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

Сдвиги Бернуллиевского типа и *p*-адические функции, используемые в генераторах псевдослучайных чисел

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

студентки 4 курса 421 группы
направления 09.03.01 «Информатика и вычислительная техника»
факультета компьютерных наук и информационных технологий
Шешиной Ольги Владимировны

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

Зав. кафедрой
к. ф.-м.н., доцент _____ Л.Б. Тяпаев
подпись, дата

Саратов 2018

Введение. Тема данной работы мотивированна криптографическими задачами, в частности задачами синтеза стойких и сверхбыстрых поточных шифраторов. Как известно, поточное шифрование относятся к методам шифрования с закрытым ключом, см. [5]. В основе поточного шифрования лежит псевдослучайная последовательность (гамма), которая порождается с помощью специального генератора. Генератор гаммы суть автономный автомат, функция переходов которого есть преобразование кольца вычетов по модулю p^n (p - простое, n - натуральное), а функция выходов - сбалансированное отображение кольца вычетов по модулю степени p^n на кольцо вычетов по модулю степени p^m (m - натуральное). Начальное состояние генератора является секретным ключом. Начиная функционирование из этого начального состояния генератор такт за тактом порождает последовательности длины m каждая. Совокупность порождённых таким образом последовательностей образует искомую гамму.

Шифрование является совершенным тогда и только тогда, когда гамма есть случайная последовательность (согласно теоремам Шеннона и Котельникова), см., например, [5]. Можно ли построить быстрый алгоритм, который производит случайные числа (например, случайные бинарные строки)? Отрицательный ответ на данный вопрос следует из теоремы сложности Колмогорова [16]. Возникает следующий вопрос. Действительно ли нужна случайная гамма для обеспечения безопасности поточного шифрования? Если противник не может определить, является ли данная бинарная последовательность случайной или нет, то шифр следует считать защищённым от атак противника (идеальный шифр). В действительности противник может запустить только ограниченный набор T статистических тестов, чтобы определить, является ли гамма случайной или нет; и если гамма проходит все тесты из набора T, то шифр столь же безопасен от атак противника, как идеальный шифр. Таким образом, возникает задача построения быстрого алгоритма генерации гаммы, которая пройдет все тесты из набора T.

Например, как только T является множеством всех полиномиальных (по времени) тестов, алгоритм, который создает последовательности, которые проходят все эти тесты, называется псевдослучайным (в рамках теории сложности). В теории сложности доказано, что псевдослучайные генераторы существуют тогда и только тогда, когда существуют односторонние функции; существование односторонних функций означает, что существуют неразрешимые задачи (те, которые не могут быть решены за полиномиальное время). Однако сегодня никто не может доказать, что неразрешимые проблемы (а также, односторонние функции) существуют. Поэтому все "доказательства безопасности" в теории сложности условны.

Более того, хотя в теории сложности строятся генераторы, которые доказуемо псевдослучайны, при условии, что некоторые известные задачи (такие как задача факторизации натурального числа и проблема дискретного логарифмирования) действительно неразрешимы, эти генераторы слишком медленны, и поэтому их использование в шифрах очень ограничено. Таким образом, вышеуказанная проблема всё ещё остаётся открытой.

С начала 1990-х годов в криптографии проводились интенсивные исследования на основе теории хаоса. Действительно, если взять хаотическое отображение $f\colon [0,1] \to [0,1]$ вещественного отрезка [0,1] вещественной прямой $\mathbb{R}$ в себя, и взять значение функции с точностью 2^{-n}, то траектория, казалось бы, будет выглядеть случайной, поскольку отображение хаотично (т.е. траектория чувствительна к малым возмущениям начального состояния, т.е. ключа). Такой простой подход оказался довольно неутешительным: для дискретного аналога $x_{i+1} \equiv 2 \cdot x_i (mod\ 2^n)$ отображения $f(x) = 2 \cdot x\ mod\ 1$ (сдвига Бернулли), x_i становится равным 0 не более, через n итераций! Для дискретного аналога хаотического отображения $f(x) = 1 - 2\,|x - 1/2\,|$ (отображения "палатка"), заданного на отрезке $[0,1]$, все значения попадают на очень короткий цикл, не более длины n. Для дискретного аналога

логистического отображения $f(x) = \left(4 \cdot x \cdot (1-x)\right) mod\ 1$ значения функции становятся равными нулю через $\frac{n}{2}$ итераций!

