Решение диссертационного совета Д 501.001.84 на базе ФГБОУ ВО «Московский государственный университет имени М.В. Ломоносова», о приеме к защите диссертации Дергача Петра Сергеевича «Алфавитное кодирование регулярных языков с полиномиальной функцией роста» на соискание ученой степени **кандидата физико-математических наук** по специальности 01.01.09 – дискретная математика и математическая кибернетика.

Диссертация **Дергача Петра Сергеевича** «Алфавитное кодирование регулярных языков с полиномиальной функцией роста» на соискание ученой степени **кандидата физико-математических наук** по специальности 01.01.09 – дискретная математика и математическая кибернетика поступила в совет **5 апреля 2016 года** и размещена на сайте http://mech.math.msu.su/~snark/index.cgi, http://istina.msu.ru/dissertations/21301300/.

Рассмотрев заявление П.С. Дергача о принятии диссертации к защите и документы по списку ВАК, диссертационный совет **27 мая 2016 года протокол № 8(3 П)** назначил комиссию для подготовки заключения по диссертации в составе: профессор А.С. Подколзин, д.ф.-м.н., профессор С.Б. Гашков, д.ф.-м.н., профессор Н.П. Редькин.

Соискателем были представлены следующие документы:

1. Заявление соискателя на имя председателя диссертационного совета Д 501.001.84 на базе ФГБОУ ВО МГУ имени М.В. Ломоносова, д.ф.-м.н., профессора Чубарикова Владимира Николаевича — 1 экз.
2. Анкета с фотокарточкой, заверенная в установленном порядке – 2 экз.
3. Заверенная в установленном порядке копия документа государственного образца о высшем образовании – 2 экз.
4. Удостоверение о сдаче кандидатских экзаменов – 2 экз.
5. Диссертация – 6 экз. (один экз. не переплетён).
6. Автореферат диссертации.
7. Заключение кафедры математической теории интеллектуальных систем механико-математического факультета ФГБОУ ВО «Московский государственный университет имени М. В. Ломоносова» от **1 апреля 2016 года № 4(15/16)** – 2 экз.
8. Отзыв научного руководителя д.ф.-м.н., академика, профессора Кудрявцева Валерия Борисовича (Московский государственный университет имени М.В. Ломоносова) — 2 экз.
9. 4 маркированных почтовых карточки с указанием адреса соискателя и адреса диссертационного совета.

Заключение комиссии о диссертации

Представленная работа является исследованием в области дискретной математики и математической кибернетики. Целью работы является разработка нового автоматно-алгебраического подхода к решению проблемы однозначности алфавитного декадирования (ОАД), доставляющего полиномиальные верхние оценки на сложность решения проблемы в классах тонких языков и регулярных языков с полиномиальной функцией роста. Так же необходимо было разработать модель, демонстрирующую практическую ценность применения этого подхода.

Диссертация состоит из введения, раздела благодарностей, 6 глав, заключения, краткого списка обозначений и библиографии. Во введении приведен исторический обзор по теме диссертации, поставлены ее основные цели и задачи, обоснованы научная новизна и практическая значимость работы, сформулированы методология и выносимые на защиту положения, описана структура и краткое содержание диссертации.

В первой главе изложено новое автоматно-алгебраическое доказательство алгоритмической разрешимости проблемы ОАД в случае, когда кодируемое множество слов является произвольным регулярным множеством. Приводятся необходимые определения. Также описаны следствия из этого доказательства для случая, когда множества имеют полиномиальную функцию роста. В заключение, приводятся некоторые примеры,

показывающие существенную неулучшаемость предложенного алгоритма.

Во второй главе описывается класс тонких языков T(A), приводится критериальное описание его элементов в терминах прогрессивных множеств. Особо выделяется случай, когда общая ограничивающая константа на количество слов фиксированной длины в языке равна 1. Такие языки называются 1-тонкими и соответствующий им класс обозначается через T1(A). Для класса T1(A), так же как и для класса T(A), приводится критериальное описание, использующее такие понятия, как спектральная независимость и общепрогрессивное множество.

В третьей главе описывается класс языков RP(A), приводится критериальное описание его элементов в терминах множеств правильного линейного вида. Кроме того, выявляется связь введенного ранее в главе 2 класса T(A) с классом регулярных языков с не более чем линейной функцией роста.

В четвертой главе приводится решение проблемы ОАД для класса T(A) тонких языков в некотором произвольном алфавите A.

