УДК 681.3
© Ю. Костів[1], В. Максимович[1], О. Гарасимчук[1], М. Мандрона[1], 2013

АПАРАТНА РЕАЛІЗАЦІЯ І ДОСЛІДЖЕННЯ МОДИФІКОВАНИХ ГЕНЕРАТОРІВ ФІБОНАЧЧІ

В роботі запропоновані структурні схеми модифікованих генераторів Фібоначчі, що можуть використовуватись для формування псевдовипадкової бітової послідовності і керованою по частоті пуасанівської імпульсної послідовності. Досліджені їхні статистичні характеристики.

The structural schemes of modified Fibonacci generators that can used for formation of pseudorandom bit sequence and Poisson pulse sequence, which frequency can changed, are representing in the work. Their statistic characteristics are investigated.

1. ВСТУП

Генератори Фібоначчі, відомі як пристрої для формування псевдовипадкових чисел і бітових послідовностей, в основному призначені для програмної реалізації [1]. Це пояснюється складністю апаратної реалізації алгоритму

$$x_{j+1} = (x_j + x_{j-1}) \bmod m \qquad (1)$$

при умові, що m – просте або будь-яке число, що не дорівнює степені двійки. Якщо ж $m = 2^s$ (s – ціле додатне число) статистичні характеристики генератора є незадовільними. Отже, існує необхідність удосконалення структури і алгоритму роботи генератора Фібоначчі з метою забезпечення необхідних характеристик його вихідних сигналів.

Метою роботи є розробка модифікованих схем і алгоритму генераторів Фібоначчі, які можуть використовуватись для формування керованого по частоті пуассонівського імпульсного потоку і бітової псевдовипадкової імпульсної послідовності. Таким чином, генератори можуть використовуватись як в вимірювальній техніці для імітації випадкових сигналів, так і для криптографічних перетворень.

2. СТРУКТУРНІ СХЕМИ ГЕНЕРАТОРІВ

В результаті проведених досліджень авторами запропоновані схеми генераторів зображені на рис. 1–2. Власне модифіковані генератори Фібоначчі (МГФ) складаються з регістрів (Рг), Рг1 – Рг5, комбінаційних суматорів (КС), КС1 – КС3 і логічної схеми (ЛС). Схема порівняння (СП) і логічний елемент (І) забезпечують формування імпульсного потоку з пуассонівським законом розподілу.

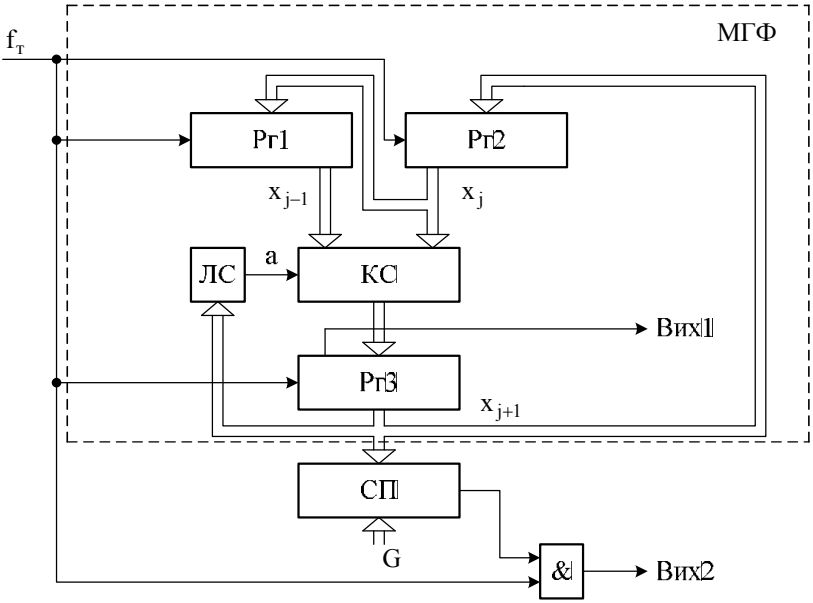

Рис. 1. Модифікований генератор Фібоначчі (варіант А)