Несмотря на огромное количество публикаций в области криптографии на основе хаоса, влияние этого исследования на традиционную криптографию весьма незначительно. Это объясняется двумя причинами: во-первых, почти все криптографические алгоритмы, основанные на хаосе, используют динамические системы, определенные на множестве действительных чисел, и поэтому для практической реализации сложны. Во-вторых, безопасность и эффективность почти всех предлагаемых хаотических методов не анализируются с точки зрения методов, разработанных в криптографии. Более того, большинство предлагаемых методов генерируют криптографически слабые и медленные алгоритмы [16].

Цифровые компьютеры абсолютно неспособны показать истинную динамику некоторых хаотических систем, включая отображение "палатка", сдвиг Бернулли и их аналоги, даже в высокоточной арифметике с плавающей запятой. Хотя результаты не могут быть напрямую обобщены на большинство хаотических систем, использование цифровых компьютеров для численного изучения непрерывной динамики рискованно [16].

Для обеспечения высокой стойкости и быстродействия поточного шифрования требуется использовать теорию неархимедовых динамических систем, в частности, p-адическую эргодическую теорию: функция переходов генератора должна быть эргодическим преобразованием кольца целых p-адических чисел, а функция выходов генератора должна сохранять меру Хаара [1, 10, 11, 16, 17, 18, 20, 21, 22].

Целью данной дипломной работы является изучение p-адических функций, p-адических аналогов сдвигов Бернуллиевского типа и генераторов псевдослучайных чисел (ПСГ), в которых они применяются. Для достижения цели работы необходимо решить следующие задачи:

1. изучить элементы p-адической эргодической теории;

2. изучить элементы математической теории генераторов псевдослучайных чисел;
3. изучить механизм сдвигов Бернулли и их p-адических аналогов;
4. реализовать программу для построения графиков p-адического аналога Бернуллиевского сдвига в единичном квадрате евклидовой плоскости на языке программирования Python 3.6.3.

Работа выполнена на 55 страницах машинописного текста, содержит введение, 6 разделов, 17 рисунков и одно приложение. Список источников содержит 23 наименования.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ.

В первом разделе "Представление информации в компьютере" описывается неархимедова математика. Даётся краткое представление о работе компьютера с информацией. В компьютере числа являют собой строчки, представленные в двоичном виде, то есть последовательностью нулей и единиц. Причём записываются они в порядке от младших разрядов к старшим, то есть справа налево. Любой человек скажет, что, например, последовательность из шестнадцати единиц есть число 65535 в системе исчисления с основанием 10 и будет прав. Однако в компьютере данная последовательность будет интерпретирована как минус единица (-1).

Дело в том, что компьютерная метрика является неархимедовой метрикой. То есть для неё не выполняется аксиома Архимеда, которая, например, для отрезков, гласит, что: если даны два отрезка, то отложив достаточное количество раз меньший из них, можно покрыть больший. То есть, если мы будем прибавлять к отрезку такой же отрезок сколько бы то ни было раз, в конечном итоге отрезок обязательно удлинится. Математические структуры, для которых свойство Архимеда выполняется, называются *архимедовыми*, например *архимедово поле* и *архимедова группа*, а те, для которых не выполняется, — *неархимедовыми* [12].

На множестве $\mathbb{Z}$ выполняется свойство: для любой тройки $a, b, c \in \mathbb{Z}$ справедливо неравенство

$$d_p(a, b) \leq \max\{d_p(a, c), d_p(c, b)\}.$$

Это свойство называется сильным неравенством треугольника, а метрика, удовлетворяющая ему, называется неархимедовой метрикой или ультраметрикой, см., например [12].

В разделе 2 "p-адические целые числа" даются основные определения и понятия из p-адической теории.

Элементы кольца Z_p называются *целыми p-адическими числами,* при $p \geq 2$, где p - простое число [2, 6, 7, 9, 10, 12, 13, 16, 20]. В случае $p = 2$ будем говорить о кольце Z_2 2-адических чисел.