В пятой главе приводится решение проблемы ОАД для класса RP(A) регулярных языков с полиномиальной функцией роста в некотором произвольном алфавите A.

В шестой главе изучаются две проблемы вложения: проблема вложения классов допустимых регулярных языков, задаваемых функциями алфавитного кодирования (сокращенно - ВКД1) и проблема вложения классов допустимых функций алфавитного кодирования, задаваемых регулярными языками (сокращенно -ВКД2). Исследуется алгоритмическая разрешимость этих проблем.

1. Получены верхние полиномиальные оценки на сложность решения проблемы однозначности алфавитного кодирования в классах T(A) и RP(A).
2. Построена полная не избыточная классификация внутренней структуры элементов из класса T(A) в терминах конечных объединений прогрессивных множеств.
3. Построена полная не избыточная классификация внутренней структуры элементов из класса RP(A) в терминах конечных объединений множеств правильного линейного вида.
4. Найдена квадратичная зависимость между сложностью представления множеств в прогрессивном и правильном линейном видах.
5. Доказана алгоритмическая разрешимость проблемы ВКД1.
6. Доказана алгоритмическая разрешимость проблемы ВКД2 для случая, когда мощность входного алфавита равна двум.
7. Предложена модель, демонстрирующая применение полученных результатов на практике.

В работе используются методы дискретной математики, теории чисел и теории автоматов.

Научные результаты диссертации, выносимые на защиту, получены лично автором, являются новыми и обоснованы в виде строгих математических доказательств.

Основное содержание диссертации опубликовано в следующих работах автора:

1. П. С. Дергач. Об однозначности алфавитного декодирования. Дискретная математика -М.: Наука, том 24, номер 4, стр. 80-90, 2012.
2. П. С. Дергач. Об однозначности алфавитного декодирования общерегулярных сверхязыков. Дискретная математика -М.: Наука, том 26, номер 1, стр. 32-48, 2014.
3. P. S. Dergach. On uniqueness of alphabetical decoding of q-regular languages. Discrete Mathematics and Applications, издательство V S P (Netherlands), том 24, номер 3, стр. 139-152, 2014.
4. П. С. Дергач. О каноническом регулярном представлении S-тонких языков. Интеллектуальные системы, изд. МГУ, М., том 18, номер 1, стр. 211-242, 2014.
5. П. С. Дергач. О проблеме вложения допустимых классов. Интеллектуальные системы, изд. МГУ, М., том 19, номер 2, стр. 143-174, 2015.

Результаты диссертации неоднократно докладывались автором на следующих научных семинарах и всероссийских и международных конференциях.

Результаты диссертации неоднократно докладывались автором на следующих

научных семинарах и всероссийских и международных конференциях.

1. Международная конференция студентов, аспирантов и молодых ученых "Ломоносовские чтения" (7-15 апреля 2011 года, 2-9 апреля 2012 года, 15-26 апреля 2013 года, 14-23 апреля 2014 года, 18-27 апреля 2016 года, Москва, МГУ).
2. XI Международный семинар "Дискретная математика и ее приложения", посвященный 80-летию со дня рождения О.Б. Лупанова (18-23 июня 2012, Москва, МГУ).
3. Семинар "Теория автоматов" под руководством академика, профессора, д.ф.-м.н. В. Б. Кудрявцева, механико-математический факультет МГУ им. М.В. Ломоносова (2008 - 2016 г.г.).
4. Семинар "Кибернетика и информатика" под руководством академика, профессора, д.ф.-м.н. В. Б. Кудрявцева, механико-математический факультет МГУ им. М. В. Ломоносова (2008 - 2016 г.г.).
5. Семинар "Вопросы сложности алгоритмов поиска" под руководством академика АТН РФ, профессора, д.ф.-м.н. Э. Э. Гасанова, механико-математический факультет МГУ им. М. В. Ломоносова (2013 - 2016 г.г.).
6. Семинар "Дискретный анализ" под руководством член-корр. АТН РФ, профессора, д.ф.-м.н. С. В. Алешина, механико-математический факультет МГУ им. М. В. Ломоносова (2013 - 2016 г.г.).
7. Семинар "Теория графов и синтез БИС" под руководством доцента, к.ф.-м.н. А. А. Часовских, механико-математический факультет МГУ им. М. В. Ломоносова (2013 - 2016 г.г.).

Работ, написанных в соавторстве, нет.

Диссертация к защите представляется впервые.

