УДК 519.6 **DOI: 10.20998/2411-0558.2016.21.12**

М.В. СЕМАНЬКІВ, канд. техн. наук, доц., ДВНЗ "Прикарпатський національний університет імені Василя Стефаника", Івано-Франківськ

ОЦІНКА СТАТИСТИЧНИХ ХАРАКТЕРИСТИК СИСТЕМ ВИПАДКОВИХ ЧИСЕЛ

Подано результати дослідження статистичних характеристик послідовностей псевдовипадкових чисел, що утворені методом Галуа на основі циклічних зсувів, за допомогою пакету статистичних тестів Diehard. Відзначено ефективність використання даного типу генератора в складі аналого-цифрового перетворювача Монте-Карло. Іл.: 3. Табл.: 1. Бібліогр.: 9 назв.

Ключові слова: псевдовипадкові числа, оцінка статистичних характеристик систем випадкових чисел, пакет статистичних тестів Diehard.

Постановка проблеми. В прикладних задачах випадкові числа знаходять досить широке застосування, зокрема, в області математичної статистики, чисельних методів оптимізації, імітаційному моделювання, комп'ютерного програмування, прийняття рішень і т.і. У різних предметних областях перед генераторами випадкових чисел стоять різні вимоги. Так, в деяких завданнях моделювання важливо, щоб послідовності випадкових чисел задовольняли рівень складності реалізації, в інших завданнях – тести на відсутність авто- та взаємної кореляції, або тести на рівномірність. Для вирішення різних завдань слід застосовувати різні генератори випадкових чисел, які для даної групи завдань є найбільш оптимальним вибором при дотриманні першочергових вимог. На сьогодні виникає питання дослідження та порівняння різних генераторів випадкових чисел з єдиних позицій. Виходом з цього положення є використання деякого стандартного набору статистичних тестів, які об'єднані єдиною методикою обчислення необхідних показників ефективності генераторів випадкових чисел і прийняття рішення про випадковість сформованих послідовностей.

Аналіз літератури. В [1, 2] подано аналіз принципів побудови і властивості генераторів псевдовипадкових чисел та описано методи оцінки якості генераторів. В [3] розкритий спосіб побудови генератора Галуа на основі циклічних зсувів. В [4 – 6] подано результати дослідження статистичних характеристик вказаного вище генератора. Способи використання тестів Diehard і рекомендації щодо інтерпретації отриманих результатів висвітлено в [7, 8]. Програмний продукт розміщений за адресою [9].

Проведений аналіз існуючих методів генерування випадкових чисел, складності їх технічної реалізацій та стабільності імовірнісних

характеристик генераторів псевдовипадкових чисел, дозволив стверджувати те, що відомі методи генерування характеризуються або складністю технічної реалізації, або низьким рівнем рівномірності розподілу, що визначає актуальність розробки нових методів генерування випадкових чисел. Слід відзначити, що останнім часом все більшої популярності набувають генератори псевдовипадкових чисел (ПВЧ). Генератори ПВЧ стали найважливішими елементами систем захисту, надійність останньої в значній мірі визначається саме властивостями використаних генераторів. Якісні генератори ПВЧ, будучи за своєю суттю детермінованими, мають проте практично всі властивості реалізацій істинно випадкових процесів і успішно замінюють їх, оскільки випадковим числам складно забезпечити необхідні статистичні характеристики [1, 2].

Важливим класом псевдовипадкових послідовностей є послідовності, які формуються генераторами на основі регістрів зсуву з лінійними зворотними зв'язками. Основними перевагами таких генераторів є: простота апаратної і програмної реалізації; висока швидкодія; достатньо високі статистичні властивості сформованих послідовностей; можливість побудови на їх основі генераторів, що формують послідовність довільної довжини або послідовність псевдовипадкових чисел з довільним законом розподілу.

