DOI 10.15276/imms.v9.no4.291
УДК 004.056

Informatics and Mathematical Methods in Simulation
Vol. 9 (2019), No. 4, pp. 291-303

РОЗРОБКА ГЕНЕРАТОРА ПСЕВДОВИПАДКОВИХ ЧИСЕЛ НА ОСНОВІ КЛІТИННИХ АВТОМАТІВ

Л.В. Дранишников, Р.Є. Бірюков

Дніпровський державний технічний університет,
вул. Дніпробудівська 2, Кам'янське, 51918, Україна: e-mail: dr-leon@ukr.net

Розроблено алгоритми генерації псевдовипадкових чисел, засновані на властивості клітинних автоматів, які мають високу швидкість обчислень. Методи дослідження базуються на використанні теорії клітинних автоматів та об'єктно-орієнтованого підходу. Алгоритм роботи генератора псевдовипадкових двійкових послідовностей включає в себе фази ініціалізації, холостого ходу (функціонування без знімання вихідної послідовності) і генерації. В роботі були розроблені алгоритми генераторів псевдовипадкових чисел на основі класичних, неоднорідних та самопрограмованих клітинних автоматів. Було проведене дослідження характеристик лавинного ефекту клітинних автоматів. Із застосуванням мови програмування Python та об'єктно-орієнтованого підходу було розроблено програмне забезпечення, яке використовує апарат клітинних автоматів для генерації псевдовипадкових двійкових послідовностей. Отримані вихідні послідовності розроблених генераторів пройшли ряд статистичних тестів статистичних пакетів NIST та RaBiGeTe. Було доведено наближення властивостей отриманих вихідних послідовностей до випадкових. Було проведено тестування швидкодії розроблених генераторів. Практична цінність отриманих результатів полягає в наступному. Розроблені алгоритми генераторів псевдовипадкових послідовностей на основі клітинних автоматів мають кращу швидкодію, ніж існуючі аналоги, а також мають статистичні характеристики вихідних послідовностей, що наближаються до статистичних показників випадкових. Можливі напрямки розвитку або продовження дослідження: напрямом продовження дослідження є пошук ліпших конфігурацій клітинних автоматів у складі генераторів псевдовипадкових послідовностей, підвищення швидкодії розроблених алгоритмів за допомогою реалізації за принципом паралельних обчислень, фізична реалізація розроблених алгоритмів на програмованій логічній інтегральній схемі, розробка алгоритмів шифрування на основі клітинних автоматів.

Ключові слова: генератор псевдовипадкових чисел, клітинний автомат, лавинний ефект, криптографія.

Вступ

Клітинні автомати широко поширені в області моделювання складних систем і генерації псевдовипадкових чисел. Пошук генераторів з хорошими показниками критеріїв статистичних тестів є досить складним завданням. Відомі практичні методи отримання псевдовипадкових чисел, що засновані на детермінованих алгоритмах, тому такі числа і звуться псевдовипадковими, оскільки наперед відомо про операції, які породжують послідовності. Зрозуміло, що вони відрізняються від справжніх випадкових послідовностей, отриманих у результаті природного фізичного процесу.

Генератори псевдовипадкових чисел повинні мати низку властивостей. Найбільш важливими властивостями з цієї точки зору є хороші результати в стандартних статистичних тестах на випадковість, обчислювальну ефективність, тривалий період (мінімальне число між повтореннями) і відтворюваність послідовності (наприклад, таким є набір тестів National Institute of Standards and Technology (NIST) [1]). Статистичні тести NIST – пакет статистичних тестів, розроблений Лабораторією інформаційних технологій (англ. InformationTechnologyLaboratory), що є головною

дослідницькою організацією Національного інституту стандартів і технологій (NIST). До його складу входять 15 статистичних тестів, метою яких є визначення міри випадковості двійкових послідовностей, породжених або апаратними, або програмними генераторами випадкових чисел. Ці тести засновані на різних статистичних властивостях, притаманних тільки випадковим послідовностям.

Мета роботи

Метою даної роботи є дослідження апарату клітинних автоматів та подальше використання в алгоритмах прикладних задач для покращення їх характеристик відносно існуючих аналогів [2,3].

Клітинні автомати використовуються в багатьох наукових сферах [4-8]. У даній роботі увага зосереджена на розробці та дослідженні алгоритмів генераторів псевдовипадкових послідовностей.

Відповідно до поставленої мети в роботі ставляться такі задачі: виконання аналізу існуючих генераторів псевдовипадкових послідовностей (ГПВП) аналогів на основі клітинних автоматів [10,11]; розроблення та дослідження властивостей власних алгоритмів ГПВП на основі клітинних автоматів; виконання тестування розроблених алгоритмів та виконання порівняння з розглянутими аналогами; відповідні висновки щодо отриманих результатів.

Основна частина

Формально класичний клітинний автомат можна визначити таким чином:

$$(C, N, Q, q^0, f),$$

де C – множина клітин; N – потужність КлА, що визначається кількістю сусідніх клітин; Q – кінцева множина станів, в яких можуть знаходитися клітини автомату; q^0– початковий стан автомату, який задається на початку його роботи; f – правило для розрахунку нового стану клітини, який залежить від поточних станів усіх її сусідів.

ККлА – це такий КлА, усі клітини якого знаходяться на двовимірній решітці (рис.1), клітини приймають в якості значення стану значення з множини {0,1}, мають одне правило переходу, яке використовується глобально на всій множині клітин, до того ж оновлення усіх клітин виконується одночасно та в дискретні проміжки часу.