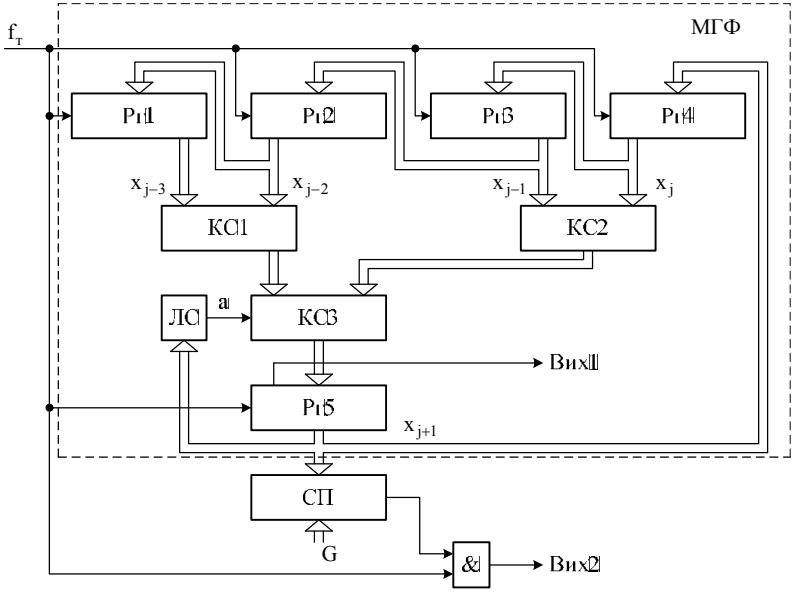

Рис. 2. Модифікований генератор Фібоначчі (варіант Б)

На виходах генераторів формуються послідовності псевдовипадкових чисел у відповідності до виразів:

$$x_{j+1} = (x_j + x_{j-1} + a) \bmod m \text{ (для варіанту А)}, \quad (2)$$

$$x_{j+1} = (x_j + x_{j-1} + x_{j-2} + x_{j-3} + a) \bmod m \text{ (для варіанту Б)}, \quad (3)$$

де $m = 2^s$, s – кількість двійкових розрядів структурних елементів. Значення змінної a визначається логічним рівнянням

$$a = a_0 \ xor \ a_1 \ xor \ a_2 \ xor \ \cdots \ xor \ a_z, \quad (4)$$

де a_i (i=0,1,…,z) – значення двійкових розрядів числа в Рг3 (варіант А) чи Рг5 (варіант Б). Кількість членів рівняння (4) може вибиратись з діапазону 0 … m-1.

Бітова псевдовипадкова імпульсна послідовність формується на виході молодшого розряду регістрів Рг3 (варіант А) чи Рг5 (варіант Б) – Вихід 1.

Генератор пуассонівської імпульсної послідовності (ГПІП) складається з генератора псевдовипадкових чисел (ГПЧ), побудованого на основі МГФ, схеми порівняння і логічного елемента, середня частота імпульсів на виході якого (Вихід 2) визначається рівнянням [1, 2]

$$f_{âèõ} = \frac{G}{x_{max}} f_{ò}, \quad (5)$$

де G – керуючий код, $x_{max} = 2^m$ – максимальне значення числа на виході ГПЧ, $f_{ò}$ – вхідна (тактова) частота.

3. ДОСЛІДЖЕННЯ СТАТИСТИЧНИХ ХАРАКТЕРИСТИК БІТОВОЇ ІМПУЛЬСНОЇ ПОСЛІДОВНОСТІ (ВИХІД 1)

За допомогою імітаційної моделі були досліджені періоди повторення МГФ (табл. 1).

Таблиця 1

Періоди повторення МГФ

Структурна схема МГФ	m	Кількість членів рівняння (4)			
		0	4	8	16 (10 для $m = 2^{10}$)
Рис. 1	2^{10}	3584	53536	8206435	727654100
	2^{20}	3670016	86933504	$>10^9$	$>10^9$
	2^{30}	$>10^9$	$>10^9$	$>10^9$	$>10^9$
Рис. 2	2^{10}	15872	758763936	$>10^9$	$>10^9$
	2^{20}	16252928	$>10^9$	$>10^9$	$>10^9$
	2^{30}	$>10^9$	$>10^9$	$>10^9$	$>10^9$

Таким чином, збільшення періоду повторення МГФ досягається при:

– збільшенні кількості регістрів, що запам'ятовують попередні значення псевдовипадкових чисел;

– збільшенні кількості розрядів структурних елементів;

– збільшенні кількості членів рівняння (4), що реалізується логічною схемою ЛС.