На основі проведеного аналізу складності технічної реалізації методів псевдовипадкового генерування як один із ефективних запропоновано метод на базі використанням незвідних поліномів над полем Галуа $GF(2)$ [3]. Формування n-розрядних псевдовипадкових чисел ($c_1, c_2, ..., c_n$) в двійковій системі числення здійснюється на основі циклічного зсуву початкової послідовності ($b_1, b_2, ..., b_n$), утворюючи послідовність ($b_2, b_3, ..., b_0$), причому елемент b_0 є сумою за модулем 2 добутків відповідних елементів послідовності $b_1, b_2, ..., b_n$ та маски $a_1, a_2, ..., a_n$, утвореної коефіцієнтами незвідного полінома над полем Галуа. Отже,

$$c_1 = b_2,\ c_2 = b_3,\ ...,\ c_n = \left(\sum_{i=1}^{n} b_i a_i\right) mod 2. \qquad (1)$$

Всі n-розрядні числа псевдовипадкової послідовності трансформують у відліки десяткової системи числення. Даний метод названо *методом генерування Галуа на основі циклічних зсувів,* що легко апаратно реалізується на регістрах зсуву. Перевагою даного методу є простота технічної реалізації даного генератора з допомогою регістрів зсуву, що є суттєвою перевагою у застосуванні даного генератора для методу статистичного моделювання Монте-Карло, зокрема для аналого-цифрого перетворення Монте-Карло [3].

Для аналого-цифрового перетворювача (АЦП) Монте-Карло на періоді перетворення (області інтегрування) сформують 2^n значень послідовності псевдовипадкових чисел і відповідно здійснюють 2^n порівнянь, підраховують кількість одиниць результату порівнянь, що є пропорційна інтегралу функції аналогового значення вхідного сигналу перетворення, та здійснюють подальше інтегрування значення вхідного параметру на наступній області інтегрування. Даний тип АЦП відповідає за швидкодією та простотою технічної реалізації розгортаючому АЦП, проте зі значно вищою точністю, яка досягається внаслідок застосування методу Монте-Карло. Одним зі складових елементів АЦП, що визначає точність даного пристрою, є генератор псевдовипадкових чисел. Якщо використання генератора Галуа на основі циклічних зсувів забезпечує простоту технічної реалізації, то постає питання дослідження статистичних характеристик послідовності псевдовипадкових чисел даного методу генерування.

Мета статті – дослідження статистичних характеристик послідовностей псевдовипадкових чисел, що сформовані генератором Галуа на основі циклічних зсувів за допомогою пакету тестів Diehard.

Дослідження послідовностей псевдовипадкових чисел. На сьогоднішній день розроблено безліч методів тестування псевдовипадкових послідовностей. Всі методи тестування генераторів ПВЧ можна розділити на три групи: евристичні, графічні і статистичні. До евристичних тестів належать: перевірка швидкості формування чисел, перевірка періоду, тест на точність визначення деяких констант методом Монте-Карло, перевірка на криптостійкість. Дані тести дають відносну оцінку послідовностям випадкових чисел. Графічні тести (автокореляційна функція, спектральний тест, рівномірність розподілу чисел і ін.) відображають результати у вигляді гістограм і графіків, що характеризують властивості досліджуваної послідовності, але не дають кількісної оцінки (рис. 1). Статистичні ж тести дають можливість виконати чисельну оцінку якості послідовності ПВЧ. Статистичні тести зазвичай об'єднуються в пакети тестування (серед них можна виділити тести DIEHARD, тести NIST та ін.).

На рис. 1 графічно зображено розподіл точок послідовності псевдовипадкових чисел, генерованих методом Галуа на циклічних зсувах на площині (*а*) та в просторі (*б*).

Особливу роль в тестуванні генераторів ПВЧ зіграли роботи Джорджа Марсалі і Дональда Кнута, які запропонували цілий набір тестів. Ще одним стандартним набором тестів послідовностей ПВЧ є стандарт NIST STS 800-22 Національного інституту стандартизації і технологій NIST.