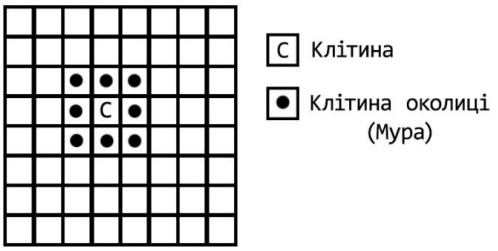


Рис. 1. Класичний КлА

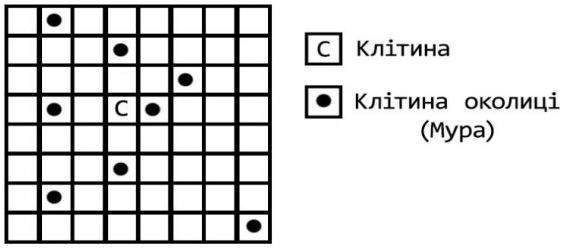


Рис. 2. Неоднорідний КлА з розрізненою околицею

Неоднорідний клітинний автомат (НКлА, рис.2) – це модифікація ККлА, клітини якої знаходяться на двовимірний решітці, клітини приймають в якості значення стану значення з множини {0,1}, оновлення усіх клітин виконується одночасно та в дискретні проміжки часу; на відміну від ККлА мають або декілька правил, що застосовуються

клітинами за встановленим алгоритмом (зазвичай обираються випадковим чином), або розрізнену (неоднорідну) конфігурацію околиці.

У випадку розрізненої конфігурації околиці, для кожної клітини випадковим чином обирається множина сусідів згідно з обраною потужністю, множина сусідів кожної клітини є сталою на всіх наступних ітераціях. До конфігурації додається складова C_N, яка відповідає множині клітин сусідів.

У випадку наявності декількох правил КлА, кожній клітині може бути призначене одне правило, яке буде діяти постійно, також можливий варіант, коли на кожній ітерації правило визначається випадковим чином. Схематично такий НКлА не відрізнятиметься від ККлА.

Самопрограмований клітинний автомат (СПКлА) – це КлА, в якому правило переходу змінюється залежно від значення клітин даного або суміжного автомату. Використання правил, що змінюються динамічно, дозволяє уникнути шаблонів, які утворюються, коли клітини мають постійні правила.

СПКлА (рис.3) можна реалізувати у вигляді двох пов'язаних КлА. Один з них (нижній) залежить від іншого (верхній) при виборі правила, яке потрібно застосувати на наступному кроці. Кожна клітина нижнього автомату орієнтується на значення відповідної клітини верхнього автомату при виборі правила, тобто якщо значення клітини верхнього автомату 0, то клітина нижнього автомату переходить у наступний стан за одним правилом, а якщо 1 – за іншим. Використання верхнього автомату додає випадковості клітинному автомату.

Рис. 3. Самопрограмований КлА

Для оцінки властивостей криптографічних перетворень в роботі використано поняття «лавинного ефекту», яке було введено Хорстом Фейстелем в 1973 р. Лавинний ефект показує, наскільки сильно змінюється вихід деякого перетворення при зміні одного біта вхідних даних. F_0

Будемо розглядати КлА, що розташований на двовимірній решітці розміром $M_X \times M_Y$. Оскільки решітка КлА є тором, обчислення координат здійснюються за модулем відповідного розміру решітки.

Введемо поняття відстані між клітинами КлА як максимальне абсолютне значення різниці відповідних координат. З урахуванням закручування решітки КлА в тор відстань $\Delta\left(m_{(x_1,y_1)}, m_{(x_2,y_{21})}\right)$ між клітинами $m_{(x_1,y_1)}$ та $m_{(x_2,y_2)}$ задається формулою:

$$\Delta\left(m_{(x_1,y_1)}, m_{(x_2,y_2)}\right) = \max\left(\min(|x_1 - x_2|), M_X - |x_1 - x_2|), \min(|y_1 - y_2|), M_Y - |y_1 - y_2|)\right)$$

Очевидно, що максимально можлива відстань між двома осередками КлА дорівнює:

$$\Delta_{\max} = \max\left(\left|\frac{M_X - 1}{2}\right|, \left|\frac{M_Y - 1}{2}\right|\right)$$

Розглянемо два ідентичних КлА, тобто з однаковими розмірами решітки $M_X \times M_Y$, однією тією ж локальною функцією зв'язку й однаковими заповненнями співпадаючих за координатами клітин. Позначимо через $m^t_{(x,y)}$ заповнення клітини першого КлА з координатами (*x*,*y*); для аналогічної клітини другого КлА будемо використовувати позначення $\widehat{m}^t_{(x,y)}$. У момент часу *t*=0 виконаємо зміну значення клітини з координатами (0,0) другого КлА на протилежне (оскільки в силу однорідності всі клітини невиразні за своїми властивостями, то вибір конкретної клітини не обмежує спільності):

$$\widehat{m}^t_{(x,y)} \leftarrow 1 - m^t_{(x,y)}$$

Лавинний ефект відображає поширення змін, викликаних у другому КлА зміною заповнення однієї комірки пам'яті. Введемо інтегральну і просторову числові характеристики лавинного ефекту. Якщо зміни поширюються рівномірно у всіх напрямках з максимально можливою лінійною швидкістю (у даному випадку становить одну клітину в кожному напрямку за такт роботи) і при цьому змінюється заповнення половини всіх осередків, то такий лавинний ефект ми називаємо оптимальним.

Інтегральною характеристикою лавинного ефекту $\eta(t)$ в КлА назвемо залежність за часом відношення кількості не співпадаючих заповнень клітин для клітин з однаковими координатами до загальної кількості клітин на решітці КлА:

$$\eta(t) = \sum_{\substack{0 \le X \le M_X \\ 0 \le Y \le M_Y}} \frac{\widehat{m}^t_{(x,y)} \oplus m^t_{(x,y)}}{M_X M_Y}$$

Інтегральна характеристика оптимального лавинного ефекту має вигляд:

$$\eta(t) = \begin{cases} \dfrac{(2t+1)^2}{2M_X M_Y}, & 2t+1 \le M_Y \\ \dfrac{(2t+1)}{2M_X}, & M_Y < 2t+1 \le M_X \\ \dfrac{1}{2}, & M_X < 2t+1 \end{cases}$$

У загальному випадку інтегральна характеристика лавинного ефекту $\eta(t)$ має у середньому прямувати до значення 0.5, що свідчить про відмінність КлА у середньому на половину усіх клітин, за умови відмінності одного КлА від іншого в момент часу *t*=0 на один біт.

