МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ Н. Г. ЧЕРНЫШЕВСКОГО»**
Кафедра дискретной математики и информационных технологий

БЕТА-ПРОЕКЦИИ АВТОМАТНЫХ ФУНКЦИЙ

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

студента 4 курса 421 группы
направления 09.03.01 — Информатика и вычислительная техника
факультета КНиИТ
Теребина Филиппа Владиславовича

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

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

Саратов 2020

ВВЕДЕНИЕ

При изучении возможностей абстрактных вычислительных машин, прежде всего машин Тьюринга, возникает важный вопрос о возможности вычислений функций действительного аргумента с помощью таких машин. В частности, вычисления действительных чисел на машинах Тьюринга составляют основу теории вычислимых функций. Как известно, машины Тьюринга находятся на вершине иерархии абстрактных вычислительных машин — они обладают максимальной вычислительной мощностью. Автоматы Мили, также известные как (синхронные) автоматы-преобразователи, на самом деле, являются машинами Тьюринга, головки которых движутся только в одном направлении, а значит (синхронные) автоматы в сравнении с машинами Тьюринга обладают меньшей вычислительной мощностью. Однако, ряд процессов реального мира можно смоделировать с помощью таких автоматов в силу того, что они могут рассматриваться как дискретные динамические системы (см., например, [2], [3], [6], [8], [22], [23], [24], [25], [26], [27]). Теория функций, вычисляемых абстрактными машинами, имеет множество приложений не только в математике (например, в действительном анализе, p-адическом анализе, теории чисел, теории сложности, теории динамических систем), но также в области компьютерных наук, физики, лингвистики, психологии и многих других областях (см., например, монографии [1], [2], [3], [4], [5], [6]).

Исследование поведения автоматов и автоматных функций в задачах криптографии (при моделировании криптографических примитивов, используемых в поточных шифраторах и хэш-функциях) с помощью экспериментального наблюдения пар входных и выходных последовательностей (пар входных и выходных слов автоматов-преобразователей), ассоциированных с точками ограниченной области евклидовой плоскости (формирующих проекции — «графики» автоматных функций) выявило характерное распределение точек этих графиков – для автоматов с конечным числом состояний точки графиков таких автоматов (т.е. автоматных функций) образуют линейные структуры (см. [2], [3], [9] - [27]) и могут быть интерпретированы как интерференционные картины в квантовой физике (например, интерференция фотонов на двух щелях). Однако, структуры из класса C^2 дважды непрерывно дифференцирумых функций (кроме линейных) экспериментально не наблюдаются. Вопрос о том, какие функции могут быть вычислены

с помощью автоматов (другими словами, какие геометрические структуры могут быть заданы автоматными отображениями) неразрывно связан, вероятно, с формализмом квантовой механики. Почему математический формализм квантовой теории, который базируется на теории линейных операторов (на гильбертовых пространствах) *линеен*, и при этом, ряд квантовых явлений демонстрирует нелинейное поведение? Обсуждение этого вопроса возникло в ряде работ по квантовым основаниям и преквантовой статистической теории поля (см., например, [28], [29]).

Наблюдение поведения физической системы можно мыслить как эксперимент с физической системой. Под экспериментом с физической системой понимается воздействие на (физическую) систему и наблюдение за реакцией системы на эти воздействия. Экспериментатор оказывает *конечное* число воздействий на систему. Эти воздействия *дискретны* по своей природе. Более того, разумно считать справедливым *закон причинности*: отклик системы на воздействие (акт измерения) в текущий момент времени не зависит от будущих воздействий, а зависит только от текущего воздействия и от воздействий на систему в прошлые моменты времени. В силу этого, естественной математической моделью данного эксперимента является модель *конечного автомата*. В силу того, что закон причинности в математическом представлении есть автоматное отображение, каждому эксперименту сопоставляется конечный автомат, входной и выходной алфавиты которого есть множество $\{0, 1, \dots, p-1\}$, где p простое число. Здесь стоит отметить, что выбор множества $\{0, 1, \dots, p-1\}$ не должен казаться искусственным, поскольку наблюдательные данные (в эксперименте) всегда можно нормировать, и считать в дальнейшем, что наблюдательные данные в этом случаем будут представлены как числа, записанные в системе счисления с основанием p. Тогда, автоматное отображение суть преобразование кольца целых p-адических чисел, которое удовлетворяет условию Липщица с константой равной 1 (см., например [6]) (этот факт был открыт еще в 1960-е годы (см. [30]), однако специалистам по теории автоматов долгое время был не известен; при этом 1-Липшицевы функции, конечно же, изучались в рамках p-адического анализа). Физический закон с точки зрения математического формализма есть *аппроксимация* конечного числа измерений. Естественным требованием к математическому описанию поведения физической системы является *гладкость*

