УДК 004

АЛГОРИТМИ ОТРИМАННЯ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ

Хамза І.С.

Харківський національний автомобільно-дорожній університет, Харків

Вступ. Задача генерації випадкових послідовностей чисел зустрічається під час програмування різноманітних задач комп'ютерного моделювання, від якості таких послідовностей у значній мірі залежить адекватність отримуваних результатів моделювання.

Щоб сформувати справді випадкове число, комп'ютеру потрібно використовувати природний недетермінований процес – це коштовно й повільно, тому більшість програм, що працюють на персональних комп’ютерах не мають справжніх генераторів випадкових чисел.

Існують різноманітні способи генерування «псевдовипадкових» чисел, і псевдовипадкові числа в більшості випадків відповідають потребам програмістів.

У роботі розглянуто популярні алгоритми отримання псевдовипадкових чисел та способи вимірювання випадковості послідовності чисел.

Чому використовується алгоритми генерування псевдовипадкових чисел. Щоб кількісно визначити або виміряти випадковість послідовності чисел застосуємо понятння про складність об’єкта Колмогорова. Об’єктом може бути набір чисел – довжина комп’ютерної програми, що призводить до створення цього об’єкта. Це міра обчислювальних ресурсів, необхідних для створення об'єкта.

Випадковість Колмогорова [1] визначає об’єкта як випадковий тоді і тільки тоді, коли будь-яка комп'ютерна програма, яка може створити цей рядок, має принаймні таку ж складність, як і у самого об’єкту. Випадковий об’єкт у цьому сенсі є "нестисливим", оскільки неможливо "стиснути" об’єкт у програму, яка коротша за сам об’єкт.

Тому жоден алгоритм не здатний генерувати справді випадкові числа, і для задоволення цієї потреби використовуються алгоритми створення псевдовипадкових чисел.

Вимірювання випадковості набору чисел. Алгоритми створення псевдовипадкових чисел - це алгоритм генерації послідовності чисел, властивості яких наближаються до властивостей послідовностей випадкових чисел. Послідовність, створена послідовність не є справді випадковою, оскільки вона повністю визначається початковими значенням.

Федеральне відомство з інформаційної безпеки Німеччини (Bundesamt für Sicherheit in der Informationstechnik, BSI) встановило чотири критерії якості детермінованих генераторів випадкових чисел [2]:

1. Має бути велика ймовірність того, що генеровані послідовності випадкових чисел відрізняються одна від одної.

2. Послідовність чисел неможливо відрізнити від "справді випадкових" чисел за результатами багатьох спеціальних статистичних тестів, а саме перевірка того, наскільки випадковою є послідовність бітів – має нулі та одиниці з однаковою частотою; після послідовності n нулів (або одиниць), наступний біт одиниця (або нуль) з однаковою ймовірністю; будь-яка вибрана підпослідовність не містить інформації про наступні елементи в послідовності.

3. Не повинно бути можливим обчислити або вгадати з будь-якої заданої послідовності попередні чи майбутні значення у послідовності або внутрішній стану генератора.

4. Не повинно бути можливим обчислити або вгадати за внутрішнім станом генератора будь-які попередні або наступні числа в послідовності і внутрішні стани генератора.

За умови відповідності усім цім критеріям алгоритм генерації псевдовипадкових послідовностей може вважатися безпечним для використання у програмному забезпеченні.

Метод середньої квадрата. Ранній комп'ютерний АСПЧ, запропонований Джоном фон Нейманом у 1946 році, відомий як метод

середньої квадрата [3]. Алгоритм такий: візьміть будь-яке число, возведіть його в квадрат, видаліть середні цифри отриманого числа як "випадкове число", а потім використовуйте це число для наступної ітерації. Наприклад, при возведенні у квадрат числа "1111" виходить "1234321", яке можна записати як "01234321", 8-значне число є квадратом 4-значного числа. Це дає "2343", яке ми можемо використовувати як "випадкове" число, повторення цієї процедури дає "4896" як наступний результат і т. д. Фон Нойман використовував 10-значні числа, але процес був ідентичним.

Проблема методу середнього квадрата полягає в тому, що всі послідовності з часом повторюються, деякі дуже швидко.

