

ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА Д 002.077.05
НА БАЗЕ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО
УЧРЕЖДЕНИЯ НАУКИ ИНСТИТУТА ПРОБЛЕМ ПЕРЕДАЧИ
ИНФОРМАЦИИ им. А. А. ХАРКЕВИЧА РОССИЙСКОЙ АКАДЕМИИ НАУК
ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ
ДОКТОРА НАУК

аттестационное дело № _____

решение диссертационного совета

от «01» октября 2018 года, протокол № 39

О присуждении Трифонову Петру Владимировичу ученой степени доктора технических наук.

Диссертация «Методы построения и декодирования многочленных кодов» по специальности 05.13.17 – Теоретические основы информатики (технические науки), принята к защите 14 мая 2018 года, протокол № 36, диссертационным советом Д 002.077.05 на базе Федерального государственного бюджетного учреждения науки Института проблем передачи информации им. А. А. Харкевича Российской академии наук (127051, Москва, Б. Каретный пер., 19, строение 1, приказ о создании диссертационного совета от «10» июля 2015 года № 784/нк).

Соискатель Трифонов Петр Владимирович, гражданин Российской Федерации 1980 года рождения, в 2003 году окончил Санкт-Петербургский государственный политехнический университет, работает заведующим лабораторией «Помехоустойчивое кодирование в компьютерных сетях» Федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский политехнический университет Петра Великого».

Диссертацию на соискание ученой степени кандидата технических наук на тему «Адаптивное кодирование в многочастотных системах» по специальности 05.13.01 – Системный анализ, управление и обработка

информации (информатика) защитил в 2005 году в диссертационном совете, созданном на базе Санкт-Петербургского государственного политехнического университета.

Диссертация на соискание ученой степени доктора технических наук выполнена в высшей школе «Программная инженерия» института компьютерных наук и технологий Федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский политехнический университет Петра Великого» (далее СПбПУ).

Официальные оппоненты:

1. Егоров Сергей Иванович, гражданин РФ, доктор технических наук, профессор, профессор кафедры вычислительной техники Федерального государственного бюджетного образовательного учреждения высшего образования «Юго-Западный государственный университет» (далее ЮЗГУ),
2. Кабатянский Григорий Анатольевич, доктор физико-математических наук, советник ректора по науке Автономной некоммерческой образовательной организации высшего образования «Сколковский институт науки и технологий» (далее Сколтех),
3. Кудряшов Борис Давидович, доктор технических наук, профессор, профессор кафедры информационных систем Федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики» (далее ИТМО)

дали **положительные** отзывы о диссертации.

Ведущая организация – Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения» (далее ГУАП) - в своем **положительном** отзыве, подписанном заведующим кафедрой № 52 Инфокоммуникационных систем, доктором технических наук,

профессором Тюрликовым Андреем Михайловичем и заведующим кафедрой № 51 Безопасности информационных систем, кандидатом технических наук, доцентом Овчинниковым Андреем Анатольевичем и утверждённом ректором ГУАП, доктором экономических наук, профессором Антохиной Юлией Анатольевной, указала, что теоретическая значимость работы весьма велика и что, в частности, концепция многочленных кодов и циклотомический алгоритм БПФ должны войти во все учебники по теории кодирования и быстрым алгоритмам. Результаты диссертационной работы рекомендуются к использованию в учебном процессе и для организации канального кодирования, например, в системах мобильной связи 5G, в таких организациях, как Институт проблем передачи информации им. А.А.Харкевича Российской академии наук, Сибирский государственный университет телекоммуникаций и информатики, Новосибирский государственный университет, ГУАП, СПбПУ, Московский государственный университет имени М. В. Ломоносова, Московский физико-технический институт (государственный университет), Национальный исследовательский университет «Московский институт электронной техники», Национальный исследовательский университет «Высшая школа экономики», Автономная некоммерческая образовательная организация высшего образования «Сколковский институт науки и технологий», ООО Техкомпания Хуавэй. Отзыв заслушан и одобрен на совместном заседании кафедр № 51 Безопасности информационных систем и № 52 Инфокоммуникационных систем ГУАП «01» июня 2018 г. (протокол № 9/2017- 2018).

