Міністерство освіти і науки України

Харківський національний автомобільно-дорожній університет

«КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ І МЕХАТРОНІКА»

(30 травня 2019 р.)

ЗБІРНИК НАУКОВИХ ПРАЦЬ

ЗА МАТЕРІАЛАМИ МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

Харків,

2019

УДК 004:629:656:658

Комп'ютерні технології і мехатроніка. Збірник наукових праць за матеріалами міжнародної науково-практичної конференції. – Харків, ХНАДУ, 2019. – 282 с.

Збірник містить результати теоретичних та практичних наукових досліджень та розробок, які були виконані науково-педагогічними працівниками вищої школи, науковими співробітниками, докторантами, аспірантами, магістрантами, студентами ті фахівцями різних організацій і підприємств.

Для викладачів, наукових працівників, докторантів, аспірантів, магістрантів, студентів, фахівців.

Матеріали доповідей конференції відтворено з авторських оригіналів

Конференцію проведено згідно з планом проведення міжнародних, всеукраїнських науково-практичних і науково-методичних конференцій і семінарів Харківського національного автомобільно-дорожнього університету у 2019 р. (посвідчення УкрІНТЕІ № 666 від 20 грудня 2018 р.)

УДК 519.237.3:519.669:681.51

ОЦІНКА ЯКОСТІ ПОСЛІДОВНОСТЕЙ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ

Поперешняк С.В., к.ф.-м.н., доц., кафедра програмних систем і технологій, КНУ імені Тараса Шевченка

Постановка проблеми. У програмному забезпеченні практично всіх ЕОМ є вбудована функція генерації послідовності псевдовипадкових квазірівномірно розподілених чисел. Однак для проведення статистичного моделювання до генерації випадкових чисел пред'являються підвищені вимоги. Якість результатів такого моделювання безпосередньо залежить від якості генератора рівномірно розподілених випадкових чисел, тому що ці числа є також джерелами (вихідними даними) для отримання інших випадкових величин із заданим законом розподілу.

На жаль, ідеальних генераторів не існує, а список їх відомих властивостей поповнюється переліком недоліків. Це призводить до ризику використання в комп'ютерному експерименті поганого генератора. Тому перед проведенням комп'ютерного експерименту необхідно або оцінити якість вбудованої в ЕОМ функції генерації випадкових чисел, або вибрати відповідний алгоритм генерації випадкових чисел.

Мета дослідження – провести короткий огляд відомих підходів до тестування послідовностей на випадковість та запропонувати підхід до тестування послідовностей псевдовипадкових чисел з використанням багатовимірних статистик в основі яких застосовуються принципи s-ланцюжків.

Основний матеріал. Отже, в математичному плані, основна вимога до датчика випадкових чисел полягає в тому, що послідовність яку вони виробляють повинна бути в статистичному сенсі такою, що не відрізняється від послідовності незалежних і однаково розподілених випадкових величин, тобто повинна відповідати гіпотезі випадковості H_0 (узгоджуватися з нею).

Тепер ми уточнимо постановку задачі, яку будемо обговорювати далі.

Нехай задана послідовність з n випадкових величин (вибірка)

$$\gamma_1, \gamma_2, \ldots, \gamma_n, \qquad (1)$$

де γ_i приймають значення з скінченої множини (алфавіту) $\mathrm{E} = \{1, 2, \ldots, \mathrm{N}\}$, відносно якої потрібно перевірити гіпотезу H_0 про те, що ці випадкові величини в сукупності незалежні і рівномірно розподілені на множині E, тобто $\mathrm{P}\{\gamma_i = \mathrm{j}\} = \frac{1}{N}$, j = 1, 2, . . . , N. i = 1, 2, . . . , n [1]. Гіпотеза H_0 це гіпотеза про ідеальний датчик: якщо гіпотеза H_0 вірна, то датчик, що виробляє послідовність (1), реалізує «ідеальну » схему незалежних випробувань з рівноімовірними наслідками. Але ідеальних датчиків не існує, більше того, часто датчик виробляє послідовність (1) програмним способом (тобто ці числа можуть бути навіть детермінованими), але тоді ці числа повинні бути такими, що «практично не відрізняються» (або дуже схожі) від незалежних і рівноімовірних чисел. У математичному плані це розуміється так: вибірка (1) не повинна спростовувати гіпотезу H_0 ніяким тестом. Практично ж ідуть на наступний компроміс: визначається деяка сукупність статистичних критеріїв (тестів) і, ґрунтуючись на вибірці (1), перевіряють гіпотезу H_0 по кожному з цих контрольних тестів.