На самом деле мы рассматриваем бесконечную строчку $\ldots a_i a_{i-1} \ldots a_0$ над алфавитом $\{0, 1, \ldots, p-1\}$ как "представление в системе с основанием p" целого p-адического числа a:

$$a = \ldots a_i a_{i-1} \ldots a_0 = \sum_{i=0}^{\infty} a_i \cdot p^i.$$

Это представление называется *каноническим.*

Отметим, что для $a, b \in \mathbb{Z}_p$ метрика на пространстве всех целых p −адических чисел всегда будет следующей:

$$d_p(a, b) = {}^{1}/_{p^i},$$

для подходящего $i = 0,1,2, \ldots, \infty$ (случай $i = \infty$ означает просто, что $d_p(a, b)$= 0, т.е., что $a = b$). Более того, $d_p(a, b) = p^{-i}$ тогда и только тогда, когда

$$a = \ldots a_i a_{i+1} c_{i-1} \ldots c_0;$$
$$b = \ldots b_i b_{i+1} c_{i-1} \ldots c_0,$$

и $a_i \neq b_i$.

Таким образом, расстояние между бесконечными 2-адическими числами зависит от длины их общего начала. Соответственно, оно либо равно 1, при $i = 0$, либо $1/2^i$, где i - это количество совпадающих начальных цифр.

В разделе 3 "T-функции" приводятся основные понятия и теоремы, связанные с совместимыми функциями.

T-функция - это отображение множества слов, длины n во множество слов той же длины, причём такое, что каждый новый i-ый бит образа зависит только от $(i+1)$ младших битов прообраза. Например, все арифметические операции (сложение, умножение) являются T-функциями, все поразрядные логические операции (такие как XOR, AND, и т.д.) также являются T-

функциями, т.е. все элементарные команды процессора, кроме циклических сдвигов и сдвигов в сторону младших разрядов, являются T-функциями.

T-функции, по сути, являются непрерывными 2-адическими отображениями [16]: T-функция может быть представлена как отображение не последовательности столбцов, а как последовательность бесконечных строк, если считывать строчку за строчкой сверху вниз, где под строчкой подразумевается бесконечная двоичная последовательность, то есть целое 2-адическое число. В p-адической математике T-функциями являются функции, удовлетворяющие условию Липшица с константой 1, т.е. *отображение является 1-Липшицевым в* $\mathbb{Z}_2$*, если:*

$$|f(a) - f(b)|_2 \leq |a - b|_2.$$

Функция, определенная и принимающая значения на элементах алгебраической системы называется *совместимой*, если она сохраняет все конгруэнции этой системы.

Так как все конгруэнции кольца Z_p являются отношениями сравнимости по модулю p^k при $k = 1, 2$,. , ., приходим к выводу, что T-функции являются совместимыми функциями на кольце $\mathbb{Z}_2$ и наоборот.

Криптографические примитивы на базе T-функций, их свойства (например, сбалансированность, равномерное распределение, высокая линейная сложность и т.д.), играют огромную роль в криптографии. Особенно успешно они используются для построения быстрых и стойких поточных шифров.

В разделе 4 "Псевдослучайные числовые последовательности" говорится о применении псевдослучайных последовательностей, а именно псевдослучайных генераторов (в частности - поточных шифраторах [14]). В этом разделе представлены элементы теории автоматов [3], а также даётся описание основных определений и понятий p-адической эргодической теории, на основе которой строятся хорошие ПСГ.

Псевдослучайные последовательности см., например [4], играют важную роль в поточном шифровании. Так как на практике числовые

последовательности строятся с помощью компьютерной программы, которая всего лишь реализует некий алгоритм, то полученная таким образом последовательность (гамма) не может быть случайной. Она является *псевдослучайной*.

Согласно теореме Шеннона, см. [15], шифр является *абсолютно стойким*, или *совершенным*, если гамма является случайной и равновероятной последовательностью. Но, как уже было сказано выше, последовательность не может быть случайной. Она является псевдослучайной. Поэтому задача сводится к построению *хороших* псевдослучайных последовательностей, плохо отличимых от случайных [9].

Таким образом, *псевдослучайный генератор (ПСГ)* - это алгоритм, который, грубо говоря, берёт короткую случайную последовательность, называемую ключом или начальным состоянием, и следуя некому закону, делает из неё очень длинную последовательность, которая и используется в качестве гаммы в потоковом шифре.

