інфотехнології. Установлені аналітичні залежності між системами функцій дозволили аналітично описати та реалізувати відповідні процедури перетворення форми інформації.

1. Палагин А.В., Николайчук Я.Н. Опыт разработки микропроцессорных распределенных систем реального времени. – К.: Знание, 1988. – 19 с.
2. Романов В.А., Ключан П.С. Преобразователи формы информации для персональных ЭВМ. – К.: Знание, 1988. – 16 с.
3. Вариченко Л.В., Лабунец В.Г., Раков М.А. Абстрактные алгебраические системы и цифровая обработка сигналов. – К.: Наукова думка, 1986. – 248 с.
4. Петришин Л.Б. Теоретико-числові основи кодових систем Галуа / Івано-Франк. держ. техн. ун-т нафти і газу. – Івано-Франківськ, 1995. – 101 с. Моногр. деп. в ДНТБ України 20.12.95 №57 - Ук 96.
5. Залманзон Л.А. Преобразования Фурье, Уолша, Хаара и их применение в управлении, связи и других областях. – М.: Наука, 1989. – 496 с.
6. Орнатский П.П. Теоретические основы информационно-измерительной техники. – К.: Вища школа, 1983. – 455 с.
7. Ефимов А.В. Математический анализ (специальные разделы). – М.: Высшая школа, 1980. – 279 с.
8. Алексич Г. Проблемы сходимости ортогональных рядов. – М.: Инлитиздат, 1963. – 359 с.

From sole the positions of number-theoretic transformations the analysis is carried out and a set of intermediate systems of functions, that form the corresponding codes or code systems, is set. It is built the order and procedures of their creation and mutual transformations, that permitted to classify and in following to estimate efficiency of discrete harmonic analysis in the considered systems of functions.

Key words: *unitary functions, Rademacher functions, discrete harmonic analysis, code systems, analytical relations of system of functions.*

УДК 004.421.5
ББК 32.811.4

М.В. Лаврів, Л.Б. Петришин

ГЕНЕРАТОРИ РІВНОМІРНО РОЗПОДІЛЕНИХ ПСЕВДОВИПАДКОВИХ ВЕЛИЧИН

Запропоновано два нові методи генерування псевдовипадкових чисел; описано процеси генерування випадкових чисел згідно із запропонованими методами; подано порівняльну характеристику ступеня рівномірності даних методів генерування згідно із статистичними методами визначення типу розподілів – χ^2 та Колмогорова – Смірнова.

Ключові слова: *генератори випадкових чисел, метод χ^2, метод Колмогорова – Смірнова.*

Методи та засоби генерування випадкових чисел застосовують при вирішенні прикладних задачах інформатики, зокрема при статистичних дослідженнях Монте-Карло, імовірнісному моделюванні, кодуванні, перетворенні форми та цифровій обробці інформації, тестуванні, чисельному аналізі, системах прийняття рішень, комп'ютерному програмуванні, у криптографії та системах захисту. Як на недоліки методів генерування випадкових чисел слід указати на складність їх технічної реалізації, обмеження швидкодії формування відліків, неможливість відтворення отриманих характеристик розподілів, передбачення генерованих послідовностей через їх випадковий характер, що стали причиною використання на практиці математичних методів синтезу псевдовипадкових послідовностей, які реалізуються здебільшого алгоритмічно за допомогою рекурентних залежностей. При цьому кожне наступне число утворюється з визначеної кількості попередніх шляхом обчислення за деякою заданою функцією. Серед методів генерування псевдовипадкових розподілів широке застосування отримали методи з рівномірним розподілом, для яких кожен із відліків характеризується однаковою ймовірністю появи в процесі генерування.

Лінійний конгруентний метод характеризується простотою алгоритму генерування та задовільними ймовірнісними характеристиками розподілу, що зумовило його широке практичне застосування [1, 2]. Такий метод визначається вихідними параметрами: m – модуль ($m > 0$), a – множник ($0 \le a < m$), b – приріст ($0 \le b < m$), x_0 – початкове значення ($0 \le x_0 < m$). Процедура генерування здійснюється згідно із залежністю $x_{n+1} \equiv (ax_n + b) \bmod m$. Період

генерованого псевдовипадкового розподілу визначається вибором значень модуля, множника та приросту. Даний метод генерування визначено як рівномірний [2]. Є декілька способів модифікації конгруентного методу, наприклад метод Фібоначчі, що є модифікованим методом класу конгруентних, для якого генерування здійснюється згідно із залежністю $x_{n+1} = (x_n + x_{n-1}) \bmod m$, де n – порядковий номер числа, m – модуль).

