

Список використаних джерел:

1. Про внесення змін до деяких законів України щодо забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів: Проект Закону України № 7152 від 13.03.2022. URL: <https://itd.rada.gov.ua/billInfo/Bills/Card/39215>. – Дата звернення: 05.06.2022 р.
2. Fire Has Destroyed OVH's Strasbourg Data Center (SBG2). – URL: <https://www.datacenterknowledge.com/uptime/fire-has-destroyed-ovh-strasbourg-data-center-sbg2>. – Last access: 27.05.2022.
3. Uptime Institute Issued Awards. – URL: <https://uptimeinstitute.com/uptime-institute-awards/list>. – Last access: 27.05.2022.
4. Postmortem: VSTS 4 September 2018. – URL: <https://devblogs.microsoft.com/devopsservice/?p=17485>. – Last access: 27.05.2022.
5. BusinessViews: список самых крупных аварий в дата-центрах мира. – URL: <https://businessviews.com.ua/ru/business/id/avarii-v-data-centrah-2248>. – Дата обращения: 27.05.2022 г.
6. Telecommunications Industry Association: Standards. – URL: <https://www.datacenterknowledge.com/uptime/fire-has-destroyed-ovh-strasbourg-data-center-sbg2>. – Last access: 05.06.2022.

Ключові слова: хмарні технології, державні інформаційні ресурси, відмовостійкість, стандарти телекомунікаційної інфраструктури.

Key words: cloud technologies, state information resources, fault tolerance, telecommunication infrastructure standards.

ЩЕРБИНА ЮРІЙ ВОЛОДИМИРОВИЧ

*Національний університет «Одеська юридична академія»,
доцент кафедри інформаційних технологій,
кандидат технічних наук, доцент*

КАЗАКОВА НАДІЯ ФЕЛКСІВНА

*Національний університет «Одеська юридична академія»,
професор кафедри кібербезпеки, доктор технічних наук, професор*

РАНДОМІЗАЦІЯ ПРОГРАМНИХ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ

Сучасний розвиток обчислювальної техніки робить комп'ютерне моделювання важливим етапом проектування технічних систем, які забезпечують коректне протікання таких складних процесів як розподілення потоків в транспортних та інформаційно-телекомунікаційних системах, в управлінні виробництвом та інфраструктурними і подібними їм складними об'єктами.

Моделювання уявляє собою симуляцію поведінки реальної системи шляхом її відтворення у вигляді обчислювального процесу відповідно з правилами, закладеними у математичній моделі. Воно дає можливість отримати початкову інформацію про поведінку системи у заданих умовах експлуатації. Разом з тим, його використання в сучасних умовах стримується наявністю наступних проблем. По-перше, обчислювальна техніка – це детермінований дискретний автомат і вона не дає можливості моделювати справжні випадкові процеси. По-друге, визначення на основі емпіричних даних закону, яким описується поведінка системи, що підлягає дослідженню, – це достатньо складна задача. І, нарешті, побудована модель має оцінюватись на предмет адекватності закладеному в неї математичному закону розподілення ймовірностей. Якщо останні дві проблеми так або інакше вирішуються, то рішення першої проблеми вимагає проведення додаткових досліджень [1].

Зазвичай, для створення комп'ютерної моделі використовують або метод зворотних функцій, або метод Монте-Карло. Якщо для функції розподілення ймовірностей процесу, який необхідно моделювати існує зворотна функція, краще скористуватись першим методом.

Враховуючи, що для переважної більшості відомих розподілень існують зворотні функції, а для тих із них, що такої функції не мають, існують варіанти їх описання їх через ряди, ціллю досліджень є розроблення методики рандомізації генераторів псевдовипадкових чисел, які входять до складу більшості програмних середовищ і використовуються як джерело ентропії в комп'ютерних моделях, побудованих на основі методу зворотних функцій.

Рандомізація потоку псевдовипадкових чисел

Суть імітаційного комп'ютерного моделювання полягає у заміні реальних вимірювальних величин їх псевдовипадковими аналогами, сформованими як результат обчислювального процесу. У разі використання запропонованого Н. В. Смірновим методу зворотних функцій [2], генерація випадкових величин із заданою функцією розподілення $F(x)$ відбувається шляхом модифікації послідовності чисел, рівномірно розподілених на інтервалі $[0, 1]$.

