На правах рукописи

Милославская Вера Дмитриевна

Методы построения и декодирования полярных кодов

05.13.01 – Системный анализ, управление и обработка информации (информатика)

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Санкт-Петербург – 2014

Работа выполнена в *федеральном государственном автономном образовательном учреждении высшего образования «Санкт-Петербургский государственный политехнический университет»*.

Научный руководитель:	*кандидат технических наук,* *доцент,* *Трифонов Пётр Владимирович*
Официальные оппоненты:	*Кудряшов Борис Давидович,* *доктор технических наук* *профессор,* *профессор кафедры информационных систем,* *ФГАОУ ВО «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»,* *Беззатеев Сергей Валентинович,* *доктор технических наук,* *доцент,* *зав. кафедрой технологий защиты информации,* *ФГАОУ ВПО «Санкт-Петербургский государственный университет аэрокосмического приборостроения»*
Ведущая организация:	*ФГБУН «Институт проблем передачи информации им. А.А. Харкевича» РАН*

Защита состоится 19.03.2015 в 16:00 часов на заседании диссертационного совета *Д 212.229.18* при *ФГАОУ ВО «Санкт-Петербургский государственный политехнический университет»*, расположенном по адресу: *195251, г. Санкт-Петербург, ул. Политехническая, д. 29*

С диссертацией можно ознакомиться в библиотеке *ФГАОУ ВО «Санкт-Петербургский государственный политехнический университет»* и на сайте www.spbstu.ru.

Автореферат разослан «____» _____ 2014 г.

Ученый секретарь
диссертационного совета,
кандидат технических наук, доцент *Васильев Алексей Евгеньевич*

Общая характеристика работы

Актуальность темы исследования. Технологии помехоустойчивого кодирования являются неотъемлемой частью современных систем хранения и передачи информации. За годы развития теории помехоустойчивого кодирования было построено большое число разнообразных кодов исправляющих ошибки. Однако их характеристики остаются весьма далекими от теоретических пределов, а вероятность ошибки декодирования, демонстрируемая ими при использовании в системах передачи информации, оказывается значительно хуже принципиально достижимой. Одной из причин этого является невозможность практического использования оптимальных алгоритмов декодирования, сложность которых оказывается чрезмерно высокой.

В 2008 году Е. Ариканом были предложены полярные коды и было показано, что они достигают пропускной способности широкого класса каналов передачи информации. Последнее означает, что для любой сколь угодно малой величины $p > 0$ существует такое целое число m, что полярный код длины $n = 2^m$ со скоростью R, меньшей пропускной способности канала, обеспечивает вероятность ошибки меньше p.

Степень разработанности темы исследования. Конструкция полярных кодов была обобщена С.Б. Корадой, Е. Сасоглу и Р.Л. Урбанке. Кроме того, было показано, что полярные коды относятся к классу обобщенных каскадных кодов, предложенных Э.Л. Блохом и В.В. Зябловым. Полярные коды могут быть также представлены как многоуровневые коды. Последние были предложены Х. Имаи и исследованы У. Ваксманном, Р.Ф. Фишером и Д.Б. Хубером. Конструкции кодов, достигающих пропускной способности канала, рассматривались ранее в работах Дж.Д. Форни, Э.Л. Блоха, В.В. Зяблова, А.М. Барга, Ж. Земора, Р.М. Рота, В. Скачека и некоторых других исследователей. Отличительной особенностью полярных кодов является простота процедур их построения, кодирования и декодирования, что делает их привлекательными для практического использования.

Однако, эксперименты показывают, что вероятность ошибки декодирования полярных кодов с практически значимыми параметрами, то есть значениями n порядка нескольких тысяч, оказывается значительно больше, чем у кодов с малой плотностью проверок на четность (МППЧ) и турбо-кодов с аналогичными параметрами. Это обусловлено малым минимальным расстоянием полярных кодов и субоптимальностью алгоритма последовательного исключения, используемого для их декодирования. И. Талом и А. Варди был предложен алгоритм списочного декодирования, построенный на базе алгоритма последовательного исключения и обеспечивающий декодирование полярных кодов почти по максимуму правдоподобия. Также ими был предложена конструкция полярных кодов с контрольной суммой, демонстрирующая существенно меньшую вероятность ошибки декодирования по сравнению с классическими полярными кодами. К. Нию и К. Чень предложили обобщение стекового алгоритма К.Ш. Зигангиро-

ва. При меньшей вычислительной сложности этот алгоритм обеспечивает ту же вероятность ошибки декодирования, что и списочный алгоритм Тала-Варди. Тем не менее, сложность декодирования полярных кодов остается выше, чем существующих аналогов. Указанные проблемы препятствуют широкому практическому применению полярных кодов.

