Министерство образования и науки Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ Н. Г. ЧЕРНЫШЕВСКОГО»

Кафедра дискретной математики и
информационных технологий

ЛИНЕЙНАЯ СЛОЖНОСТЬ ЭРГОДИЧЕСКИХ СОВМЕСТИМЫХ ФУНКЦИЙ И ГЕНЕРАТОРЫ ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

студента 4 курса 421 группы
направления 09.03.01 — Информатика и вычислительная техника
факультета КНиИТ
Щеголева Александра Владимировича

Научный руководитель
к.ф.-м.н., доцент _____ Л. Б. Тяпаев

Заведующий кафедрой
к.ф.-м.н., доцент _____ Л. Б. Тяпаев

Саратов 2018

ВВЕДЕНИЕ

Генераторы псевдослучайных чисел широко используются в численных приложениях, особенно при компьютерном моделировании (например, в методе квази-Монте Карло) и криптографии (например, в поточных шифраторах). В криптографии такие генераторы производят последовательности, которые кажутся случайными. Построение последовательностей именно случайных величин опирается на предположения что, во-первых, имеется компьютер, который умеет работать с действительными числами, а во-вторых, имеется генератор, который умеет генерировать равномерно распределенную последовательность на отрезке $[0, 1]$ [1]. Тем не менее, вопрос о том, как получить из равномерно распределенной последовательности последовательность случайных величин с заданным распределением весьма актуален. Иногда под «случайной последовательностью» понимается, на самом деле, псевдослучайная последовательность [2].

Работа содержит в себе пять разделов:

1. Генераторы псевдослучайных чисел
2. Элементы p-адического анализа
3. Автоматные отображения
4. Линейная сложность
5. Реализация графиков отображения

Целью данной работы является экспериментальное наблюдение линейной сложности последовательности, порождаемой с помощью эргодического совместимого преобразования пространства целых p-адических чисел. Для достижения этой цели возникает задача создания приложения, способного строить проекции данных преобразований в единичном квадрате евклидовой плоскости. Данное приложение позволит получить информацию о распределении орбит динамических систем в фазовом пространстве целых p-адических чисел. Эта информация важна как для понимания эргодической динамики, так и для приложений: при синтезе поточных шифраторов (для генераторов псевдослучайных чисел) и в теории автоматов.

Разработанное приложение должно быть универсальным (необходим запуск под различные операционные системы), быстрым и предоставлять пользователю возможность самостоятельного ввода функции.

1 Основное содержание работы

В первом разделе описывается принцип работы и основные характеристики генераторов псевдослучайных чисел. При поточном шифровании псевдослучайная последовательность (гамма) генерируется с помощью автономного автомата $A = (\mathbb{X}, \mathbb{Y}, f, g)$ с конечным числом внутренних состояний. Функция переходов такого автомата $f\colon \mathbb{X} \to \mathbb{X}$, где $\mathbb{X} = \{0,1\}^n$, каждому состоянию x_i ставит в соответствие состояние x_{i+1}; начальное состояние x_0 — секретный ключ, а последовательность

$$x_0, x_1 = f(x_0), x_2 = f(x_1), \ldots, x_{i+1} = f(x_i), \ldots$$

есть траектория ключа, возникающая в результате итерирования функции переходов f. Функция выходов $g\colon \mathbb{X} \to \mathbb{Y}$, где $\mathbb{Y} = \{0,1\}^m$, каждому состоянию x_i (строке из n бит) ставит в соответствие выходной сигнал y_i (строку из m бит). Таким образом, возникает последовательность

$$y_0 = g(x_0), y_1 = g(x_1), \ldots, y_i = g(x_i), \ldots,$$

которая играет роль гаммы.

Так как множество состояний $\mathbb{X}$ конечно, то выходная последовательность обязательно будет в конечном счете периодической. Заметим, что выходная последовательность зависит от начального состояния x_0. Таким образом, псевдослучайный генератор можно рассматривать как отображение из $\mathbb{X}$ на множество всех периодических последовательностей над $\mathbb{Y}$.