Показником, що відображає лінійну швидкість поширення змін по решітці КлА, є просторова характеристика лавинного ефекту $\mu(t)$, рівна відношенню максимальної відстані, на якій виявилися зміни, до максимально можливої відстані:

$$\mu(t) = \frac{1}{(M_X - 1)/2} \max_{\substack{0 \le X < M_X \\ 0 \le Y < M_Y}} ((m^t_{(x,y)} \oplus \widehat{m}^t_{(x,y)}) \cdot \Delta(m_{(0,0)}, m_{(x,y)}))$$

Просторова характеристика оптимального лавинного ефекту описується формулою:

$$\mu(t) = \begin{cases} \dfrac{t}{(M_X - 1)/2}, t < \left|(M_X - 1)/2\right| \\ 1, \quad t \geq \left|(M_X - 1)/2\right| \end{cases}$$

У загальному випадку просторова характеристика лавинного ефекту μ(t) має у середньому прямувати до значення 1, що свідчить про максимальну швидкість поширення змін у КлА, за умови відмінності одного КлА від іншого в момент часу t=0 на один біт.

У ході дослідження було розглянуто лавинні характеристики представлених клітинних автоматів. При дослідженні характеристик лавинного ефекту в конкретному КлА результат залежить від вибору початкового заповнення осередків решітки та локальної функції зв'язку. Таким чином, характеристики лавинного ефекту відображають властивості КлА в цілому і повинні розглядатися як деякий усереднений показник. Для дослідження було застосовано по 100 пар КлА кожного типу, розміром 32x32 клітини на часовому проміжку $0< t < 100$, потужність КлА, що досліджуються, обрано рівною 8, тому що вже заздалегідь відомо, що КлА з потужністю 4 мають порівняно гірші значення лавинних характеристик.

У результаті дослідження було встановлено, що лавинні характеристики прямують до оптимальних значень, що свідчить про гарні статистичні властивості. Тому розглянуті КлА можна застосовувати в криптографічних дослідженнях.

На основі розглянутих клітинних автоматів були розроблені генератори псевдовипадкових послідовностей. Генератор на основі класичних КлА (рис.4) використовується в якості аналогу, відносно якого було виконано порівняння з іншими розробленими ГПВП. Для чистоти експерименту він був реалізований та досліджений з рештою алгоритмів на спільній платформі та мові програмування.

В структуру генератора входять:

- два класичних клітинних автомати C_1 і C_2;
- регістр зсуву з лінійними зворотними зв'язками R.

На кожному такті роботи клітинні автомати C_1 і C_2 виробляють по 256 біт двійкових послідовностей, які почленно складаються за модулем 2, а результат додавання подається на вихід генератора. Оскільки послідовності, що виробляються клітинними автоматами, можуть розглядатися як незалежні, складання дозволяє поліпшити статистичні властивості вихідної послідовності генератора.

Додавання вихідних послідовностей клітинних автоматів також дозволяє ускладнити відновлення внутрішнього стану генератора (тобто значень комірок пам'яті клітинних автоматів і регістра зсуву) за вихідною послідовністю, що може бути корисно, наприклад, у криптографічних додатках.

Однією з основних проблем при використанні клітинних автоматів у складі генераторів псевдовипадкових послідовностей є непередбачуваність їх періоду, обумовлена нелінійністю функції переходів. Для забезпечення мінімального гарантованого періоду вихідної послідовності в структуру генератора вводиться регістр зсуву з лінійними зворотними зв'язками R. Вихід регістра на кожному такті роботи додається за модулем 2 до значення однієї з комірок клітинних автоматів. При цьому лавинний ефект дозволяє гарантувати, що період послідовності внутрішніх станів клітинних автоматів буде не менше періоду вихідної послідовності регістру зсуву. Початкові значення комірок пам'яті регістра зсуву також є ключем вироблення псевдовипадкової послідовності генератора в цілому, тобто визначають вибір конкретної послідовності з безлічі можливих.

У запропонованому варіанті ГПСЧ використовуються 2 класичних двовимірних бінарних синхронних клітинних автомати розміром 37x11. При чому вихідні послідовності знімаються з фіксованої частини поля автомату розміром 32x8.

Відмінність двох КлА, що є складовими частинами даного генератора, полягає у різних початкових станах КлА, а також у використанні різних функцій переходу.

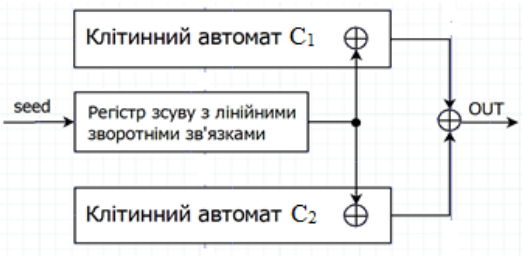


Рис. 4. Схема ГПВП на двох ККлА

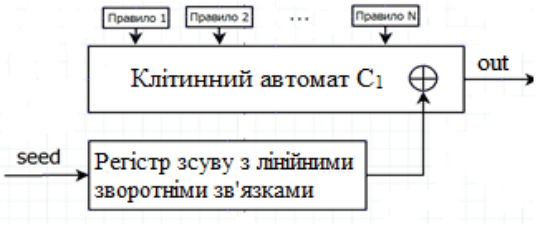


Рис. 5. Схема ГПВП на одному НКлА

Генератор на основі НКлА може бути представлений у вигляді схеми, що зображена на рисунку 5.

В структуру генератора входять:

- один неоднорідний клітинний автомат C_1;
- регістр зсуву з лінійними зворотними зв’язками R.