аппроксимирующей функции. Гладкими кривыми (класса гладкости C^2), вычислимыми конечными автоматами могут быть лишь прямые (в единичном квадрате евклидовой плоскости), и которые, при этом, являются обмотками единичного тора. Эти обмотки, в свою очередь, могут быть заданы семейством комплексно-значных экспоненциальных функций вида $e^{i(Ax-2\pi p^k B)}$ при $k = 0, 1, 2, \ldots$, где i — мнимая единица, A и B — рациональные целые p-адические числа (см. [3]). Данные функции являются уравнениями волн де Бройля $\Psi = e^{i(ax-\omega t)}$, если для автомата величину p^k интерпретировать как время t. Если предположить, что основание системы счисления p есть число $1+\epsilon$, где $\epsilon > 0$ достаточно малая величина, например, ϵ есть планковская величина, то величина p^k будет мало отличима от $1+k\epsilon$. Тогда, разумно предположить, что $k\epsilon$ есть достаточно малый интервал времени (квант времени), например, планковский интервал времени (порядка 10^{-43} секунды). Математическим описанием столь малых физических величин (например, планковского времени) может служить β-предствление числа (при $\beta = 1+\epsilon$) (см. [31]). Таким образом, построение проекций автоматных отображений в β-представлении при $\beta > 1$ (и при этом $\beta \to 1$) мотивировано физическими соображениями о поведении квантовых систем. Более того, проекция автоматного отображения в таком β-представлении, на самом деле, есть приближение волновой функции (волны де Бройля) (т.е. наблюдается «эффект волновой интерференции»). Кроме этого, автоматы, которые могут быть выбраны в качестве модельных, обязательно должны быть *бинарными*, в силу того, что при $\beta \to 1$, входным и выходным алфавитом будет множество $\{0, 1, \ldots, \lfloor\beta\rfloor\}$, т.е. входной и выходной алфавиты — бинарны, состоят из двух элементов $\{0, 1\}$.

Проекции (синхронно) автоматных отображений при $\beta = p$ подчиняются закону «0 и 1» – мера Лебега проекции равна либо 0, либо 1 (см. [2]). Более того, проекции (асинхронно) автоматных отображений, которые при этом являются локальными 1-Липшицевыми функциями (т.е. удовлетворяют условию Липшица только локально: в окрестности некоторой точки), подчиняются закону «нуля» (мера Лебега проекции равна 0) (см. [26], [27]).

Целью данной выпускной квалификационной работы является создание программного обеспечения, которое позволит строить бета-проекции автоматных функций на единичном квадрате евклидовой плоскости при значении

$1 < \beta \leq 2$ и при различных натуральных значениях k количества разрядов, поступающих на вход автоматов строк и экспериментальное наблюдение за данными проекциями.

Задачи выпускной квалификационной работы представляют собой:

— Изучение элементов теории автоматов и автоматных отображений на кольце целых p-адических чисел $\mathbb{Z}_p$;

— Изучение возможности описания поведения физических систем, в частности квантовых систем, с помощью вычислимых автоматных отображений;

— Реализация построения проекций значений автоматных отображений, заданных на кольце целых p-адических чисел в единичном квадрате евклидовой плоскости в бета-представлении;

— Экспериментальное наблюдение проекций значений автоматных отображений, заданных на кольце целых p-адических чисел в единичном квадрате евклидовой плоскости в бета представлении;

— Экспериментальное наблюдение линейной сложности автоматных отображений, используемых в криптографии.

КРАТКОЕ СОДЕРЖАНИЕ

1) Элементы теории автоматов на кольце $\mathbb{Z}_p$

Подраздел 1.1 «Целые p-адические числа» знакомит с p-адическими числами — бесконечными в одну сторону строками, каждый символ которой находится в множестве $\{0, 1, ..., p-1\}$. В данном разделе определяется порождаемая данными числами не-архимедова метрика, а также некоторые свойства целых p-адических чисел. Данные числа используются в качестве входных и выходных данных автоматных отображений, рассматриваемых в подразделе 1.2 «Свойства автоматных отображений».

В подразделе 1.2 «Свойства автоматных отображений» дается определение автоматам, автоматным отображениям, рассмотрены основные теоремы и свойства. В данном подразделе определены сдвиг Бернулли и сложный сдвиг.

