УДК 004.421.5+681.5.032

М.М. Мандрона, В.М. Максимович,
Ю.М. Костів, О.І. Гарасимчук

МОДИФІКАЦІЯ АДИТИВНОГО ГЕНЕРАТОРА ФІБОНАЧЧІ З ЗАПІЗНЕННЯМ

Запропоновано спосіб модифікації адитивного генератора Фібоначчі з запізненням, що може використовуватись для формування псевдовипадкової бітової послідовності. Розроблено узагальнену структурну схему модифікованого генератора. Досліджено статистичні характеристики і періоди повторення класичного і модифікованого генераторів Фібоначчі з запізненням. Виявлено покращення статистичних характеристик послідовностей сформованих модифікованим генератором. Дослідження здійснювалось з допомогою набору тестів NIST.

Ключові слова: псевдовипадкова бітова послідовність, адитивний генератор Фібоначчі з запізненням, період повторення, статистичні характеристики.

Постановка проблеми в загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями.

Сучасна наука широко використовує псевдовипадкові бітові послідовності в різних додатках. При цьому від якості використовуваних генераторів псевдовипадкових послідовностей залежить якість отриманих результатів.

Попит на генератори псевдовипадкових бітових послідовностей (ГПВБП) із заданим ймовірнісним розподілом, а також на самі випадкові послідовності настільки зріс, що з'явились науково-виробничі фірми, що займаються їх виробництвом.

Можливі сфери застосування псевдовипадкових чисел:

- моделювання;
- числовий аналіз;
- програмування;
- криптографія;
- апаратні пристрої для захисту інформації;
- розваги.

Актуальним є питання про визначення якості ГПВБП – міри його відповідності до ідеалу. Впевненість у генераторі ґрунтується на одному з важливих елементів – статистичних характеристиках.

У багатьох працях проводилось дослідження роботи і статистичних характеристик адитивних генераторів Фібоначчі з запізненням [1-6]. При цьому були виявленні варіанти їх побудови, що забезпечують високу якість, однак більшість з них орієнтовані на програмну реалізацію. В цій роботі акцентується увага на знаходженні нових алгоритмів роботи генераторів Фібоначчі із забезпеченням задовільних статистичних характеристик з можливістю апаратної реалізації, яка б забезпечувала високу швидкодію роботи.

Метою статті є модифікація адитивного генератора Фібоначчі із запізнення, розробка його узагальненої схеми і знаходження нових алгоритмів роботи адитивних генераторів Фібоначчі із забезпеченням задовільних статистичних характеристик з можливістю подальшої апаратної реалізації.

Виклад основного дослідження

Адитивні генератори Фібоначчі з запізненням (АГФЗ), відомі як пристрої для формування псевдовипадкових чисел і бітових послідовностей. Узагальнена формула роботи такого генератора [1, 2]

$$x_n = (x_{n-l} + x_{n-k}) \bmod m, \quad l > k > 0 \qquad (1)$$

де l і k – коротке і довге запізнення, відповідно (k > p), m визначає максимальний період генератора.

За допомогою імітаційної моделі авторами було досліджено статистичні характеристики та період повторення АГФЗ з такими параметрами: кількість регістрів – 8, алгоритм роботи $x_n = (x_6+x_1) \bmod m$. На рис. 1 наведено його статистичний портрет.

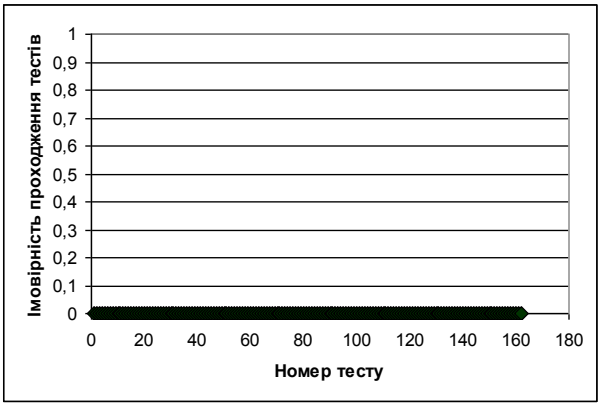


Рис. 1. Статистичний портрет АГФЗ

Із рис 1. видно, що АГФЗ не прошов жодного тесту із 15 тестів набору NIST. Дослідження показали, що збільшення кількості регістрів (табл. 1) не покращує якості вихідної послідовності, а отже, послідовності, які формуються таким генератором є невипадковими.

