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

Автоматные отображения с задержкой и их проекции в евклидовой плоскости

АВТОРЕФЕРАТ МАГИСТЕРСКОЙ РАБОТЫ

студента 2 курса 271 группы
направления 09.04.01 «Информатика и вычислительная техника»
факультета компьютерных наук и информационных технологий
Орлова Дмитрия Сергеевича

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 Актуальность работы. 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 $[0, 1]$. Тем не менее, вопрос о том, как получить из равномерно распределенной последовательности последовательность случайных величин с заданным распределением (например, нормальным) вполне разумен. Нередко, под случайными последовательностями понимаются, на самом деле, псевдослучайные.

При поточном шифровании псевдослучайная последовательность (так называемая, гамма) генерируется с помощью автономного автомата 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 это ключ (он секретен), 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 автомата $g\colon \mathbb{X} \to \mathbb{Y}$, $\mathbb{Y} = \{0, 1\}^m$ каждому состоянию x_i (строке из n бит) ставит в соответствие выходной сигнал y_i (строчку из m бит); возникает последовательность $y_0 = g(x_0), y_1 = g(x_1), \ldots, y_i = g(x_i), \ldots$, которая играет роль гаммы.

Для построения стойкого и быстрого поточного шифратора необходимо применить методы неархимедовой (в частности, p-адической) криптографии, в рамках которой генератор гаммы есть неархимедова динамическая система (косое произведение динамических систем (т.е. сплетение автоматов) – в случае повышенных требований к стойкости). Такая динамическая система понимается как тройка $(\mathbb{S}, \mu, F)$, где $\mathbb{S}$ есть неархимедо (ультраметрическое) пространство (называемое конфигурационным), наделенное метрикой

μ, и F есть измеримое (относительно меры μ) и непрерывное (относительно неархимедовой метрики, заданной на $\mathbb{S}$) отображение пространства $\mathbb{S}$ в себя: $F\colon \mathbb{S} \to \mathbb{S}$. Роль конфигурационного пространства играет $\mathbb{Z}_p$ – пространство целых p-адических чисел, наделенное мерой; а функция $F\colon \mathbb{Z}_p \to \mathbb{Z}_p$ – измеримое и непрерывное преобразование, итерирование которого порождает для каждой точки $x_0 \in \mathbb{Z}_p$ (начального состояния) орбиту

$$x_0, F(x_0), F(F(x_0)), \ldots, F(F(F(...(x_0)) \ldots)), \ldots$$

Изучение поведения таких орбит – основная задача динамики. Для криптографии интерес представляют орбиты, порождаемые сохраняющими меру и эргодическими отображениями, которые можно задать с помощью композиций арифметических и поразрядных логических операций или же с помощью автоматов. Последние, в свою очередь, допускают аналитическое представление на языке p-адического анализа.

Целью настоящей магистерской работы является экспериментальное наблюдение проекций автоматных отображений с задержкой в евклидовой плоскости и определение меры Лебега для них.

Для достижения вышеозначенной цели были поставлены следующие задачи: изучение алгоритмов построения проекций автоматных отображений (с задержкой и без нее) в евклидовой плоскости, написание программы, реализующей данные алгоритмы, проведение экспериментов с различными автоматами, определение меры Лебега на основе полученных результатов.

Работа выполнена на 59 страницах машинописного текста, состоит из введения, 8 глав, заключения, содержит 30 рисунков, 1 приложения, список литературных источников содержит 18 наименований.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ. В первой главе описывается пространство слов. Пусть X - конечное множество. Назовем это множество алфавитом. Для заданного алфавита X, обозначим через X^* свободный моноид, порожденный множеством X. Элементы моноида X^* выражаются в виде слов $x_0x_1 \dots x_{n-1}$ включая пустое слово $\varnothing$.

