УДК 681.32

В. П. Семеренко
О. О. Гудименко

ДОСЛІДЖЕННЯ МАТЕМАТИЧНИХ ВЛАСТИВОСТЕЙ ЛІНІЙНИХ КОНГРУЕНТНИХ ГЕНЕРАТОРІВ

Вінницький національний технічний університет

Анотація

Запропоновано використати для опису лінійних конгруентних генераторів теорію лінійних послідовнісних схем в кінцевих полях Галуа. Проведено дослідження довжин періодів псевдовипадкових послідовностей чисел, які генерують різні типи конгруентних генераторів.

Ключові слова: *лінійний конгруентний генератор, поля Галуа, лінійна послідовнісна схема*.

Abstract

The theory of the linear finite-state machine (LFSM) to describe a linear congruential generators is suggested. The lengths of periods of pseudo-random sequences which are produced of different types of congruential generators are investigated.

Keywords: *linear congruential generator, Galois fields, linear finite-state machine*.

Випадкові числа використовуються давно та в різних сферах: в комп'ютерному моделюванні, криптографії, в системах прийняття рішень та різноманітних іграх.

Генератори псевдовипадкових чисел можуть працювати по різних алгоритмах. Одним з найпростіших генераторів є лінійний конгруентний генератор (ЛКГ), який формує числа за формулою

$$x_{i+1} = (a \times x_i + b) \bmod m, \qquad (1)$$

де a, b, m – цілочислові константи, x_i та x_{i+1} – попереднє та наступне число псевдовипадкової послідовності ($i = 1, 2, 3, \dots$), x_0 – початкове значення (зародок, *seed*).

Хоча ЛКГ і не властива висока криптостійкість, він широко використовується, зокрема в бібліотеках компіляторів різних мов програмування та є перспективним для засобів малоресурсної криптографії [1].

Незважаючи на багаторічні дослідження, поки що відсутні чіткі правила для отримання довгої та статистично хорошої послідовності чисел ЛКГ. До цього часу головною теоретичною основою ЛКГ залишається теорема з відомої монографії Д. Кнута [2] про вибір констант a, b, m.

Проведемо дослідження властивостей ЛКГ з позицій кінцевих полів Галуа. Як відомо, кінцеві поля Галуа $GF(m)$ існують лише в тому випадку, якщо кількість елементів m поля є простим числом, або степенем простого числа [3]. В цьому випадку операції додавання та множення в полі $GF(m)$ є відповідно додаванням та множенням за модулем m.

Таким чином, якщо константа m буде простим числом (а не взаємно простим числом відносно інших констант, як у [2]), тоді аналогом формули (1) буде функція станів (переходів), яка описує функціонування лінійної послідовнісної схеми в полі $GF(m)$ [4]:

$$S(t+1) = A \times S(t) + B \times U(t), \quad GF(m). \qquad (2)$$

Формули (1) і (2) реалізують примітивно-рекурсивну функцію з одним змінним параметром: час t для ЛПС і x_i для ЛКГ. При правильному виборі констант в (1) ЛКГ буде генерувати достатньо довгу і статистично хорошу послідовність чисел, аналогічну М-послідовності для ЛПС.

Оскільки ЛПС є кінцевим автоматом, тому її автоматно-графову модель можна використати для аналізу властивостей як ЛПС, так і ЛКГ [5]. Якщо ЛПС генерує псевдовипадкову послідовність максимальної довжини $2^r - 1$ (М-послідовність), тоді її графова модель містить основний нульовий цикл із $2^r - 1$ вершин та тривіальний нульовий цикл із одної вершини.

Відносно ЛКГ це означатиме наявність як періоду максимальної довжини $m-1$, так і наявність періоду одиничної довжини, коли ЛКГ буде видавати лише одне число. Така ситуація буде можливою, якщо існує цілочислове значення виразу

$$\left(\frac{b}{1-a}\right)\bmod m,$$

і воно буде обрано зародком псевдовипадкової послідовності.

Аналізуючи різні співвідношення між константами a, b, m можна побудувати відповідні графові моделі і визначити довжини псевдовипадкових послідовностей та їх статистичні властивості.

На основі запропонованого підходу можна провести аналіз також інших видів генераторів чисел:

– мультиплікативного конгруентного генератора (якщо $b=0$),

– інверсного конгруентного генератора, який формує обернену псевдовипадкову послідовность.

Останній вид генератора вимагає наявності оберненого елемента, який можливий лише в полях Галуа [6], отже для функціонування такого генератора можна використати темпоральні моделі [7].

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Семеренко В. П. Дослідження примітивів малоресурсної криптографії / В. П. Семеренко. // Інформаційні технології та комп'ютерне моделювання : матеріали статей Міжнародної науково-практичної конференції, м. І-Франківськ, 23 – 28 травня, 2016. – І-Франківськ, 2016. – С. 123–127.
2. Кнут Д. Искусство программирования, том 2. Получисленные алгоритмы. / Д. Кнут. – Изд. 3-е ; пер. с англ. – М. : Издательский дом «Вильямс», 2007. – 832 с.
3. Кларк Дж., мл. Кодирование с исправлением ошибок в системах цифровой связи / Дж. Кларк мл., Дж. Кейн ; пер. с англ. – М. : Радио и связь, 1987. – 392 с.
4. Гилл А. Линейные последовательностные машины / А. Гилл ; пер. с англ. – М. : Наука, 1974. – 288 с.
5. Семеренко В. П. Теорія циклічних кодів на основі автоматних моделей : монографія / В. П. Семеренко. – Вінниця : ВНТУ, 2015. – 444 с
6. Блейхут Р. Теория и практика кодов, контролирующих ошибки / Р. Блейхут ; пер. с англ. – М. : Мир, 1986. – 576 с.
7. Семеренко В. П. Темпоральные модели параллельных вычислений / В. П. Семеренко // Austrian Journal of Technical and Natural Sciences. – 2014. – Vol. 1. – P. 13–25.

Василь Петрович Семеренко – канд. техн. наук, доцент, кафедра обчислювальної техніки, Вінницький національний технічний університет, Вінниця, e-mail: vasilsemerenko@gmail.com

Олександр Олександрович Гудименко – студент групи 1КІ-14б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: ogelcast@gmail.com

Vasyl P. Semerenko – PhD, Associate Professor, Department of computer technique, Vinnytsia National Technical University, Vinnytsia, , e-mail: vasilsemerenko@gmail.com

Oleksandr O. Gudymenko – student, Department of computer technique, Vinnytsia National Technical University, Vinnytsia, e-mail: ogelcast@gmail.com