**Дослідження та порівняння алгоритмів генерації**

**псевдовипадкових чисел**

*Круглікова А. Д.*

*Полтавський національний технічний університет*

*ім. Ю.Кондратюка, Україна, Полтава*

*У статті розглянуті деякі алгоритми генерації псевдовипадкових чисел, сфери їх використання та зроблений статистичний аналіз декількох алгоритмів.*

***Ключові слова:*** *псевдовипадкові числа, генератори псевдовипадкових чисел, лінійна конгруентна послідовність, датчики Фібоначчі, Х2-критерій.*

Вступ

Мета роботи полягає в проведенні порівняльного аналізу базових алгоритмів генерації псевдовипадкових чисел.

Для досягнення зазначеної мети поставлено і вирішено наступні завдання:

* Вивчення літературних джерел і проведення теоретичного аналізу алгоритмів.
* Дослідження сфер прикладного застосування псевдовипадкових чисел.
* Встановлення особливостей релізації алгоритмів генерації

псевдовипадкових чисел.

* Розробка відповідних програмних компонентів, проведення експериментів, порівняльні результати роботи.

Сучасна інформатика широко використовує випадкові й псевдовипадкові числа в самих різних додатках.

Найпоширеніші сфери застосування випадкових чисел:

1. Імітаційне моделювання;
2. Криптографія;
3. Ігрова індустрія;
4. Рішення прикладних математичних завдань.

Генерація істинно випадкових послідовностей на комп'ютерах, споконвічно спроектованих у термінах детермінованості й повторюваності результатів обчислень, є нездійсненним завданням, якщо тільки в нашому розпорядженні немає апаратних засобів, принцип роботи яких заснований на використанні яких-небудь фізичних генераторів шумів (теплових, дробових і т.п.) Однак можна побудувати функції, що видають серії чисел, що володіють необхідними властивостями й проходять ряд статистичних тестів.

Для забезпечення безпеки комп'ютерних систем критично важливо мати алгоритми, що задовольняють такому критерію як непередбачуваність. Іншими словами, навіть знаючи алгоритм генератора й всі попередні елементи послідовності, повинне бути максимально трудомістким обчислення наступних елементів.

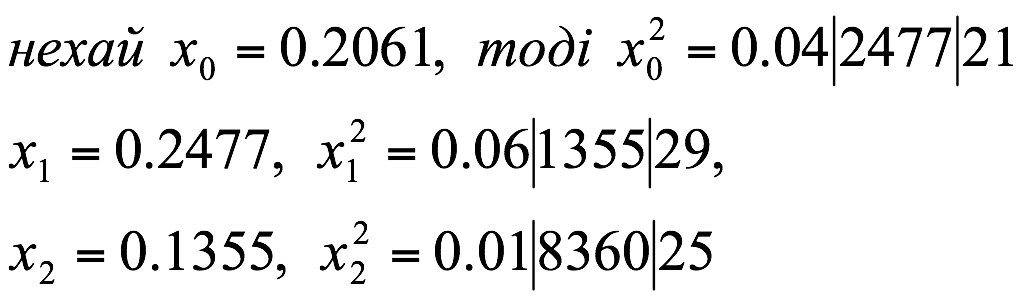
Основна частина

Першим алгоритмічний метод одержання рівномірно розподілених псевдовипадкових чисел запропонував Джон фон Нейман (один з основоположників кібернетики). Метод одержав назву "метод середини квадрата".

Суть методу: попереднє випадкове число зводиться у квадрат, а потім з результату витягаються середні цифри.

Наприклад:

(1) і т.д.



Як видно метод середини квадрата досить добре повинен "перемішувати" попереднє число. Однак він має недоліки:

Якщо який-небудь член послідовності виявиться рівним нулю, то всі наступні члени також будуть нулями.

У цей час найбільш популярними генераторами випадкових чисел є генератори, у яких використається схема, запропонована Д. Г. Лехмером в 1949 році - лінійний конгруентний метод.

Виберемо чотири "чарівних числа":

- m, модуль; 0 < m;

- а, множник; 0 < a < m;

- с, приріст; 0 < с < m;

- X0, початкове значення; 0 < X0 < m.

Потім одержимо бажану послідовність випадкових чисел (Хn), маючи на увазі

*Xn+1 = (а\* Xn+ с) mod m, n > 0.* (2)

Ця послідовність називається *лінійною конгруентною послідовністю*.

Особливості розподілу випадкових чисел, що генеруються лінійним конгруентним алгоритмом, унеможливлюють їхнє використання в статистичних алгоритмах, що вимагають високого дозволу.

У зв'язку із цим лінійний конгруентний алгоритм поступово втратив свою популярність і його місце зайняло сімейство алгоритмів Фібоначчі, які можуть бути рекомендовані для використання в алгоритмах, критичних до якості випадкових чисел. В англомовній літературі датчики Фібоначчі такого типу називають звичайно «Subtract-with-borrow Generators» (SWBG).

Найбільшу популярність датчики Фібоначчі одержали у зв'язку з тим, що швидкість виконання арифметичних операцій з речовинними числами зрівнялася зі швидкістю цілочисельної арифметики, а датчики Фібоначчі природно реалізуються в речовинній арифметиці.

Один із широко розповсюджених датчиків Фібоначчі заснований на наступній ітеративній формулі:

(3)



де *Xk* — речовинні числа з діапазону *[0,1)*, *a,b* — цілі позитивні числа, називані *лагами*. Для роботи датчику Фібоначчі потрібно знати *max{a,b}* попередніх генерованих випадкових чисел. При програмній реалізації для зберігання генерованих випадкових чисел використається кінцева циклічна черга на базі масиву. Для старту датчику Фібоначчі потрібно *max{a,b}* випадкових чисел, які можуть бути генеровані простим конгруентним датчиком.