Вышесказанное даёт основание утверждать:

Диссертация является научно-квалификационной работой, в которой содержится решение проблемы однозначности алфавитного декадирования (ОАД), доставляющее полиномиальные верхние оценки на сложность решения проблемы в классах тонких языков, классах регулярных языков с полиномиальной функцией роста, и удовлетворяет пункту 9 «Положения о порядке присуждения учены степеней» ВАК РФ. Результаты диссертации могут быть использованы в дискретной математике, теории кодирования и теории автоматов.

Диссертация удовлетворяет требованиям, предъявляемым к кандидатским диссертациям. Комиссия рекомендует принять диссертацию к защите.

Рекомендуемые официальные оппоненты и ведущая организация:

Ведущая организация: ФГБОУ ВО «Московский технологический университет». Адрес: 119454 г. Москва, проспект Вернадского, дом 78. Ректор: д.т.н., профессор Станислав Алексеевич Кудж.

Официальные оппоненты:

Доктор физико-математических наук, профессор Орлов Валентин Александрович. Место работы: ФГБОУ ВПО «Московского государственного технического университета имени Н.Э. Баумана», кафедра «Информационная безопасность». Специальность: 01.01.09.

Кандидат физико-математических наук Летуновский Алексей Александрович. Место работы: ООО «Техкомпания Хуавей», консультант. Специальность: 01.01.09.

Выбор официальных оппонентов и ведущей организации обосновывается: ФГБОУ ВО «Московский технологический университет» – один из ведущих вузов страны, в котором работают специалисты по теме диссертации. Официальные оппоненты являются специалистами в дискретной математики и теории автоматов (имеются работы, близкие к теме диссертации соискателя).

Работы официальных оппонентов, близкие к теме диссертации:

доктор физико-математических наук, профессор Орлов Валентин Александрович имеет следующие работы, близкие к теме диссертации:

1. Орлов В.А. О полноте систем конечных автоматов. Дискретная математика, т.9, в.2, М., 1997
2. Орлов В.А., Конявский В.А. Общеавтоматное шифрование. Безопасность информационных технологий. №2, 2009
3. Орлов В.А., Карташова М.В. О псевдослучайных последовательностях на основе линейных преобразований. Безопасность информационных технологий, № 3, 2009.
4. Орлов В.А., Баканов В.М. Программная и техническая реализация криптоалгоритмов. Программная и техническая реализация криптоалгоритмов. Учебное пособие. -М.: МГУПИ, 2009.
5. Орлов В.А., Мельников Д.А. Современная криптография и архитектура безопасности компьютерных сетей. Современная криптография и архитектура безопасности компьютерных сетей. Учебное пособие-М.: МГУПИ, 2009.

кандидат физико-математических наук Летуновский Алексей Александрович, имеет следующие работы, близкие к теме диссертации:

1. Летуновский А.А. Задача выразимости автоматных функций относительно расширенной суперпозиции, Автореферат диссертации на соискание ученой степени кандидата физико-математических наук. Москва, 2015.
2. Летуновский А.А. О выразимости константных автоматов. Ин- теллектуальные системы, т.9, вып.1-4, 2005, с.457–469.
3. Летуновский А.А. О выразимости константных автоматов су- перпозициями. Интеллектуальные системы, т.13, вып.1-4,2009, с.397–406.
4. Летуновский А.А. О выразимости суперпозициями автоматов с разрешимыми группами. Интеллектуальные системы, т.14, вып.1- 4, 2010, с.379–393.
5. Летуновский А.А. О задаче выразимости автоматов относительно суперпозиции для систем с фиксированной добавкой. Интеллектуальные системы, т.15, вып.1-4, 2011, с.401–412.
6. Летуновский А.А. Цикловые индексы автомата. Дискретная математика, т.25, вып.4, 2013, с.24–29.

Работы сотрудников ФГБОУ ВО «Московский технологический университет» (ведущей организации), близкие к теме диссертации:

к. ф.-м. н., доцент Карташов Сергей Иванович; имеет следующие работы, близкие к теме диссертации:

1. Карташов С.И., О строении решеток замкнутых классов некоторых функциональных систем типа Поста, Материалы Всесоюзного семинара по дискретной математике и ее приложениям, МГУ, 1986г.