Усі ці фактори також істотно впливають на статистичні характеристики бітової послідовності (Вихід 1), що було досліджено з допомогою статистичних тестів NIST. Відповідні статистичні портрети наведені на рис. 3.

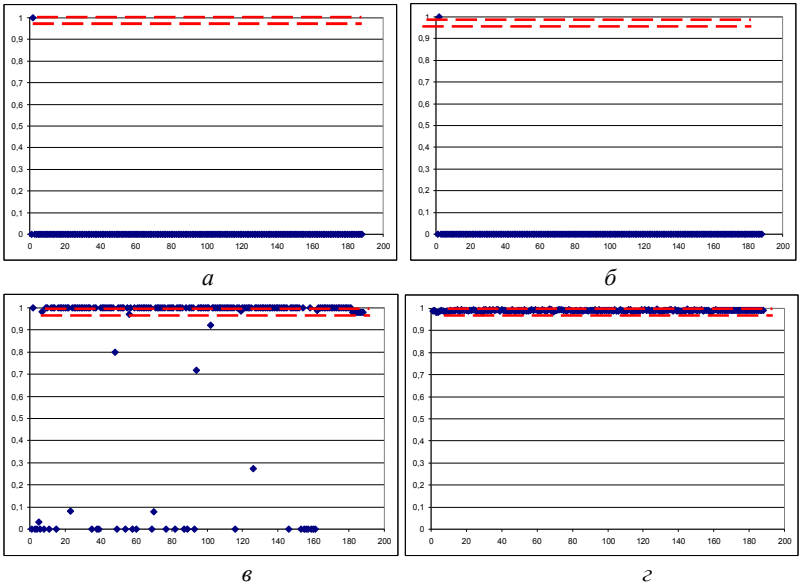

Рис. 3. Статистичні портрети бітової послідовності (Вихід 1) для структурної схеми МГФ варіанту Б (рис. 2) при $m = 2^{30}$ *і різній кількості членів рівняння (4): а – 0, б – 4, в – 8, г –16.*

По вісі абсцис відкладено номер тесту NIST, по вісі ординат – імовірність проходження тесту. Тест вважається пройденим, у тому випадку, коли імовірність проходження тесту потрапить у межі від 0,98 до 1,00, в іншому випадку – тест не пройдено [3, 4]. Для наочності межі довірчого інтервалу позначені червоними пунктирними лініями.

4. ДОСЛІДЖЕННЯ СТАТИСТИЧНИХ ХАРАКТЕРИСТИК КЕРОВАНОЇ ПУАССОНІВСЬКОЇ ІМПУЛЬСНОЇ ПОСЛІДОВНОСТІ (ВИХІД 2)

Для дослідження статистичних характеристик була запропонована наступна методика.

Потік вхідних імпульсів ГПІП розділяється на n однакових груп, кожна з яких складається з $i_{\max}$ імпульсів (рис. 4). Максимальна кількість груп – $n_{\max}$. Групам вхідних імпульсів відповідають групи вихідних імпульсів з числом імпульсів k_1, k_2, …, $k_{n_{\max}}$.

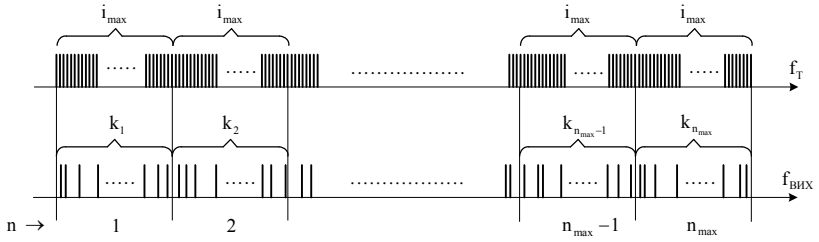

Рис. 4. Розбиття вхідних і вихідних імпульсних потоків на групи

Запропонована методика ґрунтується на класичній методиці перевірки гіпотези про розподіл генеральної сукупності за законом Пуассона з використанням критерію Пірсона (критерію χ^2) [5]. При цьому, враховуючи специфіку побудови ГПІП, були запропоновані наступні доповнення:

– фіксується номінальне (теоретичне) середнє значення чисел k_1, k_2 … $k_{n_{\max}}$ – $k_{\tilde{n}}$, незалежно від значення керуючого коду G.

