Лекция

фрагменты

математической статистики

и теории вероятностей

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 (т.е. повторять последовательность чисел)

Генератор псевдослучайных чисел

Большинство простых арифметических генераторов обладают большой скоростью, но имеют недостатки:

- короткий период последовательности чисел;
- последовательные значения не являются независимыми;
- некоторые биты «менее случайны», чем другие;
- неравномерное одномерное распределение.

Наиболее распространённые программные алгоритмы ГПСЧ:

- линейный конгруэнтный метод,
- метод с регистром сдвига с линейной обратной связью,
- метод с регистром сдвига с обобщённой обратной связью.

Распространённый метод генерации случайных чисел — **линейный конгруэнтный метод** (его вариант — **аддитивный конгруэнтный метод).** Эти методы генерируют последовательность чисел, удовлетворяющую условию случайности.

Генератор псевдослучайных чисел

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

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

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

a — множитель (0< a < m) ,

c — приращение (0< c < m),

$\mathbf{X_0}$ — начальное значение (X_0 < m).

Такой ряд называется *линейной конгруэнтной последовательностью.* ЛКП, определенная числами ***m***, ***a***, ***c*** *и* $\boldsymbol{X_0}$, периодична с периодом, не превышающим ***m***.

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

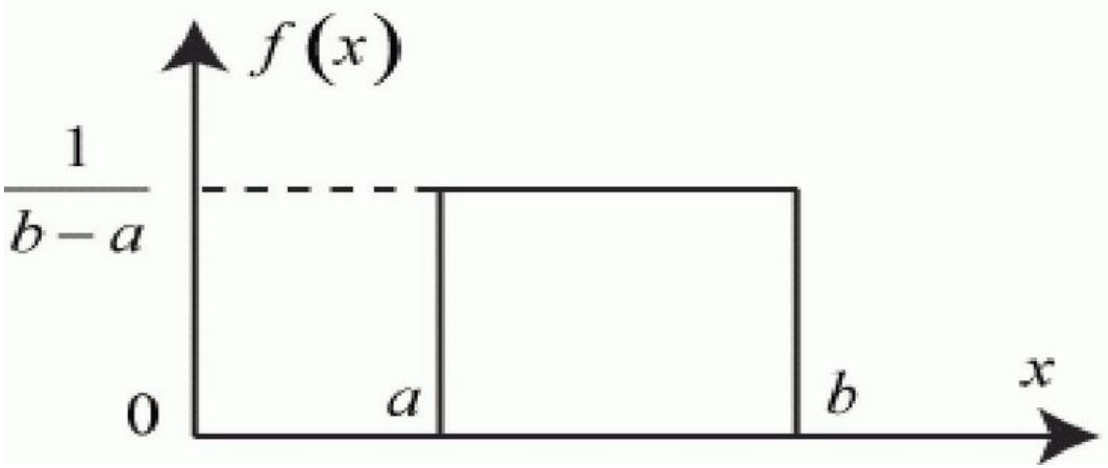
числа ***c*** и ***m*** взаимно простые (они не имеют никаких общих делителей);

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^e***,
где ***e*** — 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 * 0.4656613e–9;
    ax = ix;
    return (rnd);
}
```

ГПСЧ 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;
}
```

ГПСЧ Mersenne twister

Наиболее распространённым вариантом является алгоритм *MT19937*, период которого составляет ($2^{19937} - 1$) (т.е. приблизительно $43 \bullet 10^{6000}$).
«Вихрь Мерсенна» является алгоритмом с регистром сдвига с обобщённой обратной связью (twisted generalised feedback shift register). «Вихрь» — это преобразование, которое обеспечивает равномерное распределение генерируемых псевдослучайных чисел в 623 измерениях (по сравнению с линейным конгруэнтным генератором с 5 измерениями).
Функция корреляции между двумя последовательностями выборок в выходной последовательности «вихря Мерсенна» пренебрежимо мала!

Таблица 1

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

«Вихрь Мерсенна» алгоритмически реализуется двумя основными частями: рекурсивной и упрочняющей.
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.
Регистр сдвига состоит из 624 элементов, в общей сложности из 19937 бит.
Каждый элемент имеет длину 32 бита, за исключением первого элемента, который имеет только 1 бит.
Процесс генерации начинается с логического умножения на битовую маску, отбрасывающей 31 бита (кроме наиболее значащих).
Следующим шагом выполняется инициализация (x0, x1,..., x623) любыми беззнаковыми 32-разрядными целыми числами.
Последующие шаги включают в себя объединение и переходные состояния.
Алгоритм выполняется в шесть этапов:

Алгоритм Mersenne twister

Шаг 0. Предварительно инициализируется значение констант ***u1***, ***h1***, ***a*** *u1* ← 10…0 битовая маска старших *w-r* бит,
h1 ← 01…1 битовая маска младших *r* бит,
a ← $a_{w-1}a_{w-2}\ldots a_0$ последняя строка матрицы *A*.

Шаг 1. ***x***[0], ***x***[1],…, ***x***[n-1] // начальное заполнение

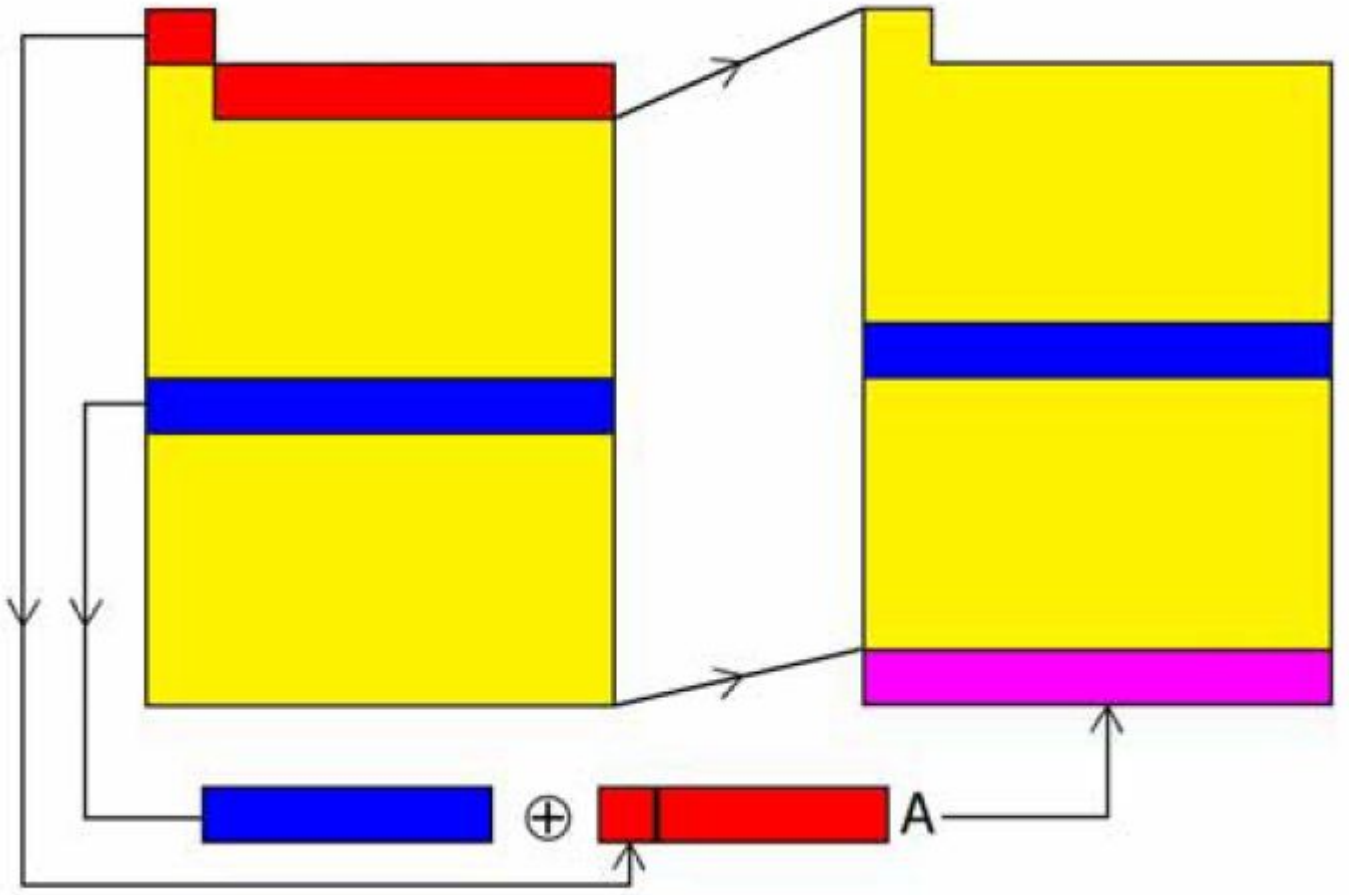
Шаг 2. Вычисление $(x_i^u \mid x_{i+1}^l)$ // upper-lower
y ← (***x***[i] AND *u1*) OR (***x***[(i + 1) mod n] AND *h*1)