Если $u = x_0x_1 \dots x_{n-1} \in X^*$, то $|u| = n$ длина слова u. Длина $\varnothing$ равна нулю. Наряду с конечными словами из X^* также рассматриваются бесконечные слова вида $x_0x_1x_2 \dots$, где $x_i \in X$. Множество таких бесконечных слов обозначим через X^∞. Для произвольных $u \in X^*$ и $v \in X^* \cup X^\infty$ определяется произведение (конкатенация) $uv \in X^\infty$. Слово $u \in X^*$ является началом или префиксом слова $w \in X^*(\in X^\infty)$ если $w = uv$ для некоторого $v \in X^*(\in X^\infty)$. Множество X^∞ является бесконечным декартовым произведением X^N. На X^N можно ввести топологию прямого Тихоновского произведения для конечных дискретных топологических пространств X. В этой топологии X^∞ гомеоморфно канторовому множеству. Для заданного конечного слова $u \in X^*$, множество uX^∞ всех слов, начинающихся с u, замкнуто и открыто одновременно в заданной топологии; семейство всех таких множеств $\{uX^\infty : u \in X^*\}$ является базой топологии.

Положим метрику d_π на X^∞ зафиксировав число $\pi > 1$ и установив $d_\pi(u, v) = \pi^{-\ell}$, где ℓ это длина самого длинного общего префикса слов u и v. Расстояние между одинаковыми словами равно нулю.

Вторая глава описывает пространство $\mathbb{Z}_p$. Элементами пространства $\mathbb{Z}_p$ являются целые p-адические цисла, которые мыслятся как (односторонние) бесконечные последовательности над алфавитом из p символов $\mathbb{F}_p = \{0, 1, 2, \dots, p-1\}$, где p простое число. Целое p-адическое число x допускает уникальное представление (так называемое, каноническое)

$$x = \sum_{i=0}^{\infty} x_i \cdot p^i = x_0 + x_1p + x_2p^2 + x_3p^3 + \dots = \dots x_3x_2x_1x_0,$$

где $x_0, x_1, x_2, \dots \in \mathbb{F}_p = \{0, 1, 2, \dots\}$ – цифры в записи числа x (в системе счисления с основанием p). Пространство $\mathbb{Z}_p$ образует алгебраическое кольцо (является коммутативной абелевой группой и полугруппой по умножению), обладает структурой проективного предела (является проективным пределом колец $\mathbb{Z}/p^n\mathbb{Z}$ вычетов по модулю p^n при $n = 1, 2, 3, \ldots$).

На $\mathbb{Z}_p$ можно задать метрику $d_p = |x - y|_p$, индуцированной p-адической нормой $|\cdot|_p$, которая, на самом деле, является ультраметрикой (неархимедовой метрикой), а, следовательно, $\mathbb{Z}_p$ ультраметрическое (неархимедово) пространство. Более того, пространство $\mathbb{Z}_p$ вполне несвязно и компактно.

Отображение $F\colon \mathbb{Z}_p \to \mathbb{Z}_p$ сохраняет меру, если $\mu_p(F^{-1}(T)) = \mu_p(T)$ для всякого измеримого подмножества $T \subset \mathbb{Z}_p$. Отображение $F\colon \mathbb{Z}_p \to \mathbb{Z}_p$ эргодично, если оно сохраняет меру и не имеет собственных инвариантных подмножеств, кроме меры 0 и меры 1, т.е. из условия $F^{-1}(T) = T$ следует $\mu_p(T) = 0$, либо $\mu_p(T) = 1$.

Если справедливо неравенство $|f(x) - f(z)|_p \leq |x - z|_p$ для любых $x, z \in \mathbb{Z}_p$, то говорят, что функция удовлетворяет условию Липшица с константой 1 (для краткости, 1-Липшицева). Очевидно, что из условия 1-Липшицевости функции следует ее непрерывность.

Условие 1-Липшицевости равносильно условию совместимости функции: $f(x) \equiv f(z) \pmod{p^n}$ как только $x \equiv z \pmod{p^n}$. Здесь $\mathrm{mod} p^n$ суть эпиморфизм кольца $\mathbb{Z}_p$ на кольцо вычетов $\mathbb{Z}/p^n\mathbb{Z}$ (с ядром $p^n\mathbb{Z}_p = B_{p^{-n}}(0)$): целому p-адическому числу $x = \sum_{i=0}^{\infty} x_i \cdot p^i$ ставится в соответствие число $x \bmod p^n = \sum_{i=0}^{n-1} x_i \cdot p^i$. Совместимой функцией на $\mathbb{Z}_p$, например, является любой полином над $\mathbb{Z}_p$ с целыми p-адическими коэффициентами, в частности, с целыми коэффициентами.