Суть цього методу полягає в тому, що числа на виході генератора рівномірно розподілених псевдовипадкових чисел (ПВЧ) розглядаються як значення функції розподілення ймовірностей випадкового процесу $F(x)$, який моделюється комп'ютером, а сама випадкова величина x_i обчислюється як зворотна від неї функція $F^{-1}(x_i)$, так, як це показано на рисунку 1.

Особливість цього методу полягає в його надзвичайно високій чутливості до рівномірності розподілення чисел на виході генератора ПВЧ. Враховуючи, що майже всі сучасні середовища програмування використовують у якості генератора ПВЧ лінійний конгруентний генератор (Linear congruent generator LCG) або генератор, відомий під назвою Вихор Мерсенна (Mersenne twister, MT) [3], не забезпечують необхідної рівномірності розподілення чисел на їх виході, доводиться вводити до складу моделі додаткові функції їх рандомізації.

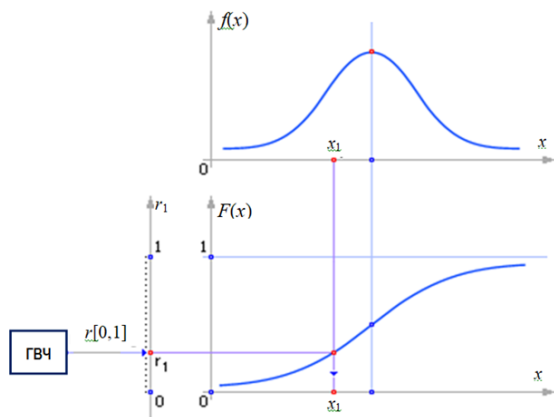


Рис. 1. Принцип моделювання методом зворотних функцій

Існує достатньо велика кількість способів оцінки відповідності розподілення числового потоку заданому закону. Однак основним вважається критерій Пірсона χ^2 [3], по-перше, через його незалежність від перевіряемого типу розподілення і, по-друге, через те, що у разі негативного результату перевірки, малоймовірно, що використання інших критеріїв дасть кращий результат [4].

На рисунках 2 і 3 показані результати дослідження LCG та MT генераторів методом гістограм. Число інтервалів обиралось рівним 16, а розмір вибірки дорівнював 1024 числам.

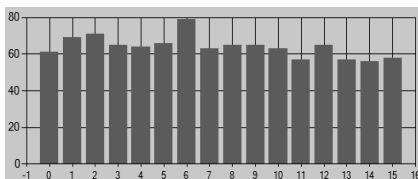


Рис. 2. Гістограма розподілення ПВЧ отриманих за допомогою функції rand()

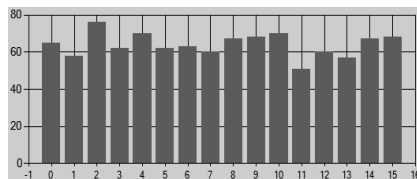


Рис. 3. Гістограма розподілення ПВЧ отриманих за допомогою функції uniform_real_distribution<> mersenne(0, 1)

Показник якості обчислювався як

$$\chi^2 = \sum_{i=1}^k \frac{(n_i - N_i^*)^2}{N_i^*},$$

де k – це кількість сегментів гістограми;

n_i і N_i^* – кількість випадкових чисел вихідного потоку, що реально попала в i -й інтервал та їх очікувана кількість, відповідно.

Як це видно з наведених рисунків і отриманих значень обчислених показників χ^2 для обох генераторів, обидва потоки псевдовипадкових чисел не відповідають вимогам рівномірності розподілення чисел.

Для вирішення проблеми, враховуючи припустимість таких операцій як об'єднання числових потоків, їх «відбілювання» або «просіювання», було використано «вирівнювання» розподілення ймовірності чисел потоку шляхом видалення з його складу «зайвих» елементів [4].

Очікується, що у разі рівномірного розподілення у кожний сегмент гістограми має попадати однакова кількість випадкових чисел, яка дорівнює $N_i^* = N/k$. Математичне очікування величини, що має потрапити в сегмент, обмежений умовами $x_{min} \leq x_i < x_{max}$, визначається як $m_i = (x_{min} + x_{max})/2$. Тоді кількість чисел, що попали в i -тий сегмент s_i , орієнтовно буде дорівнювати величині $S_i^* = N_i^* m_i$. Звичайно, що кожного разу ця сума буде або менше S_i^* , або більше S_i^* , але суттєвої різниці не буде. Якщо сума чисел s_i , що попали в i -тий сегмент гістограми перевищує величину S_i^* , то всі інші числа що в нього попадають пропускаються [5]. В результаті, кількість чисел в сегментах залишиться різною, але нерівномірність вибірки стане меншою.