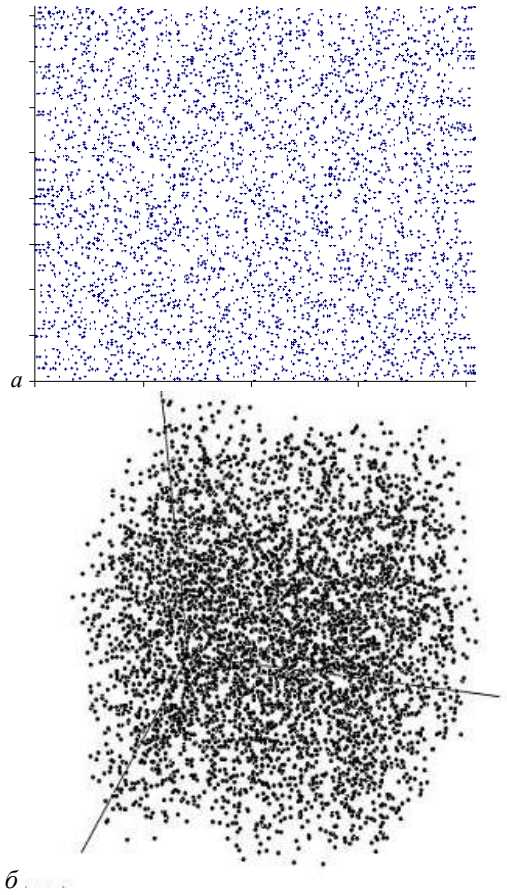

Рис. 1. Розподіл 12-розрядних відліків, генерованих методом Галуа:
а – на площині; *б* – в просторі

Перевагою тестів Д. Кнута є існування швидких алгоритмів виконання; недоліком є невизначеність у трактуванні результатів та відсутня програмна реалізація. Послідовність ПВЧ, що сформовані запропонованим генератором Галуа на основі циклічних зсувів, досліджено тестами Д. Кнута і результати опубліковані в [4, 5]. Результати використання пакету NIST STS, основною перевагою якого є однозначна інтерпретація результатів, подані в роботі [6]. Результати проведених досліджень на визначення типу розподілу послідовності псевдовипадкових чисел генерованих зазначеним методом Галуа показали високу якість рівномірності розподілу.

Одним з статистичних критеріїв є оцінка помилки відтворення закону розподілу дискретної випадкової величини. При тестуванні генераторів ПВЧ необхідно використати якомога більшу кількість відомих статистичних критеріїв, відшуковуючи в послідовності ПВЧ всі можливі закономірності. В даній статті подано результати дослідження

генератора Галуа за допомогою пакету статистичних тестів DIEHARD [7 – 9]. Diehard це набір статистичних тестів для вимірювання якості набору випадкових чисел, який розглядають як один з найбільш строгих існуючих наборів тестів. Слід відзначити і недоліки даного програмного продукту: нема детального опису тестів і методики трактування їх результатів, більшість тестів є евристичними, проходження тесту має тільки два значення "так" або "ні". Тести Diehard формують на виході числа *p-значення*, які рівномірно розподілені в інтервалі [0; 1], якщо вхідний потік чисел дійсно випадковий. Є 13 тестів в пакеті Diehard, деякі з них повторюються з різними параметрами і вони видають 181 *p*-значень в цілому. Оскільки у деяких тестах використовувались декілька наборів параметрів, тому обчислювалось середнє арифметичне для цього тесту усіх поданих *p*-значень. Результати проведеного тестування подано в таблиці.

Таблиця

Результати статистичного дослідження за допомогою пакету Diehard

№	*Назва тесту*	*Усереднені p-значення*	*К-сть отриманих значень*
1	Дні народження (Birthday Spacings)	0,612331	9
2	Перестановки, що перетинаються (Overlapping Permutations)	0,067450	2
3	Ранги матриць (Ranks of matrices)	0,503214	27
4	Потік бітів (The bitstream test)	0,393214	20
5	Мавпячі тести (Monkey Tests)	0,450123	32
6	Підрахунок одиничок (Count the 1’s)	0,382041	27
7	Тест на парковку (Parking Lot Test)	0,630916	10
8	Тест на мінімальну відстань (Minimum Distance Test)	0,563491	20
9	Тест випадкових сфер (Random Spheres Test)	0,110556	20
10	Тест стискання (The Squeeze Test)	0,400146	1
11	Тест сум, що перетинаються (Overlapping Sums Test)	0,856011	10
12	Тест послідовностей (Runs Test)	0,431583	2
13	Тест гри в кості (The Craps Test) (for no. Of wins/ for throws/game)	0,902469	1