Шаг 3. Вычисляется значение следующего элемента последовательности по рекуррентному выражению
x[i] ← ***x***[(i + m) mod n] XOR (***y***>>1) XOR *a* если младший бит ***y***=1
или ***x***[i] ← ***x***[(i + m) mod n] XOR (***y***>>1) XOR 0 если младший бит ***y***=0

Шаг 4. Вычисление ***x***[i]*T*
y ← ***x***[i] ***y*** ← ***y*** XOR (***y***>>*u*) ***y*** ← ***y*** XOR ((***y***<<*s*) AND **b**)
y ← ***y*** XOR ((***y***<<*t*) AND **c**) ***z*** ← ***y*** XOR (***y***>>*l*)
вывод *z*

Шаг 5. i ← (i + 1) mod n

Алгоритм Mersenne twister



Логическая схема алгоритма

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

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

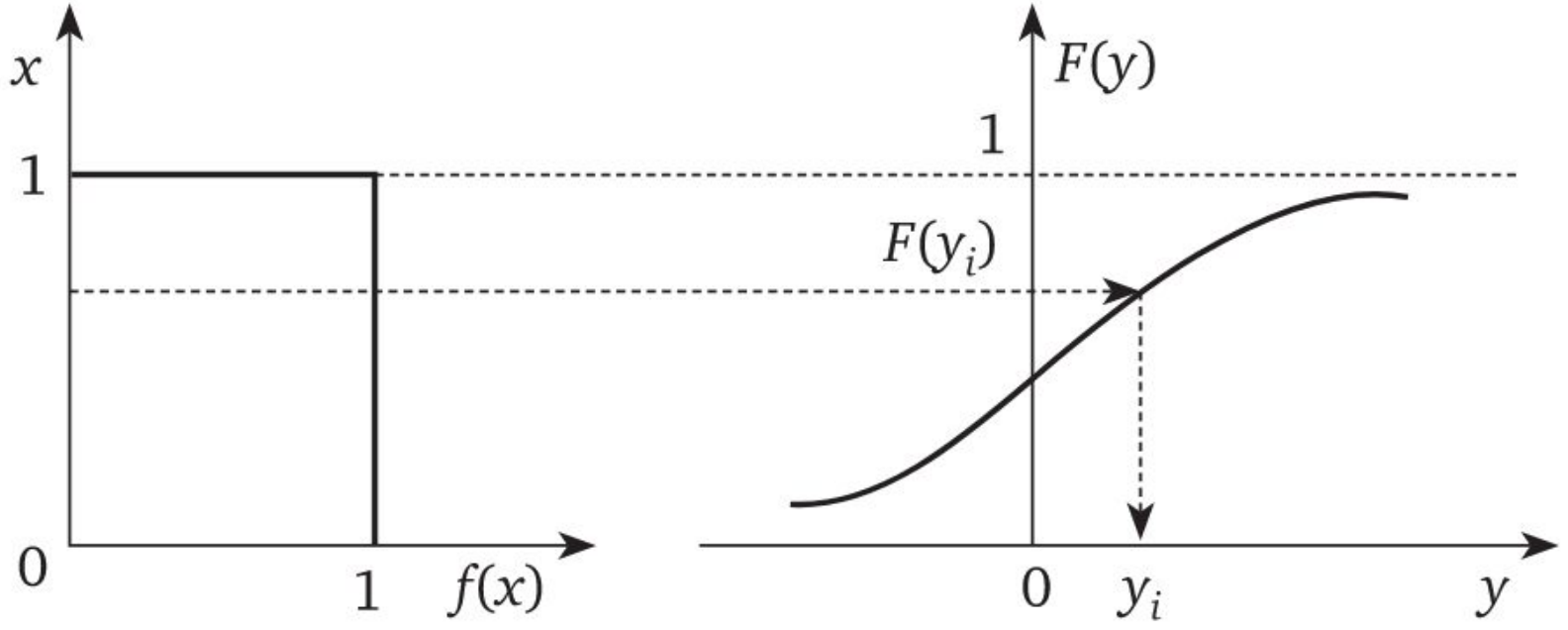
Здесь функция random() – стандартный ГПСЧ в интервале [0..1)

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) ~



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

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

Произвольное распределение

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

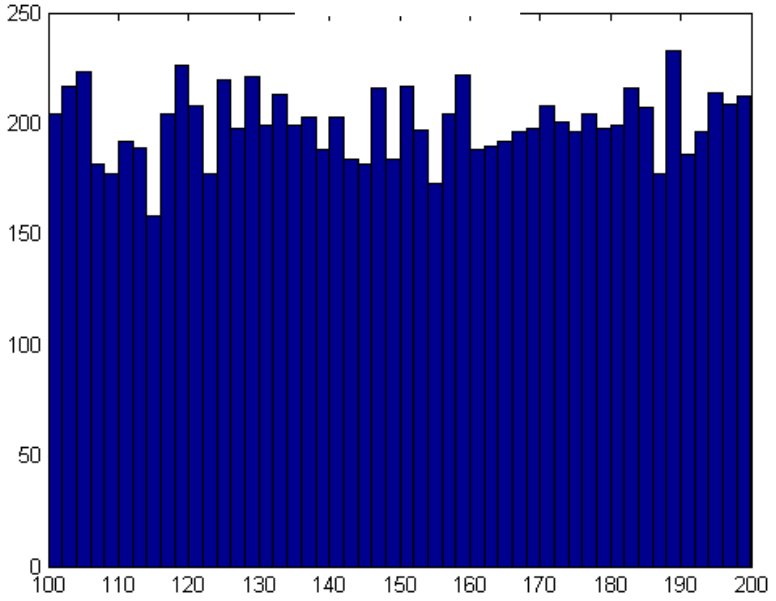
Используя генератор стандартного непрерывного равномерного распределения, можно получить выборку из распределения, задаваемого функцией распределения ***F(x)***.

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

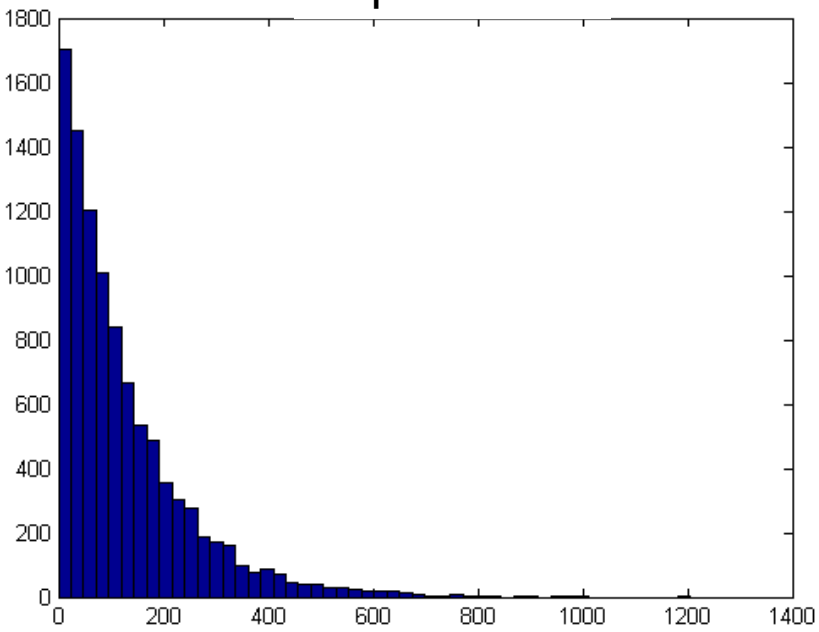
При *биективном* отображении каждому элементу одного множества соответствует ровно один элемент другого множества, при этом определено обратное отображение, которое обладает тем же свойством. Поэтому *биективное* отображение называют ещё взаимно-однозначным отображением (соответствием).