У даному ГПВП використовується лише один НКлА, що має значно поліпшити показники швидкодії програмної реалізації, причому без погіршення статистичних властивостей вихідних послідовностей, що пов’язано з кращими характеристиками лавинного ефекту у порівнянні з ККлА.

Використаний НКлА базується на принципі розрізненості правил та може використовувати 2 або більше правил для оновлення кожної клітини. Для ускладнення поведінки НКлА на кожному такті роботи для кожної клітини правило обирається випадковим рівно вірогідним чином.

Також для покращення швидкодії планується збільшити розміри вихідної послідовності, що знімається з виходу, до 32x32 та 64x64 біт за так роботи генератора. При цьому збільшиться час на ініціалізацію ГПВП, але зменшиться час на вироблення випадкової послідовності у довгостроковій перспективі.

Для ускладнення відновлення стану за вихідною послідовністю генератора на вихід генератора подається частина клітин генератора.

Для покращення статистичних характеристик та збільшення мінімального періоду вихідної послідовності використовується регістр зсуву з лінійними зворотними зв’язками розміром 256 біт. Вихід регістру на кожному такті роботи підмішується складанням за модулем 2 до клітини НКлА, що не входить до множини клітин, які подаються на вихід генератора. Причому клітина, до якої виконується підмішування виходу регістру зсуву, не повинна знаходитися на границі з клітинами, які передаються на вихід генератора. Для ліпшого покращення статистичних властивостей можна розглянути варіант з додаванням ще одного регістра зсуву.

Конфігурація НКлА з виходом 32x32 біти, у складі ГПВП має вигляд, який наведено на рис 6. Про необхідність додавання другого регістру зсуву слід стверджувати вже після тестування генератору за допомогою пакетів статистичних тестів.

Алгоритм роботи генератора псевдовипадкових двійкових послідовностей включає в себе фази ініціалізації (установки початкових значень), холостого ходу (функціонування без знімання вихідної послідовності) і генерації.

Крок 1. Ініціалізація:

Крок 1.1. Занесення ключа вироблення випадкової послідовності у комірки пам’яті регістра зсуву з лінійними оберненими зв’язками R;

Крок 1.2. Встановлення випадкових значень комірок пам'яті клітинних автоматів C_1 та C_2, при чому кількість 0 та 1 має бути рівною;

Крок 1.3. Встановлення розміру підмножини клітин вихідної послідовності для клітинних автоматів C_1 та C_2;

Крок 1.4. Збереження координат клітини для підмішування вихідних значень регістру зсуву;

Крок 1.5. Перехід до фази холостого ходу (п.2).

Крок 2. Холостий хід:

Крок 2.1. Привласнити значення лічильника тактів $t = 0$;

Крок 2.2. Розрахувати нові значення комірок пам'яті клітинних автоматів C_1 та C_2, використовуючи встановлені функції переходів до околиці кожної клітини;

Крок 2.3. Додати вихідне значення регістру зсуву до відповідних комірок пам'яті клітинних автоматів C_1 та C_2;

Крок 2.4. Розрахувати нове значення регістру зсуву R;

Крок 2.5. Збільшити значення лічильника тактів *t* на 1;

Крок 2.6. Якщо значення лічильника t менше значення тривалості холостого ходу idle, то перейти на *Крок 2.2*, інакше перейти до фази генерації (п.3).

Крок 3. Фаза генерації:

Крок 3.1. Розрахувати нові значення комірок пам'яті клітинних автоматів C_1 та C_2, використовуючи встановлені функції переходів до околиці кожної клітини;

Крок 3.2. Додати вихідне значення регістру зсуву до відповідних комірок пам'яті клітинних автоматів C_1 та C_2;

Крок 3.3. Розрахувати нове значення регістру зсуву R;

Крок 3.4. Сформувати вихідні значення клітинних автоматів C_1 та C_2 із зазначеної підмножини клітин;

Крок 3.5. Розрахувати вихідне значення генератору шляхом складання відповідних вихідних значень клітинних автоматів C_1 та C_2 за модулем 2;

Крок 3.6. Якщо довжина отриманої послідовності достатньої довжини, то робота алгоритму завершується, інакше переходимо на *Крок 3.1*.

Генератор на основі СПКлА може бути представлений у вигляді схеми, що зображена на рисунку 7.

В структуру генератора входять: один самопрограмований клітинний автомат C_1; регістр зсуву з лінійними зворотними зв'язками R.

У даному ГПВП використовується один СПКлА, який складається з двох шарів: керуючий шар є ККлА з 1 контрольним правилом, що слугує для визначення правил основного шару; основний шар є НКлА з 2 правилами, які для кожної клітини визначаються станом керуючого шару, слугує для генерації вихідної послідовності.

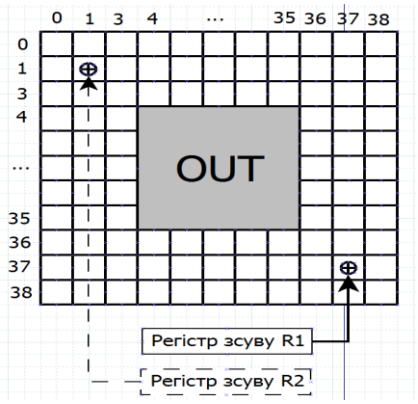


Рис. 6. Структура НКлА у складі генератора

Рис.7. Схема ГПВП на одному СПКлА

Для покращення швидкодії у порівнянні до ГПВП на основі ККлА планується збільшити розміри вихідної послідовності, що знімається з виходу, до 32х32 та 64х64 біт за так роботи генератора. При цьому збільшиться час на ініціалізацію ГПВП, але зменшиться час на виробку випадкової послідовності у довгостроковій перспективі.

Для ускладнення відновлення стану за вихідною послідовністю генератора на вихід генератора подається частина клітин основного шару генератора.