В подразделе 1.3 «T-функции» рассматриваются требования, выдвигаемые к современным криптографическим функциям, дается определение T-функции.

2) Элементы p-адической математической физики

Подраздел 2.1 «Неколмогоровские теории вероятностей» содержит в себе описание частотной модели, приводятся некоторые ее отличия от колмогоровской модели. Описывается ансамбль-модель, приводятся ее отличия от колмогоровской модели. Иллюстрируется происхождение p-адических ансамбль-вероятностей, анализируется такое явление как отрицательная вероятность.

В подразделе 2.2 «Свойства квантовых систем» рассматриваются различные точки зрения относительно свойств квантовых систем – реализм (реализм со значениями свойств до акта измерения и реализм со значениями свойств после акта измерений), эмпиризм и идеализм. Также определены различные интерпретации квантового состояния системы: ансамбль-реалистическая, индивидуально-реалистическая, ансамбль-эмпирическая, индивидуально-эмпирическая. Приводится одно из противоречий между квантовым и классическим вероятностным исчислениями.

В подразделе 2.3 «Анализ возможности описания физических систем вычислимыми автоматными отображениями» приводится описание такого понятия как «эксперимент», приводятся его свойства, которые позволяют

отождествлять эксперимент с конечным дискретным детерминированным автоматом. Приводится формула семейства комплескно-значных функций, задающий обмотки тора, а также уравение волн де Бройля. Производится анализ данных функций, в результате которого делается предположение о возможности их отождествления. Одним из результатов анализа является требование к значению β, $1 < \beta \leq 2$. $\beta = 1 + k\varepsilon$, где $k\varepsilon$ является малой величиной, сопоставимой с планковской (например, с планковским временем).

3) Разработка системы построения проекций значений автоматных отображений

В подразделе 3.1 «Разработка графического интерфейса» описывается создание пользовательского интерфейса программы. Пользователь может редактировать вид функции, количество разрядов поступающих на вход автомата p-адических строк, а также значение β. Значение β определяется как $\beta = \sqrt[z]{2}$, где z — натуральное число, вводимое пользователем.

Подраздел 3.2 «Разработка калькулятора математических выражений» содержит в себе описание алгоритма, по которому осуществляется интерпретация формул, вводимых пользователем, а также производится анализ возможных решений данной задачи с последующим выбором и описанием наиболее подходящего.

В подразделе 3.2.1 «Разработка сортировочной станции» описывается реализация алгоритма, позволяющего преобразовать формулу из привычной для пользователей инфиксной нотации в эффективную для вычислений ЭВМ постфиксную нотацию.

В подразделе 3.2.2 «Разработка стекового калькулятора» описывается реализация калькулятора, основанного на стековой структуре данных.

Подраздел 3.3 «Разработка преобразователя двоичных строк» содержит в себе описание алгоритма, по которому осуществляется преобразование 2-адических строк в координаты на единичном квадрате евклидовой плоскости.

Подраздел 3.4 «Разработка графического модуля» содержит в себе описание процесса формирования изображения проекции значений автоматной функции, основанной на вычисляемых координатах.

4) Экспериментальное наблюдение проекций автоматных отображений

В данном разделе описываются результаты экспериментальных наблюдений за автоматными отображениями. Особый интерес в рамках анализа исследования возможности описания физических (квантовых) систем вычислимыми автоматными отображениями представляют линейные автоматные функции. Описываются наблюдаемые тенденции, некоторые зависимости проекций от задаваемой пользователем конфигурации.

5) Экспериментальное наблюдение линейной сложности автоматных отображений в криптографии

Линейная сложность описывает криптографическую функцию с точки зрения стойкости. Разработанное программное обеспечение позволяет оценивать данный параметр следующим образом: проекция функции с высокой линейной сложностью представляет собой равномерное распределение точек на единичном квадрате евклидовой плоскости, иначе, в случае с параллельными прямыми, функция обладает низкой линейной сложностью – сложностью, стремящейся к 2.

Также в разделе рассматриваются проекции рассматриваемых криптографических функция в β-представлении, $1 < \beta \leq 2$, хотя в настоящее время криптографиеские функции основываются лишь на $\beta = 2$.

Подраздел 5.1 «Линейная сложность функции $f(x) = x + 2x^2$» содержит в себе результаты наблюдения за линейной сложностью функции, используемой при RC6 шифровании. При всех значениях числа разрядов k функция генерирует проекцию с равномерным распределением точек. Рассмотрены проекции при малых значениях β и различных значениях k.