Соискатель имеет 66 опубликованных работ, из них 26 по теме диссертации, в том числе 26 работ, опубликованных в рецензируемых научных изданиях, включенных в перечень изданий для опубликования основных научных результатов диссертаций. Соискателем опубликовано 14 работ в материалах всероссийских и международных конференций и симпозиумов. Все основные результаты, представленные в диссертации, принадлежат лично Трифонову

П.В. В диссертации отмечен вклад автора в работы, опубликованные совместно с соавторами.

Наиболее значимые работы по теме диссертации:

1. Trifonov, P. Polar subcodes / P. Trifonov, V. Miloslavskaya // IEEE Journal on Selected Areas in Communications. — 2016. — February. — Vol. 34, no. 2. —P. 254–266.
2. Trifonov, P. Efficient design and decoding of polar codes / Peter Trifonov //IEEE Transactions on Communications.—2012.—November.—Vol. 60, no. 11.—P. 3221 – 3227
3. Trifonov, P. Efficient interpolation in the Guruswami-Sudan algorithm /P. Trifonov // IEEE Transactions on Information Theory.—2010.—September.—Vol. 56, no. 9.—P. 4341–4349.
4. Trifonov, P. Efficient interpolation in Wu list decoding algorithm / P. Trifonov, M. H. Lee // IEEE Transactions on Information Theory.—2012.—September.—Vol. 58, no. 9.—P. 5963–5971.
5. Трифонов, П. В. Метод быстрого вычисления преобразования Фурье над конечным полем / П. В. Трифонов, С. В. Федоренко // Проблемы передачи информации.-2003. – Т. 39, № 3. _С. 3–10.

На диссертацию и автореферат поступило 12 отзывов, включая отзывы официальных оппонентов и ведущей организации, каждый из которых содержит **положительную оценку** работы Трифонова П.В. и вывод о её соответствии требованиям, предъявляемым Высшей аттестационной комиссией к докторским диссертациям на соискание степени доктора технических наук по специальности 05.13.17 – «Теоретические основы информатики».

В отзыве ведущей организации сделаны следующие замечания, которые не оказывают влияния на общую положительную оценку работы.

- 1) Предложенная концепция многочленных кодов не дает фундаментального пересмотра сложившейся теории.
- 2) Очень большой объем списка при декодировании. Для кода Рида-Соломона (31,15) объем списка 16384 не кажется приемлемым.

- 3) Недостаточно хорошо описана модель хранения данных.
- 4) Отсутствует сравнение предлагаемых алгоритмов декодирования расширенных кодов БЧХ с ранее известными алгоритмами.
- 5) Сложность некоторых алгоритмов БПФ в Таблице 6.1 сильно устарела, в ней не указаны современные алгоритмы.

В отзыве официального оппонента доктора технических наук, профессора Егорова Сергея Ивановича отмечен ряд недостатков, которые не снижают научную и практическую ценность работы. Замечания следующие:

- 1) В диссертации приводятся оценки вычислительной сложности алгоритмов декодирования в среднем, что достаточно для оценки сложности низкоскоростных декодеров, к которым к тому же не предъявляются жесткие требования по задержке декодирования. Однако для высокоскоростных декодеров с высокой степенью параллелизма важно получить оценки сложности для худших случаев.
- 2) Предложенные звездные полярные подкоды, судя по представленным результатам, допускают не более чем 3-кратное распараллеливание в декодере без существенной потери корректирующей способности.
- 3) Неясно, способен ли предложенный последовательный алгоритм обеспечить декодирование рассматриваемых в работе кодов по максимуму правдоподобия
- 4) Неясно, какой объем оперативной памяти требуется для реализации предложенного последовательного алгоритма декодирования.
- 5) В диссертации не показана целесообразность использования быстрого алгоритма двумерной интерполяции в быстродействующих декодерах кодов Рида-Соломона, используемых на практике. Не дана сравнительная оценка сложности предлагаемого декодера и стандартного декодера, исправляющего ошибки в пределах половины минимального кодового расстояния для популярных кодов Рида-Соломона.
- 6) В работе не описана процедура построения алгоритма умножения на двоичную матрицу A , использованная в предложенном циклотомическом

алгоритме быстрого преобразования Фурье.

