Лабораторная работа №1

Тема: тестирование генератора псевдослучайных чисел

Задание

– Создать генератор последовательности равномерно распределенных случайных чисел на основе смешанного алгоритма Лемера. Подобрать параметры генератора, который дает максимальный период.
– Для сгенерированной выборки построить гистограмму (20+ интервалов).
– Используя критерии хи-квадрат и КС, подтвердить гипотезу о равномерности последовательности.
– Отобразить результаты графически.
– Сделать вывод о согласованности аналитических расчетов и визуализации.

Optional

Реализовать и протестировать генератор
– “усеченного” нормального распределения
– или треугольного распределения.

Алгоритм Лемера

Исходные данные:
– x_0 – начальное значение (x_0 ε 0);
– a – множитель (a > 0);
– c – приращение (cε0);
– m – модуль (m>a, m>c, m>x_0).
Тогда искомая последовательность псевдослучайных чисел получается из соотношения:

$$x_{n+1} = (a * x_n + c) \% m, n\varepsilon 0. \quad (1)$$

Она называется линейной конгруэнтной последовательностью.
Для обозначения линейных конгруэнтных датчиков с c=0 и c≠0 применяются соответственно термины мультипликативный и смешанный метод.
Равномерно распределенная на [0; 1) последовательность псевдослучайных чисел (u_0, u_1,..., u_n,...) получается из соотношения $u_n=x_n/m$ (или $u_n=x_nm^{-1}$, что более быстро выполняется компьютером).

Достаточное условие периода максимальной длины

Чтобы получить период максимальной длины m, множитель a и приращение c в линейном конгруэнтном датчике должны удовлетворять следующим условиям:
– c и m - взаимно простые числа;
– b=a–1 кратно p для любого простого p, являющегося делителем m;
– b кратно 4, если m кратно 4.

Универсальные тесты для анализа случайных последовательностей

Критерий χ2. Предположим, что все возможные результаты испытаний разделены на k категорий. Проводится n независимых испытаний (исход каждого испытания не влияет на исход остальных). Пусть p_s - вероятность того, что результат испытания попадет в категорию s, и пусть Y_s – число испытаний, которые действительно попали в категорию s. Сформируем статистику:

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

Формулу (3) можно преобразовать к виду, более удобному для вычислений:

$$V = \frac{1}{n} \sum_{s=1}^{k} \left(\frac{Y_s^2}{p_s} \right) - n \quad (3)$$

Затем V сравнивается с числом из таблицы для распределения $|^2$ при количестве степеней свободы $\{$=k–1. Если V меньше значения, соответствующего p=0.99, или больше значения, соответствующего p=0.01, то результаты бракуются как недостаточно случайные. Если p лежит между 0.99 и 0.95 или между 0.05 и 0.01, то результаты считаются "подозрительными". При значениях p, заключенных между 0.95 и 0.90 или 0.10 и 0.05,

результаты "слегка подозрительны". Часто с помощью критерия $|^2$ проверяют по крайней мере три разные части исследуемого ряда чисел. Если не менее двух раз из трех результаты оказываются подозрительными, числа отбрасываются как недостаточно случайные.

Возникает вопрос о длине n последовательности случайных чисел, которую необходимо выбрать для данного теста. Теоретические расчеты показывают, что достоверные оценки получаются в том случае, когда в каждую из категорий попали не менее 5 испытаний, т.е. выполняется условие $Y_s > 4$, s=1..k.

Критерий Колмогорова–Смирнова (КС–критерий). Критерий $|^2$ применяется в тех случаях, когда результаты испытаний разделяются на конечное число k категорий. Однако часто случайные величины могут принимать бесконечно много значений. В теории вероятностей и математической статистике непрерывные случайные величины описываются с помощью функции распределения:

$$F(x)=p\{X\delta x\} \tag{4}$$

Используя значения x_1, x_2, ..., x_n случайной величины X, можно построить эмпирическую функцию распределения

$$F(x)=\frac{1}{n}\sum_{i=1}^{n}k(x_i), \tag{5}$$

где $k(x)=\begin{cases} 1, \text{если } X \le x \\ 0, \text{в противном случае} \end{cases}$.