Одним из наиболее широко используемых классов корректирующих кодов являются коды Рида-Соломона. При этом остается актуальной задача построения эффективных алгоритмов их мягкого декодирования. Следует отметить, что сложность существующих алгоритмов мягкого декодирования кодов Рида-Соломона, таких как метод Кёттера-Варди, является достаточно высокой. Это приводит к тому, что системы передачи и хранения информации, использующие коды Рида-Соломона, демонстрируют энергетический проигрыш порядка 3 дБ по сравнению с теоретическим пределом. Наиболее трудоемким шагом алгоритма Кёттера-Варди является построение полинома от двух переменных, имеющего корни различной кратности. Вопрос построения быстрых алгоритмов, реализующих этот шаг, исследовался Р. Кёттером, Р.Р. Нильсоном, К. Ли и М.Е. О'Салливаном. Следует отметить, что метод Кёттера-Варди не обеспечивает декодирование кодов Рида-Соломона по максимуму правдоподобия, и открытой остается задача построения алгоритмов декодирования с большей корректирующей способностью.

Цели и задачи. Цель диссертационной работы состоит в создании методов кодирования и декодирования информации, основанных на теории полярных кодов, обеспечивающих меньшую вероятность ошибки и меньшую сложность декодирования по сравнению с существующими аналогами с практически значимыми параметрами. Для достижения поставленной цели необходимо решить следующие задачи:

1. Разработать быстрый алгоритм мягкого декодирования двоичных полярных кодов, обеспечивающий меньшую вероятность ошибки декодирования по сравнению с методом последовательного исключения.
2. Разработать конструкции кодов, декодирование которых может быть выполнено с помощью предложенного быстрого алгоритма, обладающих при этом большим минимальным расстоянием по сравнению с полярными кодами с ядром Арикана.
3. Разработать метод укорочения полярных кодов.
4. Разработать быстрый алгоритм мягкого декодирования кодов Рида-Соломона.
5. Разработать высокопроизводительный метод кодирования информации для отказоустойчивых систем хранения данных.

Научная новизна:

1. Предложена конструкция полярных подкодов Боуза-Чоудхури-Хоквингема с минимальным расстоянием большим, чем у полярных кодов с ядром Арикана с аналогичными параметрами.
2. Разработан новый метод построения укороченных полярных кодов.

3. Предложен новый метод последовательного декодирования полярных кодов, основанный на использовании оценок максимума апостериорных вероятностей кодовых слов.
4. Разработан новый алгоритм декодирования кодов Рида-Соломона, основанный на методе последовательного декодирования полярных кодов.
5. Предложен новый алгоритм, реализующий этап двумерной интерполяции в методе Кёттера-Варди декодирования кодов Рида-Соломона.
6. Разработан новый высокопроизводительный метод кодирования информации укороченными полярными подкодами (в частности, полярными кодами) для отказоустойчивых систем хранения данных.

Теоретическая и практическая значимость работы. В работе представлен набор методов построения и декодирования полярных кодов, а также кодов Рида-Соломона. Эти методы могут найти свое применение в современных и перспективных системах передачи информации.

Предложен метод построения подкодов расширенных кодов Боуза-Чоудхури-Хоквингема (полярных подкодов БЧХ), обеспечивающих меньшую вероятность ошибки при декодировании с помощью стекового и списочного алгоритмов последовательного исключения, чем известные классы полярных кодов, в частности, полярные коды с ядром Арикана. Предложенный метод построения укороченных полярных кодов позволяет получить коды произвольной длины, демонстрирующие высокую корректирующую способность при использовании метода последовательного исключения. Полярные коды с произвольным двоичным ядром, построенные для двоичного стирающего канала с помощью предложенного алгоритма, обеспечивают малую вероятность ошибки декодирования и в Гауссовском канале.

В отличие от классического метода последовательного декодирования и алгоритма последовательного исключения, предложенный метод декодирования полярных кодов оперирует оценками максимума апостериорных вероятностей кодовых слов. Предложенный метод декодирования полярных кодов имеет существенно меньшую вычислительную сложность по сравнению со стековым и списочным алгоритмами последовательного исключения, при незначительном увеличении вероятности ошибки декодирования. Основанный на нем алгоритм декодирования кодов Рида-Соломона в случае коротких кодов обеспечивает меньшую вероятность ошибки декодирования, чем метод Кёттера-Варди мягкого декодирования кодов Рида-Соломона. Разработанный алгоритм двумерной интерполяции позволяет снизить вычислительную сложность метода Кёттера-Варди.

Одной из возможных сфер применения предложенных методов кодирования и декодирования являются системы мобильной связи. При этом применение предлагаемого метода декодирования полярных кодов позволяет существенно снизить энергопотребление приемного оборудования, в то время как использование полярных подкодов БЧХ позволяет расширить зону уверенного приема по сравнению с аналогичными системами, использующими коды МППЧ.

Разработанный метод кодирования информации укороченными полярными подкодами (в частности, полярными кодами) был использован компанией ООО «Санкт-Петербургский Центр Разработок ЕМС» при разработке высокопроизводительных отказоустойчивых систем хранения данных, что подтверждается актом о внедрении. Предложенный метод превосходит по производительности существующие аналоги, а также предотвращает неравномерный износ носителей информации.