– значення $i_{\max}$ є змінним, залежить від значення G і визначається рівнянням

$$i_{\max} = \frac{x_{\max}}{G} k_{\tilde{n}}. \qquad (6)$$

Подальша перевірка гіпотези відбувається таким чином.

1. За емпіричним розподілом, отриманим в результаті моделювання роботи ГПІП, знаходять вибіркову середню величину значень k_1, k_2 … $k_{n_{\max}}$ – $k_{\hat{a}}$.

2. Приймають в якості параметра λ розподілу Пуассона вибіркову середню – $\lambda = k_{â}$.

3. Знаходять, за формулою Пуассона

$$P_j = \lambda^j \frac{e^{-\lambda}}{j!} = k_{â}{}^j \frac{e^{-k_{â}}}{\text{j!}} \tag{7}$$

імовірності появи рівно j імпульсів (на інтервалі $i_{\max}$) в $n_{\max}$ випробуваннях (j = 0, 1, 2, …).

4. Знаходять теоретичні частоти

$$Q_j = P_j \cdot n_{\max}. \tag{8}$$

5. В процесі моделювання знаходять емпіричні частоти – N_j.

6. Для кожного значення j з допомогою критерію Пірсона визначають

$$S_j = \frac{(N_j - Q_j)^2}{Q_j}, \tag{9}$$

$$\chi_c^2 = \sum_{j=0}^{j_{\max}} S_j. \tag{10}$$

7. При необхідності значення N_j, P_j і Q_j, що відповідають малим імовірностям P_j об'єднуються в одну чи дві групи, і обчислення (9), (10) виконуються з урахуванням цього факту.

8. Визначається число степенів свободи

$$r = d - 2, \tag{11}$$

де d – кількість груп, що залишились після можливого об'єднання.

9. За таблицями критичних точок розподілу χ^2 [5], за вибраними рівнем значимості α (звичайно α надають одне з трьох значень – 0,1; 0,05; 0,01) і числом степенів свободи r знаходять критичне значення $\chi^2_{êð}$. Якщо $\chi^2_{ñ} < \chi^2_{êð}$ – немає підстав не приймати гіпотезу про відповідність імпульсного потоку пуассонівському закону розподілу.

Результати використання запропонованої методики дослідження статистичних характеристик вихідних сигналів ГПІП, для деяких варіантів побудови МГФ, наведено на рис. 5. Тут позначення XOR=0, XOR=4 вказують на відповідну кількість членів рівняння (4).

Для усіх варіантів побудови МГФ були зафіксовані значення: $n_{\max} = 1000$, $k_{ñ} = 10$. Початкові стани регістрів були вибрані випадковим чином.