Для покращення статистичних характеристик та збільшення мінімального періоду вихідної послідовності використовується регістр зсуву з лінійними зворотними зв'язками розміром 256 біт. Вихід регістру на кожному такті роботи підмішується складанням за модулем 2 до клітини основного шару СПКлА, що не входить до множини клітин, які подаються на вихід генератора. При чому клітина, до якої виконується підмішування виходу регістру зсуву, не повинна знаходитися на границі з клітинами, які передаються на вихід генераторау. Конфігурація СПКлА з виходом 32х32 наведено на рисунку 8.

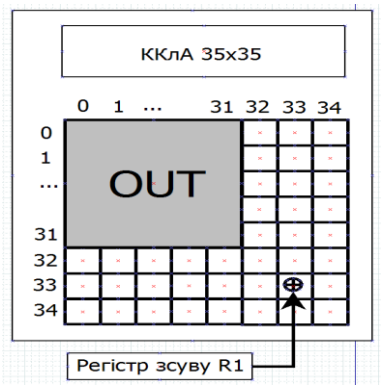


Рис. 8. Структура СПКлА у складі генератора

Було визначено швидкодію генератора псевдовипадкових послідовностей як кількість вироблених генератором біт за 1 секунду роботи. При чому, час роботи генератора складається з часу, витраченого на ініціалізацію, та часу генерації послідовності заданої величини. Для виконання порівняння швидкодії, усі розроблені ГПВП мають згенерувати послідовність розміром 1024000 біт, а в якості результату приймається середнє значення серед 100 екземплярів кожного типу генератора.

У процесі тестування брали участь ГПВП з такими параметрами:

- ГПВП на основі ККлА (CAPRNG) – еталонний генератор, відносно якого буде проведено порівняння та зроблено висновок відносно розроблених алгоритмів (згідно з рекомендацією автора, даний генератор має розмір 11*37 клітин, розмір вихідних значень 8*32 (256 біт), потужність 8 та час холостого ходу 40);
- 2 ГПВП на основі НКлА (CAPRNGm4) – генератор на основі неоднорідності правил: перший генератор має розмір 40*40 клітин, розмір виходу 32*32 (1024 біт), потужність 8 та час холостого ходу 10 згідно з лавинними характеристиками; другий генератор має розмір 70*70 клітин, розмір виходу 64*64 (4096 біт), потужність 8 та час холостого ходу 10 згідно з лавинними характеристиками (кількість правил не чинить суттєвого впливу на швидкодію);
- 2 ГПВП на основі СПКлА (CAPRNGm6) – генератор за схемою самопрограмування: перший генератор має розмір 40*40 клітин, розмір виходу 32*32 (1024 біт), потужність 8 та час холостого ходу 40; другий генератор має розмір 70*70 клітин, розмір виходу 64*64 (4096 біт), потужність 8 та час холостого ходу 40.

Порівняння часу ініціалізації показало, що зі збільшенням розміру клітинних автоматів, експоненціально збільшується час ініціалізації ГПВП. Подальше збільшення розмірів КлА є недоцільним через різке збільшення часу ініціалізації.

Порівняння часу генерації (без урахування ініціалізації), а також порівняння значень швидкодії (біт/с) (рис. 9) говорить про те, що розроблені алгоритми ГПВП мають перевагу у швидкодії у порівнянні з еталонним ГПВП.

Можна зробити висновок, що найгірший час генерації псевдовипадкової послідовності має еталонний ГПВП, а найкращий – ГПВП на основі неоднорідного за правилами КлА з розміром виходу 64*64. Відповідно, найгіршу швидкодію має еталонний ГПВП, а найкращу – ГПВП на основі неоднорідного за правилами КлА з розміром виходу 64*64.

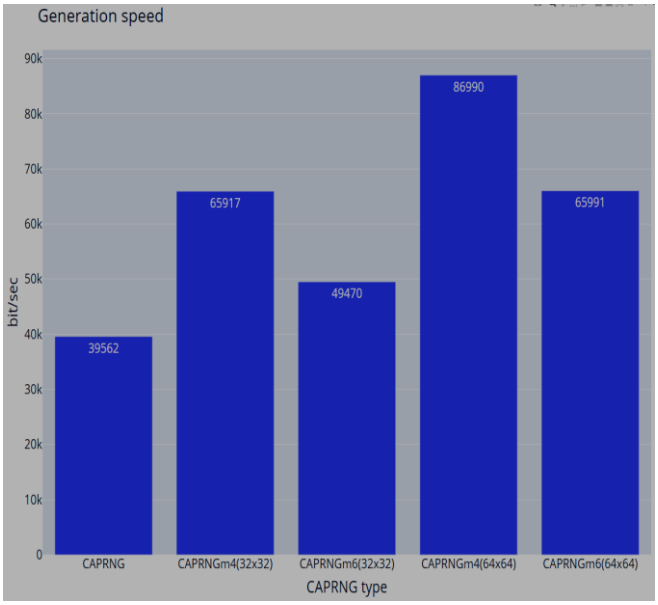


Рис. 9. Порівняння швидкодії ГПВП на основі КлА

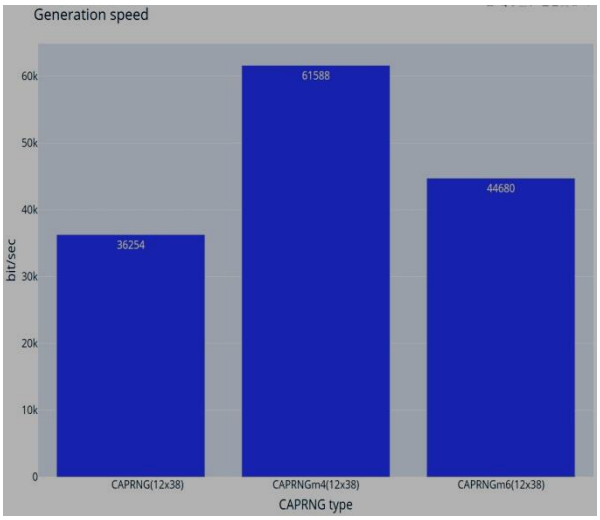


Рис. 10. Порівняння швидкодії ГПВП на основі КлА (за однакових конфігурацій)

Приріст швидкості у відсотках відносно еталонного ГПВП можна зобразити у вигляді таблиці 1.