Положения, выносимые на защиту:

1. Метод построения кодов, являющихся подкодами расширенных кодов Боуза-Чоудхури-Хоквингема и обеспечивающих меньшую вероятность ошибки декодирования с помощью стекового алгоритма последовательного исключения, чем полярные коды.
2. Метод построения укороченных полярных кодов.
3. Метод последовательного декодирования двоичных полярных кодов и основанный на нем алгоритм декодирования коротких кодов Рида-Соломона.
4. Быстрый алгоритм, реализующий этап двумерной интерполяции в методе Кёттера-Варди декодирования кодов Рида-Соломона.
5. Метод кодирования информации укороченными полярными подкодами (в частности, полярными кодами) для отказоустойчивых систем хранения данных.

Степень достоверности и апробация результатов. Основные результаты диссертации докладывались на следующих конференциях: IEEE R8 International Conference on Computational Technologies in Electrical and Electronics Engineering 2010, 8-th IEEE International Symposium on Wireless Communication Systems 2011, International Workshop on Algebraic and Combinatorial Coding Theory 2012, International Symposium on Information Theory and Applications 2014, IEEE Information Theory Workshop 2012, 2013 и 2014. Кроме того, результаты были представлены на семинарах в институте проблем передачи информации им. А.А. Харкевича Российской академии наук (руководитель Л.А. Бассалыго) и Санкт-Петербургском государственном университете аэрокосмического приборостроения (руководитель Е.А. Крук).

Предлагаемые алгоритмы были реализованы на языке программирования C++. Выполнено сопоставление результатов статистического моделирования с известными опубликованными данными.

Публикации. Материалы диссертации опубликованы в 9 печатных работах [2, 4–11], из них 2 статьи в рецензируемых журналах [2, 8], включенных в список ВАК, и 7 статей в сборниках трудов конференций.

Получено свидетельство о государственной регистрации программы для ЭВМ [1]. Подана заявка на патент [3].

Личный вклад автора. Содержание диссертации и основные положения, выносимые на защиту, отражают персональный вклад автора в опубликованные работы. Подготовка к публикации полученных результатов проводилась совместно с соавторами, причем вклад диссертанта был определяющим. Все представленные в диссертации результаты получены лично автором.

Структура и объем диссертации. Диссертация состоит из введения, пяти разделов, заключения и библиографии. Общий объем диссертации 206 страниц, из них 187 страниц текста, включая 67 рисунков. Библиография включает 83 наименования на 10 страницах.

Содержание работы

Во Введении обоснована актуальность диссертационной работы, сформулирована цель и аргументирована научная новизна исследований, показана практическая значимость полученных результатов, представлены выносимые на защиту научные положения.

В первой главе рассматриваются полярные коды и коды Рида-Соломона. Рассматривается структура как полярных кодов с ядром $A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, так и полярных кодов с ядром, построенным на базе расширенных кодов Боуза-Чоудхури-Хоквингема (БЧХ). Приведено описание алгоритма систематического кодирования, разработанного Ариканом для полярных кодов с ядром A. Изложен алгоритм последовательного исключения, используемый для декодирования полярных кодов, а также его обобщения, позволяющие обеспечить меньшую вероятность ошибки декодирования. Кроме того, рассмотрен вопрос эффективной реализации данных алгоритмов.

Выполнен анализ существующих методов декодирования полярных кодов. Алгоритм последовательного исключения обладает малой сложностью, при этом его корректирующая способность также низка. Списочный/стековый алгоритм последовательного исключения при достаточном размере списка/стека способен обеспечить декодирование по максимуму правдоподобия, однако вычислительная сложность оказывается чрезвычайно высокой. Актуальной задачей является построение эффективных алгоритмов декодирования полярных кодов, обладающих малой сложностью.

Даже при декодировании по максимуму правдоподобия корректирующая способность полярных кодов малой длины оказывается ниже, чем у других распространенных кодов с аналогичными параметрами, к примеру, кодов МППЧ. Это обусловлено малым минимальным расстоянием полярных кодов.

Кроме того, в главе приведено определение кодов Рида-Соломона, а также описание метода Кёттера-Варди, позволяющего реализовать их мягкое декодирование. Особое внимание уделено интерполяционному шагу метода Кёттера-Варди, являющемуся наиболее трудоемким. Следует отметить, что метод Кёттера-Варди не обеспечивает декодирование по максимуму правдоподобия, поэтому актуальной является задача построения для кодов Рида-Соломона алгоритмов декодирования с большей корректирующей способностью.