Подраздел 5.2 «Линейная сложность функции $f(x) = x + (x^2 \vee C)$» содержит в себе результаты наблюдения за линейной сложностью функции, именуемой функцией Климова-Шамира. При обычных значениях констант, удовлетворяющих требованиям к данной функции, выдвигаемых в разделе 1.3, при всех значениях k, функция генерирует проекцию с равномерным распределением точек. Однако для некоторых констант, также удовлетворяющих условиям, может наблюдаться нарушение — график проекции начинает устремляться к параллельным прямым, что свидетельствует о ненадежности данной функции при данных значениях констант. Данная аномалия проявляется при малых значениях k. Также были приведены примеры проекции данной функции в β-представлении, $1 < \beta \leq 2$.

Подраздел 5.3 «Линейная сложность функции $f(x) = x \oplus (x^2 \vee C)$» содержит в себе результаты наблюдения за линейной сложностью функции, используемой в сетях Фейстеля. Результаты наблюдения за данной функцией аналогичны результатам наблюдения за функцией Климова-Шамира, с единственным отличием в форме графика при проявлении аномалии.

ЗАКЛЮЧЕНИЕ

При подготовке выпускной квалификационной работы была определена следующая цель — создание программного обеспечения, которое позволяет строить бета-проекции автоматных функций на единичном квадрате евклидовой плоскости при значении $1 < \beta \leq 2$ поступающих на вход автоматов строк, а также экспериментальное наблюдение данных проекций.

В процессе реализации данной цели были решены следующие задачи:

— Изучены элементы теории автоматов и автоматных отображений на кольце целых p-адических чисел $\mathbb{Z}_p$;

— Изучена возможность описания поведения физических систем, в частности квантовых систем, с помощью вычислимых автоматных отображений;

— Реализовано построения проекций значений автоматных отображений, заданных на кольце целых p-адических чисел в единичном квадрате евклидовой плоскости в бета-представлении;

— Произведено экспериментальное наблюдение проекций значений автоматных отображений, заданных на кольце целых p-адических чисел в единичном квадрате евклидовой плоскости в бета представлении;

— Произведено экспериментальное наблюдение линейной сложности автоматных отображений, используемых в криптографии.

В работе были рассмотрены автоматные отображения $f : \mathbb{Z}_p \to \mathbb{Z}_p$, определены основные свойства автоматов, автоматных отображений.

Рассмотрены различия между частотной моделью и «колмогоровской» моделями вероятностей, а также происхождение p-адических ансамбль-вероятностей и такое явление как отрицательные вероятности.

Определены различные точки зрения относительно свойств квантовых систем — реализм (реализм при значениях до акта измерения значений свойств; реализм при значениях после акта измерения значений свойств), эмпиризм, идеализм. Также определены различные интерпретации квантового состояния системы: ансамбль-реалистическая, индивидуально-реалистическая, ансамбль-эмпирическая, индивидуально-эмпирическая. Также рассмотрено противоречие между квантовым и классическим вероятностным исчислениями.

Определены требования, выдвигаемые к автомату, способному описать

физический эксперимент (для квантовых систем) — автомат должен быть конечным дискретным детерминированным. Рассмотрен пример физического эксперимента, для которого существует теоретическая возможность поставить в соответствие автоматное отображение. Обосновано взятие значения β в рамках $1 < \beta \leq 2$.

Реализовано программное обеспечение для построения проекций значений автоматных отображений, заданных на кольце целых p-адических чисел в единичном квадрате евклидовой плоскости в бета-представлении на языке программирования Java.

Произведены экспериментальные наблюдения за различными автоматными отображениями при различной длине входных строк, при различных значениях β.

Произведены экспериментальные наблюдения за линейной сложностью некоторых криптографических функций.

При написании программного обеспечения велась активная работа по оптимизации программного кода для повышения производительности. Однако сложность вычислений растет экспоненциально с ростом длины входных строк. Для проведения дальнейших исследований требуется кардинальное изменение программы, включающее в себя новые технологии для множественных параллельных вычислений, а также значительное увеличение аппаратных ресурсов.

Написанное программное обеспечение может быть использовано для оценки линейной сложности криптографических функций, а также для определения изменения проекций значений автоматных отображений с возможностью изменения длины поступающих на вход автомата строк и значения β.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 J.-P. Allouche and J. Shallit, Automatic Sequences. Theory, Applications, Generalizations. Cambridge Univ. Press, 2003.