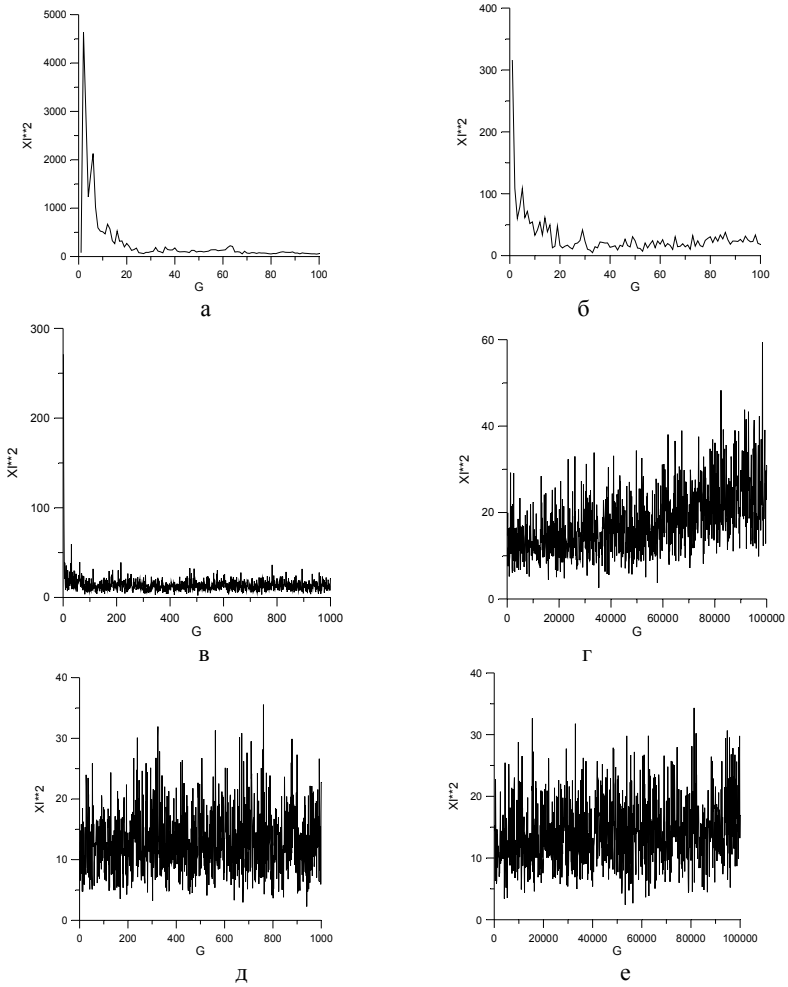

Рис. 5. Залежності $\chi^2_{\tilde{n}}$ від керуючого коду G при:
а – МГФ-варіант А, m=2^{10}, XOR=0, G=1…100;
б – МГФ-варіант А, m=2^{10}, XOR=4, G=1…100;
в – МГФ-варіант А, m=2^{20}, XOR=4, G=1…1000;
г – МГФ-варіант А, m=2^{20}, XOR=4, G=100…100000;
д – МГФ-варіант Б, m=2^{20}, XOR=4, G=1…1000;
е – МГФ-варіант Б, m=2^{20}, XOR=4, G=100…100000.

5. ВИСНОВКИ

За результатами проведених досліджень можна зробити висновок, що основним фактором, який дозволив істотно покращити статистичні характеристики вихідних сигналів модифікованих генераторів Фібоначі, є введення до їх структури логічної схеми ЛС. Це пояснюється тим, що завдяки додаванню до молодшого розряду вихідного комбінаційного суматора (КС для варіанту А чи КС3 для варіанту Б) МГФ біту, значення якого залежить від певної кількості розрядів вихідного регістру (Рг3 для варіанту А чи Рг5 для варіанту Б), формування усіх його розрядів наближається до випадкового процесу. Подальше удосконалення наведених пристроїв може бути пов'язане з оптимізацією вибору кількості запам'ятовуючих регістрів, кількості їх розрядів, логічної функції ЛС і пошуком принципових схем, що забезпечують максимальну швидкодію.

1. Иванов М.А. Теория, применение и оценка качества генераторов псевдослучайных последовательностей / Иванов М.А., Чугунков И.В. – М.: КУДИЦ – ОБРАЗ, 2003. – 240 с. 2. Гарасимчук О. І. Генератори пуассонівського імпульсного потоку на основі генераторів М-послідовностей / О.І. Гарасимчук, В.М. Максимович // Вісник НУ "Львівська політехніка". "Комп'ютерні науки та інформаційні технології", – 2004. – №521 – С. 17-23. 3. NIST SP 800-22. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications [Електронний ресурс]. Режим доступу: http://csrc.nist.gov/publications/nistpubs//SP800-22rev1a.pdf. 4. Горбенко І.Д. Прикладна криптологія: Теорія. Практика. Застосування: монографія / І.Д. Горбенко, Ю.І. Горбенко. – Харків: Вид-во «Форт», 2012. – 880 с. 5. Критерій узгодженості Персона [Електронний ресурс]. Доступний з: http://uk.wikipedia.org/wiki/Критерій_узгодженості_Пірсона.