Во второй главе показано, как может быть выполнено декодирование произвольного линейного блокового кода длины 2^m методом последовательного

исключения или его аналогами. Предложена конструкция полярного подкода заданного расширенного кода БЧХ, обеспечивающая минимизацию вероятности ошибки декодирования методом последовательного исключения. Также предложен метод выбора полярных подкодов БЧХ заданной размерности, обеспечивающий минимизацию вероятности ошибки их декодирования заданным алгоритмом. Также рассматриваются полярные коды с произвольным двоичным ядром, предложен алгоритм их построения для случая двоичного стирающего канала. Кроме того, представлен алгоритм построения укороченных полярных кодов с ядром Арикана.

Результаты второй главы опубликованы в работах [6, 11].

В разделе 2.1 решается задача построения кодов, декодирование которых может быть эффективно выполнено с помощью списочного/стекового алгоритма последовательного исключения и его аналогов. Классический полярный $(n = 2^m, k)$ код $\widehat{C}$, то есть полярный код построенный посредством заморозки битовых подканалов с наибольшими вероятностями ошибки, обеспечивает наименьшую возможную вероятность ошибки при декодировании методом последовательного исключения. Однако могут существовать (n, k) линейные коды, обеспечивающие меньшую вероятность ошибки декодирования при использовании списочного/стекового алгоритма последовательного исключения, чем полярный код $\widehat{C}$. Все рассматриваемые в данном разделе полярные коды являются полярными кодами с ядром Арикана.

Для обеспечения возможности декодирования произвольного линейного кода длины $n = 2^m$ методом последовательного исключения или его аналогами введем понятие динамически замороженных символов, равных линейным комбинациям информационных символов. Далее изложен предлагаемый подход к декодированию таких кодов.

В основе полярного кода лежит матрица поляризующего преобразования $G_n = \Lambda A^{\otimes m}$, где операция $\otimes m$ обозначает m-кратное Кронекеровское произведение матрицы с собой и Λ – перестановочная матрица, соответствующая обратной перестановке битов индексов входной последовательности. Используется такая проверочная матрица H кода C, что матрица $V = HG_n^T$ удовлетворяет условиям: $V_{j,i_j} = -1$ и для любого $t \in \{0, \ldots, 2^m - 1\}$ существует не более одного $j : i_j = t$, где $i_j = \max\{t \in \{0, \ldots, n-1\} \,|V_{j,t} \neq 0\}, 0 \leq j < n - k$. Если рассматривать $u_0^{n-1} V^T = 0$ как систему из $n-k$ линейных уравнений относительно элементов последовательности $u_0^{n-1} \in \mathbb{F}_q^n$, то все решения данной системы можно представить как последовательности, состоящие из k произвольных элементов $u_t \in \mathbb{F}_q$ при $t \in \mathcal{N}$, где $\mathcal{N} = \{0, \ldots, n-1\} \setminus \mathcal{F}$ при $\mathcal{F} = \{i_j | 0 \leq j < n - k\}$, и $n - k$ зависящих от них элементов

$$u_{i_j} = \sum_{t=0}^{i_j - 1} V_{j,t} u_t, 0 \leq j < n - k. \tag{1}$$

Переход от замороженных символов, равных нулю, к динамически заморожен-

ным символам не влияет на вероятности ошибки P_i декодирования символов u_i при использовании алгоритма последовательного исключения. Таким образом, вероятность ошибки декодирования кода C методом последовательного исключения равна $P^{(e)}(\mathcal{F}) = 1 - \prod_{i \notin \mathcal{F}}(1 - P_i)$.

В общем случае, множество незамороженных символов, построенное для произвольного кода C с помощью данного метода, включает много символов u_i с большими P_i, в то время как многие символы с малыми P_i оказываются замороженными. Вероятность ошибки декодирования при использовании метода последовательного исключения оказывается значительно выше, чем в случае других современных методов декодирования. Показано, что у кодов Рида-Маллера и расширенных кодов БЧХ, в общем случае, замороженными оказываются символы, которым соответствует большая вероятность ошибки, однако, некоторые из таких символов остаются незамороженными. Это ведет к необходимости использования списочного алгоритма последовательного исключения с чрезвычайно большим размером списка для обеспечения вероятности ошибки декодирования, сравнимой с таковой других алгоритмов декодирования.

Для получения $(2^m, k, \geq d)$ кода, декодирование которого может быть эффективно выполнено с помощью списочного/стекового алгоритма последовательного исключения и его аналогов, предлагается использовать ограничения для динамически замороженных символов высокоскоростного $(2^m, k', d)$ расширенного кода БЧХ с достаточно большим минимальным расстоянием d, и дополнительно заморозить $k' - k$ символов u_i с наибольшими вероятностями P_i. Эти вероятности могут быть вычислены с помощью метода эволюции плотностей. Предлагаемый класс кодов назван полярными подкодами БЧХ. На Рис. 1 представлен график зависимости вероятности ошибки декодирования от отношения сигнал/шум для классического полярного кода с ядром Арикана и для полярного подкода.

