УДК 519.213
Клімов В.О.
студ. гр. КНТ-813 НУ «Запорізька політехніка»

ГЕНЕРАЦІЯ ЛІНІЙНОЇ КОНГРУЕНТНОЇ ПОСЛІДОВНОСТІ

Псевдовипадкові генератори чисел використовуються в сферах, де потрібні випадкові числа без високих вимог до їхньої непередбачуваності. Основними застосуваннями є моделювання та симуляції, зокрема у методах Монте-Карло для оцінки ймовірностей. У випадковому виборі, псевдовипадкові числа застосовуються для вибірки учасників опитувань або створення лотерейних результатів. У тестуванні програмного забезпечення ці генератори забезпечують випадкові вхідні дані для перевірки стійкості алгоритмів.

Для генерації послідовності рівномірно розподілених випадкових чисел було реалізовано лінійний конгруентний метод. Цей метод ґрунтується на використанні операції mod(x, y), яка визначає залишок від ділення першого числа на друге. Кожне наступне псевдовипадкове число генерується за допомогою попереднього числа за математичною формулою:

$$r_{i+1} = \mathbf{mod}(k * r_i + b, M),$$

де M − модуль (0<M); k − множник (0≤k<M); b − приріст (0≤b<M) r_0 − початкове значення (0≤ r_0<M).

Теорема. Лінійна конгруентна послідовність, визначена параметрами M, k, b й r0 , має період довжиною M тоді й тільки тоді, коли числа b й M взаємно прості; k – 1 є кратним p для кожного простого p, що є дільником M; k – 1 є кратним 4, якщо M є кратним 4.

Засобами C++ реалізовано генератор випадкових чисел з параметрами $M = 2^{31} - 1$; k = 1 220 703 125; b = 7; r_0 = 7. Доведено, що такі значення параметрів дозволяють отримати неповторювані числа з періодом, рівним 7

мільйонам. Для перевірки якості реалізованого генератора було проведено експерименти по генерації 100, 1000, 10000 псевдовипадкових чисел.

Фрагмент програмного коду:

```
{     long long k = 1220703125;
    int n = 10000;
    vector<long long> x1(n);
    x1[0] = 7;
    const long long MOD = (1LL << 31) - 1;
    for (int i = 1; i < n; i++) {
        x1[i] = (k * x1[i - 1] + 7) % MOD;
    }
```

На рис.1 показано результат проведеного експерименту.

```
number of hits in each interval:
interval 1 (from 0.00 to 0.10): 1020 hits
interval 2 (from 0.10 to 0.20): 1004 hits
interval 3 (from 0.20 to 0.30): 1021 hits
interval 4 (from 0.30 to 0.40): 1032 hits
interval 5 (from 0.40 to 0.50): 1002 hits
interval 6 (from 0.50 to 0.60): 978 hits
interval 7 (from 0.60 to 0.70): 1023 hits
interval 8 (from 0.70 to 0.80): 982 hits
interval 9 (from 0.80 to 0.90): 991 hits
interval 10 (from 0.90 to 1.00): 947 hits
xisq: 6.11
uniform
```

Рисунок 1 – Реалізація лінійного конгруентного генератора.

Далі проводилося перевірка за тестом χ^2 Пірсона статистичної гіпотези H_o про те, що задана вибірка відповідає генеральній сукупності з рівномірним розподілом на рівні значущості 0,1. Для всіх проведених експериментів гіпотеза H_o прийнято. Також, експериментальне значення лежить в діапазоні між двома значеннями, які відповідають, рівню значущості 0,5 та 0,75, що дає підстави вважати, що згенерована послідовність є послідовністю випадкових чисел. Лінійний конгруентний метод є простим у реалізації і досить ефективним для багатьох задач, де не потрібно досягати високої ступені випадковості.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Knuth, D. E. The art of computer programming. Vol. 2: Seminumerical algorithms / D. E. Knuth. – Reading (MA): Addison Wesley, 1998. – P. 93–118. – ISBN 978-0-201-89684-8.

2. Amrullah, A. Analysis of linear congruent methods and multiplicative random number generator in computer-based test / A. Amrullah,

A. Al-Khowarizmi, F. Rizky // Indonesian Journal of Electrical Engineering and Computer Science. – 2023. – Vol. 32, no. 3. – P. 1521–1532. – DOI: 10.11591/ijeecs.v32.i3.pp1521-1532.