

Лабораторна робота № 1
ГЕНЕРУВАННЯ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ

Написати програму, що реалізує десять генераторів псевдовипадкових чисел. Кожний генератор викликати за допомогою меню, яке реагує на ввід цілого числа: 1, ..., 10. Згенерувати послідовність псевдовипадкових чисел, яка має якнайдовший період (не менше 100). Перевірка умов застосування алгоритмів є обов'язковою.

Побудувати гістограму, яка ілюструє розподіл чисел на інтервалах $[0;1]$ (для нормального розподілу), $[-3;3]$ (для нормального розподілу), $[0; 100]$ – для решти розподілів. Гістограму подати у вигляді таблиці. Наприклад, для рівномірного розподілу вона виглядатиме приблизно так. Частота обчислюється як дріб, чисельником якого є кількість потраплянь випадкових чисел в певний інтервал, в знаменнику – повна кількість згенерованих чисел.

Інтервал	Частота
$[0; 0,1]$	0.05
$[0.1;0.2]$	0.15
$[0.2;0.3]$	0.1
$[0.3;0.4]$	0.12
$[0.4;0.5]$	0.1
$[0.5;0.6]$	0.15
$[0.6;0.7]$	0.05
$[0.7;0.8]$	0.08
$[0.8;0.9]$	0.16
$[0.9;1.0]$	0.04

Генератори псевдовипадкових чисел, як правило, породжують ціле число X , яке лежить в інтервалі від 0 до деякого заздалегідь заданого числа m . Тому дійсні псевдовипадкові числа, рівномірно розподілені між 0 і 1, обчислюються за формулою $U = X/m$.

I. МЕТОДИ ГЕНЕРУВАННЯ РІВНОМІРНО РОЗПОДІЛЕНИХ ЧИСЕЛ

I.

1. Лінійний конгруентний метод. [Кнут, т.2., с. 29–39]

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

$$U_{n+1} = \frac{X_{n+1}}{m}, n \geq 0,$$

де m – модуль, $m > 0$, a – множник, $0 \leq a < m$, c – приріст, $0 \leq c < m$, X_0 – початкове значення, $0 \leq X_0 < m$.

Вибір модуля. Модуль повинен бути достатньо великим, оскільки період не може містити менше m чисел. Нехай w – довжина комп'ютерного слова, наприклад, 2^{32} . В якості m рекомендується брати найбільше просте число, яке не перевищує w .

Вибір множника. Цей вибір визначається наступною теоремою: лінійна конгруентна послідовність, визначена числами m , a , c і X_0 має період m тоді і лише тоді, коли виконуються три умови:

- 1) числа c і m є взаємно простими;
- 2) число $b = a-1$ є кратним числу p для кожного простого числа p , яке є дільником числа m ;
- 3) число b є кратним 4, якщо число m є кратним 4.

2. Квадратичний конгруентний метод [Кнут, т.2., с. 46, 57 (вправа 8)]

$$X_{n+1} = (dX_n^2 + aX_n + c) \bmod m,$$

$$U_{n+1} = \frac{X_{n+1}}{m}, n \geq 0.$$

Вибір параметрів. Цей вибір визначається наступною теоремою: квадратична конгруентна послідовність, визначена числами m, a, c, d і X_0 , має період m тоді і лише тоді, коли виконуються чотири умови:

- 1) числа c і m є взаємно простими;
- 2) числа d і $a-1$ є кратними числу p для всіх чисел p , які є простими непарними дільниками числа m ;
- 3) число d є парним і $d \equiv a-1 \pmod{4}$, якщо число m є кратним 4;
число $d \equiv a-1 \pmod{2}$, якщо число m є кратним 2;
- 4) $d \not\equiv 3c \pmod{9}$, якщо число m є кратним 3.

3. Числа Фібоначчі [Кнут, т.2., с. 47]

$$X_{n+1} = (X_n + X_{n-1}) \bmod m, n \geq 0.$$

$$U_{n+1} = \frac{X_{n+1}}{m}$$

4. Оборнена конгруентна послідовність [Кнут, т.2., с. 53, 61 (вправа 36)]

$$X_{n+1} = (aX_n^{-1} + c) \bmod p,$$

$$U_{n+1} = \frac{X_{n+1}}{m}, n \geq 0,$$

де p – просте число, число X_n набуває значень із множини $\{0, 1, \dots, p-1, \infty\}$, а обертання визначається за правилами $0^{-1} = \infty$, $\infty^{-1} = 0$. В інших випадках $XX^{-1} \equiv 1 \pmod{p}$. [Кнут, т.2., с. 53]

Вибір параметрів. Оборнена конгруентна послідовність

$$X_{n+1} = (aX_n^{-1} + c) \bmod 2^e, X_0 = 1, e \geq 3$$

має період 2^{e-1} , якщо $a \bmod 4 = 1$ і $c \bmod 4 = 2$.