У генераторах даного класу необхідно реалізувати операції додавання, множення елементів, знаходження остачі від ділення, а для методу Фібоначчі потрібні ще додаткові запам'ятовуючі пристрої (операції виконуються не тільки над попереднім числом), що ускладнює реалізацію даних генераторів.

На основі аналізу складності технічної реалізації методів псевдовипадкового генерування одним з ефективних запропоновано метод на базі використання незвідних поліномів над полем Галуа $GF(2)$ [3]. Формування n-розрядних псевдовипадкових чисел (c_1, c_2, ..., c_n) у двійковій системі числення здійснюється на основі циклічного зсуву 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:

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

Усі n-розрядні числа псевдовипадкової послідовності трансформують у відліки десяткової системи числення. Даний метод визначено *методом рекурсивного генерування в кодах Галуа*, який технічно реалізується на регістрах зсуву. Згідно з даним методом при генеруванні послідовностей із періодом N отримують $2^n - 1$ різних n-розрядних чисел ($N = 2^n - 1$). На рис.1 графічно зображено розподіл точок (i, j) на площині, де i – порядковий номер генерованого числа (що вказує порядок відліку в часі), j – число, генероване 12-розрядним генератором Галуа на періоді $[1, 2^{12} - 1]$.

Згідно з другим запропонованим способом генерування псевдовипадкових чисел кожен із їх відліків як n-розрядний двійковий код утворюється в результаті рандомізації ваг у дзеркально відображеному порядку розрядів двійкового коду поточного значення числа лінійно зростаючої двійкової послідовності чисел: $c_1 = b_n$, $c_2 = b_{n-1}$, ..., $c_n = b_1$. На рис.2 зображено псевдовипадковий розподіл відліків 12-розрядних чисел, генерованих методом рандомізації двійкових розрядів. Після перетворення всі числа інтервалу $[0, 2^n - 1]$ відображаються в числа інтервалу $[0, 2^n - 1]$ за умови повної взаємно однозначної відповідності.

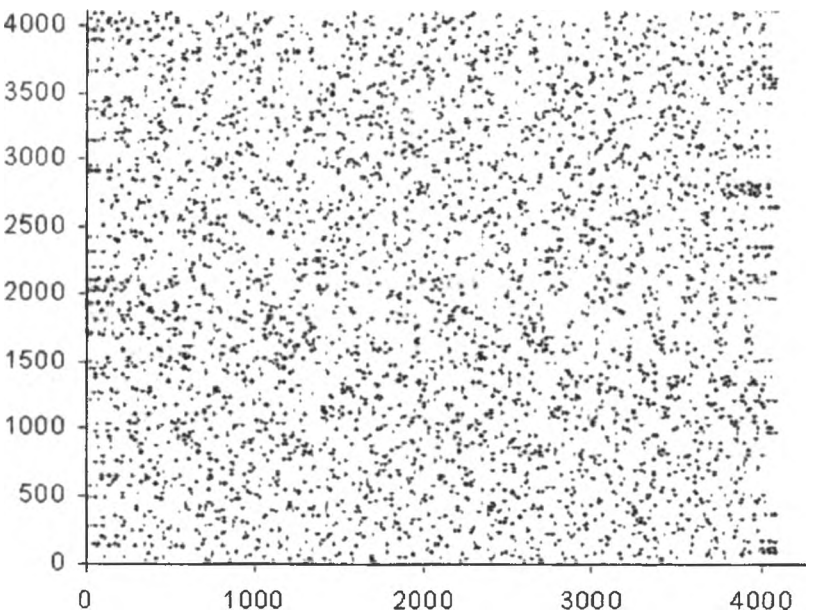

Рис.1. Розподіл на площині 12-розрядних відліків, генерованих методом Галуа Перевагою даного методу є простота технічної реалізації даного генератора за допомогою регістрів зсуву