Якщо гіпотеза H_0 успішно проходить таке тестування, то вона приймається як істина, і числа (1) рекомендуються для використання в відповідних цілях як незалежні і рівномірно розподілені на множині E; випадкові числа.

Загальноприйняті в наш час набор тестів складається з [2]:

1. 11 тестів: Donald Knuth (Stanford University);
2. 15 тестів: NIST Statistical Test Suite;
3. 12 тестів: DIEHARD;
4. 11 тестів: TestU01;
5. 5 тестів: Crypt-XS.

Але роботи по удосконаленню методів тестування випадкових і псевдовипадкових тестів продовжується. В роботі пропонується критерій типу хі-квадрат для перевірки гіпотези H_0 якій заснований на підрахунку частот s-ланцюжків в послідовності (1).

Ідею побудови цього тесту можна пояснити наступним чином [1]. Оскільки гіпотеза H_0 – проста (вона однозначно фіксує розподіл спостережень (1)), то, в принципі для її перевірки можна було б використовувати класичний критерій хі-квадрат. Але цей критерій «працює» лише за умови незалежності спостережень (1): він дієздатний проти альтернатив, які враховують зміну лише ймовірностей появи результатів, але зберігають припущення про незалежність спостережень. Але ж саме це припущення про незалежність і потрібно піддати перевірці! Тому критерій хі-квадрат Пірсона не вирішує цю проблему. Зберігаючи ідеологію методу хі-квадрат (порівняння емпіричних частот деяких подій з їх гіпотетичними можливостями за допомогою міри хі-квадрат), можна спробувати сконструювати тест, який буде «реагувати» на альтернативи того чи іншого типу залежності між даними (1), розглядаючи замість частот окремих випадків в послідовності (1) частоти ланцюжків результатів деякої фіксованої довжини s> 2, причому ланцюжки повинні перекриватися.

Дамо точне визначення: s -ланцюжком (або S-грамою) називається будь-яка підпослідовність послідовності (1), яка складається із s послідовно розташованих її членів.

Проілюструємо (рис. 1) застосування s -ланцюжків для перевірки сумісності розподілів деяких статистик випадкових бітових векторів для малої вибірки n, $n = 20$, і деяких значень k_1 та k_2 [3].

На рис. 1 представлено бульбашкову діаграму, в якій перший параметр (горизонтальна вісь) – значення k_1, другий (вертикальна вісь) – значення k_2, третій (розмір бульбашки) – ймовірність події $\{\eta(t\ t^*) = k_1, \eta(t\ 1\ t^*) + \eta(t\ 0\ t^*) = k_2\}$, яка подана в відсотках.

Висновки. В роботі запропоновано підхід до тестування послідовностей псевдовипадкових чисел з використанням багатовимірних статистик в основі яких застосовується принцип s-ланцюжків. Наведено приклад застосування критерію для перевірки (0, 1)-послідовностей невеликої довжини (до 100 біт), за допомогою багатомірних статистик.