Таблиця 1

Результати дослідження класичного генератора Фібоначчі з запізненням

Алгоритм роботи	**Кількість регістрів**	**Кількість не пройдених тестів NIST з 162**	**Період повторення**
$\mathbf{x_n=(x_6+x_1+a)}$	7	(-162)	111104
	8	(-162)	261632
	9	(-162)	7680
	10	(-162)	304640
	11	(-162)	419328

Результати дослідження показали, що існує необхідність удосконалення структури і алгоритму роботи АГФЗ з метою забезпечення необхідних характеристик його вихідних сигналів.

Для вирішення цієї проблеми, авторами було запропоновано спосіб модифікації схеми генератора. Модифікація АГФЗ полягає у доповненні класичного варіанту логічною схемою (ЛС), на виході якої формується двійковий сигнал, що надходить на вхід переносу комбінаційного суматора (КС). Це дозволяє формувати псевдовипадкові числа у відповідності до рівняння (2) із забезпеченням задовільних статистичних характеристик

$$x_n = (x_{n-l} + x_{n-k} + a) \bmod m \ , \qquad (2)$$

при умові, що $m = 2^S$, де s – кількість двійкових розрядів структурних елементів схеми – регістрів і комбінаційного суматора. На рис. 2 наведено узагальнену схему модифікованого адитивного генератора Фібоначчі з запізненням (МАГФЗ).

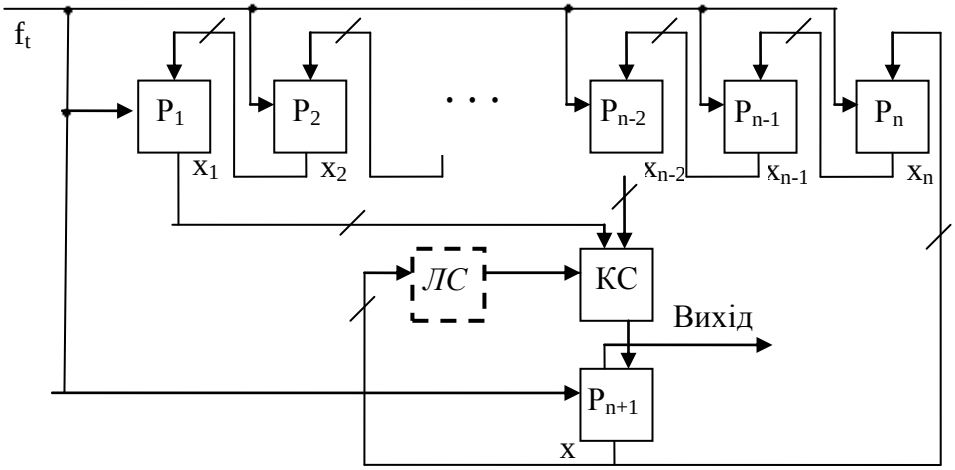


Рис. 2. Узагальнена схема модифікованого адитивного генератора Фібоначчі з запізненням

Для дослідження ефективності запропонованого генератора, у роботі за допомогою імітаційної моделі, досліджується МАГФЗ (рис. 2), який складається з різної кількості регістрів Р1 - Рn, комбінаційного суматора (КС) і логічної схеми (ЛС). Під час імітаційного моделювання в модифікованому генераторі змінювалась кількість структурних елементів і кількість розрядів, які подаються на ЛС з регістра P_{n+1}.

На виході генератора формується послідовність псевдовипадкових чисел у відповідності до виразу (2).