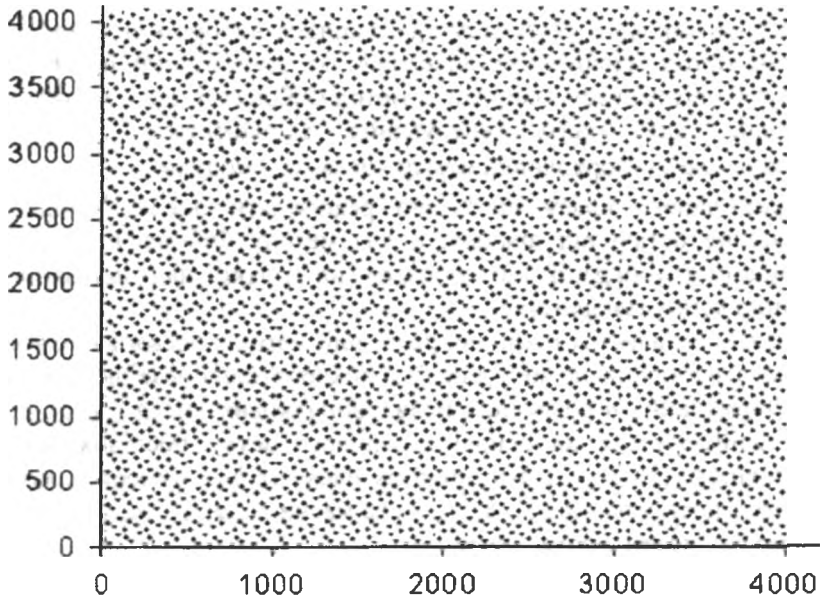

Рис.2. Розподіл на площині відліків 12-розрядних чисел, генерованих методом рандомізації двійкових розрядів

З метою визначення та порівняння характеристик рівномірності розподілу запропонованих методів, крім наведених, були також досліджені конгруентний метод і метод Фібоначчі.

При технічній реалізації методу Галуа на регістрах зсуву множина цілих додатних чисел розбивається на підмножини чисел $[0, 2^n - 1]$, де $n = 1, 2, ...$, на яких було здійснено генерування чисел, що, у свою чергу, і визначало період даних генераторів. Дані розбиття визначають розряди генераторів Галуа на регістрах зсуву. Згідно з цим результати дослідження наводяться для розрядів $n = 8, ..., 20$. Це, у свою чергу, вплинуло на вибір значення модуля при використанні конгруентного методу та адитивного генератора Фібоначчі.

Було здійснено дослідження генерованих чисел даними методами для визначення типу розподілу даних псевдовипадкових чисел. Для цього було використано статистичні методи знаходження закону розподілу випадкових чисел – метод χ^2 і метод Колмогорова – Смірнова [2, 4]. Згідно з даними методами на основі вибірки отриманих значень визначено ступінь наближення розподілів даних методів до рівномірного. При використанні методу χ^2 діапазон генерування розбивається на підмножини-категорії й обчислюються статистики V:

$$V = \sum_{1 \le s \le k} \frac{(Y_s - np_s)^2}{np_s},$$

де n – кількість генерованих чисел, k – кількість категорій, p_s – імовірність того, що результат генерування потрапляє в категорію s, і Y_s – кількість випробувань, які дійсно потрапили в категорію s.

При порівнянні отриманих значень найбільшими відхиленнями від рівномірного розподілу (великі значення обчислених статистик) володіє метод Фібоначчі, за ним ідуть конгруентний метод та метод Галуа. Найкращі показники отримано для методу рандомізації двійкових розрядів, причому при збільшенні розрядності (у свою чергу, і проміжку генерування та кількості елементів) величина відхилення зростає лінійно, на відміну від результатів застосування інших методів, що подані в таблиці 1.