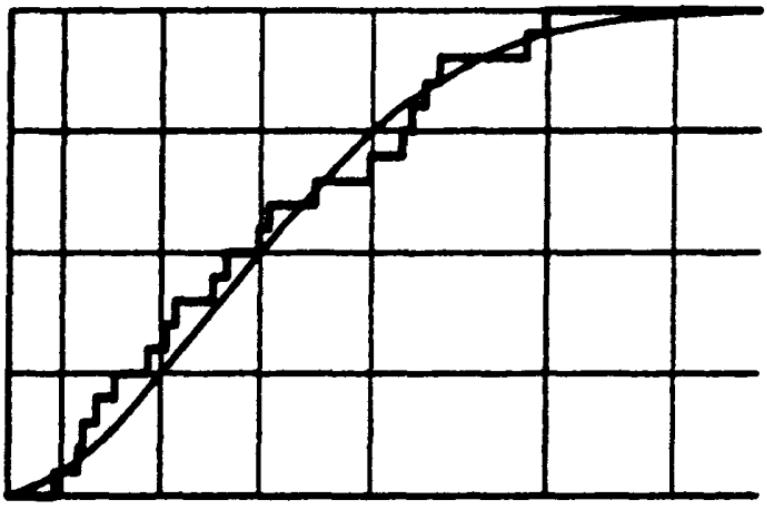

Рис. Пример теоретической и эмпирической функций распределения

При увеличении n функции $F_n(x)$ должны все более точно аппроксимировать F(x). КС-критерий можно использовать в тех случаях, когда F(x) не имеет скачков, и он должен указать, насколько маловероятны большие расхождения между $F_n(x)$ и F(x). Для этого используются следующие статистики:

$$K_n^+=\sqrt{n}\max_{-\infty<x<+\infty}(F_n(x)-F(x))$$
$$K_n^-=\sqrt{n}\max_{-\infty<x<+\infty}(F(x)-F_n(x)) \tag{6}$$

K_n^+ показывает, каково максимальное отклонение для случая $F_n>F$, а K_n^- для $F_n<F$. Множитель $\sqrt{n}$ нормирует статистики (7) таким образом, чтобы стандартное отклонение не зависело от n. Далее, как и в случае критерия $|^2$, сравнивают значения (7) с табличными и определяют, имеют ли они высокую или низкую значимость.

Формулы (7) не годятся для машинных расчетов, так как требуется отыскать максимальное среди бесконечного множества чисел. Однако, учитывая, что F(x) неубывающая функция, а $F_n(x)$ имеет конечное число скачков, можно определить статистики (7) с помощью следующего алгоритма.

1. Определяются выборочные значения x_1, x_2, ... , x_n.
2. Значения x_i располагаются в порядке возрастания так, чтобы $x_1\delta x_2\delta...\delta x_n$.
3. Статистики (7) вычисляются по следующим формулам:

$$K_n^+ = \sqrt{n} \max_{1 \le j \le n} \left(\frac{j}{n} - F(x_j) \right)$$
$$K_n^- = \sqrt{n} \max_{1 \le j \le n} \left(F(x_j) - \frac{j-1}{n} \right) \quad (7)$$

Критические значения КС-критерия определяются формулой a – b / sqrt(n).

p	0.99	0.95	0.75	0.5	0.25	0.05	0.01
a	0.0709	0.1601	0.3793	0.5887	0.8326	1.2239	1.5174
b	0.15	0.14	0.15	0.15	0.16	0.17	0.2

Отображение результатов

Опция 1. Инструменты табличного процессора.
Опция 2. Библиотека matplotlib из Python.
Пример скрипта приведен ниже.

```
import matplotlib.pyplot as plt

if __name__ == '__main__':
    random_numbers = [
        0.7619, 0.0612, 0.2, 0.7483, 0.0612, 0.7143, 0.415, 0.9,
        0.7143, 0.0544, 0.0816, 0.1633, 0.619, 0.619, 0.1973, 0.51
    ]
    plt.hist(random_numbers)
    plt.show()
```

Deadline **4.10 23:59**

Структура отчета

Код датчика
Результаты трех прогонов для критерия $|^2$:
- гистограмма
- значения V и p

Результаты трех прогонов для КС-критерия
- графики теоретического и эмпирического распределений
- значения K+, K-, p-отрезка в который попадают.

Артефакты для СЭО

- отчет
- архив с кодами для тестирования датчиков