Конфігурація КлА в ГПВП має безпосередній вплив на швидкодію ГПВП. Порівняємо розроблені ГПВП за умови, що конфігурації усіх генераторів однакові. Отриманий результат швидкодії наведено на діаграмі, що зображена на рисунку 10.

Як бачимо, на діаграмі на рис 10 результати тестування швидкодії свідчать про те, що навіть за однакової конфігурації КлА у складі ГПВП, найкращий показник має ГПВП на основі неоднорідного КлА, а найгірший – еталонний ГПВП на основі класичних КлА. Приріст швидкодії у відсотках наведено в таблиці 2.

Таблиця 1.

Приріст швидкості ГПВП

ГПВП	CAPRNG	CAPRNGm4 32x32	CAPRNGm4 64x64	CAPRNGm6 32x32	CAPRNGm6 64x64
Швидкодія (біт/с)	39562	65917	49470	86990	65991
Приріст	-	+66.6%	+25%	+119.9%	+66.8%

Таблиця 2.

Приріст швидкості ГПВП (за однакової конфігурації)

ГПВП	CAPRNG 12x38	CAPRNGm4 12x38	CAPRNGm6 12x38
Швидкодія (біт/с)	36254	61588	44680
Приріст	-	+69.9%	+23.2%

Розроблені ГПВП були протестовані на наборах тестів NIST та RaBiGeTe. У процесі тестування брали участь такі ГПВП: еталонний ГПВП на основі ККлА; ГПВП на основі НКлА з 2, 4, 8 та 16 правилами; ГПВП на основі СПКлА.

Тестування та порівняння статистичних властивостей алгоритмів. Розроблені ГПВП були протестовані на наборах тестів NIST та RaBiGeTe. У процесі тестування брали участь такі ГПВП: еталонний ГПВП на основі ККлА; – ГПВП на основі НКлА з 2, 4, 8 та 16 правилами; – ГПВП на основі СПКлА.

Для початку розглянемо результати тестів, проведених за допомогою набору тестів RaBiGeTe. Даний набір тестів в якості результату надає графік розподілення p-значень, які мають бути максимально наближені до «ідеальної лінії» (рис.11,12).

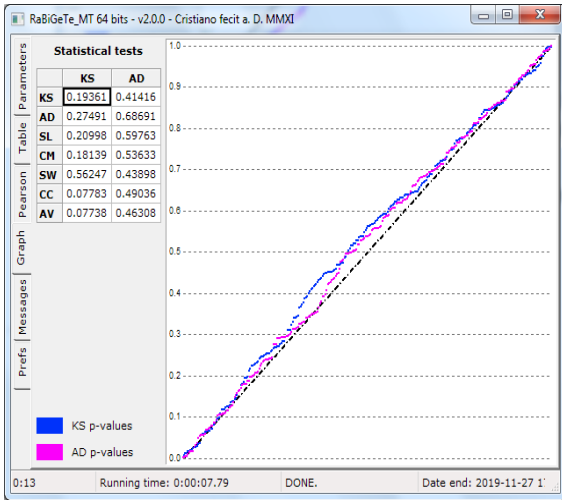


Рис.11. Результат тестування ГПВП на основі НКлА (16 правил)

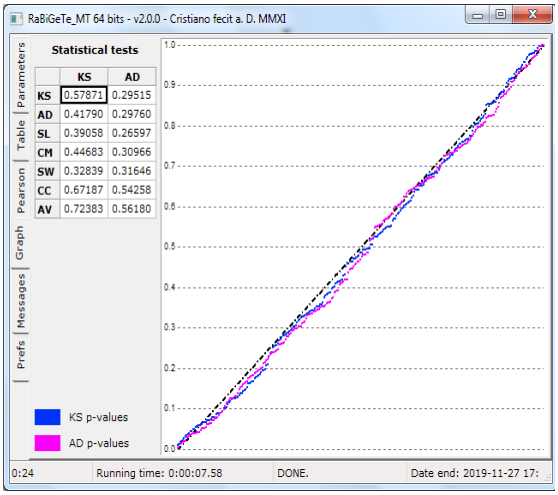
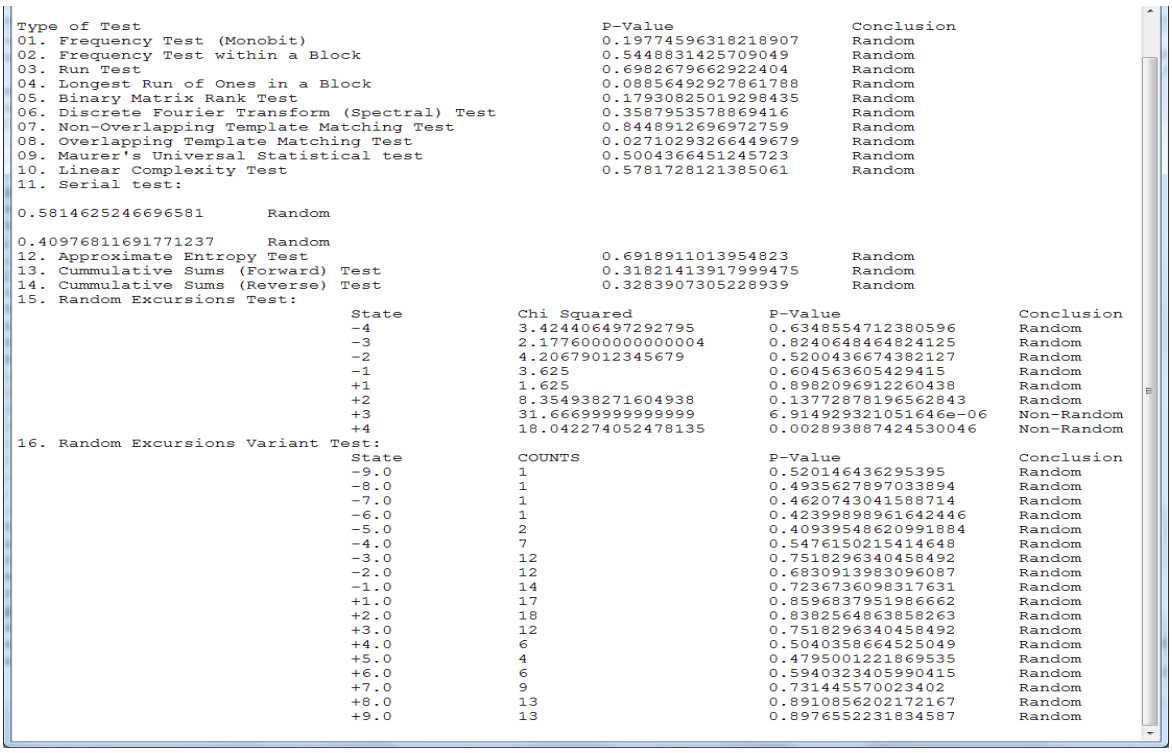