Таблиця 1

Метод χ^2

Розрядність	Конгруентний метод	Метод Фібоначчі	Метод Галуа на регістрах зсуву	Метод рандомізації двійкових розрядів
8	8,52	34,39	5,14	0,33
10	4,546667	14,15333	6,64	0,246667
12	27,64333	50,67133	28,92267	1,787333
14	63,56	787	559,6	26,77875
16	673,8	1062,883	740,728	33,18783
18	902,5106	1133,867	905,0131	28,63763
20	939,02	1068,147	895,07	44,004

Відповідно до кількості генерованих чисел за таблицею χ^2-розподілу було зіставлено критичні значення розподілу з обчисленими статистиками. Обчислені значення не перевищують критичних точок, що відповідають відхиленню 1–5% (відсоткові точки методу χ^2), що дало змогу підсумувати рівномірний характер досліджуваних розподілів на інтервалах $[0, 2^n - 1]$, де $n = 8, 10, ..., 20$.

На рис.3 подано графічну залежність характеристик розподілів за розрядами.

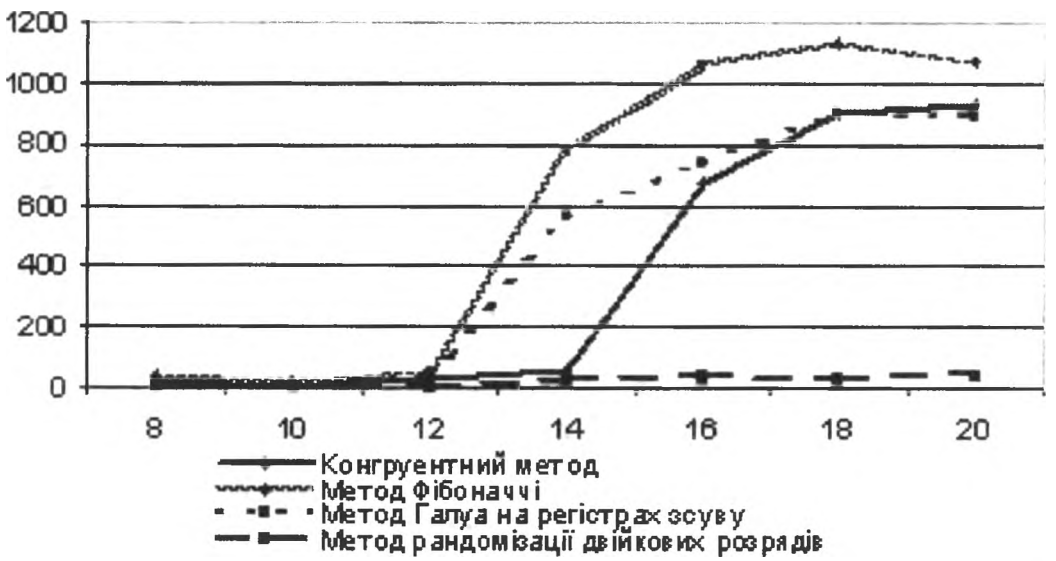

Рис.3. Діаграма характеристик розподілів різної розрядності, досліджених методом χ^2

Дані методи генерування псевдовипадкових чисел було досліджено на рівномірність розподілу на площині, для чого модифіковано метод χ^2: площину генерованих чисел $[0, 2^n - 1] \times [0, 2^n - 1]$ розбито на однакові квадрати заданої площі, та підраховано кількість чисел, що попадають у відповідні квадрати й застосовано метод χ^2 до новоутвореної послідовності, результати чого подані в таблиці 2, де за вибраною розрядністю можна простежити величину відхилень для даних методів.

Таблиця 2

Метод χ^2 на площині

Розрядність	**Конгруентний метод**	**Метод Фібоначчі**	*Метод Галуа на регістрах зсуву*	**Метод рандомізації двійкових розрядів**
8	45,98	28,92	46,97	1,968842
10	99,19111	120,1644	66,92444	8,844444
12	1191,249	1218,223	571,6547	15,403
14	1687,183	1661,968	1699,79	159,574
16	2578,172	2592,477	2421,245	269,3505
18	2467,75	2612,756	2697,289	282,437
20	2438,827	2530,642	2637,283	337,5114

Згідно з отриманими результатами побудовано діаграму характеристик розподілів різної розрядності (рис.4).