Генератор гаммы должен удовлетворять следующим требованиям [3]

1. Псевдослучайность: функция переходов f должна обеспечить псевдослучайность, в частности, равномерное распределение и максимальную длину периода последовательности состояний.
2. Стойкость: функция выходов g должна обеспечивать псевдослучайность выходной последовательности — равномерное распределение и длинный период. Более того, для данного y_i нахождение x_i из уравнения $y_i = g(x_i)$ должно быть вычислительно сложной задачей.
3. Быстродействие: для программной реализации генератора функции f и g должны быть простыми композициями элементарных арифметических и поразрядных логических операций.

Для выполнения этих требований требуются использовать методы p-адического анализа и неархимедовой динамики: функция переходов генератора должна быть эргодической на пространстве целых p-адических чисел, а функция выходов — сохранять меру.

Во втором разделе работы вводятся важные понятия, используемые в работе в дальнейшем, такие как p-адические числа, целые p-адические числа, кольцо, поле, норма кольцо целых p-адических чисел, 1-Липшицевы функции.

Кроме того, описывается способ построения проекций преобразований кольца $\mathbb{Z}/p^k\mathbb{Z}$ в евклидовом единичном квадрате. Отображение $f : \mathbb{Z}_p \to \mathbb{Z}_p$ можно изучать с помощью, так называемого, «графика». Пусть для $k = 1, 2, \ldots$ множество $E_k(f)$ есть множество точек $e_k^f(x)$ единичного квадрата $[0,1] \times [0,1] \subset \mathbb{R}^2$ вида:

$$e_k^f(x) = \left(\frac{x \mod p^k}{p^k}, \frac{F(x) \mod p^k}{p^k} \right), x \in \mathbb{Z}_p,$$

где $x = \ldots x_k x_{k-1} \ldots x_1 x_0 \in \mathbb{Z}_p$, ставится в соответствие элемент кольца вычетов по модулю p_k (так называемая редукция по модулю p_k): $x \mod p^k = x_{k-1} \ldots x_1 x_0 \in \mathbb{Z}/p^k\mathbb{Z}$. Образ отображения $f(x) \in \mathbb{Z}_p$ заменяется своей редукцией по модулю p_k: $f(x) \mod p^k \in \mathbb{Z}/p^k\mathbb{Z}$; затем редукции $x \mod p^k f(x) \mod p^k$ (неотрицательные целые, не превосходящие p^k) делятся на p^k (тем самым, становятся точками отрезка $[0,1]$).

Графиком такого отображения в евклидовом квадарате будет замыкание в топологии действительной плоскости всех полученных точек. Строго говоря, полученный результат будет не графиком — наиболее точным будет его определение как проекция p-адического графика на наш реальный мир.

Данные «графики» представляют собой различные геометрические структуры: прямые линии, параболы, фракталы, полосы и т.д. Более того, некоторые из этих «графиков» сильно зависят от n. Полученная при построении такого «графика» информация, иногда имеет важное значение, например, когда вы собираетесь использовать функцию f как функцию перехода состояния псевдослучайных генераторов, так как упомянутый «график» отражает статистическое качество созданной последовательности. Кроме того, такой «график» предоставляет информацию о поведении соответствующих

автоматов.

В третьем разделе определяются такие понятия как автомат, автоматные отображения и динамические системы. Генератор псевдослучайных чисел можно мыслить как динамическую систему в фазовом пространстве целых p-адических чисел: функция переходов является функцией динамики, а порождаемая генератором последовательность является т.н. наблюдаемой последовательностью.

В четвертом разделе вводится понятие линейной сложности. Лилейная сложность является характеристикой псевдослучайной последовательности.