Псевдослучайный генератор гаммы, представленный на рисунке 1, на самом деле является автономным автоматом, а именно пятёркой

$$\mathfrak{A} = (B_2^n, B_2^m, f, G, x_0)\ ,\ \text{где}$$

B_2^n - это множество состояний, $B_2 = \{0,1\}$, n - натуральное;

B_2^m - конечный выходной алфавит, m - натуральное;

$f: B_2^n \to B_2^n$ функция переходов;

$G: B_2^n \to B_2^m$ функция выходов;

x_0 (секретный ключ) - начальное состояние автомата, n - длина ключа, m - длина выходной последовательности, порождаемой генератором за один такт.

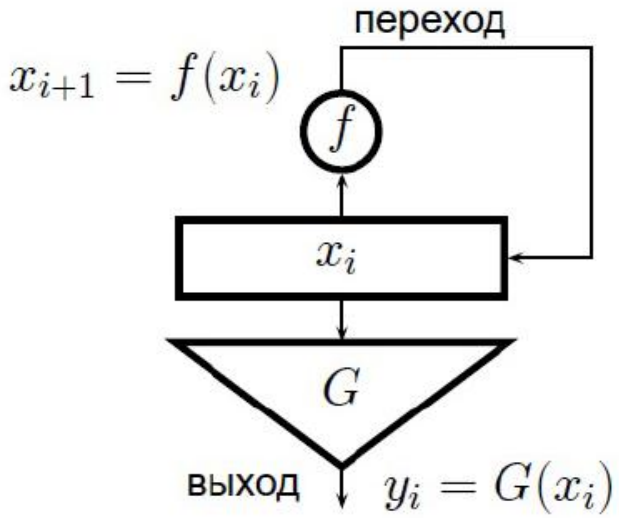

Рисунок 1 - Стандартный псевдослучайный генератор (ПГС)

Этот автомат функционирует в дискретном целочисленном времени $t = 0,1,2,...$ (по тактам). В начальный момент времени $t = 0$ автомат находится в начальном состоянии x_0 - оно же является ключом - и наблюдаем реакцию автомата y_0 . С каждым тактом работы автомат меняет своё состояние $x_0, x_1, x_2, ...$ и порождает реакции y_i, $i = 0,1,2....$ Смена состояний происходит за счёт функции переходов автомата $f : B_2^n \to B_2^n$, сопоставляющей бинарной строчке длины n строчку той же длины; генерация реакции автомата - за счёт функции выходов $G : B_2^n \to B_2^m$, которая состоянию (строчке длины n) сопоставляет реакцию автомата (строчку длины m) на это состояние, см., например [21, 22].

Множество $\mathbb{S}$ с заданной на нём *мерой* μ называется *измеримым пространством*.

В теории динамических систем есть два очень важных понятия: сохранение меры и эргодичность.

Отображение $F : \mathbb{S} \to \mathbb{Y}$ измеримого пространства $\mathbb{S}$ в измеримое пространство $\mathbb{Y}$ с вероятностными мерами μ и ν соответственно называется *сохраняющим меру* (или, иногда, *равновероятным*) если

$$\mu\left(F^{-1}(S)\right) = \nu(S)$$

для каждого измеримого подмножества $S \subset \mathbb{Y}$. В случае, когда $\mathbb{S} = \mathbb{Y} = \mathbb{Z}_p$, будем говорить, что функция $f : \mathbb{Z}_p \to \mathbb{Z}_p$ измеримого пространства $\mathbb{Z}_p$ с мерой Хаара $\mu = \mu_{\text{p}}$ *сохраняет меру*, если $\mu(f^{-1}(\text{S})) = \mu(\text{S})$ для каждого измеримого подмножества $S \subset \mathbb{Z}_p$. Заметим, что сохранение меры совместимой функции равносильно её обратимости (биективности).

Измеримое отображение $F : \mathbb{S} \to \mathbb{Y}$ называется *эргодическим*, если одновременно:

1. F сохраняет меру μ, т.е. $\mu\left(F^{-1}(S)\right) = \mu(S)$ для каждого μ-измеримого подмножества $S \subset \mathbb{Y}$.
2. если для любого измеримого подмножества S, такого что $F^{-1}(S) = S$ (т.е S - инвариантное подмножество) выполняется либо $\mu(S) = 1$ либо $\mu(S) = 0$.