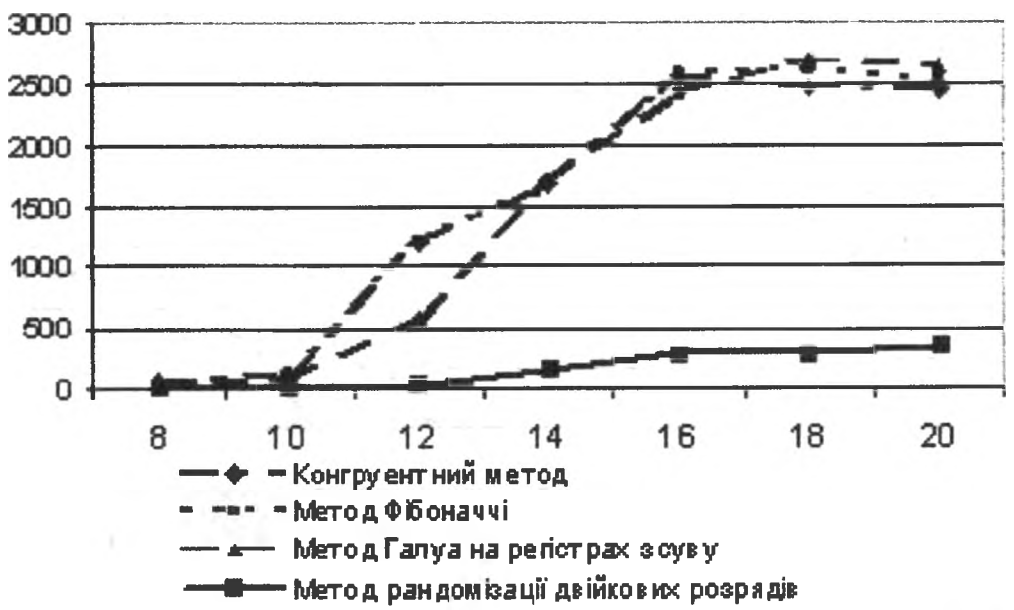

Рис.4. Діаграма характеристик розподілів різної розрядності, досліджених методом χ^2 на площині

Дані результати дозволяють ствердити рівномірний характер розподілу, отриманого за допомогою методу Галуа на регістрах зсуву. Крім того, метод рандомізації двійкових розрядів відзначився мінімальним значенням відхилення від рівномірного розподілу.

Для визначення характеристик рівномірних розподілів генерованих чисел також було використано метод Колмогорова – Смірнова, який дозволив визначити статистики відхилень і встановити величину відхилень побудованих емпіричних функцій та рівномірного розподілу. При використанні методу Колмогорова – Смірнова для розглянутих методів були побудовані: функція розподілу рівномірно розподілених величин на інтервалах $[0, 2^n - 1]$, де $n = 8, 10, ..., 20$, та функції розподілів кожного методу згідно з формулою:

$$F_n(x) = \frac{\textit{кількість таких } X_1, X_2, ..., X_n, \textit{які} \le x}{n},$$

де n – кількість елементів, X_i – генеровані числа ($i = 1, 2, ..., n$). Також визначено максимальні відхилення значень отриманих функцій розподілів від значень функції рівномірно розподілених псевдовипадкових величин.

У таблиці 3 подано отримані результати для методу Колмогорова – Смірнова.

Таблиця 3

Метод Колмогорова – Смірнова

Розрядність	Конгруентний метод	Метод Фібоначчі	Метод Галуа на регістрах зсуву	Метод рандомізації двійкових розрядів
8	0,84024	0,745562	0,6272	0,130178
10	0,47619	1,183673	0,86395	0,108844
12	1,433286	1,60396	1,062235	0,141914
14	0,015962	0,078993	0,109686	0,00244
16	0,008016	0,014997	0,01401	0,001023
18	0,05538	0,09177	0,10223	0,002433
20	0,088	0,083831	0,0986	0,003107

Аналогічно для модифікованого методу Колмогорова – Смірнова та обчислень для площини (таблиця 4).

