# Статистичне дослідження генераторів випадкових чисел

М.В. Семаньків
кафедра інформатики
Прикарпатський національний університет
імені Василя Стефаника
Івано-Франківськ, Україна
dlyamarii@gmail.com

# The statistical study of random number generators

M. Semankiv
Department of Computer Science
Vasyl Stefanyk Precarpathian
National University
Ivano-Frankivsk, Ukraine
dlyamarii@gmail.com

***Анотація*—Проведено аналіз існуючих пакетів статистичних досліджень, визначено їх переваги та недоліки. Подано результати дослідження послідовності псевдовипадкових чисел, яка сформована методом Галуа на основі циклічних зсувів, проведеного за допомогою пакету RaBiGeTe.**

***Abstract*—Analysis of existing packages statistical studies are done, their advantages and disadvantages are listed. Results of research on the package RaBiGeTe sequence of random numbers, which is formed by Galois through cyclic shifts, are submitted.**

***Ключові слова—генератор випадкових чисел, RaBiGeTe***

***Keywords—random number generator, RaBiGeTe***

## I. Вступ

Для реалізації методу аналого-цифрового перетворення Монте-Карло необхідно застосовувати генератори випадкових значень опорних сигналів, перед якими ставляться вимоги простоти реалізації та забезпечення рівномірності розподілу генерованих чисел. Саме рівномірність розподілів впливає на точність перетворення для даного методу аналог-цифрового перетворення. На основі аналізу складності технічної реалізації методів псевдовипадкового генерування як один із ефективних запропоновано метод на базі використанням незвідних поліномів над полем Галуа [1]. Запропонований спосіб генерування псевдовипадкових чисел Галуа на основі циклічних зсувів легко реалізується програмно і апаратно. Постало питання визначення статистичних характеристик за допомогою потужного пакету статистичних досліджень, що дозволив би оцінити якість розподілу генерованих вказаним методом послідовностей псевдовипадкових чисел.

## II. Аналіз програм для статистичного аналізу випадкових чисел

На сьогоднішній день запропоновано безліч методів тестування псевдовипадкових послідовностей. Умовно всі методи тестування генераторів випадкових чисел можна розділити на три групи: евристичні, графічні і статистичні [2]. До евристичних тестів належать: перевірка швидкості формування чисел, перевірка періоду, тест на точність визначення деяких констант методом Монте-Карло, перевірка на криптостійкість. 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. Для встановлення чисельної оцінки якості послідовностей використовують статистичні тести. Статистичні тести за звичай об'єднуються в пакети тестування (серед них можна виділити тести DIEHARD, NIST STS, PractRand, testu01, RaBiGeTe та ін.) [3].

Серед відомих слід відзначити тести Д.Кнута, для яких характерні швидкі алгоритми виконання але невизначеність у трактуванні результатів, зокрема відсутня програмна реалізація. Тести DIEHARD є найбільш строгими з відомих, проте для них нема детального опису тестів і методики трактування їх результатів, крім того більшість тестів є евристичними. Великої популярності

набув пакет статичних тестів NIST STS, проте він має незручний для використання інтерфейс. При використанні програм PractRand і testu01 найлегше за все інтерпретувати висновок. PractRand і Dieharder, як правило, найпростіші для автоматизації тестування за допомогою інтерфейсу командного рядка. PractRand і RaBiGeTe були єдиними, що здійснюють підтримку багатопотокового тестування. RaBiGeTe і NIST STS обидва мають наочні інтерфейси.

RaBiGeTe враховуючи недоліки попередніх пакетів статистичних досліджень включила в себе основні тести вказаних пакетів [4]. Програма включає 24 тести, в склад яких потрапили вибрані тести пакетів NIST DFT, Diehard, тести Д.Кнута, Маурера та додаткові статистичні тести. Користувач надає двійковий файл з генерованими числами та змінює параметри тестування в залежності від потреб. RaBiGeTe має зручний інтерфейс та надає можливості налаштування параметрів тестування, отримані результати подаються у чисельному та графічному вигляді. Зазначені переваги стали причиною вибору даного програмного продукту для статичного аналізу послідовностей псевдовипадкових чисел, що утворені методом Галуа на основі циклічних зсувів.

## III. Результати дослідження генератора Галуа

Програма RaBiGeTe містить шість закладок: Parameters (Параметри тестів), Table (Таблиця), Pearson (Пірсон), Graph (Графік), Messages (Повідомлення), Preferences (Налаштування).

- Параметри сторінки: здійснення налаштування випробувань, а саме включення тестів, зміна параметрів тестування, довжини послідовності, кількості послідовностей для тестування і т.д.
- Таблиця: показує хід виконання тесту і відображення числових результатів ("KC" – тест Колмогорова-Смірнова, "AD" – Андерсона-Дарлінга і "Bino" – біноміальний тест. pvals: кількість дійсних p-значень. pv min: найменше p-значення в рядку. pv max: найбільше p-значення в рядку).