Другими словами, эргодичность означает, что нет инвариантных подмножеств, кроме меры ноль и единицы. Более того, эргодичность совместимой функции $f : \mathbb{Z}_p \to \mathbb{Z}_p$ равносильна её транзитивности, т.е. редукция $f \bmod p^n : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ есть одноцикловая перестановка для любого натурального n, см., например [9, 10]. Кроме того, эргодичность, с точки зрения теории генераторов псевдослучайных чисел, означает, что всякая орбита динамической системы является равномерно распределённой: при практической реализации ПСГ все орбиты циклические, с максимальной длиной цикла (равной 2^n) и каждый элемент на этом цикле встречается ровно один раз.

Вообще говоря, эргодическая теория это очень богатая математическая теория, имеющая многочисленные приложения. Поэтому рассматриваем применение p-адической эргодической теории только к псевдослучайным генераторам, особенно к потоковым шифрам.

В разделе 5 "Сдвиги Бернуллиевского типа" содержится описание механизмов сдвигов Бернулли и их p-адических аналогов.

На пространстве целых p-адических чисел $\mathbb{Z}_p$ можно задать отображение сдвига

$$S(x) = \frac{x - x_0}{p},$$

где $x \in \mathbb{Z}_p: x = x_0 + x_1 p + x_2 p^2 + \dots$.

Если $x \in \mathbb{Z}$, то

$$S(x) = \left\lfloor \frac{x}{2} \right\rfloor$$

означает сдвиг на один разряд.

Итерирование отображения S будет определяться как

$$S^k(x) = \frac{x - (x_0 + x_1 p + x_2 p^2 + \cdots + x_{k-1} p^{k-1})}{p^k}.$$

Отображение S^k является p-адическим аналогом сдвига Бернулли. Более того, отображение S^k можно задать с помощью асинхронного автомата $\mathfrak{B}$ - преобразователя "буква-в-слово", который читает входное слово и порождает в качестве выходного слова входное слово без первых k букв, т.е. сдвигает входное слово на k символов [11].

Любую совместимую функцию можно представить следующим образом.

Для данного $k \in N$ и любого целого p-адического x:

$$f(x) = \left(f(x \bmod p^k)\right) \bmod p^k + p^k\left(G_z(t)\right),$$

где $t = p^{-k}\left(x - (x \bmod p^k)\right)$, $z = x \bmod p^k$ и G_z - некоторая совместимая функция.

В случае сдвига Бернулли (на k разрядов) получаем:

$$f(x) = p^{-k}\left(x - (x \bmod p^k)\right),$$

где x - бесконечная влево строчка, $(x \bmod p^k)$ - первые k символов строки (префикс длины k). Запись $\left(x - (x \bmod p^k)\right)$ в таком случае означает

обнуление первых k символов строки x, а деление на p^k - есть сдвиг на k разрядов строки $\left(x - (x\ mod\ p^k)\right)$.

Обобщением отображения S^k является отображение $f_{\mathfrak{C}}$, реализуемое асинхронным автоматом $\mathfrak{C}$, который читая входное слово буква за буквой, в течении первых k тактов работы не порождает выхода, а затем печатает некоторое выходное слово: по одной букве на каждую букву входного слова [21, 22]. Разумно использовать сдвиги Бернуллиевского типа в композиции с совместимыми функциями для повышения как стойкости, так и быстродействия поточного шифратора.

В разделе 6 "Построение графиков сдвигов", основываясь на изученном теоретическом материале, приводится подробная характеристика программы, которая реализует построение графиков p-адического аналога Бернуллиевского сдвига в единичном квадрате евклидовой плоскости на языке программирования Python 3.6.3 см., например [8, 23]. В этом разделе содержится описание интерфейса приложения, его функций и особенностей, алгоритм, а так же примеры работы программы.

ЗАКЛЮЧЕНИЕ

Сдвиги Бернуллиевского типа плодотворно изучались в рамках различных разделов математики, в частности в теории динамических систем, и привлекали внимание многих исследователей в силу того, что сдвиги являются математически простыми закономерностями, порождающими при этом хаотическую динамику. Более того, некоторые авторы (см., например [17]) подробно изучали некоторые сдвиги Бернуллиевского типа, свойства которых идентичны классическому сдвигу Бернулли. Сдвиги Бернуллиевского типа могут быть использованы в генераторах псевдослучайных чисел, см. [17, 19].