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

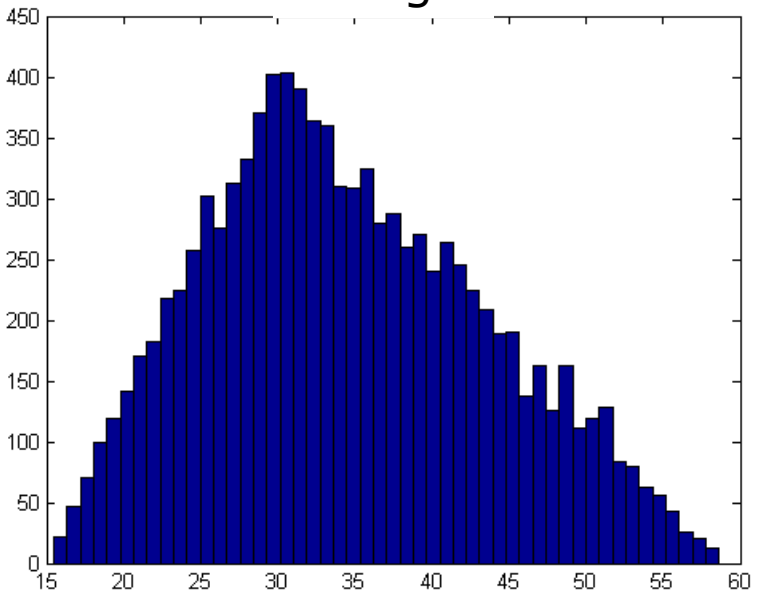
uniform



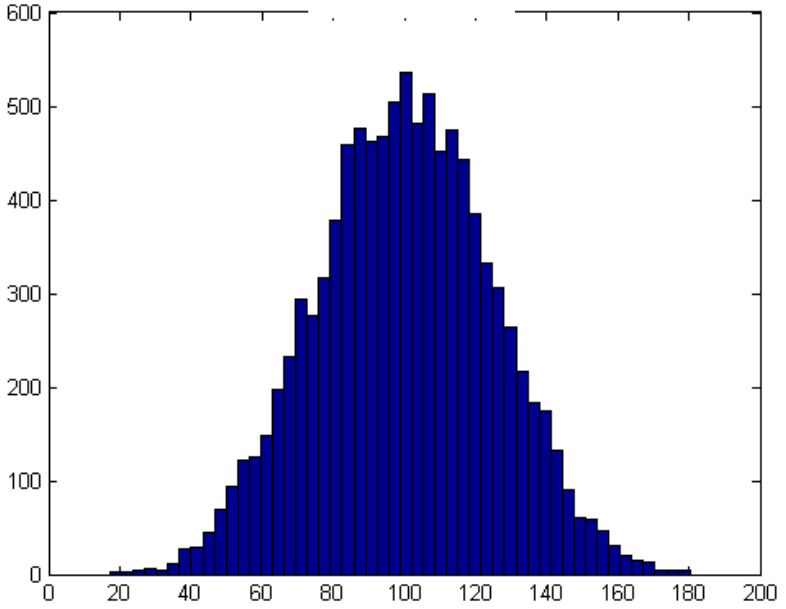
exponential



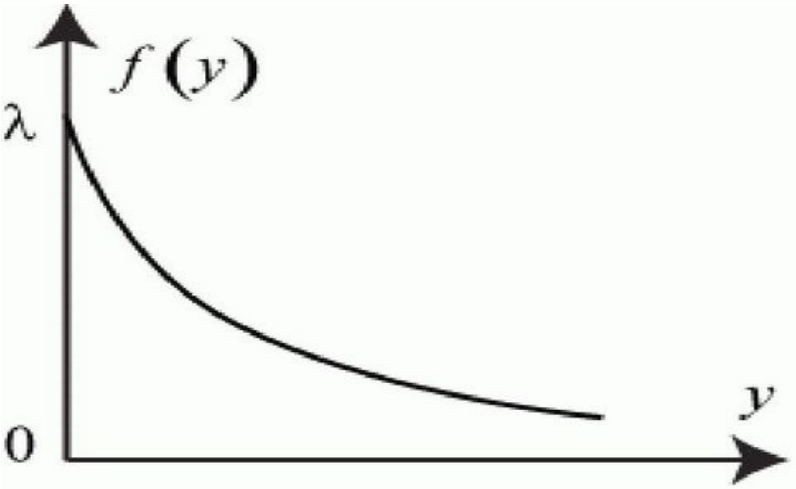
triangle

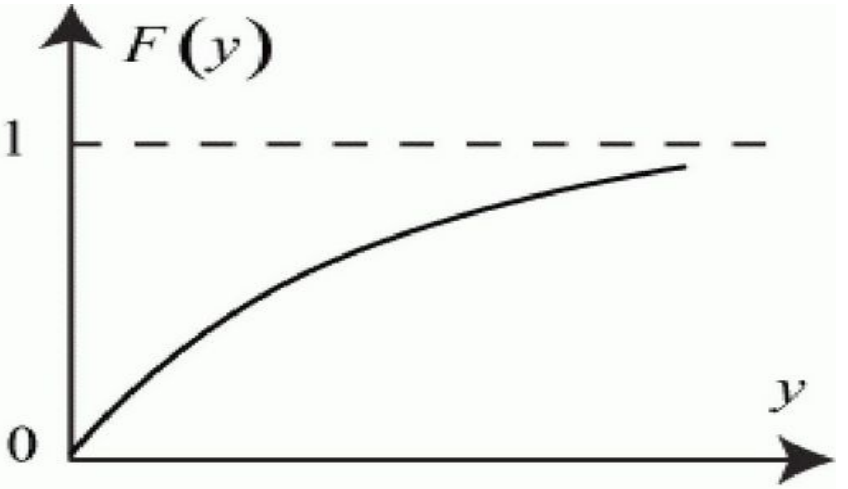


normal



Экспоненциальное распределение





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

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

Плотность распределения

Функция распределения

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

$x_i \in$ RAND; $\quad e^{-\lambda y_i}=1-x_i;\ -\lambda y_i=\ln(1-x_i);\ y_i=-\frac{1}{\lambda}\ln(1-x_i)$

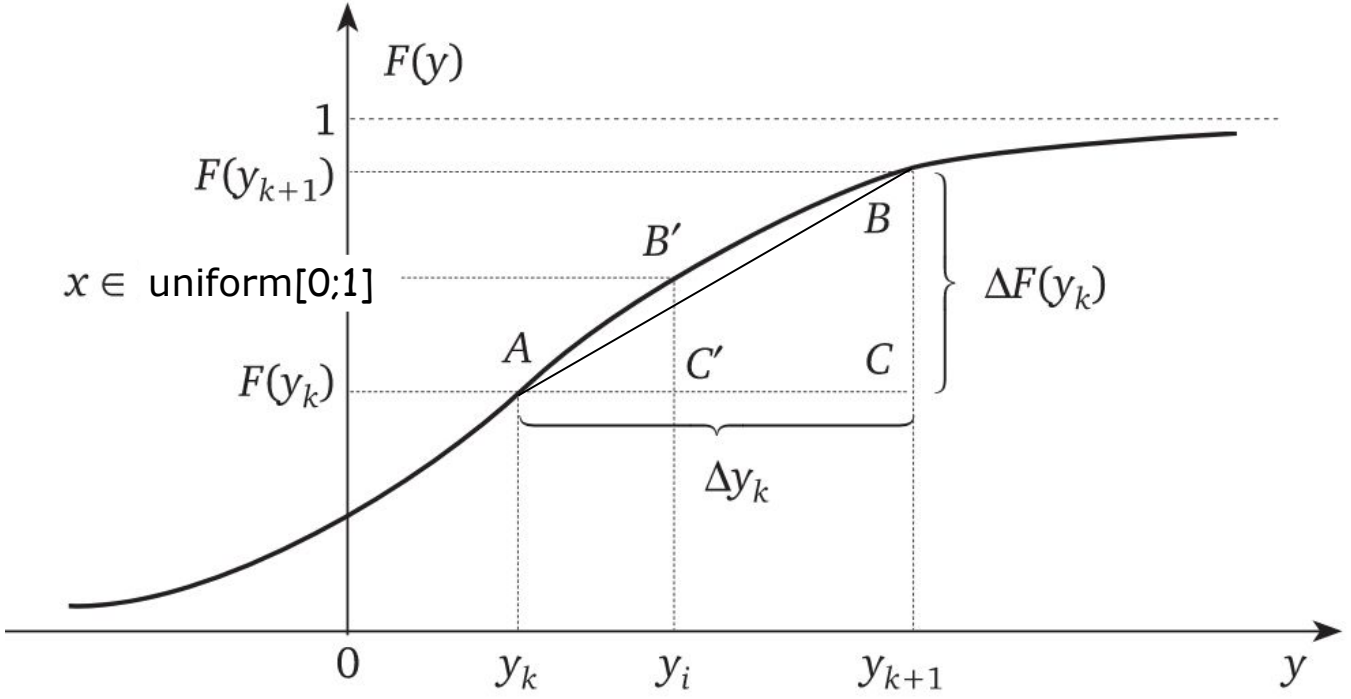
```
y = - 1/λ *
ln(RAND)
```

Пример функции экспоненциального распределения

```
double exponential(double lambda)
{
   return -1.0 / lambda *log(random())
;
}
```