Лаги *a* й *b* — «магічні» й їх не слід вибирати довільно. Рекомендуються вибирати наступні значення лагів*: (a,b)=(55,24), (17,5)* або *(97,33)*. Якість одержуваних випадкових чисел залежить від значення константи *a.* Чим воно більше, тим вище розмірність простору, у якому зберігається рівномірність випадкових векторів, утворених з отриманих випадкових чисел. У той же час, зі збільшенням величини константи *a* збільшується об'єм використовуваної алгоритмом пам’яті.

Із сучасних ГПВЧ широке поширення одержав вихор Мерсенна, запропонований в 1997 році Мацумото й Нишимурой. Їхня робота ґрунтується на властивостях простих чисел Мерсенна (звідси назва) і забезпечує швидку генерацію високоякісних псевдовипадкових чисел.

Перевагами цього методу є колосальний період (219937-1), рівномірний розподіл в 623 вимірах (лінійний конгруентний метод дає більш-менш рівномірний розподіл від сили в 5 вимірах), швидка генерація випадкових чисел (в 2-3 рази швидше, ніж стандартні ГПВЧ, що використають лінійний конгруентний метод). Однак існують складні алгоритми, що розпізнають послідовність, породжувану за допомогою вихрячи Мерсенна як невипадкову. Це робить вихор Мерсенна невідповідним для використання в криптографії.

Генеровані алгоритмом „Вихор Мерсенна” псевдовипадкові числа успішно проходять тести DIEHARD, що говорить про їх гарні статистичні властивості.

Будемо позначати х — вектори слова над полем F2={0,1}. Вихор Мерсенна генерує послідовність векторів-слів, які є псевдовипадковими числами із діапазоні від 0 до 2w-1. Якщо поділити отримані числа на 2w-1, то отримаємо псевдовипадкові числа з діапазону [0,1].

Алгоритм працює за наступним рекурентним співвідношенням:

(4)



де:

n — ціле, яке позначає ступінь рекурентності.

m — ціле, .



A — матриця розміром .

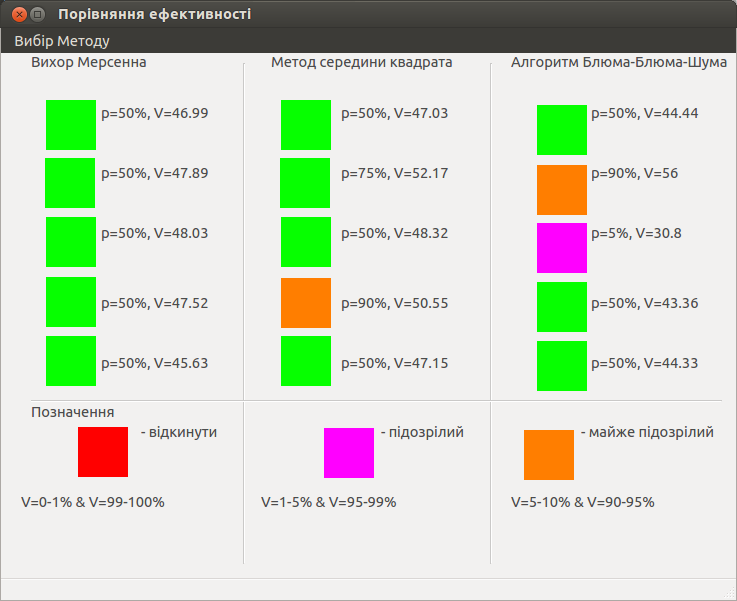


| - побітове АБО (OR).

°- сума по модулю 2 (XOR).

Одним із способів порівння ефективності алгоритмів є відомий статичтичний метод “Х2-критерій”. На його основі можна зробити порівняння деяких алгоритмів генерації псевдовипадкових чисел і відобразити результати візуально:

Висновки



Генератор псевдовипадкових чисел є алгоритмом, що генерує послідовність чисел, елементи якої майже незалежні один від одного і підкоряються заданому розподілу. Використання подібних генераторів в сучасній техніці украй важливо, оскільки на їх базі можуть створювати ключі для шифрування, різні захисні послідовності для тих або інших даних і пакетів даних і багато що інше. Необхідне подальше вивчення і вдосконалення генераторів псевдовипадкових чисел, яке надалі повною мірою розкриє їх потенціал.

Список літератури

1. Андрій Зубинський. В поисках случайности // Компьютерное обозрение. — 2003. — № 29.
2. Галуєв Г. А. Математические основы криптологии: Учебно-методическое пособие. Таганрог: Изд-во ТРТУ 2003.-120с.
3. Дональд Э. Кнут. Глава 3. Случайные числа // Искусство программирования = The Art of Computer Programming. — 3-е изд. — М.: Вильямс, 2000. — Т. 2. Получисленные алгоритмы. — 832 с. — 7000 экз. — ISBN 5-8459-0081-6
4. Каханер Д. Численные методы и математическое обеспечение: Пер. с англ. / Д. Каханер, К. Моулер, С. Нэш. М.: Мир, 1998. – 575 с., ил.
5. Коробейніков А. Г, Ю. А. Гатчин. Математические основы криптологии. Учебное пособие. СПб: СПб ГУ ИТМО, 2004. – 106 с, илл.
6. Математические основы криптологии: Учебное пособие / Харін Ю.С., Бернік В.И., Матвеєв Г.В. – Мн.: БГУ. 1999. – 319 с.
7. М. А. Іванов, И. В. Чугунков. Глава 4. Методика оценки качества генераторов ПСП. // Теория, применение и оценка качества генераторов псевдослучайных последовательностей. — М.: КУДИЦ-ОБРАЗ, 2003 — 240 с. ISBN 5-93378-056-1