Таблиця 4

Метод Колмогорова – Смірнова на площині

Розрядність	Конгруентний метод	Метод Фібоначчі	Метод Галуа на регістрах зсуву	Метод рандомізації двійкових розрядів
8	0,055	0,093	0,081	0,02332
10	0,0383	0,02601	0,032	0,00533
12	0,0602	0,05868	0,09478	0,00727
14	0,01176	0,01235	0,01816	0,001167
16	0,00901	0,00953	0,00869	0,000712
18	0,00969	0,00964	0,011705	0,00105
20	0,0099	0,009895	0,007159	0,0099

Відхилення утворених розподілів від рівномірного для досліджених методів згідно з методом Колмогорова – Смірнова не перевищує 5%. На рис.5 зображені графіки рівномірного та отриманого 10-розрядним генератором Галуа розподілів.

Отримані результати вказують на рівномірний характер розподілів генерованих чисел методом Галуа та методом рандомізації двійкових розрядів. Причому для послідовності, отриманої методом рандомізації, характерні мінімальні значення відхилення від "ідеальної" рівномірно розподіленої послідовності чисел. Технічна реалізація вказаних методів є достатньо простою й дешевою, реалізується на одному кристалі інтегральної мікросхеми.

Тому можна підсумувати доцільність застосування запропонованих методів генерування Галуа, а особливо із рандомізацією розрядів, для отримання послідовностей рівномірно розподілених псевдовипадкових чисел, для вирішення прикладних задач статистичних досліджень Монте-Карло.

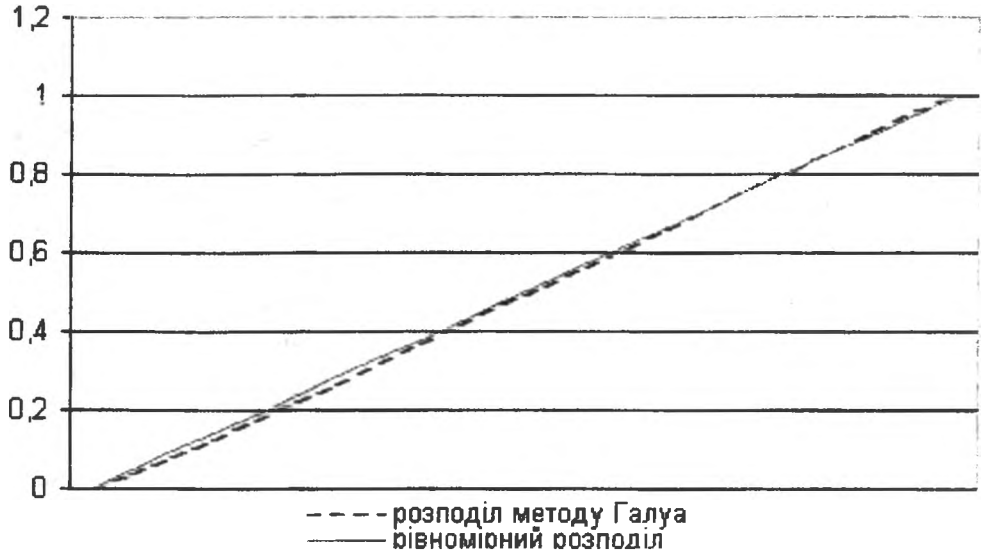

Рис.5. Графіки рівномірного та утвореного 10-розрядним генератором Галуа розподілів

1. Иванов М.А., Чугунков И.В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. – М.: КУДИЦ-ОБРАЗ, 2003. – 240 с.
2. Кнут Д. Искусство программирования для ЭВМ: Пер. с англ. – М.: Мир, 1977. – 830 с.
3. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. – М.: Мир, 1976. – 754 с.
4. Ермаков С.М., Михалков Г.А. Курс статистического моделирования. – М.: Наука, 1976.

In the article two new methods generation of pseudorandom numbers are offered; the processes generation random numbers of the accordant offered methods are described; comparative degrees description of evenness the given methods generation is resulted in obedience to the statistical methods of determination type distributing – χ^2 and Colmogorov–Smirnov methods.

Key words: *random numbers generators, χ^2 method, Colmogorov–Smirnov method.*