Определение. Пусть $Z = (z_i)_{i=0}^{\infty}$ – последовательность над коммутативным кольцом R. *Линейной сложностью* $\lambda_R(Z)$ последовательности Z над R называют наименьшее $r \in \mathbb{N}$ такое, что существуют $c, c_0, c_1, \ldots, c_{r-1} \in R$ (не все равные 0) такие, что для всех $i = 0, 1, 2, \ldots$ выполняется:

$$c + \sum_{j=0}^{r-1} c_j \cdot z_{i+j} = 0 \tag{1.1}$$

Говорят, что $\lambda_R(Z) = \infty$, если такого r не существует. Линейную сложность еще можно определить как размерность регистра сдвига с линейной обратной связью (РСЛОС) [13]. Понятие линейной сложности имеет геометрическую интерпретацию. Например, если $R = \mathbb{Z}/p^k\mathbb{Z}$ есть кольцо вычетов по модулю p^k, то геометрически $\lambda_R(Z)$ означает, что все точки с координатами $(\frac{x_i}{p^k}, \frac{x_{i+1}}{p^k}, \ldots, \frac{x_{i+r-1}}{p^k})$, $i = 0, 1, 2, \ldots$ единичного гиперкуба (размерности r) лежат на параллельных гиперплоскостях [3].

В криптографическом ракурсе нас интересует линейная сложность последовательности, генерируемой отображением $f : \mathbb{Z}_p \to \mathbb{Z}_p$ при $p = 2$.

Следует заметить, что мы используем понятие линейной сложности последовательности над кольцом в несколько более широком смысле, чем оно обычно используется. Чаще линейная сложность последовательности (x_n) элементов коммутативного кольца R понимается как наименьшее $r > 0$ такое, что существуют $c_0, \ldots, c_{r-1} \in R$, которые одновременно удовлетворяют всем уравнениям $x_{n+r} = \sum_{j=0}^{r-1} c_j x_{n+j}$ для $n = 0, 1, 2, \ldots$. В данной работе мы рассматриваем неоднородные отношения (т.е. с ненулевым постоянным коэффициентом), а также отношения, где все коэффициенты могут быть делителями нуля (однако, не все 0 одновременно).

Если R — поле, то оба понятия практически не отличаются друг от друга: если последовательность удовлетворяет соотношению $c + \sum_{i=0}^{r} c_i x_{n+i}$, где $c_r \neq 0$, то тогда она удовлетворяет и соотношению $x_{n+r+1} = c_r^{-1} c_0 x_n - \sum_{j=0}^{r-1} c_r^{-1}(c_j - c_{j+1}) x_{n+j+1}$. Наше определение является более удобным для геометрических интерпретаций.

К примеру, если $R = \mathbb{Z}/p^k\mathbb{Z}$, то тогда геометрически уравнение 1.1 означает, что все точки $(\frac{z_i}{p^k}, \frac{z_{i+1}}{p^k}, \ldots, \frac{z_{i+r-1}}{p^k}), i = 0, 1, 2, \ldots$ единичного r-мерного евклидова гиперкуба лежат на параллельных гиперплоскостях. С учетом 1-Липшецового эргодического преобразования f на $\mathbb{Z}_p$ и линейной сложности кольца вычетов $\mathbb{Z}/p^k\mathbb{Z}$ мы можем изучать распределение последовательности $(f^i(x))_{i=0}^{\infty}$ взятой по модулю p^k. Независимо от того, какое конкретно преобразование f рассматривается, эта последовательность является строго равномерно распределенной как последовательность элементов из $\mathbb{Z}/p^k\mathbb{Z}$. Длина наименьшего периода есть p^k, и каждый элемент из $\mathbb{Z}/p^k\mathbb{Z}$ встречается в периоде ровно один раз.

Однако распределение последовательных пар элементов в этой последовательности изменяется в зависимости от f. Например, хотя каждая орбита эргодического преобразования $f(x) = a + bx$ на $\mathbb{Z}_p$ строго равномерно распределена по модулю p^n для всех $n \in \mathbb{N}$, линейная сложность орбиты над $\mathbb{Z}/p^k\mathbb{Z}$ равна 2.