Третья глава представляет автоматы как непрерывные динамические системы на $\mathbb{Z}_p$. (Асинхронным) автоматом называется шестерка $\mathfrak{B} =< \mathbb{X}, \mathbb{S}, \mathbb{Y}, h, G, s_0 >$, где $\mathbb{X}, \mathbb{S}, \mathbb{Y}, h, G, s_0$ имеют тот же смысл, что и для автомата $\mathfrak{A}$ и определяются аналогичным образом, за исключением функции выходов G; здесь G есть отображение вида $G\colon \mathbb{X} \times \mathbb{S} \to \mathbb{Y}^*$, где $\mathbb{Y}^*$ обозначает множество слов над алфавитом $\mathbb{Y}$ конечной длины. Таким образом, асинхронный автомат суть преобразователь «буква в слово»: входную букву автомат $\mathfrak{B}$ преобразует в выходное слово конечной длины (в том числе, длины равной 0, в пустое слово ε).

Асинхронный автомат $\mathfrak{B}$ называется вырожденным, если найдется такое входное слово бесконечной длины (для определенности бесконечное слово записывается и читается справа налево), что прочитав это слово буква за буквой, автомат $\mathfrak{B}$ печатает (справа налево) выходное слово конечной длины (в том числе, пустое).

Пусть π есть некоторое неотрицательное целое число; и пусть $\mathbb{X}^\infty$ обозначают пространства слов бесконечной длины (записанные справа налево) над алфавитом $\mathbb{X}$. Для любой пары слов $a, b \in \mathbb{X}^\infty$ можно задать функцию расстояния (метрику) d_π следующим образом $d_\pi(a, b) = \pi^{-\ell}$, где ℓ есть наибольшая длина общего префикса слов a и b. Метрика d_π будет удовлетворять сильному неравенству треугольника $d_\pi(a, b) \leq \max\{d_\pi(a, c), d_\pi(c, b)\}$, следовательно, является ультраметрикой, а значит пространство $\mathbb{X}^\infty$ – неархимедово. Ясно, что пространство $\mathbb{Y}^\infty$ так же неархимедово.

Отображение $f\colon \mathbb{X}^\infty \to \mathbb{Y}^\infty$ является непрерывным тогда и только тогда, когда оно определяется некоторым невырожденным асинхронным автоматом.

При $\mathbb{X} = \mathbb{Y} = \mathbb{F}_p = \{0, 1, \dots p-1\}$ заключаем, что $\mathbb{X}^\infty = \mathbb{Y}^\infty = \mathbb{Z}_p$. Следовательно, автоматное отображение $f_{\mathfrak{B}}\colon \mathbb{X}^\infty \to \mathbb{Y}^\infty$, реализуемое (невырожденным) асинхронным автоматом $\mathfrak{B} =< \mathbb{F}_p, \mathbb{S}, \mathbb{F}_p, h, G, s_0 >$ суть непрерывное (относительно p-адической метрики) отображение $f_{\mathfrak{B}}\colon \mathbb{Z}_p \to \mathbb{Z}_p$; итерирование этого отображения, очевидно, порождает динамическую систему $(\mathbb{Z}_p, \mu_p, f = f_{\mathfrak{B}})$.

Отображение $f_{(n)}\colon \mathbb{Z}_p \to \mathbb{Z}_p$ называется отображением с задержкой $n \in \mathbb{N}$, если существует невырожденный асинхронный автомат $\mathfrak{B} =< \mathbb{F}_p, \mathbb{S}, \mathbb{F}_p, h, G, s_0 >$ такой, что $f_{\mathfrak{B}} = f_{(n)}$, и который преобразует входное слово $x = \dots x_2x_1x_0 \in \mathbb{F}_p^\infty$ в выходное слово $y = f_{\mathfrak{B}}(x) = \dots y_2y_1y_0 \in \mathbb{F}_p^\infty$ так, что $g(\delta_i(x), s_i) = \varepsilon$ при $i = 0, 1, 2, \dots n-1$; $s_i = h(\delta_{i-1}(x), s_{i-1})$ при $i = 1, 2 \dots n-1$; $g(\delta_{n+i}(x), s_{n+i}) = y_i$ при $i = 0, 1, 2, \dots$, $s_{n+i} = h(\delta_{n+i-1}(x), s_{n+i-1})$ для $i = 0, 1, 2, \dots$.