Розподіл усіх *p*-значень має бути рівномірним на одиничному інтервалі. Відхилення від рівномірного розподілу показують, що деякі з виявлених Diehard випробувань не цілком задовольняють умову тесту. Після сортування отриманих *p*-значень, побудовано графік, що показує

відхилення від $X = Y$ діагональної лінії отриманих p-значень (рис. 2). За допомогою дисперсії можна обчислити повне відхилення вибірки, але в контексті даної статті дані обчислення не проводились; p-значення поблизу 0 або 1 вказують на відхилення від нормального розподілу. Зокрема слід зауважити, що деякі тести мали досить велику кількість параметрів і їх значення можна вважати вагомішими за інші (а саме тести під номером № 3 – 6, № 7, 8).

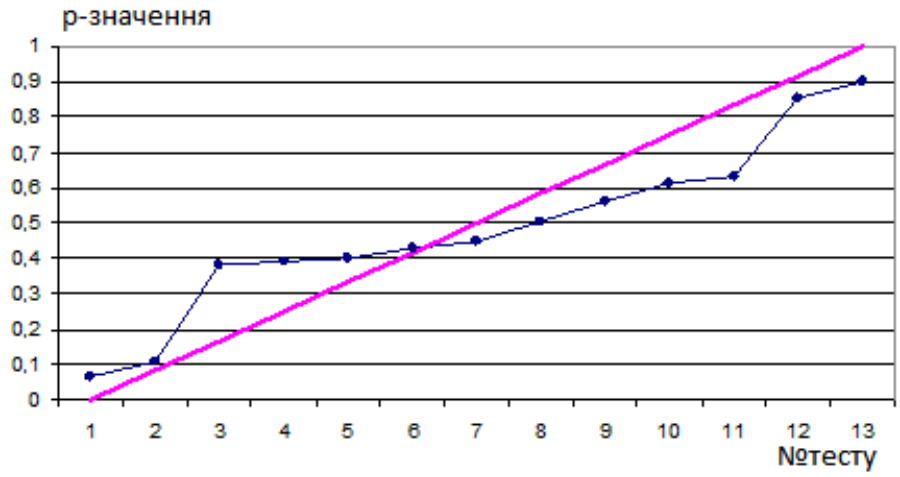

Рис. 2. Відхилення p-значень від лінії $X = Y$

Для того, щоб мати більш чітке уявлення про отримані результати, використано позначення областей на діапазоні [0, 1], де p-значення розподілені. Весь цей діапазон поділено на три області: безпечна зона, сумнівна зона, зона невдачі. Ці ділянки були визначені наступними нерівностями:

$0 < p$-значення ≤ 0.1 або $0.9 \leq p$-значення ≤ 1 – попадання в зону невдачі;

$0{,}1 < p$-значення ≤ 0.25 або $0.75 \leq p$-значення $< 0{,}9$ – попадання в сумнівну зону;

$0{,}25 < p$-значення $< 0{,}75$ – попадання в безпечну зону (рис. 3).