Следовательно, точки, соответствующие парам последовательных вычетов, попадают в небольшое число параллельных прямых в единичном квадрате (рис. 1.1), и получившийся «график» не зависит от k.

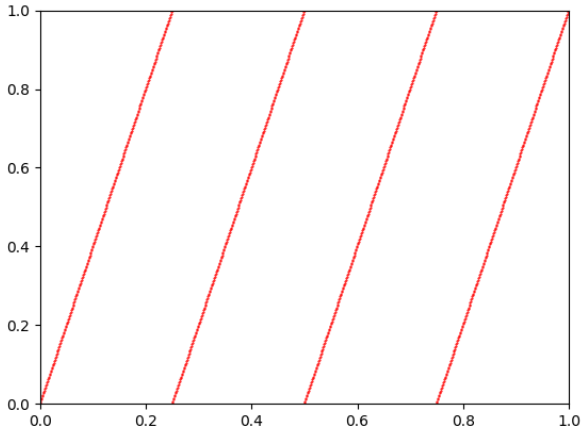

Рисунок 1.1 – $f(x) = 3 + 4x, p = 2$

В пятом разделе описывается процесс построения графиков отображения посредством компьютерной программы. Приложение для построение графиков было написано на языке Python 3.6.3 [15–17]. Для отображения графиков была использована библиотека бибилитека Matplotlib версии 2.2.2 [18], для создания интерфейса программы — PyQT5 версии 5.10.1 [19–21].

Алгоритм работы программы состоит из следующих этапов:

1. Проверка введенного p. Оно должно быть простым числом. Если p не введено, не является числом или явялется составным числом, то выдать сообщение об ошибке и прекратить дальнейшее выполнение алгоритма
2. Проверка введенного n. Если p не введено или не является числом, то выдать сообщение об ошибке и прекратить дальнейшее выполнение алгоритма
3. Проверка введенной функции. Она должна соответствовать следующим критериям:
   а) Являться композицией логических и арифметических операций над x
   б) Операция умножения обозначается как $*$
   в) Рациональные коэффициенты задаются как функция $r(prefix, period)$, где $prefix$ — начальная последовательность нулей и единиц в 2-адическом представлении этого числа, а $period$ — повторяющийся период. Например,

$$\frac{1}{3} = \ldots 010101011 = \ldots 010101 \underbrace{01}_{\text{период}} \underbrace{1}_{\text{префикс}}$$

   Таким образом, число $\frac{1}{3}$ вводится следующим образом: $r(1, 01)$.
   г) Порядок выполнения действий должен обозначаться скобками

   Если какой-либо из критериев не выполнен, то выдать сообщение об ошибке и прекратить дальнейшее выполнение алгоритма
4. По нажатию на кнопку «Построить» для каждого x из интервала $(0, 1, 2, \ldots, p^n - 1)$ внести в массивы абсцисс и ординат координаты точки

$$e(x) = \left(\frac{x \mod p^n}{p^n}, \frac{F(x) \mod p^n}{p^n} \right),$$

   где $F(x)$ — введенная функция

5. Построить график на основе массивов абсцисс и ординат
6. Если после построения пользователь изменяет положение слайдера, то соответственно изменить размеры каждой точки графика
7. По нажатию на кнопку «Сохранить» сохранить построенный график по указанному пользователем пути

ЗАКЛЮЧЕНИЕ

Важным свойством генераторов псевдослучайных чисел является линейная сложность порождаемых последовательностей. В частности, для полиномиальных генераторов степени не меньше 2 известно, что линейная сложность стремится к бесконечности с ростом степени полинома. Интерес представляют генераторы, ассоциированные с эргодическими динамическими системами на фазовом пространстве целых p-адических чисел. Свойство эргодичности характеризует равномерное распределение орбит таких динамических систем, но эргодичность никак не отражается на графиках этих отображений. Тем не менее, визуализация позволяет экспериментально наблюдать линейную сложность для некоторых, в том числе эргодических преобразований.