Отображение с задержкой n – это отображение, которое реализуется асинхронным автоматом так: автомат начинает печатать ровно по одной букве $y_0, y_1, \dots$, но только после того, как прочитает сначала n первых букв $x_0, x_1, \dots x_{n-1}$ входного слова (печатая при этом пустые слова).

Отображение $f_{(n)}\colon \mathbb{Z}_p \to \mathbb{Z}_p$ непрерывно. Простейшим примером отображения с задержкой, является отображение с задержкой $n = 1$, реализуемое, так называемым, автоматом с задержкой, который печатает в качестве выходного слова – входное слово без изменений (копирует), начиная со второй буквы (другими словами, такой автомат осуществляет сдвиг слова на одну букву). В общем случае, отображение с задержкой n, преобразует слово (прообраз) в некоторое новое слово (образ), а не копирует прообраз начиная с n-ой буквы.

В четвертой главе рассказывается про ряды Малера. Любое непрерывное отображение $f\colon \mathbb{N}_0 \to \mathbb{Z}_p$ (следовательно, и $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$, в силу плотности $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ в $\mathbb{Z}_p$) представимо рядом Малера

$$f(x) = \sum_{m=0}^{\infty} a_m \binom{x}{m} = a_0 + a_1 x + a_2 \binom{x}{2} + \ldots,$$

где коэффициенты ряда $a_m \in \mathbb{Z}_p$ определяются соотношением

$$a_m = \sum_{i=0}^{m} (-1)^i \binom{m}{i} f(m-i);$$

и

$$\binom{x}{m} = \frac{x(x-1)\cdots(x-m+1)}{m!}$$

есть биномиальный коэффициент.

Отображение $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ совместимо, тогда и только тогда, когда коэффициенты ряда Малера удовлетворяют условию

$$|a_i|_p \le p^{-\lfloor \log_p i \rfloor}, i = 1, 2, \ldots$$

Приведем достаточные условия сохранения меры и эргодичности для совместимых отображений в терминах рядов Малера.

Отображение $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ совместимо и сохраняет меру, как только выполняются следующие условия:

A1. $a_1 \not\equiv 0 \pmod p$;

A2. $a_i \equiv 0 \pmod{p^{\lfloor \log_p i \rfloor + 1}}$, $i = 2, 3, \ldots$;

Отображение $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ совместимо и эргодично, как только выполняются следующие условия:

B1. $a_0 \not\equiv 0 \pmod p$;

B2. $a_1 \equiv 1 \pmod p$ при нечетных p;

B3. $a_1 \equiv 1 \pmod 4$ при $p = 2$;

B4. $a_i \equiv 0 \pmod{p^{\lfloor \log_p(i+1) \rfloor + 1}}$, $i = 2, 3, \ldots$.

При $p = 2$ все вышеуказанные условия (A1,A2,B1,B3,B4) являются и необходимыми.

Отображение $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ является отображением с задержкой n, тогда и только тогда, когда коэффициенты ряда Малера удовлетворяют условию

$$|a_i|_p \leq p^{-\lfloor \log_{p^n} i \rfloor + 1}, i = 1, 2, \ldots.$$

Приведем достаточные условия сохранения меры и эргодичности для отображения с задержкой.

Пусть $f_{(n)}\colon \mathbb{Z}_p \to \mathbb{Z}_p$ является отображением с задержкой n. Тогда, оно сохраняет меру, как только одновременно выполняются следующие условия:

1. $a_i \not\equiv 0 \pmod p$ при $i = p^n$;
2. $a_i \equiv 0 \pmod{p^{\lfloor \log_{p^n} i \rfloor}}$ при $i > p^n$.

Отображение $f_{(n)}\colon \mathbb{Z}_p \to \mathbb{Z}_p$ эргодично, как только выполняются следующие условия одновременно:

1. $a_1 + a_2 + \ldots + a_{p^n - 1} \equiv 0 \pmod p$;
2. $a_1 \equiv 1 \pmod p$ при $i = p^n$;
3. $a_i \equiv 0 \pmod{p^{\lfloor \log_{p^n} i \rfloor}}$ при $i > p^n$.