2. Карташов С.И., О счетных решетках замкнутых классов функциональных систем типа Поста, Деп. в ВИНИТИ 01.12.86г., № 8106-В86

3 Карташов С.И., О континуальных решетках замкнутых классов функциональных систем типа Поста, Деп. в ВИНИТИ 01.12.86г., № 8107-В86

4. Карташов С.И., Конечность числа замкнутых классов в <Pk,Pk>, Логико-алгебраические конструкции, Калинин, 1987г

5. Карташов С.И., О F6 – решетке, Деп. в ВИНИТИ 22.04.87г., № 2818-В87

6. Карташов С.И., О D2 – решетке, Деп. в ВИНИТИ 22.04.87г., № 2819-В87

7. Карташов С.И., О некоторых функциональных системах типа Поста, Алгебро-логические конструкции, Калинин, 1987г.

к. ф.-м. н., доцент Макаров Владимир Владимирович; имеет следующие работы, близкие к теме диссертации:

1. Макаров В.В., О порядках элементов группы автоматных перестановок, Вестник МГУ.-1991. - №4. - С. 86 – 87.

2. Макаров В.В., О топологических свойствах группы автоматных перестановок,

Алгебра, геометрия и дискретная математика в нелинейных задачах. – МГУ. –1991. – С.91 – 97.

3. Макаров В.В., Порождающая система из элементов бесконечного порядка в группе автоматных перестановок ASn, Деп. в ВИНИТИ. -1995. -№3294 –В95. - С. 1 – 16.

4. Макаров В.В., О группах автоматных перестановок, Фундаментальная и прикладная математика. – 1996. – Том 2. Вып. 1. – С. 171 – 186.

5. Макаров В.В., О топологических характеристиках автоматных групп, Сб. Трудов Семинара по дискретной математике и ее приложениям. – 1997. – МГУ. – С. 143 – 146.

6. Макаров В.В., Группа автоматных перестановок ASn порождается элементами бесконечного порядка, Дискретная математика. – 1997. – Том 9. – Вып. 3. – С. 117 – 124.

7. Макаров В.В., О некоторых задачах выразимости в группах автоматных перестановок, Интеллектуальные системы. – 1998. – Том 3 – Вып. 1 – 2. – С. 233 – 238.

Диссертационный совет Д 501.001.84 на базе ФГБОУ ВО МГУ имени М.В. Ломоносова, вынес **решение принять** диссертацию Дергача П.С. «Алфавитное кодирование регулярных языков с полиномиальноой функцией роста» **к защите** 3 июня, протокол № 8(3п). Разместить текст диссертации, автореферата, отзыв научного руководителя и решение совета **на сайте ФГБОУ ВО МГУ имени М. В. Ломоносова** (http://mech.math.msu.su/~snark/index.cgi, http://istina.msu.ru/dissertations/21301300/.) и **на сайте ВАК Минобрнауки РФ** разместить объявление о защите диссертации и автореферат.

Постановили.

1. Новизна и актуальность темы диссертации не вызывают сомнений. Она подтверждается экспертизой. Основные результаты диссертации опубликованы в полной мере.

2. Назначить ведущую организацию:

ФГБОУ ВО «Московский технологический университет». Адрес: 119454 г. Москва, проспект Вернадского, дом 78.

Назначить официальными оппонентами:

д.ф.-м.н., профессора Орлова Валентина Александровича, ФГБОУ ВПО «Московского государственного технического университета имени Н.Э. Баумана», кафедра «Информационная безопасность»;

к.ф.-м.н. Летуновского Алексея Александровича, ООО «Техкомпания Хуавей», старший разработчик.

3. Назначить дату защиты — **21 октября 2016 года.**

4. Разрешить печатание автореферата диссертации на правах рукописи. Автореферат правильно отражает содержание диссертации.

5. Рассылку авторефератов произвести по «списку рассылки авторефератов диссертации» без изменений.

6. Поручить комиссии в составе: профессор А.С. Подколзин, д.ф.-м.н., профессор С.Б. Гашков, д.ф.-м.н., профессор Н.П. Редькин подготовку заключения по диссертации к защите по существующей форме ВАК Минобрнауки РФ.

Результаты голосования по вопросу о принятии к защите диссертации **Дергача Петра Сергеевича** на тему «Алфавитное кодирование регулярных языков с полиномиальной функцией роста» на соискание ученой степени **кандидата физико-математических наук** по специальности 01.01.09 – дискретная математика и математическая кибернетика к защите: за 18, против 0, воздержавшихся 0.

Председатель диссертационного совета
Д 501.001.84 на базе ФГБОУ ВО МГУ имени М.В. Ломоносова,
профессор В. Н. Чубариков

Учёный секретарь диссертационного совета
Д 501.001.84 на базе ФГБОУ ВО МГУ имени М.В. Ломоносова,
д.ф.-м.н., доцент В. М. Мануйлов