В разделе 2.2 приведено описание предлагаемого алгоритма построения укороченных полярных кодов. Данный алгоритм позволяет построить коды произвольной длины, обеспечивающие малую вероятность ошибки при декодировании методом последовательного исключения. При декодировании используется представление (n, k) укороченного полярного кода в виде $(2^m, k + s)$ полярного кода с динамически замороженными символами, где $s = 2^m - n$.

Укорочение произвольного $(2^m, K, D)$ линейного блокового кода C длины 2^m на s символов, задаваемых двоичным вектором S_m, состоит в выборе всех кодовых слов $c \in C$ таких, что $c_i = 0$ для $i \in \mathrm{supp}(S_m)$ и исключении из этих кодовых слов символов c_i для $i \in \mathrm{supp}(S_m)$. Полученные таким образом вектора составляют $(n = 2^m - s, k \geq K - s, d \geq D)$ линейный код.

Укороченный полярный (n, k) код задается множеством замороженных символов $\mathcal{F}$, $|\mathcal{F}| = n - k$, и шаблоном S_m веса $s = 2^m - n$, где $2^{m-1} < n \leq 2^m$. С помощью эволюции плотностей для этого кода может быть вычислена вероятность ошибки декодирования методом последовательного исклю-

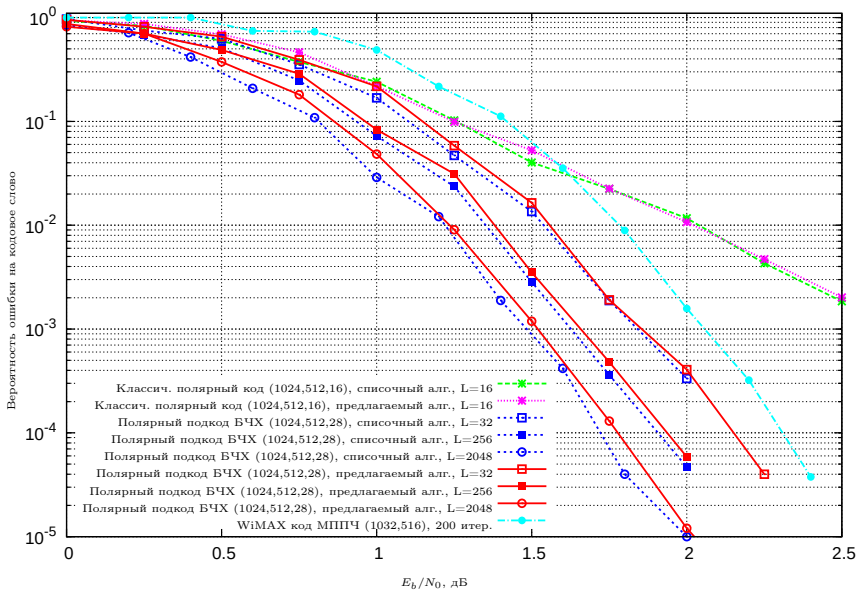

Рис. 1. Вероятность ошибки декодирования $(1024, 512)$ полярных кодов

чения $P(\mathcal{F}, S_m)$. В работе рассматривается случай аддитивного Гауссовского канала, поэтому для упрощения вычислений $P(\mathcal{F}, S_m)$ используется Гауссовская аппроксимация. Пусть $\mathcal{R}$ и $\mathcal{D}$ — множества всех шаблонов S_m веса s, и всех множеств $\mathcal{F} \subset \{0, \ldots, 2^m - 1\}$ мощности $n - k$, соответственно. Поскольку множество замороженных символов первоначального неукороченного кода может перестать быть оптимальным для укороченного кода, предлагается выполнять совместную оптимизацию множества $\mathcal{F}$ и вектора S_m: $(\mathcal{F}^*, S_m^*) = \arg \min\limits_{\substack{\mathcal{F}\in\mathcal{D} \\ S_m\in\mathcal{R}}} P(\mathcal{F}, S_m)$.

Высокорегулярная структура полярных кодов позволяет снизить сложность поиска решения данной оптимизационной задачи. Вводится понятие эквивалентности шаблонов, для эквивалентных шаблонов S_m и $\widetilde{S}_m$, в частности, выполняется $P(S_m) = P(\widetilde{S}_m)$, где $P(S_m) = \min\limits_{\mathcal{F}\in\mathcal{D}} P(\mathcal{F}, S_m)$. Предложен метод выявления эквивалентных шаблонов, позволяющий построить множество $\mathcal{G}_0 \subset \mathcal{R}$, мощность которого намного меньше $|\,\mathcal{R}\,|$, удовлетворяющее следующему условию $\forall S_m \in \mathcal{R}\ \exists \widetilde{S}_m \in \mathcal{G}_0 :\ P(\widetilde{S}_m) = P(S_m)$. Шаблон S_m^* может быть выбран среди $S_m \in \mathcal{G}_0$. Кроме того, для осуществления эффективного поиска по множеству $\mathcal{G}_0$ предлагается рекурсивно делить его на подмножества $\mathcal{G}_i$. Каждому подмножеству $\mathcal{G}_i$ сопоставляется оценка снизу для вероятностей $P(S_m)$, $S_m \in \mathcal{G}_i$. Для осуществления очередного шага рекурсии выбирается подмножество с наименьшей такой оценкой.