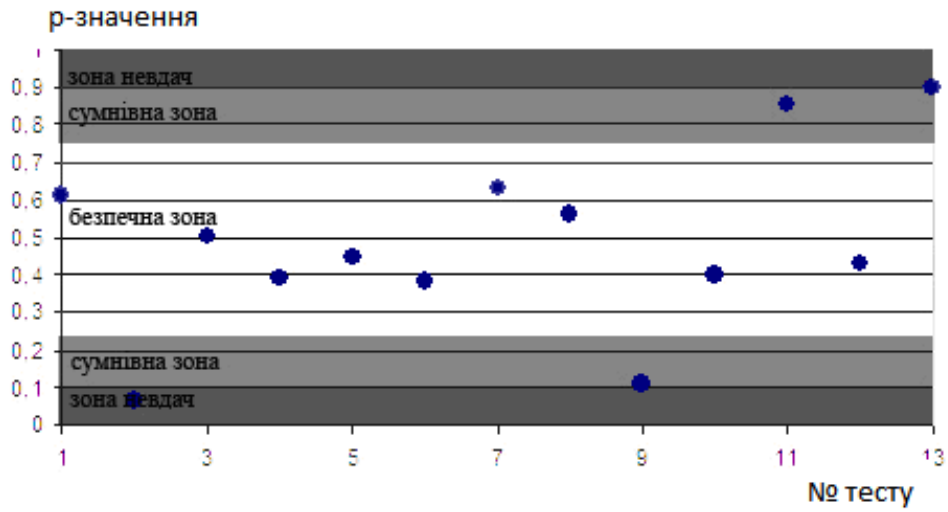

Рис. 3. Області розподілення отриманих *p*-значень

Наявність великої кількості *p*-значення в безпечній зоні вказує на те, що протестований зразок близький до хаотичності; *p*-значення в зоні невдачі є показником відхилення від випадковості, проте їх кількість досить мала для досліджуваного генератора псевдовипадкових чисел.

Висновки. Проведено дослідження статистичних характеристик генерованих послідовностей за допомогою пакету статистичних тестів Diehard. Результати проведених досліджень на визначення типу розподілу послідовності псевдовипадкових чисел, генерованих зазначеним методом, показали високу якість випадковості отриманих чисел. Рівномірність розподілу сформованих послідовностей псевдовипадкових чисел вказує на ефективність використання даного генератора в складі аналого-цифрового перетворювача Монте-Карло. Використання методу генерування псевдовипадкових чисел Ґалуа на основі циклічних зсувів дозволить регуляризувати структуру аналого-цифрового перетворювача Монте-Карло, підвищити швидкодію та технологічність виробництва і зменшити вартість продукту.

Список літератури: 1. *Иванов М.А.* Теория, применение и оценка качества генераторов псевдослучайных последовательностей / *М.А. Иванов, И.В. Чугунков.* – М.: Кудиц – Образ, 2003. – 240 с. **2.** *Donald Knuth* The Art of Computer Programming, Seminumerical Algorithms / *K. Donald.* – Volume 2, 3rd edition, Addison Wesley, Reading, Massachusetts, 1998. – 761 p. **3.** *Петришин Л. Б.* Теоретичні основи перетворення форми та цифрової обробки інформації / *Л. Б. Петришин.* – К.: ІЗіМН МОУ, 1997. – 272 с. **4.** *Лаврів М. В.* Аналіз ефективності застосування методів генерування сигналів з псевдовипадковим розподілом у системах статистичних досліджень / *М.В. Лаврів, Л.Б. Петришин* // Наукові вісті інституту менеджменту та економіки "Галицька академія". – Івано-Франківськ. – 2007. – № 2 (12). – С. 61-66. **5.** *Лаврів М.В.* Генератори рівномірно розподілених псевдовипадкових величин / *М.В. Лаврів, Л.Б. Петришин* // Вісник Прикарпатського національного університету. Фізика. – 2007. – Вип. 3. – С. 112-118.

6. *Лаврів М.В.* Методи і засоби генерування псевдовипадкових сигналів із рівномірним розподілом та аналіз результатів дослідження їх статистичних характеристик / *М.В. Лаврів, Л.Б. Петришин* // Інформаційні технології та комп'ютерна інженерія. – 2009. – № 2 (15). – С. 56-62. **7.** *Mohammed M. Alani* Testing Randomness in Ciphertext of Block-Ciphers Using DieHard Tests / *M. Alani Mohammed* // IJCSNS International Journal of Computer Science and Network Security. – 2010. – Vol. 10. – № 4. – P. 37. **8.** *Dirk Eddelbuettel, Physics, Duke University* RDieHarder: An R interface to the DieHarder suite of Random Number Generator Tests, Initial Version as of May 2007, Rebuilt on February 20, 2014 using RDieHarder 0.1.3. **9.** George Marsaglia, DIEHARD Statistical Tests: http://stat.fsu.edu/~geo/diehard.html.