5. Метод об'єднання [Кнут, т.2., с. 55]

$$Z_n = (X_n - Y_n) \bmod m,$$

$$0 \leq X_n < m, 0 \leq Y_n < m' \leq m,$$

$$U_{n+1} = \frac{Z_{n+1}}{m}, n \geq 0.$$

II. МЕТОДИ ГЕНЕРУВАННЯ НОРМАЛЬНО РОЗПОДІЛЕНИХ ЧИСЕЛ

$$N(0,1): F(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x e^{-\frac{t^2}{2}} dt$$

6. Правило “3 сігма” [Мейн, Савитч, с. 119]

$$X_n = m + (sum - 6)\sigma,$$

де m – медіана, σ – дисперсія, sum – сума дванадцяти випадкових чисел, рівномірно розподілених на інтервалі $[a, b]$. Якщо $[a, b] = [0; 1]$, то $m = 0$, а $\sigma = 1$. Правило 3-сігма стверджує, на проміжку $[m-3\sigma; m+3\sigma]$ міститься 99,7% всіх випадкових чисел, що мають розподіл $N(m, \sigma^2)$. Отже для побудови гістограми розподілу $N(0,1)$ достатньо обмежитись інтервалом $[-3; 3]$.

7. Метод полярних координат [Кнут, т.2., с. 146]

7.1. Нехай U_1 і U_2 – випадкові числа, взяті із генеральної сукупності всіх чисел, рівномірно розподілених на інтервалі $[0; 1]$. Виконати такі перетворення.

$$V_1 \leftarrow 2U_1 - 1,$$

$$V_2 \leftarrow 2U_2 - 1.$$

Числа V_1 і V_2 належать генеральній сукупності чисел, рівномірно розподілених на інтервалі $[-1; 1]$.

7.2. $S \leftarrow V_1^2 + V_2^2$.

7.3. Якщо $S \geq 1$, виконати пункти 7.1 і 7.2.

7.4. Виконати такі перетворення.

$$X_1 \leftarrow V_1 \sqrt{\frac{-2 \ln S}{S}},$$

$$X_2 \leftarrow V_2 \sqrt{\frac{-2 \ln S}{S}}.$$

7.5. Видати числа X_1 і X_2 .

8. Метод співвідношень [Кнут, т.2., с. 155]

8.1. Згенерувати дві незалежні випадкові величини, рівномірно розподілені на інтервалі $[0; 1]$: $U \neq 0$ і V .

$$8.2. X \leftarrow \sqrt{\frac{8}{e}} \frac{V - \frac{1}{2}}{U}.$$

8.3. (Необов’язкова перевірка верхньої грані.) Якщо $X^2 \leq 5 - 4e^{\frac{1}{4}U}$, то результатом є число X . Завершити алгоритм.

8.4. (Необов’язкова перевірка нижньої грані.) Якщо $X^2 \geq \frac{4e^{-1.35}}{U} + 1.4$, то повернутися на крок 8.1.

8.5. (Остаточна перевірка.) Якщо $X^2 \leq -4 \ln U$, то видати число X і завершити алгоритм, інакше повернутися на крок 8.1.

III. Методи генерування інших розподілів

9. Метод логарифму для генерування показового розподілу [Кнут, т.2., с. 157]

$$F(x) = 1 - e^{-\frac{x}{\mu}}, x \geq 0.$$

Якщо $y = F(x) = 1 - e^{-\frac{x}{\mu}}$, то $x = F^{-1}(y) = -\mu \ln(1 - y)$. Таким чином, величина

$$x = -\mu \ln(1 - U),$$

має експоненційний розподіл, якщо число U належить генеральній сукупності випадкових величин, рівномірно розподілених на інтервалі $[0; 1]$. Оскільки величина $1 - U$ має той же самий розподіл, формулу можна спростити:

$$x = -\mu \ln U.$$

10. Метод Аренса для генерування гамма-розподілу порядку $a > 1$

[Кнут, т.2., с. 159]

$$F(x) = \frac{1}{\Gamma(a)} \int_0^x t^{a-1} e^{-t} dt, x \geq 0, a > 0.$$

10.1. (Генерування кандидата.) Згенерувати випадкове число U , що належить генеральній сукупності випадкових величин, рівномірно розподілених на інтервалі $[0; 1]$. Виконати операції

$$Y \leftarrow tg(\pi U),$$

$$X \leftarrow \sqrt{2a - 1}Y + a - 1.$$

10.2. (Перша перевірка.) Якщо $X \leq 0$, повернутися на крок 10.1.

10.3. (Остаточна перевірка.) Згенерувати випадкове число V , що належить генеральній сукупності випадкових величин, рівномірно розподілених на інтервалі $[0; 1]$.

Якщо $V > (1 + Y^2) \exp\left((a - 1) \ln\left(\frac{X}{a - 1}\right) - \sqrt{2a - 1}Y\right)$, повернутися на крок 10.1.

10.4. Видати число X .