Рис. 12. Результат тестування ГПВП на основі СПКлА

Відповідно до отриманих результатів можна зробити висновок, що найкращими статистичними властивостями володіють еталонний ГПВП, ГПВП на основі НКлА з 16 правилами, а також ГПВП на основі СПКлА, через те що їх p-значення максимально наближені до ідеальної лінії. Проте, ГПВП на основі НКлА з 4 та 8 правилами мають непогані показники. ГПВП на основі НКлА з 2 правилами не пройшов статистичні тести.



```
Type of Test                                          P-Value                 Conclusion
01. Frequency Test (Monobit)                          0.19774596318218907     Random
02. Frequency Test within a Block                     0.5448831425709049      Random
03. Run Test                                          0.6982679662922404      Random
04. Longest Run of Ones in a Block                    0.08856492927861788     Random
05. Binary Matrix Rank Test                           0.17930825019298435     Random
06. Discrete Fourier Transform (Spectral) Test        0.3587953578869416      Random
07. Non-Overlapping Template Matching Test            0.8448912696972759      Random
08. Overlapping Template Matching Test                0.02710293266449679     Random
09. Maurer's Universal Statistical test               0.5004366451245723      Random
10. Linear Complexity Test                            0.5781728121385061      Random
11. Serial test:

0.5814625246696581      Random

0.40976811691771237     Random
12. Approximate Entropy Test                          0.6918911013954823      Random
13. Cummulative Sums (Forward) Test                   0.31821413917999475     Random
14. Cummulative Sums (Reverse) Test                   0.3283907305228939      Random
15. Random Excursions Test:
                                State       Chi Squared             P-Value                 Conclusion
                                -4          3.424406497292795       0.6348554712380596      Random
                                -3          2.1776000000000004      0.8240648464824125      Random
                                -2          4.20679012345679        0.5200436674382127      Random
                                -1          3.625                   0.604563605429415       Random
                                +1          1.625                   0.8982096912260438      Random
                                +2          8.354938271604938       0.13772878196562843     Random
                                +3          31.66699999999999       6.914929321051646e-06   Non-Random
                                +4          18.042274052478135      0.002893887424530046    Non-Random
16. Random Excursions Variant Test:
                                State       COUNTS                  P-Value                 Conclusion
                                -9.0        1                       0.520146436295395       Random
                                -8.0        1                       0.4935627897033894      Random
                                -7.0        1                       0.4620743041588714      Random
                                -6.0        1                       0.42399898961642446     Random
                                -5.0        2                       0.40939548620991884     Random
                                -4.0        7                       0.5476150215414648      Random
                                -3.0        12                      0.7518296340458492      Random
                                -2.0        12                      0.6830913983096087      Random
                                -1.0        14                      0.7236736098317631      Random
                                +1.0        17                      0.8596837951986662      Random
                                +2.0        18                      0.8382564863858263      Random
                                +3.0        12                      0.7518296340458492      Random
                                +4.0        6                       0.50403586645250 49     Random
                                +5.0        4                       0.4795001221869535      Random
                                +6.0        6                       0.5940323405990415      Random
                                +7.0        9                       0.731445570023402       Random
                                +8.0        13                      0.8910856202172167      Random
                                +9.0        13                      0.8976552231834587      Random
```

Рис. 13. Результат тестування ГПВП на основі НКлА (16 правил)

Для певності проведемо тестування ГПВП на основі пакетів статистичних тестів NIST. Результатом тестування є таблиця (рис.13) з розрахованими p-значеннями та висновком «Випадковий/не випадковий». З наведених результатів лише НКлА з 2 правилами не проходять усі тести. Результати тестування за допомогою NIST та RaBiGeTe збігаються, тому будемо вважати, що ГПВП, які пройшли тести з гарними показниками, генерують випадкові послідовності.

Висновки

Були проведені всі необхідні дослідження, використані сучасні методи реалізації алгоритмів, верифікації та тестування програмного забезпечення. Було проведено дослідження характеристик лавинного ефекту класичних, неоднорідних та самопрограмованих клітинних автоматів. Розроблені алгоритми генераторів псевдовипадкових чисел на основі класичних, неоднорідних та самопрограмованих клітинних автоматів. Із застосуванням мови програмування Python та об'єктно-орієнтованого підходу було розроблено програмне забезпечення, яке використовує апарат клітинних автоматів для генерації псевдовипадкових двійкових послідовностей. Отримані вихідні послідовності розроблених генераторів пройшли ряд статистичних тестів статистичних пакетів NIST та RaBiGeTe, згідно з результатами було доведено наближення властивостей отриманих вихідних послідовностей до випадкових. Проведено тестування швидкодії розроблених генераторів, відповідно до якого розроблені алгоритми мають кращу швидкодію, ніж відповідний аналог.