2 V. Anashin and A. Khrennikov, Applied Algebraic Dynamics, Walter de Gruyter GmbH & Co., Berlin — N.Y., 2009.

3 Anashin, V.S. Quantization causes waves: Smooth finitely computable functions are affine. P-Adic Num Ultrametr Anal Appl 7, 169–227 (2015).

4 Брауэр В. Введение в теорию конечных автоматов. — М.: Радио и связь, 1987.

5 Яблонский С.В. Введение в дискретную математику. — М.: Высшая школа, 2006.

6 Р. И. Григорчук, В. В. Некрашевич, В. И. Сущанский, Автоматы, динамические системы и группы, Тр. МИАН, 2000, том 231, 134–214.

7 Мищенко А. С., Фоменко А. Т., Курс дифференциальной геометрии и топологии. — М.: Изд-во «Факториал Пресс», 2000.—448 с.

8 Сагаева И.Д., Салий В.Н. Тяпаев Л.Б. Дискретная математика. Ч.1. – Lulu Publishing, USA, 2013.

9 Тяпаев Л.Б. Построение и анализ геометрических образов конечных детерминированных автоматов // Теоретические проблемы информатики и её приложений. Вып.1. – Изд-во Сарат. ун-та, 1997. С. 146–151.

10 Тяпаев Л.Б. Описание геометрических образов некоторых классов математических автоматов // Теоретические проблемы информатики и её приложений. Вып.2 – Изд-во Сарат. ун-та, 1998. С. 139–148.

11 Тяпаев Л.Б. Геометрическая модель поведения автоматов и их неотличимость // Математика, механика, математическая кибернетика. – Изд-во Сарат. ун-та, 1999. С. 139-143.

12 Тяпаев Л.Б. Геометрические модели и методы при решении задач теории автоматов. // Теоретические проблемы информатики и её приложений. Вып.3. – Изд-во Сарат. ун-та, 1999. С.131–136.

13 Тяпаев Л.Б. Аффинные классы автоматов и их преобразования. // Теоретические проблемы информатики и ее приложений, Вып. 4. – Изд-во Сарат. ун-та, 2001. С.133–135.

14 Тяпаев Л.Б. Геометрические образы автоматов как множества точек плоскости с рациональными координатами // Автоматизация проектирования дискретных систем (CAD DD'2001). Материалы IV межд. конф., Минск, Институт технической кибернетики НАН Беларуси, 2001. С.203–210.

15 Тяпаев Л.Б. Геометрическая интерпретация задач с автоматами // Проблемы теоретической кибернетики. Материалы XIII межд. конференции Ч. I,II., М.: Изд–во ЦПИ МГУ, 2002. С.178–179.

16 Тяпаев Л.Б. Применение геометрического подхода к изучению поведения автоматов // Теоретические проблемы информатики и ее приложений, Вып. 5. – Изд-во Сарат. ун-та, 2003. С.175–176.

17 Tyapaev, L.B. Geometrical Model of Automata Behaviour // CASYS'03 (Computing Anticipatory Systems). – Abstract Book, Edited by D.M. Dubois, Published by CHAOS, University of Liege, Belgium, 2003. – Symposium 3, Session 3.3, P.18.

18 Тяпаев Л.Б. Анализ геометрических образов поведения конечных автоматов // Искусственный интеллект. Интеллектуальные и многопроцессорные системы-2004, Материалы межд. науч. конференции. Т.2. Таганрог: Изд-во ТРТУ, 2004. С. 263-266.

19 Тяпаев Л.Б. О некоторых задачах для конечных автоматов, заданных геометрическими образами // Доклады академии военных наук. №1(25), 2007. С. 69-80.

20 Тяпаев Л.Б. Решение некоторых задач для конечных автоматов на основе анализа их поведения // Изв. Сарат. ун-та. Нов. сер. Сер. Математика. Механика. Информатика. 2006. Т.6. вып. 1/2. С. 121-133.

21 Матов Д. О. Аффинные преобразования геометрических образов конечных автоматов // Изв. Сарат. ун-та. Нов. сер. Сер. Математика. Механика. Информатика. 2012. Т. 12, вып. 3. С. 104-108.

22 Тяпаев Л.Б. Геометрические образы автоматов и динамические системы // Дискретная математика и ее приложения: Материалы X межд. семинара / под. ред. О.М. Касим-Заде. М.: Изд-во мех.-мат. ф-та Моск. ун-та, 2010. С.510-513.