Произвольное распределение

Метод кусочно-линейной аппроксимации функции распределения случайной величины



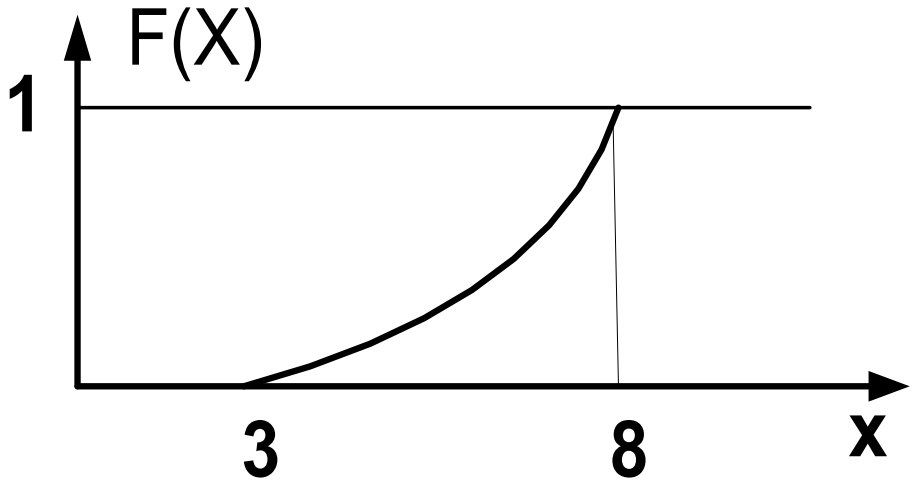
1. Генерируется случайное число x из uniform[0;1]
2. Сравнивается x со значениями $F(y)_k$, k=1,n
3. При совпадении выдается y_k
4. Иначе случайное число y_k вычисляется из подобия треугольников ABC и AB'C'

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

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



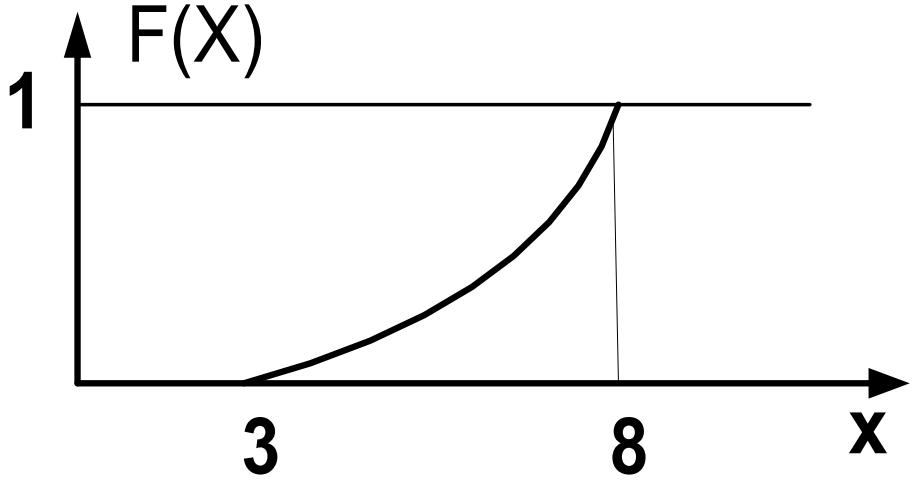
$$F(x) = b\,(x - a)^2$$

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 мат.ожиданием M[x] и дисперсией D[x] при N→∞ асимптотически стремится к нормальному распределению с M[η]=0 и D[η]=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**

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

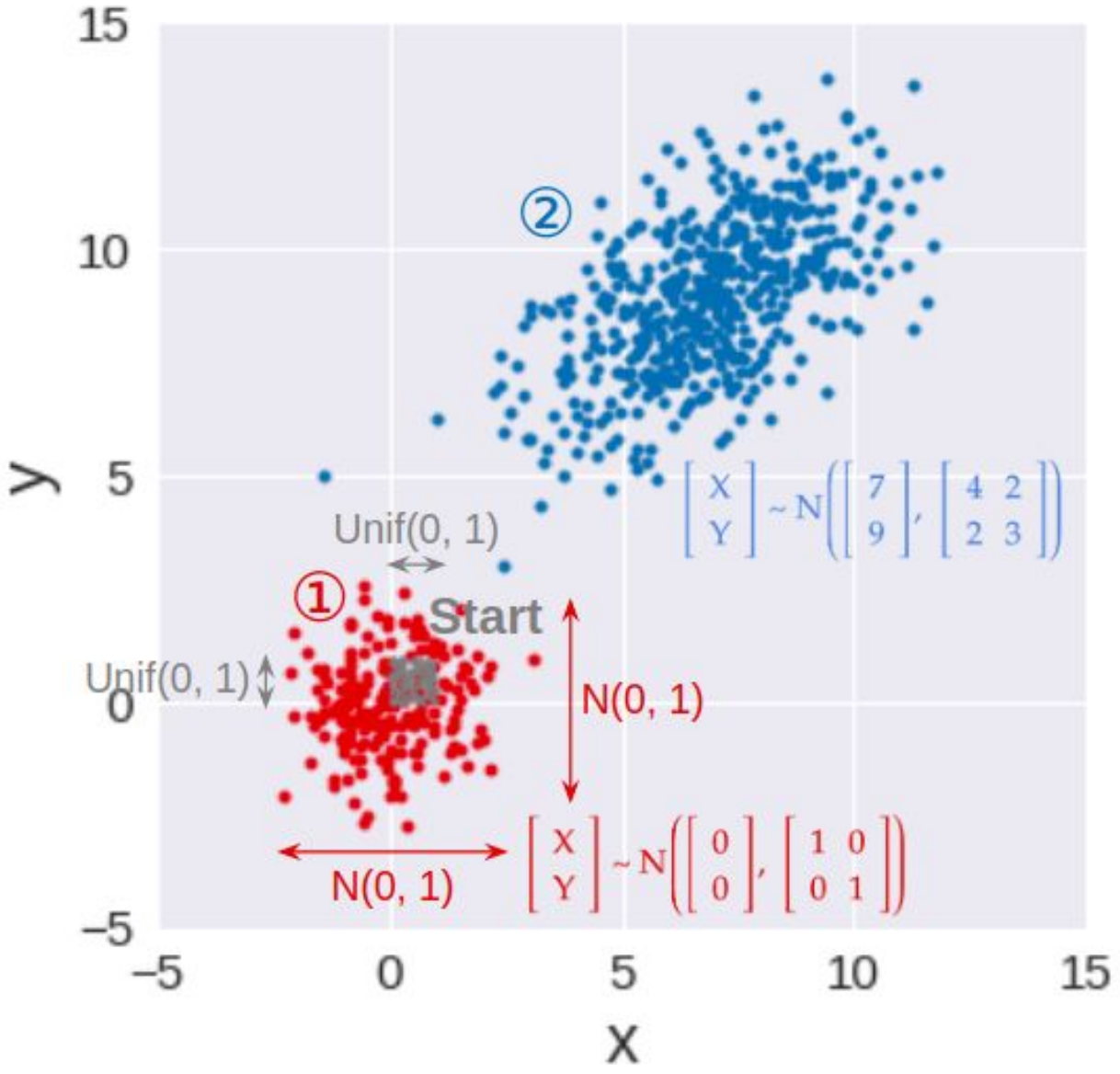
```
double normal(double m, double s)
{       // почти нормальное распределение
   double a = 0.0;
   for (int i = 0; i < 12; i++)
      a += random();

   return (m + (a - 6.0) * s);
}
```

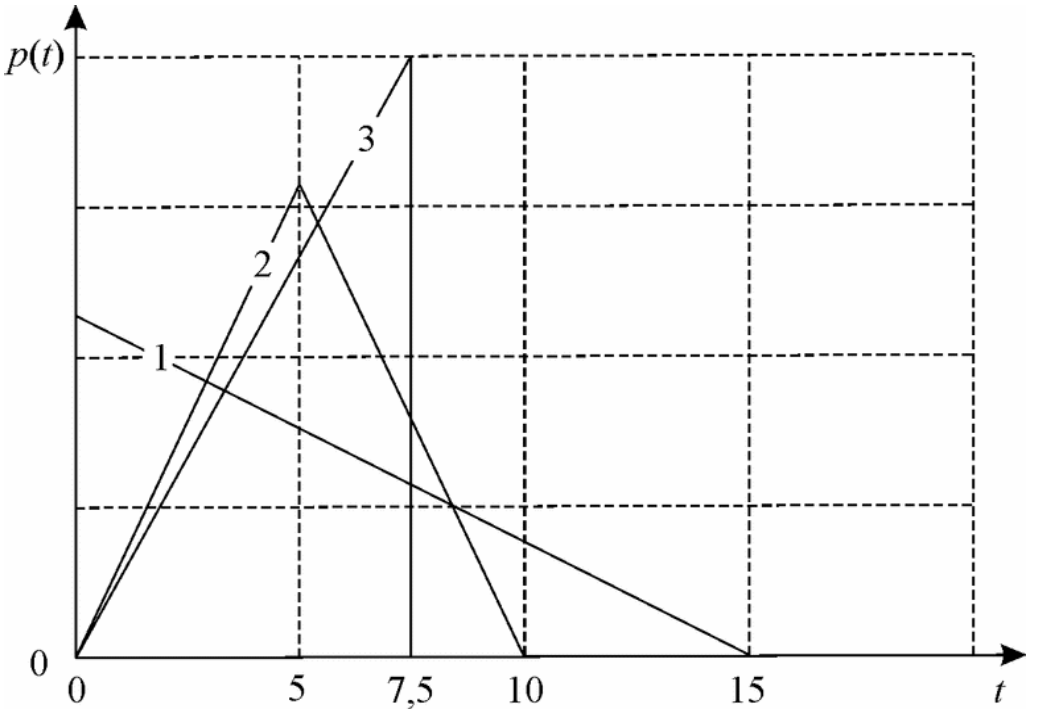
Пример функции нормального распределения

```
double randNorm(double mn, double si) {
// нормальное распределение по методу Бокса-
Мюллера
   double r =sqrt(-2.0 *log(1.0 -random()))
*si;
   double phi =2.0 * PI * random();
   return (mn + r * cos(phi));
}
```