References:

1. Ivanov, M.A. and Chuhunkov, I.V. (2003), *Theory, Application and evaluation of quality generators pseudorandom sequences*, Kudyts, Moscow, 240 p.
2. Knuth, D. (1998), *The Art of Computer Programming, Seminumerical Algorithms*, Vol. 2, 3rd edition, Addison Wesley, Reading, Massachusetts, 761 p.
3. Petryshyn, L.B. (1997), *Theoretical Foundations of converting forms and digital processing*, IZiMN, Kyiv, 240 p.
4. Lavriv, M.V. and Petryshyn, L.B. (2007), "Analysis of the effectiveness of methods of generating pseudo-random signal distribution systems in statistical studies", *Scientific Institute of Management and Economics "Galician Academy"*, Vol. 2 (12), pp. 61-66.
5. Lavriv, M.V. and Petryshyn, L.B. (2007), "Generators uniformly distributed pseudorandom values", *Bulletin Carpathian National University. Physics.* Vol. 3, pp. 112-118.
6. Lavriv, M.V. and Petryshyn, L.B. (2009), "Methods and means for generating a pseudorandom signal with uniform distribution and analysis of the survey results of the statistical characteristics", *Information technologies and computer engineering*, Vol. 2 (15), pp. 56-62.
7. *Mohammed, M.A.* (2010), "Testing Randomness in Ciphertext of Block-Ciphers Using DieHard Tests", *IJCSNS International Journal of Computer Science and Network Security*, Vol. 10, No. 4.
8. Eddelbuettel, D. (2014), *RDieHarder: An R interface to the DieHarder suite of Random Number Generator Tests*, Initial Version as of May 2007, Rebuilt on February 20, 2014 using RDieHarder 0.1.3.
9. Marsaglia, G. (1999), "DIEHARD Statistical Tests", available at: http://stat.fsu.edu/~geo/diehard.html.

Надійшла (*received*) *31.03.2016*

Статью представил д-р физ.-мат наук, проф. Прикарпатського національного університету ім. Василя Стефаника Пилипів В.М.

Semankiv Maria**,** Cand. Sci. Tech.
Associate Professor at the Department of Computer Science
Vasyl Stefanyk Precarpathian National University
Str. Shevchenko, 57, Ivano-Frankivsk, Ukraine, 76018
Tel.: (095) 469 38 58; e-mail: dlyamarii@gmail.com
ORCID ID: 0000-0002-1314-8923

УДК 519.6

Оцінка статистичних характеристик систем випадкових чисел / Семаньків М. В. // Вісник НТУ "ХПІ". Серія: Інформатика та моделювання. – Харків: НТУ "ХПІ". – 2016. – № 21 (1193). – С. 109 – 117.

Подано результати дослідження статистичних характеристик послідовностей псевдовипадкових чисел, що утворені методом Галуа на основі циклічних зсувів, за допомогою пакету статистичних тестів Diehard. Відзначено ефективність використання даного типу генератора в складі аналого-цифрового перетворювача Монте-Карло. Іл.: 3. Табл.: 1. Бібліогр.: 9 назв.

Ключові слова: псевдовипадкові числа, оцінка статистичних характеристик систем випадкових чисел, пакет статистичних тестів Diehard.

УДК 519.6

Оценка статистических характеристик систем случайных чисел / Семанькив М. В. // Весник НТУ "ХПИ". Серия: Информатика и моделирование. – Харьков: НТУ "ХПИ". – 2016. – № 21 (1193). – С. 109 – 117.

Представлены результаты исследования статистических характеристик последовательностей псевдослучайных чисел, образованных методом Галуа на основе циклических сдвигов, с помощью пакета статистических тестов Diehard. Отмечена эффективность использования данного типа генератора в составе аналого-цифрового преобразователя Монте-Карло. Ил.: 3. Табл.: 1. Библиогр.: 9 назв.

Ключевые слова: псевдослучайные числа, оценка статистических характеристик систем случайных чисел, пакет статистических тестов Diehard.

UDC 519.6

Assessment of statistical properties random numbers / Semankiv M. V. // Herald of the National Technical University "KhPI". Subject issue: Information Science and Modelling. – Kharkov: NTU "KhPI". – 2016. – № 21 (1193). – P. 109 – 117.

Study the statistical characteristics of sequences of pseudorandom numbers is presented. Numbers ahave been formed by Galois through cyclic shifts. Research have beenconducted using statistical tests Diehard package. Efficiency of this type of generator for analog-to-digital converter Monte Carlo have been confirmed. Figs.: 3. Tabl.: 1. Refs.: 9 titles.

Keywords: pseudorandom numbers, assessment of statistical properties random numbers, statistical tests Diehard package.