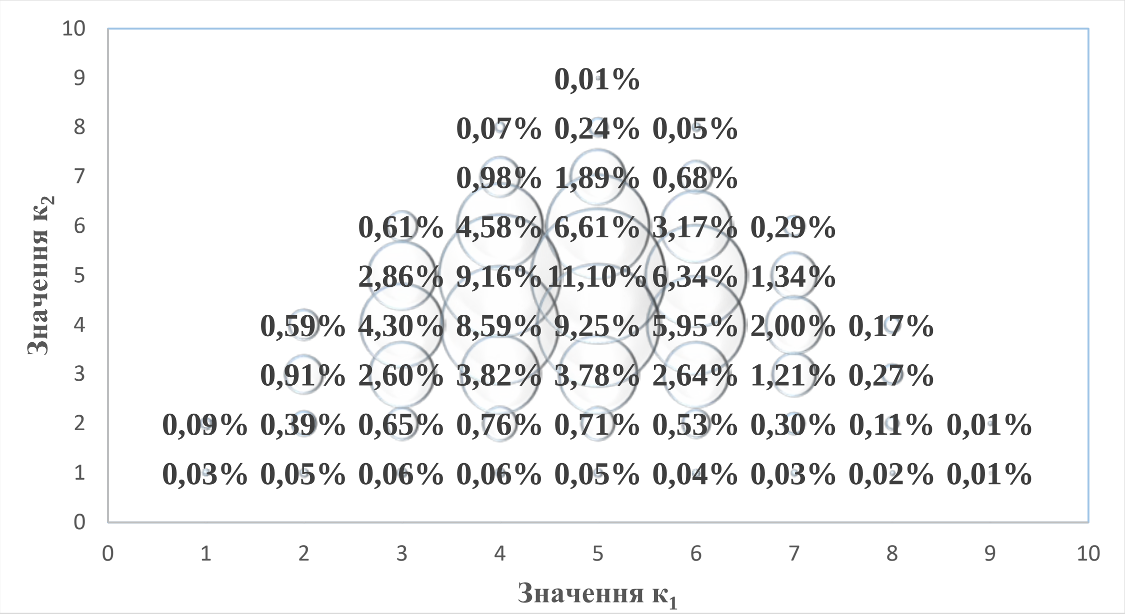

Рисунок 1 – Розподіл ймовірностей зазначеної події в залежності від k_1 та k_2.

Підхід до тестування з використанням багатомірних статистик дозволяє розраховувати на більш глибоке обґрунтування якості псевдовипадкових послідовностей, що генеруються.

Література: 1. Ивченко Г.И., Медведев Ю. И. Введеиие в математическую статистику: Учебник. М.: Издательство ЛКИ, 2010. 600 с. **2.** А.М. Коренева, В.М. Фомичёв «Статистическое тестирование псевдослучайных последовательностей» // Безопасность информационных технологий. - № 2 - 2016. **3.** Поперешняк С.В. Тестування псевдовипадкових послідовностей багатовимірними статистиками //288-290 Матеріали Міжнародної науково-практичної інтернет-конференції «Тенденції та перспективи розвитку науки і освіти в умовах глобалізації»: Зб. наук. праць. – Переяслав-Хмельницький, Вип. 45. – 2019. – с. 288-290

УДК 519.161

ПАРОСПОЛУЧЕННЯ В МОДЕЛЯХ ТРАНСПОРТНОЇ ЛОГІСТИКИ

Мацій О. Б., асистент, кафедра комп’ютерних наук, ХНАДУ,

Наумов В.С., д.т.н., проф., Cracow University of Technology, Poland

Постановка проблеми. Використання задач, які формулюються в термінах теорії паросполучень в розв’язанні оптимізаційних задач транспортної логістики.

ЗМІСТ

НАУКОВЕ ВИДАННЯ

ЗБІРНИК НАУКОВИХ ПРАЦЬ ЗА МАТЕРІАЛАМИ МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ «КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ І МЕХАТРОНІКА»

Конференцію проведено згідно з планом проведення міжнародних, всеукраїнських науково-практичних і науково-методичних конференцій і семінарів Харківського національного автомобільно-дорожнього університету у 2019 р. (посвідчення УкрІНТЕІ № 666 від 20 грудня 2018 р.)

Відповідальний за випуск д.т.н., проф. Ніконов О.Я.

Науковий редактор д.т.н., проф. Ніконов О.Я.

Технічний редактор Мнушка О.В.