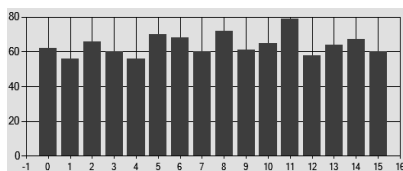


Рис. 4. Гістограма розподілення ПВЧ до рандомізації отриманих за допомогою функції `uniform_real_distribution<> mersenne(0, 1)`

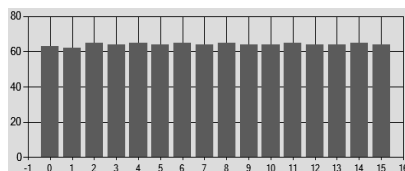


Рис. 5. Гістограма розподілення ПВЧ після рандомізації отриманих за допомогою функції `uniform_real_distribution<> mersenne(0, 1)`

Як видно із наведених на рисунках 4 і 5 гістограм, застосування описаного способу «вирівнювання» розподілення потоку на виході генератора ПВЧ приводить до сталого рівномірного розподілення чисел, що підтверджується обчисленням показника χ^2 . Звичайно, що можна застосовувати й інші аналогічні способи, в залежності від вимоги до моделювання.

Сучасне комп'ютерне моделювання передбачає використання таких програмних середовищ як Boost, Glib, C++, Python, Ruby, R, PHP, MATLAB та їм подібних пакетів. Всі вони написані мовою C++ і користуються її генераторами ПВЧ. Через це, є сенс користуватись для створення моделей стохастичних процесів програмних середовищ Visual Studio або QT5, які включають достатню кількість додаткових бібліотек, що містять різноманітні генератори ПВЧ. Причому, обов'язковою умовою є виконання попередньої рандомізації числового потоку на виході обраного

генератора та його перевірка на предмет рівномірності розподілення ймовірності сформованих чисел.

Список використаних джерел:

1. Knuth D. E. The Art of Computer Programming, Volume 2: Seminumerical Algorithms, 3rd. ed., Boston, Mass, USA : Addison-Wesley, Longman Publishing, Addison-Wesley, Reading, Mass, 1998.
2. Mark A. Pinsky, Samuel Karlin. An Introduction to Stochastic Modeling, Fourth Edition., Academic Press, 2010.
3. Ahrens J. H., Dieter U., Grube A. Pseudo-random numbers. Computing 6 (1970) 121–138). URL: <https://doi.org/10.1007/BF02241740>.
4. Neumann J. von. Various techniques for use in connection w J. von Neumann. Various techniques for use in connection with random digits. Applied Math Series, Notes by G. E. Forsythe, in National Bureau of Standards, Vol. 12, 36–38, 1951.
5. Trevisan L. Extractors and Pseudorandom Generators 1999. Journal of the ACM URL: <http://theory.stanford.edu/~trevisan/pubs/extractor-full.pdf>

Ключові слова: комп'ютерне моделювання, метод Монте-Карло, метод зворотних функцій, генератори псевдовипадкових чисел, рандомізація.

Key words: computer modeling, Monte Carlo method, inverse function method, pseudo-random number generators, randomization.

ЗАДЕРЕЙКО ОЛЕКСАНДР ВЛАДИСЛАВОВИЧ

*Національний університет «Одеська юридична академія»,
доцент кафедри інформаційних технологій,
кандидат технічних наук, доцент*

ЯНКОВСЬКИЙ ОЛЕГ ГЕОРГІЙОВИЧ

*Національний університет «Одеська юридична академія»,
доцент кафедри інформаційних технологій,
кандидат технічних наук, доцент*

ДИКА АНАСТАСІЯ ІВАНІВНА

*Національний університет «Одеська юридична академія»,
асистент кафедри інформаційних технологій*

ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ МЕСЕНДЖЕРА TELEGRAM

Велика кількість користувачів використовують для обміну інформацією різні месенджери. Однак далеко не всі користувачі віддають собі звіт у тому, наскільки є конфіденційним такий обмін інформацією