Значення змінної *a* визначається логічним рівнянням:

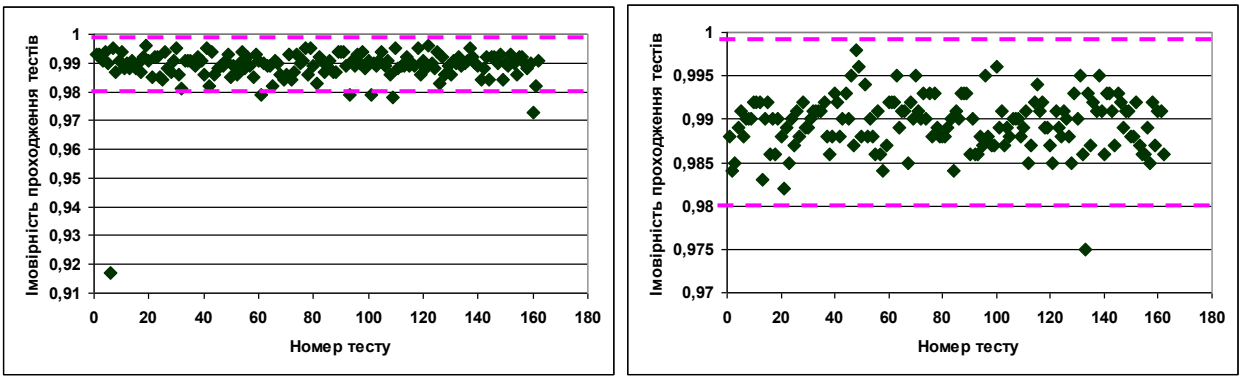
$$a = a_0 \ \ xor \ \ a_1 \ \ xor \ \ a_2 \ \ xor \ \cdots \ xor \ \ a_z, \qquad (3)$$

де *z* – кількість двійкових розрядів, що подається на ЛС з P_{n+1}, a_i (i = 0, 1,…, *z*) – значення розрядів числа в P_{n+1}. Кількість членів рівняння (3) може вибиратись з діапазону 0 … *z*. У роботі досліджуються послідовності при значеннях z – 4, 8, 10.

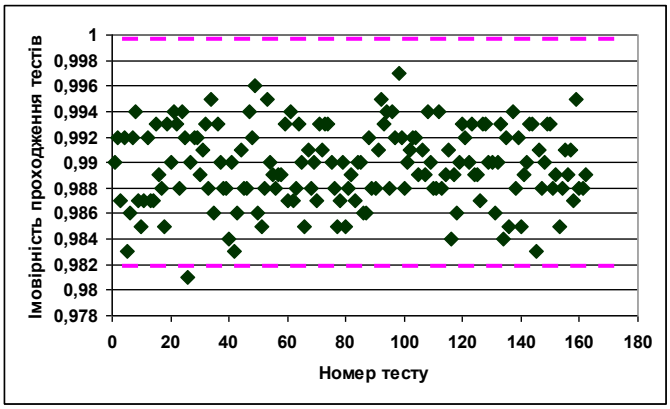
Вихідна псевдовипадкова бітова послідовність формується на виході молодшого розряду P_{n+1}.

Дослідження статистичних характеристик МАГФЗ здійснювалось з використанням набору статистичних тестів NIST [7]. Результати тестування подано на рис. 3, 4 у вигляді статистичних портретів. 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 0,998, в іншому випадку – тест не пройдено [7, 8]. Для наочності межі довірчого інтервалу позначені пунктирними лініями.

На рис. 3 наведені результати тестування МАГФЗ, який складався з 7 регістрів, алгоритм роботи $x_n=(x_6+x_1+a) \bmod 1024$ (варіант-1). У процесі тестування змінювалась кількість двійкових розрядів (z), які подаються на ЛС.



а б



в

Рис. 3. Статистичні портрети МАГФЗ варіант-1: а) z=4, б) z=8, в) z=10

Із результатів тестування видно, що збільшення кількості розрядів, які подаються на логічну схему покращують статистичні характеристики генератора. При значенні z=4 тестування не пройшло 6 тестів, при збільшенні значення z=8 – не пройдено лише 1 тест, а при z=10 усі тести успішно пройдено. Отже, можна зробити висновок, що сформована послідовність з такими параметрами відповідає вимогам випадковості.