Однако, остается открытым вопрос о скорости роста линейной сложности последовательности, порожденной эргодическим полиномом.

В процессе выполнения работы было создано компьютерное приложение, позволяющее строить графики совместимых функций в единичном квадрате евклидовой плоскости. Данное приложение может работать с высокими степенями n (до $n = 23$ включительно). Кроме того, программа универсальна: ее запуск в неизмененном виде возможен на различных операционных системах (Windows, OS X, Linux). Цель выпускной квалификационной работы достигнута.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Devroy L. Non-Uniform Random Variate Generation. — Springer, 1986, 695 с.

2 Кнут Д. Искусство программирования. Том 2. Получисленные алгоритмы. — Addison Wesley Longman, Inc., Вильямс, 2000, 832 с.

3 Anashin V.S., Khrennikov A.Yu. Applied Algebraic Dynamics. — De Gruyter, Берлин – Нью-Йорк, 2009, 533 с.

4 Каток С.Б. P-адический анализ в сравнении с вещественным. — МЦНМО, 2004, 112 с.

5 Хренников А.Ю. Неархимедов анализ и его приложения. — ФИЗМАТЛИТ, 2003, 216 с.

6 Боревич З.И., Шафаревич И.Р. Теория чисел. 3-е изд. доп. — Наука. Главная редакция физико-математической литературы, 1985, 504 с.

7 Хренников А.Ю., Шелкович В.М. Современный p-адический анализ и математическая физика: теория и приложения — Физматлит, 2012, 452 с.

8 Коблиц Н. P-адические числа, P-адический анализ и дзета-функции. — Мир, 1982, 192 с.

9 Schikhof W.H. Ultrametric Calculus: An Introduction to p-Adic Analysis. — Cambridge University Press, 2007, 320 с.

10 Салий В.Н., Сагаева И.Д., Тяпаев Л.Б. Дискретная математика. Часть 1. — Lulu Publishing, 2013.

11 Ларин М. В. Транзитивные полиномиальные преобразования колец вычетов. — Дискретная математика, 2002, т. 14, выпуск 2, с. 20–32.

12 Григорчук Р.И., Некрашевич В.В., Сущанский В.И. Автоматы, динамические системы и группы. — Тр. МИАН, 2000, т. 231, с. 134–214.

13 Фомичёв В.М. Методы дискретной математики в криптологии. — ДИАЛОГ-МИФИ, 2010, 424 с.

14 Тяпаев Л.Б. Элементы алгебраической динамики. — Lulu Publishing, 2018.

15 Бизли Д. Python. Подробный справочник, 4-е издание. — Символ, 2010, 864 с.

16 The Python Tutorial — Python 3.6.3 documentation // Welcome to Python.org[Электронный ресурс] : сайт. URL: https://docs.python.org/3/tutorial/index.html (Дата обращения 02.05.2018) Загл. с экрана. Яз. англ.

17 Hellman D. The Python Standard Library by Example. — Addison-Wesley Professional, 2011, 1302 с.

18 Tutorials — Matplotlib 2.2.2 documentation[Электронный ресурс] : сайт. URL: https://matplotlib.org/2.2.2/tutorials/index.html (Дата обращения 02.05.2018) Загл. с экрана. Яз. англ.

19 PyQt 5.10.1 Reference Guide // SourceForge - Download, Develop and Publish Free Open Source Software [Электронный ресурс] : сайт. URL: http://pyqt.sourceforge.net/Docs/PyQt5/# (Дата обращения 02.05.2018) Загл. с экрана. Яз. англ.

20 Dalheimer M.K. Programming with Qt (2nd Edition). — O'Reilly Media, 2002, 512 с.

21 Summerfield M. Rapid GUI Programming with Python and Qt. — Prentice Hall, 2015, 625 с.