В пятой главе описываются проекции p-адических отображений с задержкой в единичном квадрате $\mathbb{I}^2 \subset \mathbb{R}^2$. Пусть $f_{(n)}\colon \mathbb{Z}_p \to \mathbb{Z}_p$ отображение с задержкой $n \in \mathbb{N}$, заданное с помощью асинхронного автомата $\mathfrak{B}$. Отображение $f_{(n)}$ можно задать и аналитически – с помощью коэффициентов ряда Малера.

Для $k = 1, 2, 3, \ldots$ пусть $E_k(f_{(n)})$ есть множесто точек $e_k^{f_{(n)}}(x)$ единичного квадрата $\mathbb{I}^2 = [0, 1] \times [0, 1] \subset \mathbb{R}^2$ евклидовой плоскости, заданных координатами:

$$e_k^{f_{(n)}}(x) = \Big(\frac{x \bmod p^{k+n}}{p^{k+n}}, \frac{f_{(n)}(x) \bmod p^k}{p^k}\Big),$$

где $x \in \mathbb{Z}_p$. Здесь $x \bmod p^{n+k}$ есть префикс длины $n+k$ бесконечного слова x, которое подается на вход автомата $\mathfrak{B}$; соответсвенно, $f_{(n)}(x) \bmod p^k$ – префикс длины k бесконечного выходного слова $f_{(n)}(x)$ автомата $\mathfrak{B}$.

Пусть $\mathcal{E}(f_{(n)})$ есть замыкание множества $E(f_{(n)}) = \bigcup_{i=1}^{\infty} E_k(f_{(n)})$ в топологии плоскости $\mathbb{R}^2$ – график отображения $f_{(n)}\colon \mathbb{Z}_p \to \mathbb{Z}_p$. Множество $\mathcal{E}(f_{(n)})$ измеримо в $\mathbb{R}^2$ относительно меры Лебега (в силу замкнутости $\mathcal{E}(f_{(n)})$). Пусть $\lambda(f_{(n)})$ есть мера Лебега множества $\mathcal{E}(f_{(n)})$.

Равномерное распределение псевдослучайной последовательности $(f_{(n)}^i(x))_{i=0}^{\infty}$, генерируемое отображением $f_{(n)}\colon \mathbb{Z}_p \to \mathbb{Z}_p$ тесно связано с эргодичностью.

Следует отметить, что для 1-Липщицевой функции $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ справедлив так называемый закон «0-1»: Замыкание $\mathcal{E}(f)$ множества $E(f) = \bigcup_{i=1}^{\infty} E_k(f)$ точек плоскости $\mathbb{R}^2$, заданных следующими координатами

$$e_k^f(x) = \Big(\frac{x \bmod p^k}{p^k}, \frac{f(x) \bmod p^k}{p^k}\Big),$$

$k = 1, 2, 3, \ldots$ измеримо относительно меры Лебега, и $\lambda(f) = 0$, либо $\lambda(f) = 1$.

В шестой главе описана разработка программы. В качестве языка программирования при создании инструмента построения проекций использовался язык Python версии 3.6. Данный выбор был обоснован следующими факторами:

- Python достаточно быстр для вычислительных операций. В силу того, что Python является интерпретируемым языком программирования, он уступает по данному показателю таким компилируемым языкам, как например C или Go, но с требованиями решаемой задачи справляется без ощутимых проблем.
- Python обладает динамической системой типов, что позволяет при должной внимательности писать более гибкий программный код для работы с различными типами данных, будь-то строки, числа, либо бинарные последовательности.
- Python не имеет привязки к среде выполнения программы. Написанный на одной машине код можно легко перенести на другую, даже если они работают под управлением различных операционных систем. Од-

нако, следует быть внимательными с версиями интерпретаторов языка. Так как многие механизмы в версиях 2+ и 3+ отличаются и не имеют обратной совместимости, рекомендуется использовать интерпретаторы одной версии.