Однако в криптографии разумно использовать не сдвиги как таковые, а отображения, которые базируются на сдвигах. В частности, интерес представляет преобразование кольца вычетов по модулю 2^n вида [16] $g(x) = \frac{x(x+1)}{2}$. Известно, что это отображение биективно, то есть является перестановкой для любого натурального n. Однако остаётся открытым вопрос о существовании полинома f (или рациональной функции) над кольцом целых p-адических чисел ($p = 2$) такого, что $f(g(x)) \, mod \, 2^n$ есть одноцикловая перестановка для любого натурального n. Более того, на сегодняшний день нет полного описания полиномиальной динамики над кольцом целых 2-адических чисел, однако структура такой динамики хорошо описана для всех простых $p > 2$, см. [18].

В ходе данной работы были изучены p-адические аналоги сдвигов Бернуллиевского типа и реализована программа для построения графиков сдвига Бернулли в единичном квадрате евклидовой плоскости на языке программирования Python 3.6.3.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

[1] Анашин В. С. Равномерно распределенные последовательности целых p-адических чисел. // Дискретная математика, 2002, том 14, выпуск 4, с. 3–64.

[2] Боревич З.И., Шафаревич И.Р. Теория чисел. - М.: Наука. Главная редакция физико-математической литературы, 1985.

[3] Григорчук Р.И., Некрашевич В.В., Сущанский В.И. Автоматы, динамические системы и группы. // Тр. МИАН, 2000, том 231, с. 134–214.

[4] Д. Кнут Искусство программирования. Том 2. Получисленные алгоритмы. - М.: Вильямс, 2011.

[5] Зубов А. Ю. Совершенные шифры - М.: Гелиос АРВ, 2003.

[6] Каток С.Б. p-адический анализ в сравнении с вещественным. - М.: МЦНМО, 2004.

[7] Н. Коблиц, *p*-адические числа, *p*-адический анализ и дзета-функции. - М.: Мир, 1981.

[8] Прохоренок Н. А., Дронов В. А. Python 3 и PyQt 5. Разработка приложений. - СПб.: БХВ-Петербург, 2016.

[9] Салий В.Н., Сагаева И.Д., Тяпаев Л.Б. Дискретная математика. Часть 1. - Lulu Publishing, 2013.

[10] Тяпаев Л.Б. Элементы алгебраической динамики. - Lulu Publishing, 2018.

[11] Тяпаев Л.Б. Эргодические автоматные отображения с задержкой. // Проблемы теоретической кибернетики. Материалы XVIII международной конференции. - 2017. - С. 242-244.

[12] Хренников А. Ю. Неархимедов анализ и его приложения. - ФИЗМАТЛИТ, 2003.

[13] Хренников А.Ю., Шелкович В.М. Современный *p*-адический анализ и математическая физика. - М.: ФИЗМАТЛИТ, 2012.

[14] Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. - Триумф, 2002.

[15] Ященко В. В. Введение в криптографию - 4-е изд., доп. М.: МЦНМО, 2012.

[16] Anashin V. S., Khrennikov A. Yu., *Applied Algebraic Dynamics*, volume 49 of de Gruyter Expositions in Mathematics (de Gruyter, 2009).

[17] Christopher F. Wodcock and Nigel P. Smart, p-adic chaos and random number generation, Experiment. Math. **7** (4), 333-342 (1998).

[18] D. L. Desjardins, M. Zieve, "On the structure of polynomial mappings modulo an odd prime power," (2001) [arXiv: math/0103046v1[math.NT]].

[19] J. Kingsbery, A. Levin, A. Preygel, C. E. Silva, "Dynamics of the p-adic shift and applications," Discrete and Continuous Dynamical Systems **30** (1), 209-218 (2011) [arXiv:0903.4226v1[math.DS]].

[20] Joseph H. Silverman, *The Arithmetic of Dynamical Systems*, (Springer, 2007).

[21] L. Tyapaev, "Automata as p-adic dynamical systems," (2018) [arXiv: 1709.02644v2 [math.DS]].

[22] L.B. Tyapaev, Automata as non-Archimedean Dynamical Systems. // Дискретные модели в теории управляющих систем: X Международная конференция, Москва и Подмосковье: Труды/ Отв. ред. В.Б. Алексеев, Д.С. Романов, Б.Р. Данилов. - Москва: МАКС Пресс, 2018. - С. 27-30

[23] The Python Tutorial - Python 3.6.1 documentation // Wellcome to Python.org [Электронный ресурс] URL: https: //docs.python.org /3 /tutorial/ index.html (Дата обращения 5.06.2018) Яз. англ.

.