализаций N модели, когда в качестве показателя эффективности выступает **вероятность** свершения какого-либо события.

$$M\left[\sum_{i=1}^{N} x_i\right] = NP \qquad D\left[\sum_{i=1}^{N} x_i\right] = NP(1-P)$$

$$D\left[\overline{P}\right] = \frac{1}{N^2} NP(1-P) = \frac{P(1-P)}{N} = \sigma_P^2$$

$$P(|\overline{P} - P| < t_\alpha \sigma_{\overline{P}}) = 2\Phi(t_\alpha)$$

$$\varepsilon^2 = t_\alpha^2 \frac{P(1-P)}{N} \qquad N = t_\alpha^2 \frac{P(1-P)}{\varepsilon^2}$$

для P = 0.5

$$N_m = \frac{t_\alpha^2}{4\varepsilon^2}$$