- В Python присутствует мультиплатформенная графическая библиотека Tkinter, которая в свою очередь использует библиотеку базовых графических элементов Tk. Tkinter разработан создателем языка Python Гвидо Ван Россумом и по-умолчанию является основным средством разработки программного обеспечения с графическим интерфейсом на языке Python.
- В Python присутствует библиотека для визуализации данных двумерной графикой Matplotlib. Данная библиотека очень распространена в научной среде, так как предоставляет широкий выбор возможностей для визуализации различной степени сложности. Matplotlib является легко конфигурируемым пакетом, который в комбинации с NumPy, SciPy и Ipython предоставляет возможности, подобные MATLAB. Исходя из вышеперечисленного, было решено использовать сочетание Python 3.6 + Tkinter + Matplotlib. Разработка велась на машине под управлением операционной системы Ubuntu 18.04 LTS.

Седьмая глава содержит информацию об интерфейсе программы. Интерфейс разработанной программы содержит три основных компонента. На главном окне в верхней панели находятся переключатели режимов построения проекций.

Режим Sync реализует отображения для синхронных автоматов. Необходимыми параметрами ввода для работы в данном режиме являются функция F(x) и k, а n можно оставить пустым, либо заполнить любым значением — программа не будет его учитывать. Для ввода функции F(x) следует нажать на соответствующее поле серого цвета, после чего поверх главного окна откроется окно ввода.

Данное окно представляет собой некое подобие калькулятора, поддерживающего логические операции OR, AND и XOR. Следует учитывать, что вводимая функция должна иметь только одну переменную, именуемую как x (икс) в нижнем регистре. Операции можно вводить как нажатием на соответствующие кнопки, так и с клавиатуры, но при этом операции должны синтаксически совпадать с теми, что изображены на кнопках. Пример функции: pow(x, 4) OR 12. После ввода нужной формулы следует нажать на кнопку Submit, чтобы окно ввода закрылось, а в поле F(x) появилось введенное значение.

Режим Async реализует отображения для асинхронных автоматов с задержкой. Необходимыми параметрами ввода для работы в данном режиме являются функция F(x), k и n, где n — количество слов, на которое будет осуществлена задержка. В данном режиме F(x) задается конечным автоматом. Для ввода автомата следует нажать на соответствующее поле серого цвета, после чего откроется окно ввода.

Шаблон представляется собой JSON объект, который по принципу ключ-значение содержит набор состояний.

В вышеприведенном примере автомат является сдвигом Бернулли на 1 разряд и состоит из двух состояний s0 и s1. Если автомат находится в состоянии s0, то независимо от того, что он получит на входе, на выходе автомат напечатает пустое слово (значение по ключу out) и перейдет в состояние s1 (значение по ключу goto). Если автомат находится в состоянии s1, то получив на вход 0 он напечатает 0 и перейдет в состояние s1, а получив на вход 1 он напечатает 1 и так же перейдет в состояние s1. После ввода автомата следует нажать на кнопку Submit, чтобы окно ввода закрылось, а в поле F(x) появилось введенное значение.

Режим Bernoulli является обособленной реализацией построения отображения для асинхронного автомата. Особенность заключается в том, что в данном режиме не требуется ввод F(x), достаточно только k и n.

В любом из режимов после ввода всех необходимых параметров нужно нажать кнопку Calculate. После выполнения всех расчетов в единичном квадрате появится некоторый график.

В восьмой главе приведены экспериментальные наблюдения. Так как целью настоящей работы является экспериментальное наблюдение проекций автоматных отображений с задержкой, в этой части не были затронуты режимы Sync и Bernoulli. Для каждого автомата в режиме Async был проведен ряд экспериментов с k равными 10, 12, 16 и 18. Для построения диаграмм

Мура всех рассмотренных в работе автоматов использовалась онлайн-версия пакета утилит по автоматической визуализации графов webgraphviz.

ЗАКЛЮЧЕНИЕ В ходе проделанной работы был изучен алгоритм построения проекций автоматных отображений с задержкой. Была написана программа, реализующая такой алгоритм. С помощью программы были проведены эксперименты с различными отображениями с задержкой, наибольший интерес из которых представляют эргодические отображения и отображения сохраняющие меру, поскольку на их основе строются генераторы псевдослучайных чисел.