В отзыве официального оппонента доктора физико-математических наук, Кабатянского Григория Анатольевича указаны следующие недостатки.

- 1) Формулировка и доказательство теоремы 1 (стр. 53), которая говорит, что любой линейный код четной длины может быть получен с помощью обобщенной конструкции Плоткина, могла бы быть более понятной и близкой к конструкции Плоткина. Классическая конструкция Плоткина, также известная как $(u, u+v)$ конструкция, строит из двух кодов одинаковой длины, но разной мощности и с разным минимальным кодовым расстоянием, код удвоенной длины, мощности равной произведению мощностей исходных кодов, и с минимальным кодовым расстоянием, равным минимуму из расстояния первого кода и удвоенного расстояния второго кода. К сожалению, теорема 1 никакой информации о расстоянии построенного кода не дает (да и вряд ли может дать, так как описывает слишком общую ситуацию).
- 2) Оценка для вероятности ошибки декодирования на стр. 59 не вполне корректна.
- 3) На стр.156-158 представлены результаты статистического моделирования $(31, 15, 16)$ кода Рида-Соломона (над полем из 32 элементов). На самом деле это $(31, 15, 17)$ код. Надеюсь, что это просто опечатка, которая повторилась и в автореферате.
- 4) Неудачное название – многочленные коды. Дело в том, что понятие polynomial codes возникло еще в конце 60х годов прошлого века, и диссертант знает про эти работы, и цитирует их. Иметь в русском языке (научном) одновременно и многочленные, и полиномиальные коды кажется мне, как минимум, странным.

В отзыве официального оппонента доктора технических наук, профессора Кудряшова Бориса Давидовича отмечено, что результаты исследований представляют значительный вклад как в теорию кодирования, так

и в современное состояние технологии беспроводной связи, и приведены следующие замечания:

- 1) С точки зрения способа представления материала, работа выиграла бы, если бы ее фундаментальные положения были сформулированы в виде теорем, а промежуточные результаты, используемые как аргументы в доказательствах - в виде лемм.
- 2) Параграф 2.3, посвященный анализу вероятности ошибки декодирования, неубедителен. Замечу, что выводы, основанные на результатах анализа для стирающего канала, далеко не всегда верны для других моделей.
- 3) Представленные на Рис. 2.3 результаты сравнения сложности списочного декодера с объемом списка 1024 со сложностью алгоритма BEAST требуют более детального обсуждения. Дело в том, что с увеличением отношения сигнал-шум сложность BEAST в расчете на символ кодового слова стремится практически к нулю. Однако, на графике сложность обоих алгоритмов стремится к довольно большой константе.
- 4) Глава 4, посвященная вопросам декодирования полярных кодов, содержит много практически значимых результатов, которые относятся к разным классам кодов, и выбор лучшего решения предоставляется читателю. Однако, даже специалисту по теории кодирования трудно ориентироваться в этом множестве вариантов. Недостает иерархии решений и диаграммы, указывающей рекомендации автора в зависимости, например, от длины и скорости кодов, или от длины и ограничений на сложность декодирования.
- 5) Хотя все необходимые ссылки на известные результаты приведены, по тексту работы довольно трудно выделить те идеи и решения, которые принципиально отличают новый способ интерполяции от известных.
- 6) Еще один вопрос касается предложенной рандомизированной процедуры построения базиса Гребнера (рис. 5.2). Во-первых, сравнение с детерминированными процедурами может быть некорректным, т.к. сравнивается средняя сложность с максимальной. Во-вторых, зафиксировав начальное

состояние датчика псевдослучайных чисел, получаем неслучайную процедуру. Насколько критичен результат к выбору начального значения?