Генератор випадкових чисел Лемера. Генератор випадкових чисел Лемера [4] (названий на честь Д. Х. Лемера) - це тип генератора, який працює

$$X_{k+1} = a \cdot X_k \mod m$$

в мультиплікативній групі цілих чисел за модулем n.

Оновленна версія цього алгоритма використовується у генераторі випадкових чисел minstd_rand на C ++ 11. Наукова бібліотека GNU включає кілька генераторів випадкових чисел форми Лемера, включаючи MINSTD, RANF та генератор випадкових чисел IBM RANDU.

Лінійний конгруентний генератор. Лінійний конгруентний генератор, дає послідовність псевдорандомізованих чисел, обчислених за допомогою розривного кусково-лінійного рівняння. Метод представляє один із найдавніших і найвідоміших алгоритмів генерації псевдовипадкових чисел. Генератор визначається натурним співвідношенням:

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

Де X - послідовність псевдовипадкових значень.

Перевага лінійного конгруентного генератора полягає в тому, що при відповідному виборі параметрів період відомий і довгий. Хоча це не єдиний

критерій, занадто короткий період є фатальною вадою генератора псевдовипадкових чисел. Лінійний конгруентний генератор здатний виробляти псевдовипадкові числа, які можуть пройти офіційні тести на випадковість, але якість вихідних даних надзвичайно чутлива до вибору параметрів m та a. Наприклад, a = 1 і c = 1 створюють простий лічильник за модулем-m, який має тривалий період, але, очевидно, є невипадковим.

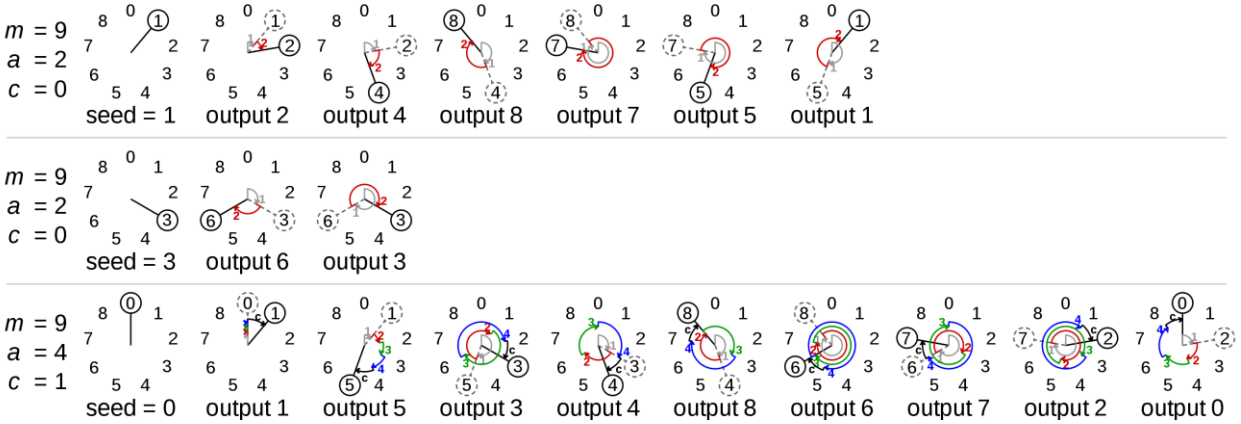

Рисунок 1 – Приклад роботи лінійної конгруентності

Висновок. У роботі проведено аналіз характеристик існуючих методів генерування псевдовипадкових чисел, які увійшли в основу реалізації відповідних функцій у мовах програмування.

Список використаних джерел

[1] А. Колмогоров, "На таблицях випадкових чисел”, 1963.

[2] В. Шиндлер, "Класи функціональності та методологія оцінки детермінованих генераторів випадкових чисел”, 1999.

[3] Джон фон Нейман, “Різні техніки, що використовуються у зв'язку із випадковими цифрами”, 1949.

[4] В.Х. Пейн; Дж. Р. Рабунг; Т.П. Боджо, "Кодування генератора псевдовипадкових чисел Лемера”, 1969.