При порівнянні статистичних портретів АГФЗ (рис. 1) і МАГФЗ (рис. 3) можна зробити висновок, що запропонований авторами спосіб модифікації дав позитивний результат. Також спостерігається покращення результатів тестування послідовностей при збільшення значення z і кількості регістрів (табл. 2).

У табл. 2 наведено результати дослідження МАГФЗ, у яких змінювалась кількість регістрів.

Таблиця 2

Результати дослідження МАГФЗ

Алгоритм роботи	**Кількість регістрів**	**АГФЗ (z=0)**		**МАГФЗ**			
		Кількість не пройдених тестів NIST	**Період повторення**	**Кількість не пройдених тестів NIST**			**Період повторення**
				z=4	**z=8**	**z=10**	
$x_n= (x_6+x_1+a)$	7 регістрів	(-162)	111104	162 (-6)	162 (-1)	162 (+)	10^9
	8 регістрів	(-162)	261632	162 (-1)	162 (+)	162 (+)	$>10^9$
	9 регістрів	(-162)	7680	162 (-4)	162 (-2)	162 (-1)	$>10^9$
	10 регістрів	(-162)	304640	162 (-1)	162 (+)	162 (+)	$>10^9$
	11 регістрів	(-162)	419328	162 (+)	162 (+)	162 (+)	$>10^9$

Дослідження показали, що для отримання оптимальних статистичних характеристик потрібно збільшити кількість розрядів (z), які подаються на логічну схему або збільшити кількість структурних елементів – регістрів.

На рис. 4 наведені статистичні портрети МАГФЗ, який складався з 7 регістрів, алгоритм роботи $x_n=(x_5+x_1+a) \bmod 1024$ (варіант-2). У процесі тестування змінювалась кількість двійкових розрядів (z), які подаються на ЛС.