- 7) Алгоритм Кнута - не самый эффективный алгоритм возведения в степень, хотя в асимптотике по длине двоичной записи степени все алгоритмы имеют примерно одинаковую эффективность. Насколько можно выиграть по сложности, выбирая более изощренные алгоритмы?
- 8) Как указывает сам автор, алгоритм Лина и др. асимптотически лучше предлагаемого алгоритма БПФ. Как соотносятся алгоритмы для конечных длин?

В отзыве на автореферат доктора технических наук, профессора Мещерякова Романа Валерьевича, проректора по научной работе и инновациям Томского государственного университета систем управления и радиоэлектроники (ТУСУР), заведующего кафедрой безопасности информационных систем, имеются следующие замечания к содержанию автореферата: отсутствуют аналитические оценки средней сложности последовательного алгоритма декодирования; неясно, как в общем случае выбирать конструктивное минимальное расстояние полярных подкодов кодов БЧХ; приведены результаты для полярных подкодов с ядрами БЧХ и Рида-Соломона, но не описана процедура, использованная для расчета надежности подканалов соответствующих поляризующих преобразований.

В отзыве на автореферат доктора технических наук, профессора Рябко Бориса Яковлевича, заведующего лабораторией информационных систем и защиты информации Института вычислительных технологий Сибирского отделения Российской академии наук (Новосибирск), содержатся замечания: отсутствует аналитическая оценка зависимости корректирующей способности полярных подкодов от параметров их конструкции и списочного/последовательного алгоритма декодирования; неясно, существует ли такой набор параметров предложенного последовательного алгоритма, который обеспечивал бы декодирование полярных подкодов по максимуму правдоподобия; предложенный последовательный алгоритм обеспечивает

снижение средней сложности декодирования, в то время как на практике во многих случаях имеет значение максимальная сложность и задержка декодирования, которые остаются весьма высокими.

В отзыве на автореферат доктора технических наук, профессора Яковлева Виктора Алексеевича, профессора кафедры защищенных систем связи Санкт-Петербургского Государственного университета телекоммуникаций имени профессора М.А.Бонч-Бруевича, к содержанию автореферата предъявлены следующие замечания: неясно, как соотносятся корректирующие способности различных рассмотренных в работе процедур декодирования кодов Рида-Соломона; неясно, насколько близка корректирующая способность предложенных полярных подкодов к фундаментальным нижним границам; неясно, какова задержка предлагаемого метода последовательного декодирования в среднем и худшем случае.

Положительные отзывы на автореферат доктора технических наук Фионова Андрея Николаевича, профессора кафедры прикладной математики и кибернетики Сибирского государственного университета телекоммуникаций и информатики (Новосибирск) и доктора физико-математических наук, профессора Соловьевой Фаины Ивановны, ведущего научного сотрудника Института математики им. С.Л.Соболева СО РАН, замечаний не содержат.

В отзыве на автореферат АО «НПО «Импульс» (Санкт-Петербург), утвержденном заместителем генерального директора по науке и производству – главным конструктором, заслуженным деятелем науки РФ, доктором технических наук, профессором Доценко Сергеем Михайловичем, также имеется ряд замечаний: неясно, какова задержка декодирования полярных подкодов с использованием предложенного последовательного алгоритма; результаты статистического моделирования представлены для случая аддитивного гауссовского канала и канала с релейскими замираниями, неясно, как ведут себя предложенные коды в более сложных каналах передачи данных; судя по приведенным результатам, энергетический выигрыш, обеспечиваемый

полярными подкодами по сравнению с LDPC кодами, сокращается с увеличением длины кода.