Пример нормального распределения



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);
}
```

Тестирование псевдослучайности

Тестирование псевдослучайных последовательностей — совокупность методов определения меры близости заданной псевдослучайной последовательности к случайной.

В качестве такой меры обычно выступает наличие равномерного распределения, или большого периода, или равной частоты появления одинаковых цифр (подстрок) и т.п. Один из самых наглядных тестов — тест на равномерное распределение частот появления каждой цифры.

ПРОВЕРКА СТАТИСТИЧЕСКИХ ГИПОТЕЗ

Статистической гипотезой ***H*** называется предположение относительно параметров или вида распределения случайной величины X.
Если распределение случайной величины X известно и по выборке наблюдений необходимо проверить предположение о значении параметров этого распределения, то такие гипотезы называются параметрическими.
Проверяемая гипотеза называется нулевой гипотезой ***H0***.
Вместе с гипотезой ***H0*** рассматривают одну из альтернативных (конкурирующих) гипотез ***H1***.
Правило, по которому принимается решение принять или отклонить гипотезу ***H0***, называется критерием. Статистика Z, на основании которой принимается решение об истинности гипотезы ***H0***, называют статистикой критерия.
При проверке параметрической гипотезы ***H0*** в качестве статистики критерия обычно выбирают ту же статистику, что и для оценки параметра θ.

Перед анализом выборки назначается некоторая малая вероятность α, называемая уровнем значимости.

Пусть V – множество значений статистики Z, а V_k – такое подмножество, что при условии истинности гипотезы H0, вероятность попадания статистики критерия в V_k равна α $\qquad P[Z \in V_k \mid H0] = \alpha$

Пусть z_B – выборочное значение статистики Z, вычисленное по выборке.
Формулировка критерия:

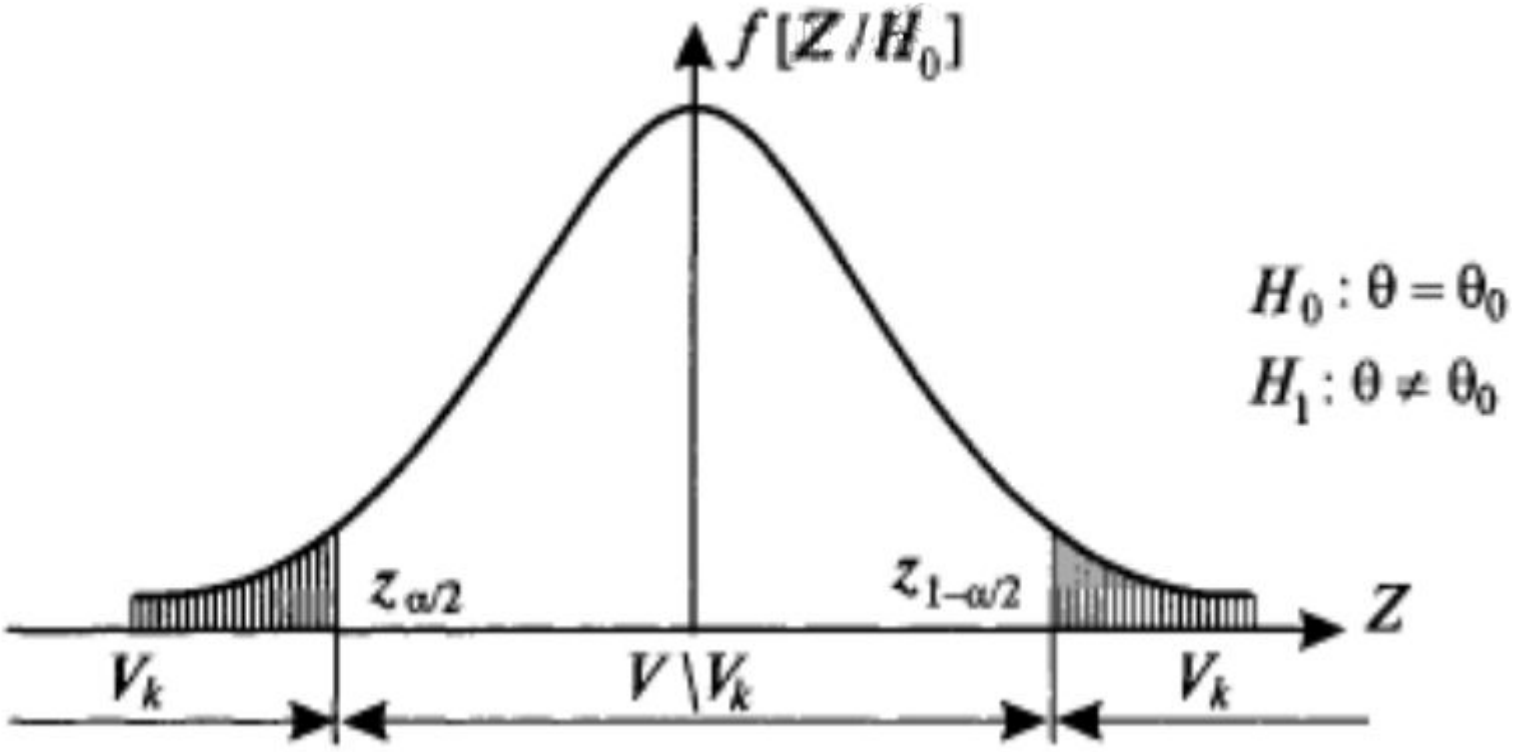
отклонить гипотезу ***H0***, если $z_B \in V_k$ (попадание в критическую область);

принять гипотезу ***H0***, если $z_B \in V \setminus V_k$ (попадание в область принятия гипотезы).

Уровень значимости ***α*** определяет размер критической области ***Vk***. Положение критической области на множестве значений статистики ***Z*** зависит от формулировки альтернативной гипотезы ***H1***.
Если альтернативная гипотеза ***H1:*** θ ≠ θ***0***, критическая область размещается на обоих хвостах плотности распределения ***Z***, то есть определяется неравенствами:

$$Z < z_{\frac{\alpha}{2}} \quad \text{и} \quad Z > z_{1-\frac{\alpha}{2}}$$

где ***z***α – квантили распределения статистики ***Z*** порядка ***α***, вычисленные при условии истинности ***H0***. В этом случае критерий называется двусторонним.



Проверка ДСЧ

Большинство тестов используют метод проверки гипотезы о случайности последовательности, используя статистические распределения.

Зная вероятностные свойства истинно случайной последовательности, можно проверять гипотезу о том, насколько сгенерированная последовательность похожа на случайную.