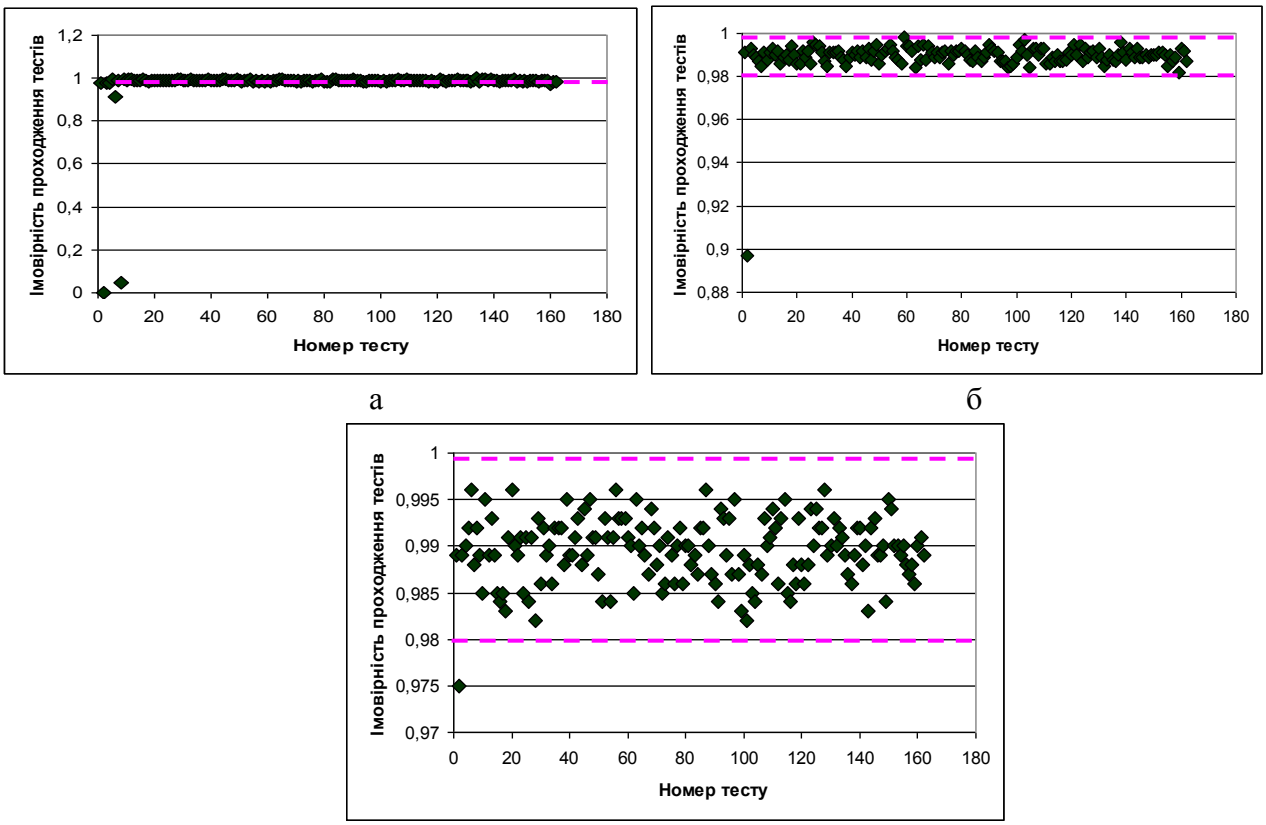


Рис. 4. Статистичні портрети МАГФЗ варіант-2: а) z=4, б) z=8, в) z=10

Із статистичних портретів видно, що збільшення кількості розрядів, які подаються на логічну схему покращують статистичні характеристики генератора. При значенні z=4 тестування не пройшло 7 тестів, при збільшенні значення z=8 – не пройдено лише 1 тест, при z=10 – не пройдено 1, але результат покращився.

У табл. 3 наведено результати дослідження МАГФЗ, у яких змінювалась кількість регістрів при незмінному алгоритму роботи.

Таблиця 3

Результати дослідження МАГФЗ

Зв'язки	**Кількість регістрів**	**АГФЗ (z=0)**		**МАГФЗ**			
		Кількість не пройдених тестів NIST	**Період повторення**	**Кількість не пройдених тестів NIST**			**Період повторення**
				z=4	**z=8**	**z=10**	
$x_n=(x_{n-3}+x_1+a)$	7 регістрів (x_5+x_1+a)	(-162)	6144	162 (-7)	162 (-1)	162 (-1)	$>10^9$
	8 регістрів (x_6+x_1+a)	(-162)	261632	162 (-1)	162 (+)	162 (+)	$>10^9$
	9 регістрів (x_7+x_1+a)	(-162)	31744	162 (+)	162 (-1)	162 (+)	$>10^9$
	10 регістрів (x_8+x_1+a)	(-162)	784896	162 (+)	162 (+)	162 (+)	$>10^9$
	11 регістрів (x_9+x_1+a)	(-162)	14336	162 (1)	162 (+)	162 (+)	$>10^9$

Відомо, що початкові числа впливають на якість сформованих послідовностей [1]. Авторами здійснено дослідження впливу значень початкових чисел на якість сформованих послідовностей МАГФЗ, результати дослідження наведено у табл. 4, 5. Для дослідження було вибрано два МАГФЗ. Перший (варіант-3) успішно пройшов усі тести NIST, він складався з 8 регістрів, алгоритм роботи $x_n=(x_6+x_1+a) \bmod 1024$, значення z=8. Другий генератор (варіант-4) не пройшов 7 тестів з набору NIST, він складався з 7 регістрів, алгоритм роботи $x_n=(x_5+x_1+a) \bmod 1024$, значення z=4.