В отзыве на автореферат кандидата технических наук Черныша Александра Викторовича, руководителя Департамента Беспроводной Передачи Информации ОАО «ГлобалИнформСервис» (Москва), содержатся следующие замечания: неясно, как влияют параметры декодера (например, длина списка) на изменение характеристик корректирующих кодов; не описан механизм реализации приоритетной очереди в последовательном алгоритме декодирования и его влияние на общую сложность алгоритма.

В отзыве на автореферат кандидата технических наук Смородинова Александра Александровича, ведущего специалиста ООО ПЛАЗ (Санкт-Петербург), есть три замечания: применение последовательного алгоритма может привести к существенному росту задержки декодирования; неясно, какой объем оперативной памяти требуется для работы предложенного последовательного алгоритма декодирования; отсутствуют оценки агрегатной сложности кода предлагаемых полярных кодов. Пояснение. Под агрегатной сложностью понимается общая сложность кода, способного кодировать/декодировать код для заранее определенного набора длин кодовых слов, кодовых скоростей и их сочетаний.

Выбор официальных оппонентов и ведущей организации обосновывается их компетентностью в исследуемой области, что подтверждается научными публикациями и патентами. Доктор технических наук, профессор Сергей Иванович Егоров является известным специалистом в области построения алгоритмов декодирования корректирующих кодов и их практической реализации, автором патентов и множества научных работ в российских и зарубежных журналах. Доктор физико-математических наук Григорий Анатольевич Кабатянский является признанным специалистом в вопросах теории кодирования и криптографии, имеет множество публикаций в профильных международных журналах. Доктор технических наук, профессор Борис Давидович Кудряшов является авторитетным специалистом к области

теории кодирования, имеет большое число высокоцитируемых публикаций в ведущих мировых изданиях. Ведущая организация Санкт-Петербургский государственный университет аэрокосмического приборостроения выполняет теоретические и прикладные исследования в области передачи и защиты информации, результаты которых публикуются в рецензируемых научных изданиях.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

- 1. разработана** математическая модель многочленных кодов, позволяющая представить линейные блочные коды в виде системы ограничений на входные символы поляризующего преобразования, называемых ограничениями динамического замораживания, и позволяющая осуществлять их декодирование с помощью метода последовательного исключения и его обобщений.
- 2. предложены** новый класс корректирующих кодов, называемый полярными подкодами, а также последовательный алгоритм декодирования полярных кодов и полярных подкодов, совместное использование которых обеспечивает одновременно лучшую корректирующую способность и меньшую сложность декодирования по сравнению с известными полярными, LDPC и турбо-кодами;
- 3. предложен** нетрадиционный подход к декодированию расширенных кодов БЧХ и Рида-Соломона, основанный на использовании разработанной математической модели линейных блочных кодов и предложенного последовательного алгоритма декодирования полярных подкодов, обеспечивающий меньшую сложность и/или лучшую корректирующую способность по сравнению с известными аналогами;
- 4. разработаны** новые быстрые алгоритмы, реализующие интерполяционный шаг методов Гурусвами-Судана и Ву списочного декодирования кодов Рида-Соломона, имеющие меньшую сложность по сравнению с известными аналогами;

5. предложен новый подход к быстрому вычислению дискретного преобразования Фурье над конечным полем, основанный на использовании структуры его классов сопряженности, и на его основе создан быстрый метод кодирования информации в отказоустойчивых системах хранения данных, использующих коды Рида-Соломона.