Для этого в каждом тесте подбирается подходящий критерий, вычисляются его значения для идеальной и сгенерированной последовательности. Если разность этих значений превышает некоторое критическое значение, установленное заранее, то последовательность считается неслучайной.

Для «хороших» последовательностей вероятность такого события крайне мала (допустим α ~0,001). Однако, существует вероятность того, что «плохая» последовательность удовлетворит критерию и будет сделан вывод о её случайности (обозначим вероятность такого события β).

На практике значения длины последовательности N, вероятности α и β связаны: задаётся α и подбирается N такое, чтобы минимизировать β.

Тестирование псевдослучайности

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

Вычисляемое значение статистики χ^2 сравнивается с табличными результатами, и в зависимости от вероятности проявления 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.

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

Рекомендуется иметь в каждом из ***k*** *интервалов разбиения измерений* $n_i > 5$.

pi - вероятность появления значения из ***i***-го интервала

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.

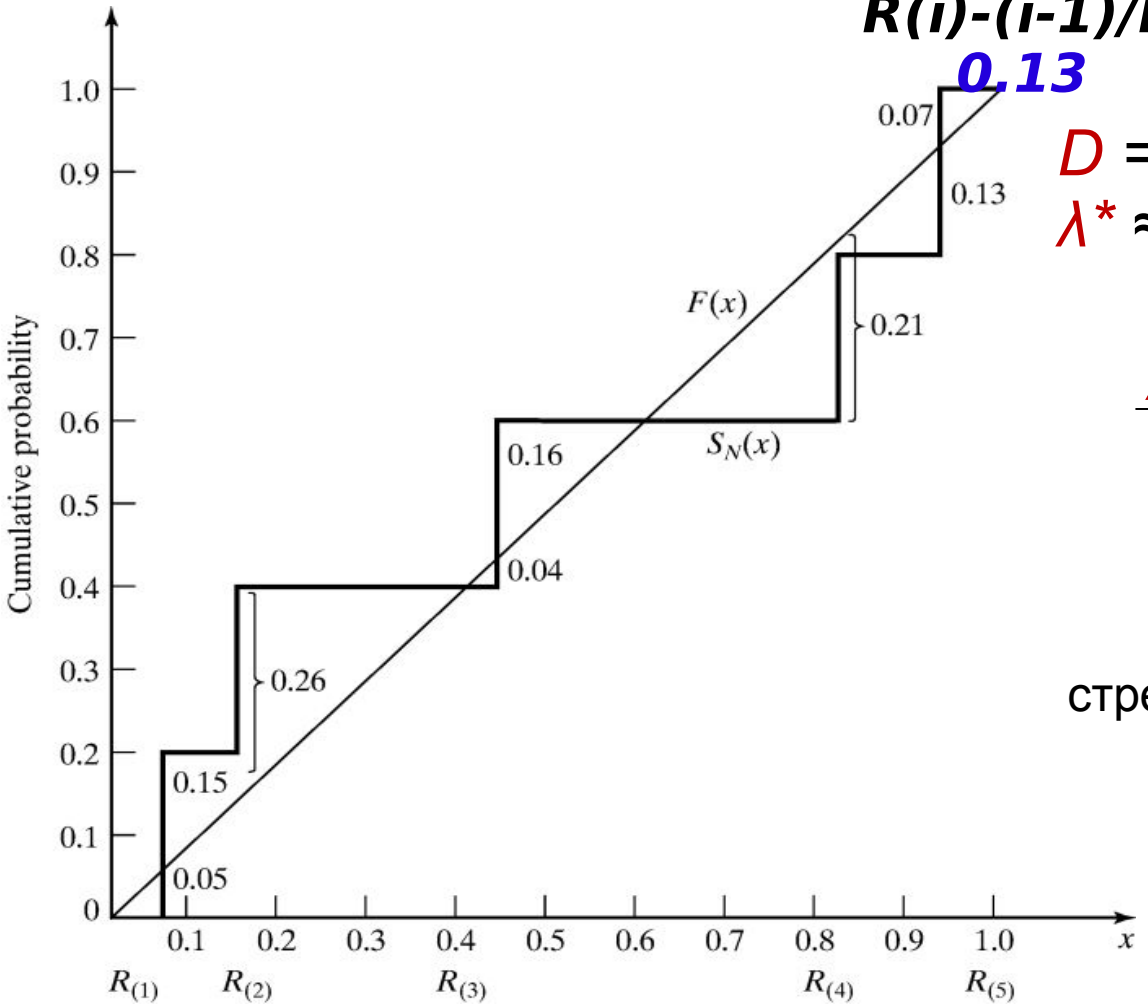
Проверка корреляции -- Данный тест проверяет взаимонезависимость элементов последовательности.

Проверка ДСЧ

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 по таблице вероятность P(λ). Малое P значит неприемлемость гипотезы!

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***	



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

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

λ	0,4	0,6	0,8	1,0	1,5
$P(\lambda)$	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;

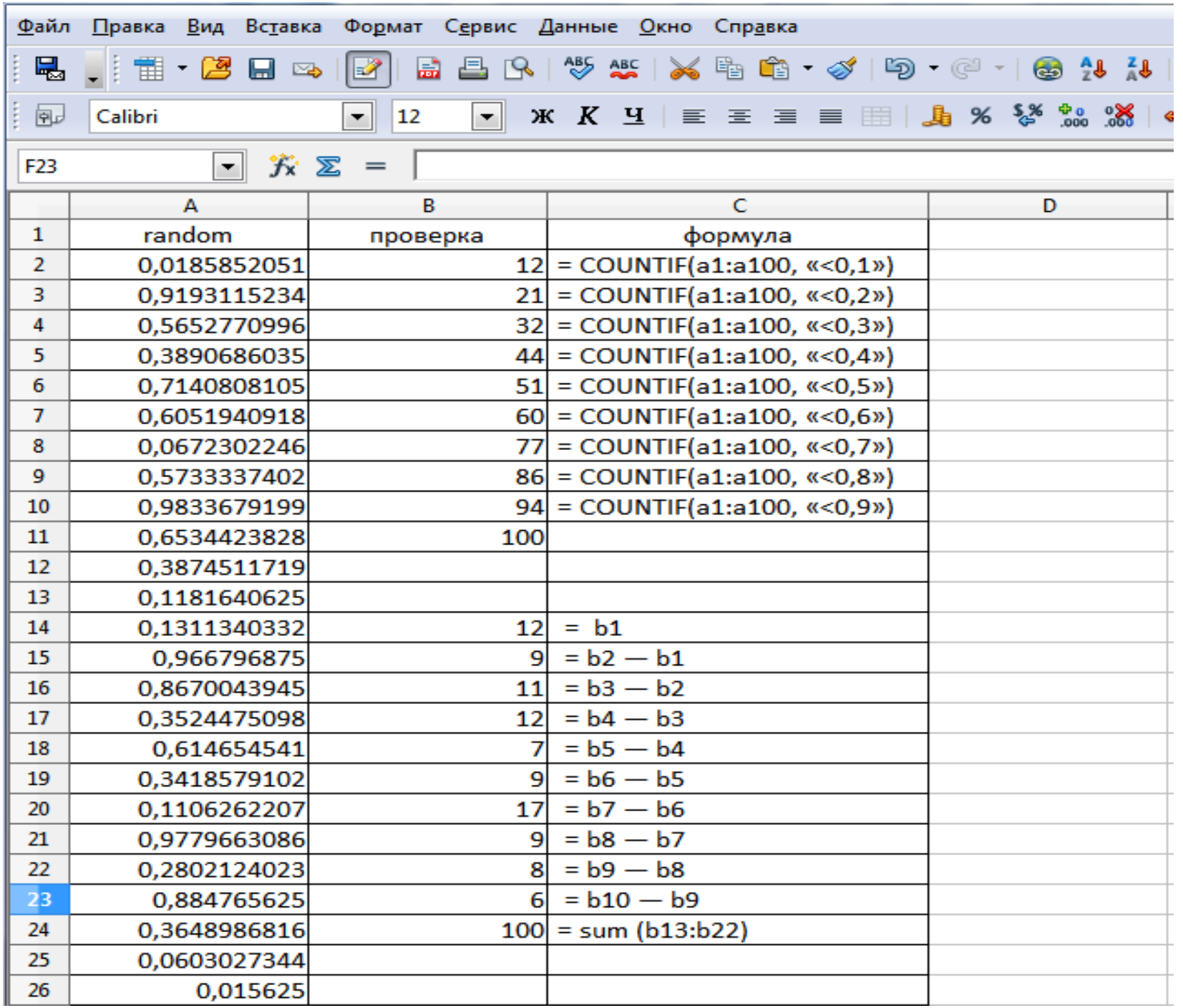
автокорреляционная функция -- предназначена для оценки корреляции между сдвинутыми копиями последовательностей и отдельных подпоследовательностей;

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

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

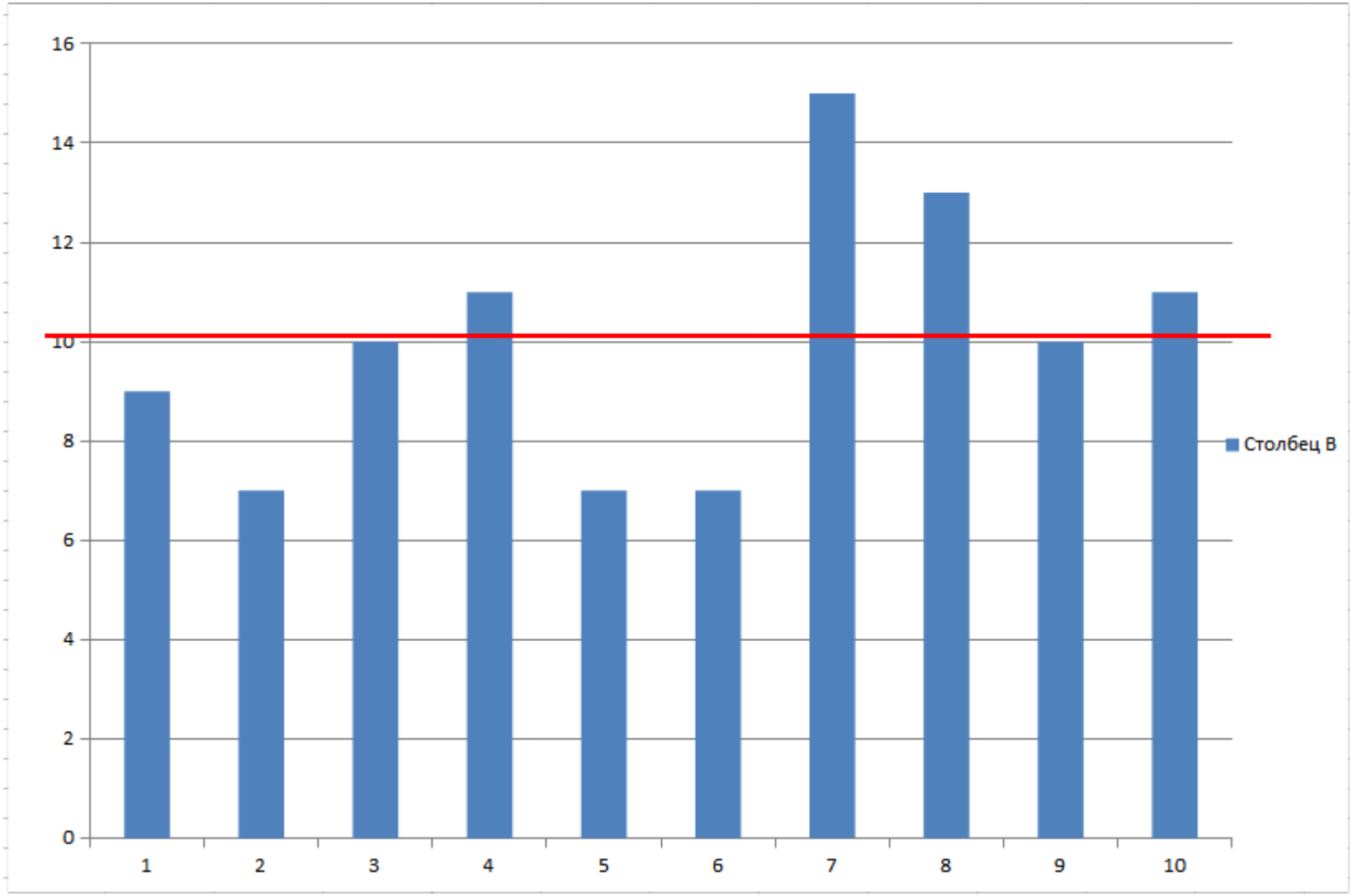
Проверка качества равномерности

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

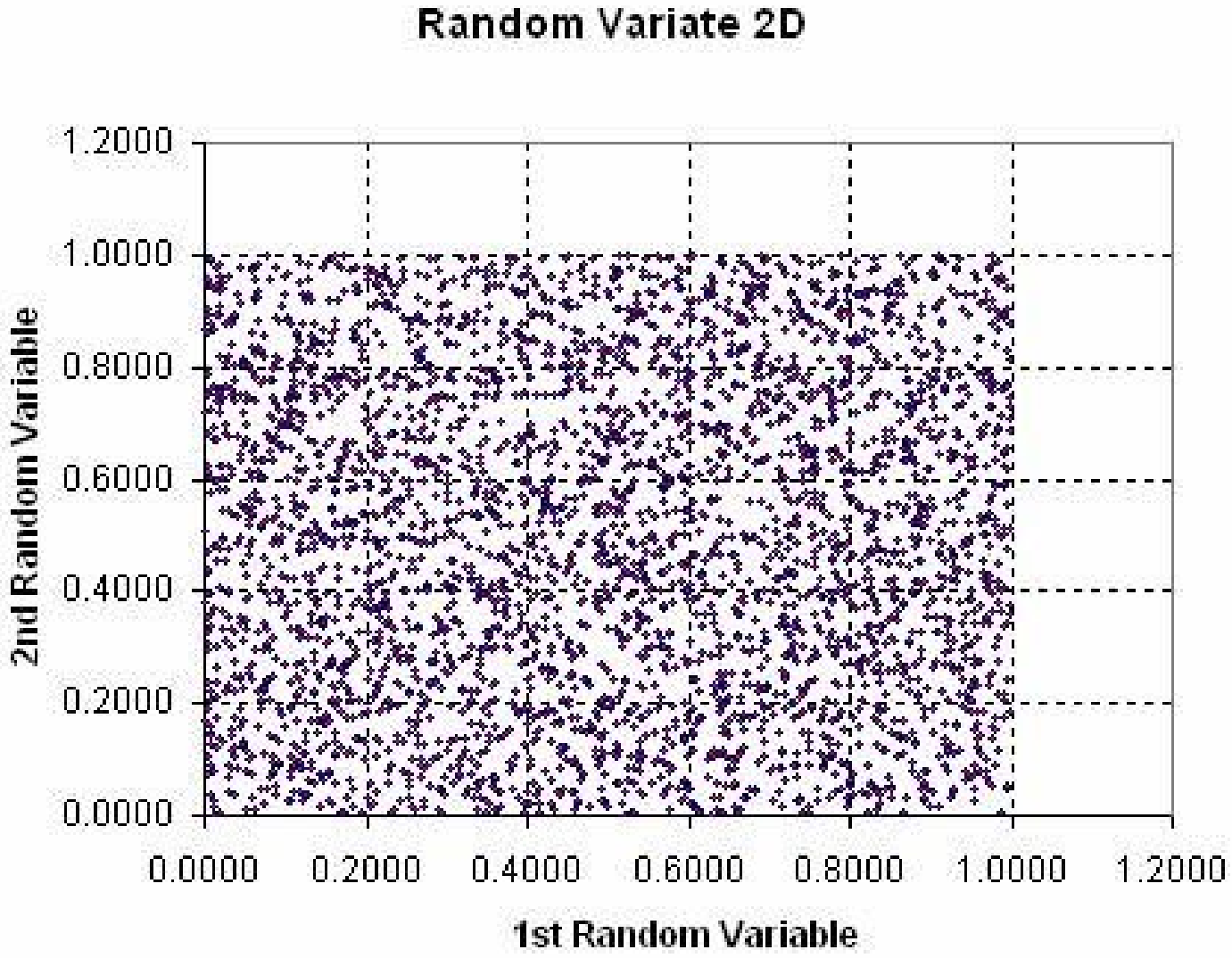


	A	B	C	D
1	random	проверка	формула	
2	0,0185852051	12	= COUNTIF(a1:a100, «<0,1»)	
3	0,9193115234	21	= COUNTIF(a1:a100, «<0,2»)	
4	0,5652770996	32	= COUNTIF(a1:a100, «<0,3»)	
5	0,3890686035	44	= COUNTIF(a1:a100, «<0,4»)	
6	0,7140808105	51	= COUNTIF(a1:a100, «<0,5»)	
7	0,6051940918	60	= COUNTIF(a1:a100, «<0,6»)	
8	0,0672302246	77	= COUNTIF(a1:a100, «<0,7»)	
9	0,5733337402	86	= COUNTIF(a1:a100, «<0,8»)	
10	0,9833679199	94	= COUNTIF(a1:a100, «<0,9»)	
11	0,6534423828	100		
12	0,3874511719			
13	0,1181640625			
14	0,1311340332	12	= b1	
15	0,966796875	9	= b2 — b1	
16	0,8670043945	11	= b3 — b2	
17	0,3524475098	12	= b4 — b3	