На Рис. 2 представлен график зависимости вероятности ошибки декодирования от отношения сигнал/шум для укороченных полярных кодов, построенных с помощью предлагаемого метода. Данные коды были построены так, что они являются подкодами заданных расширенных кодов БЧХ. Декодирование укороченных кодов выполнялось с помощью алгоритма последовательного де-

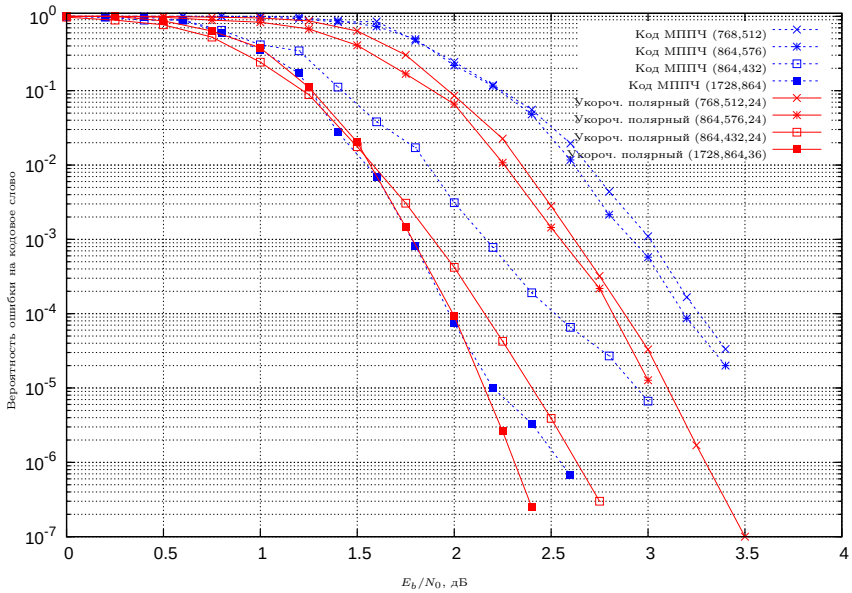

Рис. 2. Сравнение корректирующей способности укороченных полярных кодов и кодов МППЧ

кодирования, описанного в разделе 3.2 , с $L = 128$. Для сравнения показана корректирующая способность кодов МППЧ из стандарта WiMAX, для декодирования которых использовался алгоритм распространения доверия.

В разделе 2.3 предложен алгоритм построения полярных кодов с произвольным двоичным ядром поляризации. Алгоритм выполняет оптимизацию множества замороженных символов для случая двоичного стирающего канала в предположении о том, что при декодировании должен использоваться метод последовательного исключения.

Задача построения $(n = l^m, k)$ двоичного полярного кода с $l \times l$ ядром M сводится к задаче выбора $(n - k)$ замороженных символов u_i, $0 \leq i < n$, которым соответствуют наибольшие вероятности ошибки P_i декодирования методом последовательного исключения. Вероятность P_i может быть вычислена по заданному распределению логарифмических отношений правдоподобия для символа u_i. Однако задача нахождения данного распределения является крайне трудоемкой. В связи с этим, в работе рассматривается более простая задача построения полярного кода для двоичного стирающего канала. Показано, что задача построения полярных кодов для случая двоичного стирающего канала с вероятностью стирания p сводится к задаче оценки вероятностей отказа от декодирования $Q(p, \beta)$ для 0-ых информационных символов (l, μ) линейных блоковых кодов, порождаемых последними μ строками ядра M, $\mu = l - \beta$, $1 \leq \mu \leq l$. Эта вероятность может быть представлена как $Q(p, \beta) = \sum_{e=d}^{l} B_e p^e (1-p)^{l-e}$, где B_e — число неисправимых конфигураций стираний веса e, $0 \leq e \leq l$.

Предложены два метода оценки числа неисправимых конфигураций стираний B_e. Первый метод позволяет найти точное значение B_e, однако, в случае $l > 32$ сложность данного метода оказывается чрезмерно высокой для практического применения. Этот метод предполагает построение решетки, задаю-