23 Тяпаев Л.Б., Василенко Д.В., Карандашов М.В. Динамические системы, определяемые геометрическими образами автоматов // Изв. Сарат. ун-та. Нов. сер. Сер. Математика. Механика. Информатика. 2013.Т.13.№2-2. С.73-78.

24 Тяпаев Л.Б. Василенко Д.В. Динамические системы, определяемые геометрическими образами автоматов // Интеллектуальные системы. 2013. №17. С 196-201.

25 Tyapaev, L.B. Dynamical systems and geometrical images of automata // p-Adic Methods for Modeling of Complex Systems, Bielefeld University – Bielefeld, 2013.

26 Tyapaev, L. Automata as p-adic dynamical systems. – 2018. [arXiv:1709.02644v2 [math.DS]].

27 Tyapaev, L.B. Non-archimedean dynamics of the complex shift // Компьютерные науки и информационные технологии. Материалы конференции Компьютерные науки и информационные технологии, 2018. С. 406-412.

28 Khrennikov, A. Quantum mechanics from time scaling and random fluctuations at the "quick time scale". Nuovo Cimento B, 121(9):1005–1021, 2006.

29 Khrennikov, A. To quantum averages through asymptotic expansion of classical averages on infinite-dimensional space. Math. Phys., 48(1), 2007. Art. No. 013512.

30 Лунц, А.Г. Конечные p-адические автоматы, Докл. АН СССР, 1963, том 150, номер 4, 755–758.

31 Sidorov, N. Arithmetic dynamics. In S. Bezuglyi and S. Kolyada, editors, Topics in dynamics and ergodic theory, volume 310 of London Math. Soc. Lecture Note Series, pages 145–189. Cambridge University Press, Cambridge, 2003.

32 Y. Tsunoo, T. Saito, H. Kubo and T. Suzaki, "Cryptanalysis of Mir-1: A T-Function-Based Stream Cipher,"in IEEE Transactions on Information Theory, vol. 53, no. 11, pp. 4377-4383, Nov. 2007.

33 Рыков, С.В. О свойствах генератора // Дискрет. матем., 23:1 (2011), 51–71.

34 Паттерны для новичков: MVC vs MVP vs MVVM [Электронный ресурс]: [сайт]. – URL: https://habr.com/ru/post/215605/ (Дата обращения: 13.05.2020). - Загл. с экр.

35 Тестирование в Java. JUnit [Электронный ресурс]: [сайт]. – URL: https://habr.com/ru/post/120101/ (Дата обращения: 13.05.2020). - Загл. с экр.

36 Shunting Yard Algorithm [Электронный ресурс]: [сайт]. – URL: https://brilliant.org/wiki/shunting-yard-algorithm/ (Дата обращения: 3.05.2020). - Загл. с экр. - Яз. англ.

37 Глава 2. Волновые свойства частиц. [Электронный ресурс]: [сайт]. – URL: http://fn.bmstu.ru/data-physics/library/physbook/tom5/ch2/texthtml/ch2_1_text.htm (Дата обращения: 13.05.2020). - Загл. с экр.

38 Menezes, Alfred J.; Oorschot, Paul C. van; Vanstone, Scott A. Handbook of Applied Cryptography [Текст] / Menezes, Alfred J.; Oorschot, Paul C. van; Vanstone, Scott A., 2001.

39 Alexander Klimov, Adi Shamir. A New Class of Invertible Mappings [Текст] / Alexander Klimov, Adi Shamir., B.S. Kaliski Jr. et al. (Eds.): CHES 2002, LNCS 2523, pp. 470–483, 2003.

40 Криптографические основы безопасности. Лекция 6: Алгоритмы симметричного шифрования. Часть 3. Алгоритмы Rijndael и RC6. [Электронный ресурс]: [сайт]. – URL: https://www.intuit.ru/studies/courses/28/28/lecture/20420?page=3 (Дата обращения: 13.05.2020). - Загл. с экр.

41 А. Ю. Хренников, Квантовая физика и неколмогоровские теории вероятностей [Текст] / А. Ю. Хренников, 2 издание, Москва, Юрайт, 2017.

42 А. Ю. Хренников, Введение в квантовую теорию информации [Текст] / А. Ю. Хренников, Москва, Физмалит, 2008.

43 А.Ю. Хренников, В.М. Шелкович Современный p-адический анализ и математическая физика: теория и практика [Текст] / А.Ю. Хренников, В.М. Шелкович, Физмалит, 2012.