Теоретическая значимость исследования обоснована тем, что:

изложена концепция многочленных кодов, обобщающая концепции полиномиальных и мономиальных кодов, которая позволяет:

- использовать для его декодирования метод последовательного исключения, а также его списочное и последовательное обобщения;
- строить новые корректирующие коды, оптимизируя их корректирующую способность с учетом ограничений на сложность декодирования;

доказаны теоремы о структуре ограничений динамического замораживания, задающих расширенные примитивные коды БЧХ и Рида-Соломона в узком смысле, результативно использующие аппарат алгебраической теории кодирования, а также **доказаны** теоремы, обосновывающие корректность предложенного двоичного алгоритма, реализующего интерполяционный шаг методов Гурсвами-Судана и Ву списочного декодирования кодов Рида-Соломона, результативно использующие аппарат коммутативной алгебры;

разработаны метод декодирования полярных подкодов и иных кодов, представленных в виде системы ограничений динамического замораживания, быстрый метод двумерной интерполяции при списочном декодировании кодов Рида-Соломона, а также быстрый метод систематического кодирования кодов Рида-Соломона, которые позволяют снизить вычислительную сложность решения соответствующих задач;

изучены свойства линейных блочных кодов, влияющие на корректирующую способность при их декодировании методом последовательного исключения и его аналогами.

Значение полученных соискателем результатов исследования для практики

подтверждается тем, что:

- 1) результаты, связанные с концепцией полярных подкодов, а также их построением и декодированием **были использованы** ООО «Техкомпания Хуавэй»;
 - 2) **они использованы в** ООО «Санкт-Петербургский центр разработок ЕМС» при разработке высокопроизводительных отказоустойчивых систем хранения данных для сегментов среднего бизнеса, а также при решении задач создания географически распределенного объектного хранилища, что позволило повысить скорость кодирования данных и отказоустойчивость систем хранения данных;
 - 3) **они внедрены в** носимых станциях метеорной связи системы информационного обеспечения судоходства Северного морского пути;
- создана** система практических рекомендаций по выбору параметров предложенных конструкций полярных подкодов.

Оценка достоверности результатов исследования выявила:

- результаты получены на основе классического аппарата алгебраической теории кодирования, теории информации, коммутативной алгебры, теории вероятностей;
- для всех предложенных алгоритмов была создана программная реализация, с помощью которой их характеристики были исследованы методами статистического моделирования;
- полученные результаты согласуются с результатами, опубликованными другими исследователями, в том числе нижней границей Полянского-Пура-Верду и оценками вероятности ошибки декодирования по максимуму правдоподобия кодов БЧХ.

Личный вклад соискателя: научные положения и результаты, составляющие основное содержание диссертации, получены автором лично.

Представленная Трифионовым Петром Владимировичем диссертация отвечает паспорту специальности 05.13.17 – «Теоретические основы информатики» в части пункта 11 «Разработка методов обеспечения

высоконадежной обработки информации и обеспечения помехоустойчивости информационных коммуникаций для целей передачи, хранения и защиты информации; разработка основ теории надежности и безопасности использования информационных технологий».

Диссертационный совет пришел к выводу о том, что диссертация представляет собой завершенную научно-квалификационную работу, в которой решена актуальная задача построения и декодирования многочленных кодов на основе их представления в виде системы ограничений динамического замораживания, имеющая важное теоретическое и прикладное значение.

По актуальности, новизне, теоретической значимости диссертация соответствует требованиям, установленным «Положением о порядке присуждения ученых степеней», утвержденным постановлением Правительства Российской Федерации от 24 сентября 2013 года № 842, предъявляемым к диссертациям на соискание ученой степени доктора наук.

На заседании 01 октября 2018 года диссертационный совет принял решение присудить Трифонову Петру Владимировичу ученую степень доктора технических наук по специальности 05.13.17 – «Теоретические основы информатики».

При проведении тайного голосования диссертационный совет в количестве 24 человек, из них 5 докторов наук по специальности и отрасли наук рассматриваемой диссертации, участвовавших в заседании, из 36 человек, входящих в состав совета, проголосовали: за присуждение учёной степени – 23, против присуждения учёной степени – 1, недействительных бюллетеней – 0.

Председатель

диссертационного совета Д 002.077.05

Кулешов А.П.

Ученый секретарь

диссертационного совета Д 002.077.05

Цитович И.И.

«01» октября 2018 г.