Список літератури

1. Rukhin A. A statistical test suite for random and pseudorandom number generators for cryptographic applications. NIST Special Publication 800-22. 2001. 152 p.
2. Аладьев В.З. Классические однородные структуры. Клеточные автоматы. Fultus, 2009. 535 с.

3. Ершов Н.М. Клеточные автоматы. М.: ВМК МГУ, 2011. 16 с.
4. Коноплева А.П., Аноприенко А.Я. Клеточные автоматы в историческом контексте и их классификация. *Информатика и компьютерные технологии*. 2009. №7. С. 322-328.
5. Wolfram Stephen A New Kind of Science. USA.: Wolfram Media, 2002. 1192 p.
6. Аноприенко А.Я., Коноплёва А.П., Плотников Д.Ю., Малёванный Е.Ф. Применение клеточных автоматов для моделирования динамических процессов: опыт ДОННТУ. *Моделювання та комп'ютерна графіка*, матеріали IV Міжнар. конф., 5-8 жовтня 2011, Донецьк. С. 271-278.
7. Жуков А.Е. Клеточные автоматы в криптографии. Часть 1. *Вопросы кибербезопасности*. 2017. №3. С. 70-76.
8. Жуков А.Е. Клеточные автоматы в криптографии. Часть 2. *Вопросы кибербезопасности*. 2017. №4. С. 47-66.
9. Балк Е.А., Ключарёв П.Г. Исследование характеристик лавинного эффекта обобщенных клеточных автоматов на основе графов малого диаметра. *Наука и Образование*. 2016. №4. С. 92-105.
10. Сухинин Б.М. Разработка генераторов псевдослучайных двоичных последовательностей на основе клеточных автоматов. *Наука и образование* . 2010. №9. 21 с.
11. Мухамеджанов Д.Д., Левина А.Б. Генератор псевдослучайных чисел на основе клеточных автоматов. *Научно-технический вестник информационных технологий, механики и оптики*. 2018. Т.18, №5. С.894–899.

РАЗРАБОТКА ГЕНЕРАТОРА ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ НА ОСНОВЕ КЛЕТОЧНЫХ АВТОМАТОВ

Л.В. Дранишников., Р.Е. Бирюков

Днепровский государственный технический университет,
ул. Днепростроевская 2, Каменское, 51918, Украина: e-mail: dr-leon@ukr.net

Разработаны алгоритмы генерации псевдослучайных чисел, основанные на свойствах клеточных автоматов, которые имеют высокую скорость вычислений. Методы исследования базируются на использовании теории клеточных автоматов и объектно-ориентированного подхода. Алгоритм работы генератора псевдослучайных двоичных последовательностей включает в себя фазы инициализации, холостого хода и генерации. В работе были разработаны алгоритмы генераторов псевдослучайных чисел на основе классических, неоднородных и самопрограммируемых клеточных автоматов. Было проведено исследование характеристик лавинного эффекта клеточных автоматов. С применением языка программирования Python и объектно-ориентированного подхода было разработано программное обеспечение, которое использует аппарат клеточных автоматов для генерации псевдослучайных двоичных последовательностей. Полученные выходные последовательности разработанных генераторов прошли ряд статистических тестов статистических пакетов NIST и RaBiGeTe. Было показано приближение свойств полученных исходных последовательностей к случайным. Было проведено тестирование быстродействия разработанных генераторов. Практическая ценность полученных результатов. Разработанные алгоритмы генераторов псевдослучайных последовательностей на основе клеточных автоматов имеют лучшее быстродействие чем существующие аналоги, а также имеют статистические характеристики исходных последовательностей, приближающихся к статистических показателей случайных. Возможные направления развития или продолжения исследования: направлением продолжения исследования является поиск лучших конфигураций клеточных автоматов в составе генераторов псевдослучайных последовательностей, повышение быстродействия разработанных алгоритмов посредством реализации по принципу параллельных вычислений, физическая реализация разработанных алгоритмов на программируемой логической интегральной схеме, разработка алгоритмов шифрования на основе клеточных автоматов.

Ключевые слова: генератор псевдослучайных чисел, клеточный автомат, лавинный эффект, криптография.

DEVELOPMENT OF A CELLULAR AUTOMATON BASED PSEUDORANDOM NUMBER GENERATOR

L.V. Dranishnikov, R.E. Biryukov

Dnieper State Technical University,
Dniprobudivs'ka St 2 Kamianske, 51918, Ukraine; e-mail: dr-leon@ukr.net

Algorithms of pseudo-random number generation based on properties of the cellular automaton were developed that demonstrate a high speed of computation. Methods of research were based on the theory of the cellular automaton with an object-oriented approach. The algorithm of the pseudo-random binary sequence generator includes phases of initialization, dry pass and generation. Developed algorithms for pseudorandom number generation are based on classical, inhomogeneous, and self-programmable cellular automaton. A study was carried out of characteristics of avalanche effect in the cellular automaton. Using Python programming language and an object-oriented approach, software was developed that uses a cellular automaton machine to generate pseudorandom binary sequences. The resulting output sequences of the developed generators passed a variety of tests of statistical packages NIST and RaBiGeTe. It was shown that the properties of obtained initial sequences are approximated to random. The speed of the developed generators was tested as well as practical value of the results. Developed algorithms for pseudorandom sequence generators based on cellular automaton has better performance than existing analogs, and their statistical characteristics of the output sequences are approaching the ones of true random. Possible directions for the development or research are: better configurations of cellular automaton as part of pseudorandom sequence generators, increasing the speed of the developed algorithms by means of parallel computing, physical implementation of the developed algorithms on a programmable logic integrated circuit, development of encryption algorithms based on cellular automaton.

Keywords: pseudorandom number generator, cellular automaton, avalanche effect, cryptography.