BiGeTe_MT 32 bits - v2.0.0 - Cristiano fecit a. D. MMXI

| | Test | pvals | KS | AD | Bino | pv min | pv max | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| KS | | 355 | 0.5911 | 0.9420 | | | | | | | |
| AD | | 355 | 0.5877 | 0.8678 | | | | | | | |
| Bino | | 355 | 0.9927 | 0.9969 | | | | | | | |
| 1 | AMLS 2 | 50 | 0.1078 | 0.0105 | 0.0125 | 0.0021 | 0.9861 | 0.9770 | 0.0811 | 0.9698 | 0.3861 |
| 2 | AMLS 4 | 50 | 0.0455 | 0.1227 | 0.6638 | 0.0219 | 0.9979 | 0.4434 | 0.1059 | 0.7661 | 0.7146 |
| 3 | AMLS 8 | 50 | 0.2985 | 0.2029 | 0.8441 | 9e-004 | 0.9083 | 0.2820 | 0.2212 | 0.6482 | 0.9083 |
| 4 | AMLS 16 | 50 | 0.3390 | 0.3472 | 0.8599 | 0.0089 | 0.9909 | 0.7429 | 0.8235 | 0.1530 | 0.1686 |
| 5 | AMLS 32 | 50 | 0.8384 | 0.6531 | 0.8922 | 0.0409 | 0.9467 | 0.2319 | 0.8060 | 0.9290 | 0.4923 |
| 6 | AMLS 64 | 50 | 0.5227 | 0.7056 | 0.9927 | 0.0277 | 0.9917 | 0.5161 | 0.6557 | 0.4682 | 0.6053 |
| 7 | AMLS 128 | 50 | 0.8882 | 0.8755 | 0.9995 | 0.0074 | 0.9706 | 0.0249 | 0.2462 | 0.4910 | 0.8908 |
| 8 | BGdst 2 | 50 | 0.1423 | 0.0859 | 0.3155 | 0.0024 | 0.9960 | 0.7139 | 0.0050 | 0.1947 | 0.0024 |
| 9 | BGdst 4 | 50 | 0.4030 | 0.3672 | 0.6295 | 0.0805 | 0.9912 | 0.1993 | 0.7765 | 0.4544 | 0.3010 |
| 10 | BGdst 6 | 50 | 0.7139 | 0.7362 | 0.9883 | 0.0047 | 0.9988 | 0.2143 | 0.3637 | 0.5661 | 0.8243 |

Рис. 1. Результат проходження тестів для методу Галуа на основі циклічних зсувів

- Пірсон: дані p-значень тесту Пірсона хі-квадрат.
- Графік: подання на графіку розподілу упорядкованих p-значень, отриманих з кожного тесту; є дві точки (для KS і для AD) для результатів тестів з сторінки "Таблиця" і "Пірсон". Для якісного генератора випадкових чисел точки не повинні бути занадто далеко від чорної «ідеальної» лінії, тобто наближатись до неї. «Числова відстань» від ідеальної лінії наведена в лівій частині сторінки, де у таблиці подано p-значення для деяких статистичних тестів.

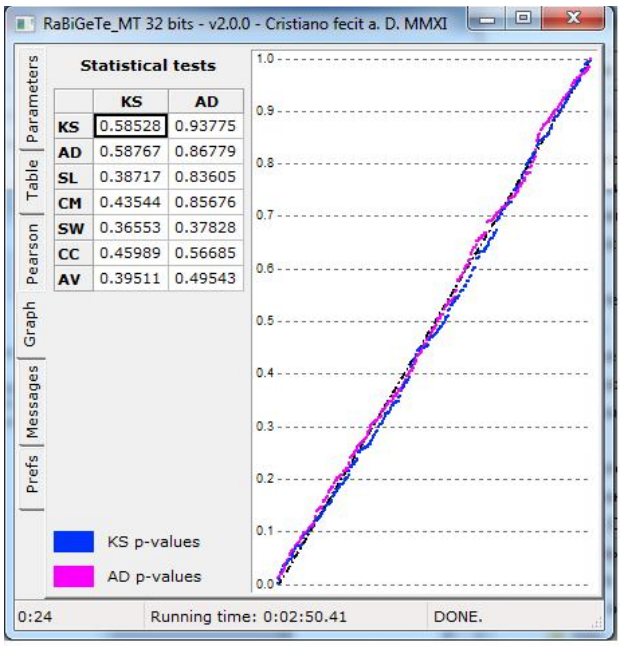


Рис. 2. Розподіл p-значень для методу Гаула на основі циклічних зсувів

- Повідомлення: відображення будь-якого виду повідомлення (інформація про попередження і помилки).
- Налаштування: основні параметрів вибору тестів та порядку відображення результатів тестування.

## Висновки

Як показують наведені в на рис. 1 та рис. 2. результати, запропонований метод на основі циклічних зсувів дозволяє отримати послідовності псевдовипадкових чисел з досить високою статистичною якістю розподілу p-значень за результатами тестування RaBiGeTe і може бути використаний для побудови генератора псевдовипадкових чисел складі аналого-цифрового перетворювача Монте-Карло. Простота реалізації, низька вартість виготовлення та отриманні результати статичного дослідження визначають перспективу використання запропонованого генератора випадкових чисел для методу Монте-Карло.

## Література References


[1] Л.Б. Петришин, Теоретичні основи перетворення форми та цифрової обробки інформації, К.: ІЗіМН МОУ, 1997.

[2] М.А. Иванов, И.В. Чугунков, Теория, применение и оценка качества генераторов, М.: КУДИЦ-ОБРАЗ, 2003.

[3] М.В Лаврів, 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

[4] http://cristianopi.altervista.org/RaBiGeTe_MT/