18	0,614654541	7	= b5 — b4	
19	0,3418579102	9	= b6 — b5	
20	0,1106262207	17	= b7 — b6	
21	0,9779663086	9	= b8 — b7	
22	0,2802124023	8	= b9 — b8	
23	0,884765625	6	= b10 — b9	
24	0,3648986816	100	= sum (b13:b22)	
25	0,0603027344			
26	0,015625			

Проверка качества равномерности

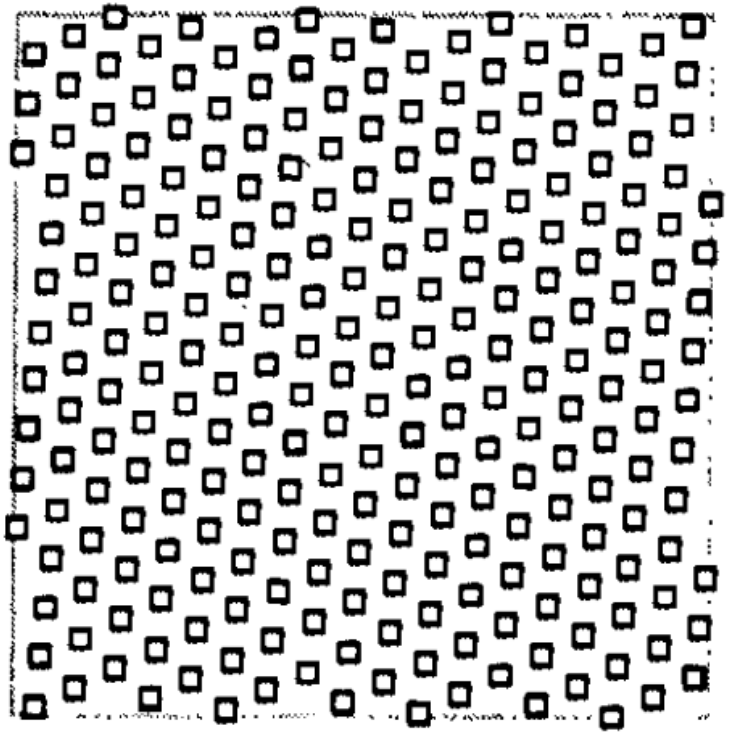


Распределение на плоскости



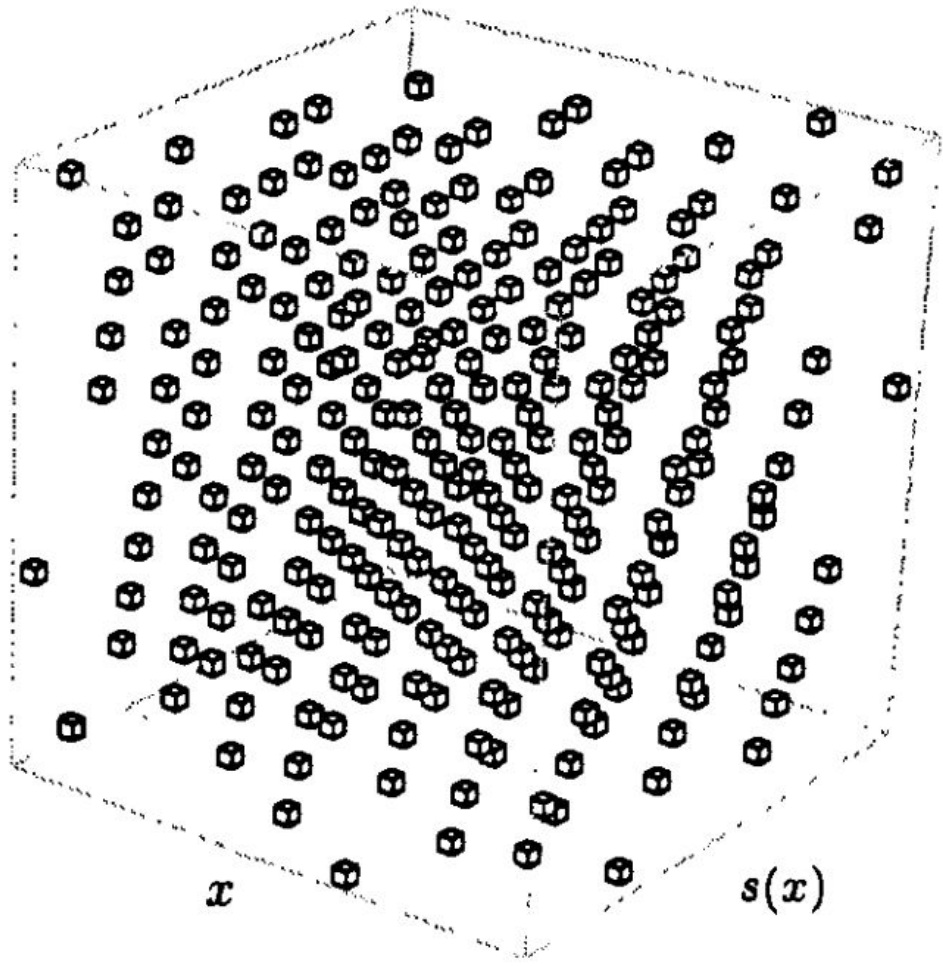
Двумерная диаграмма, построенная по парам точек (X_n; X_{n+1})

Распределение на плоскости



(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})

Основные тесты ДСЧ

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)

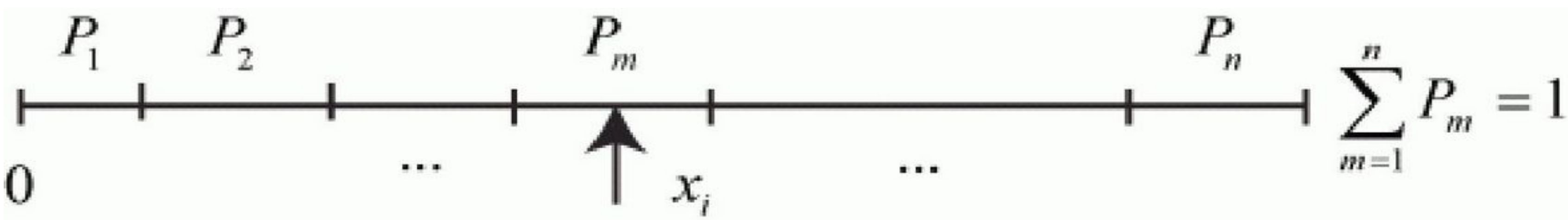
$H_0: Ri \sim independently$
$H_1: Ri \not\sim independently$

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

Моделирование событий

<u>Теорема:</u>

В полной группе несовместных событий моделью свершения события *Am*, происходящего с вероятностью *Pm*, является попадание значения x_i в отрезок, р[illegible]исловой шкалы где *n* -число несовместных событий $\sum_{m=1}^{n} P_m = 1$



Способ определения исходов по жребию

Пример: линия связи может быть в 1 из 4 состояний. Rand= 0,56. **А-?**

Состояние	**А1**	**А2**	**А3**	**А4**
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 качеством 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. 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 мат.ожидания свойство ***эргодичности*** формально выглядит так:

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

определение эргодического процесса

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

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

Этапы проекта моделирования

1. Постановка задачи моделирования
2. Анализ задачи моделирования
3. Определение параметров модели
4. Определение содержания модели
5. Обоснование критериев эффективности
6. Описание концептуальной модели
7. Построение логического алгоритма
8. Проверка достоверности модели (верификация)
9. Выбор средств, программирование модели
10. Проверка достоверности программы (валидация)
11. Планирование экспериментов с моделью
12. Проведение экспериментов и расчетов
13. Анализ результатов моделирования
14. Интерпретация результатов моделирования
15. Подведение итогов и выдача рекомендаций

Оценка адекватности имитационной модели (ИМ) объекту-оригиналу

Оценка состоит в сравнении статистических характеристик реальной и модельной систем 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 (N2 > N1). Для реальной системы и ИМ определяют значения математического ожидания и дисперсии.

Оценка адекватности имитационной модели объекту-оригиналу

Гипотезу *о равенстве средних значений* проверяют при помощи параметрического критерия Манны–Уитни 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 теоретического и эмпирического распределений* откликов реальной системы и откликов разработанной ИМ для размера выборки --

более 100 наблюдений проводят на основе критерия χ^2 ;