Таблиця 4

Результати дослідження МАГФЗ варіант-3

Розряди початкових чисел	**Значення початкових чисел**	**Результат перевірки тестами NIST**
10	11, 23, 29, 61, 67, 89, 97	162 (-1)
100	113, 393, 171, 135, 113, 393, 171	162 (+)
1000	1069, 1033, 1487, 1511, 1627, 2111, 2179	162 (+)
10000	12263, 14051, 14593, 29879, 30211, 41479, 66713	162 (+)
100000	712731, 171078, 371722, 717141, 712731, 171078, 371722	162 (-1)
змішані	11, 393, 1487, 66713, 171078, 89, 14051	162 (+)

Таблиця 5

Результати дослідження МАГФЗ варіант-4

Розряди початкових чисел	**Значення початкових чисел**	**Результат перевірки тестами NIST**
10	11, 23, 29, 61, 67, 89, 97, 11	162 (-5)
100	113, 393, 171, 135, 113, 393, 171, 113	162 (-7)
1000	1069, 1033, 1487, 1511, 1627, 2111, 2179, 1069	162 (-6)
10000	12263, 14051, 14593, 29879, 30211, 41479, 66713, 12263	162 (-6)
100000	712731, 171078, 371722, 717141, 712731, 171078, 371722, 712731	162 (-7)
змішані	11, 393, 1487, 66713, 171078, 89, 14051, 11	162 (-5)

Отже, значення початкових чисел в регістрах впливає на статистичні характеристики вихідної послідовності. Вибір цих значень, при яких досягається задовільна якість генератора може бути здійснена за допомогою імітаційного моделювання.

Висновки

Запропонований авторами спосіб модифікації генератора Фібоначчі з запізненням дозволив покращити якість генератора, за рахунок покращення статистичних характеристик його вихідних послідовностей.

1 . Включення у склад адитивного генератора Фібоначчі з запізненням логічної схеми, на вхід якої подаються розряди з вихідного регістру P_{n+1}, а вихід з'єднаний з входом переносу комбінаційного суматора дозволяє суттєво збільшити період повторення вихідних послідовностей і покращити статистичні характеристики.

2. Включення у склад генератора логічної схеми, дозволяє реалізувати алгоритм додавання чисел за mod *m*, де $m=2^w$ *(w* –кількість двійкових розрядів структурних елементів), що дозволяє істотно спростити апаратну реалізацію генератора.

3. Покращення статистичних характеристик забезпечується при збільшенні кількості регістрів і кількості розрядів вихідного регістру, що подається на логічну схему.

4. Значення початкових чисел в регістрах генератора при яких досягаються задовільні статистичні характеристики можуть бути визначенні в процесі імітаційного моделювання.

Література

1. Orue A.B. Trifork, a new pseudorandom number generator based on lagged Fibonacci maps / A.B. Orue, F. Montoya, L. Hernández Encinas // Journal of computer science and engineering. – 2010. – volume 2, issue 2. – P. 46-51.

2. Burns P. Lagged, Fibonacci Random Number Generators. [Електронний ресурс] // – Режим доступу: http://lamar.colostate.edu/~grad511/lfg.pdf (09.05.2014).

3. Mascagni M. Parallel Pseudorandom Number Generation / M. Mascagni // Advanced architecture Computers. – P. 42-48.

4. Mascagni M. Parallel pseudorandom number generation using additive lagged-Fibonacci recursions / M. Mascagni, M.L. Robinson, D.V. Pryor, S.A. Cuccaro // Springer-Verlag Lecture Notes in Statistics. – 1995. – № 106. – P. 263–277.

5. Иванов М.А. Теория, применение и оценка качества генераторов псевдослучайных последовательностей / Иванов М.А., Чугунков И.В. – М.: КУДИЦ – ОБРАЗ, 2003. – 240 с.

6. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях: учебное пособие / М.А. Иванов, И.В. Чугунков. – М.: Изд-во НИЯУ МИФИ, 2012. – 400 с.

7. 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//SP80022rev1a.pdf. (12.05.2014).

8. Мандрона М.М. Дослідження впливу параметрів генератора Голлманна на статистичні характеристики вихідного сигналу / Мандрона М.М., Максимович В.М., Костів Ю.М., Гарасимчук О.І. // Вісник кременчуцького національного університету ім. М. Остроградського. – Кременчук: КрНУ, 2013. – Вип. 4 (81). – С. 98-103.

Надійшла 12. 05. 2014р. Рецензент: д.т.н., проф. Кравченко Ю.В.