для выборок (30 < N < 100) используют

критерий Колмогорова – Смирнова;

для малых выборок – критерий Крамерса–фон Мизеса

или Колмогорова с поправкой Большева.

Верификация имитационной модели

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

Алгоритм ***верификации*** модели состоит в ряде действий:

1) анализ компонентов разработанной модели, сопоставление их с аналогичными компонентами объекта-оригинала и обоснование их наличия в ИМ;

2) покомпонентное тестирование выходных потоков;

3) формулирование и проверка статистических гипотез.

Верификация имитационной модели

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.

3) проверка на ожидаемость. На этом шаге заменяют элементы модели стохастические на детерминированные и анализируют результат моделирования.

Формальные процедуры ***верификации*** связаны с проверкой верности исходных предпосылок.

Валидация имитационной модели

… 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.

Категории И М

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. Обычно 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

Имитационная модель строится для определения характеристик некоторых случайных величин.

Такими случайными величинами могут быть (например):

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

Из характеристик случайных величин наиболее интересуют :

мат.ожидание, дисперсия, коэффициент корреляции.

Приближенное значение называют ***<u>оценка</u>*** *характеристики:*

оценка мат.ожидания, оценка дисперсии,

оценка коэффициента корреляции

Оценки точности

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

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

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

Достоверностью оценки характеристики $\overline{\Theta}$ называют вероятность α

того, что заданная точность достигается:

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

Достоверность характеризует повторяемость, устойчивость эксперимента

Уровень значимости есть вероятность того, что критерий примет нулевую гипотезу, если выборка была из распределения, отвечающего нулевой гипотезе, т.е. вероятность правильно принять нулевую гипотезу.

Оценка количества реализаций

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

В качестве оценки мат.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 мат.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 <u>малом</u> числе степеней свободы ***k = N — 1*** ***(~ 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 :

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

<u>Фрагмент таблицы распределения Стьюдента</u>

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.

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

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

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

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