щей смежный класс кода с проверочной матрицей Γ, состоящей из μ последних строк ядра M. Данный смежный класс состоит из кодовых слов z_0^{l-1}, удовлетворяющих условию $\Gamma\left(z_0^{l-1}\right)^T = \begin{pmatrix}1 & 0 & \dots & 0\end{pmatrix}^T$, где $a_{j,\mathcal{D}}^h$ — подвектор вектора a_j^h, состоящий из элементов $a_s, s \in \mathcal{D} \cap \{j, \dots, h\}$. Построенная решетка преобразуется в двоичное дерево решений (ДДР) $\overline{BDD}$, соответствующее функции $\overline{f}(E)$, являющейся характеристической функцией для множества $\overline{Y} = \left\{E | E_i = 1 - z_i, \Gamma\left(z_0^{l-1}\right)^T = \begin{pmatrix}1 & 0 & \dots & 0\end{pmatrix}^T\right\}$. В свою очередь, ДДР $\overline{BDD}$ преобразуется в ДДР BDD, соответствующее функции $f(E) = \bigvee_{S \in \overline{Y}} (\bigwedge_{i:S_i=0} \neg E_i)$, путем выполнения рекурсивных операций для поддеревьев. B_e вычисляется как количество путей в ДДР BDD из корня в терминальную вершину "0".

При размерности поляризующего ядра M более 32 явное построение множества всех исправимых конфигураций стираний с помощью описанного метода становится невозможным. В связи с этим, предлагается использовать приближенный метод вычисления B_e, сформулированный в виде теоремы, основанной на работе Р. Хеллера.

Теорема 1. *При $e < \lfloor (3d+1)/2 \rfloor$ число неисправимых конфигураций стираний $B_e = \sum_{i=d}^{e} \binom{l-i}{e-i} A_i$, где d — наименьший вес кодового слова $c_0^{l-1} = u_0^{\mu-1}\Gamma$ при $u_0 = 0$ и $u_1^{\mu-1} \in \{0,1\}^{\mu-1}$, A_i — число кодовых слов c_0^{l-1} веса i. При $e \geq \lfloor (3d+1)/2 \rfloor$ число неисправимых конфигураций стираний ограничено сверху $B_e \leq \min\left(\sum_{i=1}^{e} \binom{l-i}{e-i} A_i, \binom{l}{e}\right)$.*

Заметим, что при вычислении $Q(p, \beta)$ наиболее важно знать точные значения B_e для небольших e. Поэтому использование приведенной верхней границы для B_e не приводит к возникновению значительной погрешности. Полученные численные результаты свидетельствуют о том, что построенные полярные коды демонстрируют хорошую корректирующую способность и в случае аддитивного Гауссовского канала.

В третьей главе рассматриваются предлагаемые алгоритмы декодирования полярных кодов. Результаты этой главы опубликованы в работах [8–11].

В разделе 3.2 представлен алгоритм последовательного декодирования полярных кодов с ядром Арикана и полярных подкодов с ядром Арикана, в основе которого лежит стековый алгоритм последовательного исключения. Стек содержит несколько входных последовательностей u_0^i различной длины. На каждой итерации стекового алгоритма последовательность u_0^i с наибольшим значением метрики удлиняется на один элемент. Общепринятой метрикой для пути u_0^i является вероятность $P(u_0^i | y_0^{n-1})$. Если длина пути с наибольшей метрикой равна n, то данный путь возвращается в качестве результата декодирования. Предложена новая метрика пути, то есть новый метод предсказания того, какое начало пути u_0^i может соответствовать решению задачи декодирования. Задача декодирования состоит в поиске пути u_0^{n-1}, $u_{0,\mathcal{F}}^{n-1} = 0$, которому соответствует наибольшее значение вероятности

$p^* = P(u_0^{n-1}|y_0^{n-1})$. Если решение задачи декодирования соответствует u_0^i, то $p^* = \max\limits_{u_{i+1}^{n-1}:u_{i+1,\mathcal{F}}^{n-1}=\mathbf{0}} P(u_0^{n-1}|y_0^{n-1})$. Вычисление вероятности $T(u_0^i, y_0^{n-1})$ на i-ой фазе алгоритма последовательного исключения является крайне трудоемкой задачей. Рассмотрим пути $v[j]_0^{n-1}$ такие, что $v[j]_0^i = u_0^i$ и $v[j]_{i+1}^{n-1} \in \{0,1\}^{n-i-1}$, $0 \le j < 2^{n-i-1}$. Предположим, что u_0^i соответствует наиболее вероятному кодовому слову. Пусть J – случайная величина, равная j, если наиболее вероятное кодовое слово полярного кода соответствует пути $v[j]_0^{n-1}$. Заметим, что $J = j$ предполагает $v[j]_h = 0, h \in \mathcal{F}$. Мы предлагаем оценить $T(u_0^i, y_0^{n-1})$ как $T(u_0^i, y_0^{n-1}) \approx E_J[P(v[J]_0^{n-1}|y_0^{n-1})] = \sum_{j=0}^{2^{n-i-1}-1} P(v[j]_0^{n-1}|y_0^{n-1}) P\{J=j\} \ge \underbrace{P(v[\alpha]_0^{n-1}|y_0^{n-1})}_{R(u_0^i, y_0^{n-1})} P\{J=\alpha\}$, где $\alpha = \arg\max\limits_{0\le j<2^{n-i-1}} P(v[j]_0^{n-1}|y_0^{n-1})$. Вероятность $P\{J=\alpha\}$, усредненная по всем принятым последовательностям, ограничена снизу вероятностью $\hat{\Omega}(i) = \prod\limits_{j\in\mathcal{F}, j>i} (1-P_j)$, где P_j – вероятность ошибки декодирования символа u_j при условии того, что известны правильные значения предыдущих символов $u_{j'}$, $j' < j$. Таким образом, получаем следующую оценку для $T(u_0^i, y_0^{n-1})$:

$$\hat{T}(u_0^i, y_0^{n-1}) = R(u_0^i, y_0^{n-1})\hat{\Omega}(i). \tag{2}$$

Вычисление значения вероятности $R(u_0^i, y_0^{n-1})$ осуществляется рекурсивно согласно выражениям

$$R(u_0^{2i}, y_0^{n-1}) = \max_{u_{2i+1}\in\{0,1\}} R\left(u_{0,even}^{2i+1} \oplus u_{0,odd}^{2i+1}, y_0^{n/2-1}\right) R\left(u_{0,odd}^{2i+1}, y_{n/2}^{n-1}\right), \tag{3}$$

$$R(u_0^{2i+1}, y_0^{n-1}) = R\left(u_{0,even}^{2i+1} \oplus u_{0,odd}^{2i+1}, y_0^{n/2-1}\right) R\left(u_{0,odd}^{2i+1}, y_{n/2}^{n-1}\right) \tag{4}$$

с начальным условием $R(b, y_j) = P(b|y_j)$, $b \in \{0,1\}$. Величина $\hat{\Omega}(i)$ может рассматриваться как оценка снизу для вероятности $P\{J=\alpha\}$, усредненной по множеству принятых последовательностей.

На Рис. 1 представлен график зависимости вероятности ошибки декодирования от отношения сигнал/шум для предлагаемого алгоритма, списочного алгоритма Тала-Варди и алгоритма направленного поиска, описанного в разделе 3.1 . Корректирующая способность алгоритма направленного поиска совпадает с таковой списочного/стекового алгоритма последовательного исключения. Результаты приведены как для $(1024, 512, 16)$ классического полярного кода с ядром Арикана и $(1024, 512, 28)$ полярного подкода с ядром Арикана, так и для $(1032, 516)$ кода МППЧ.

Численные результаты показывают, что предлагаемый подход обеспечивает многократное снижение сложности по сравнению со стековым алгоритмом последовательного исключения, при незначительном ухудшении корректирующей способности. Заметим, что асимптотическая сложность обоих алгоритмов декодирования равна $O(Ln\log n)$.

Таблица 1. Средняя сложность декодирования, $\times 10^3$ вещественных операций

E_b/N_0, dB	Предлагаемый подход						МППЧ, алг. распр. дов.	
	Сложения			Сравнения			Слож.	$\log\tanh(\frac{x}{2})$
	$L=32$	$L=256$	$L=2048$	$L=32$	$L=256$	$L=2048$	≤ 200 ит.	≤ 200 ит.
0	141	833	5231	227	1332	8374	2617	1307
0.5	133	752	4265	218	1224	6968	2333	1112
1	73	286	1232	122	477	2065	1469	722
1.5	32	88	267	54	151	461	394	185
2	18	27	42	31	48	74	140	62

Таблица 1 иллюстрирует число операций над вещественными числами, выполняемых при декодировании полярных кодов с использованием предлагаемого подхода и при декодировании кодов МППЧ с помощью алгоритма распространения доверия с не более чем 200 итерациями.

В разделе 3.3 описано обобщение предлагаемого метода последовательного декодирования на случай полярных кодов с произвольным двоичным ядром. Выполнено обобщение процедуры вычисления метрики пути, задаваемой выражением (2). Вероятности $R(u_0^i, y_0^{n-1})$ вычисляются также рекурсивно, однако, на каждом шаге рекурсии выполняется поиск двух наиболее вероятных кодовых слов в коде, порожденном последними строками $l \times l$ ядра поляризации. Алгоритм предполагает использование для этих кодов декодеров, работающих почти по максимуму правдоподобия. Численные результаты показывают, что предлагаемый подход позволяет выполнять декодирование полярных кодов с ядром БЧХ почти по максимуму правдоподобия. Сложность последовательного алгоритма декодирования можно оценить в $O(Ln\log_l n)$ базовых операций, где базовая операция соответствует поиску наиболее вероятного кодового слова в коде, порожденном последними строками ядра поляризации.

В разделе 3.5 рассматривается обобщение предложенного в разделе 3.2 алгоритма последовательного декодирования на случай расширенных кодов Рида-Соломона над полем $\mathbb{F}_{2^m}$. При декодировании используется представление расширенных кодов Рида-Соломона, описанное в разделе 2.1 .

На каждой итерации алгоритма путь u_0^i с наибольшей метрикой (2) удлиняется на один элемент. Для информационного символа u_i рассматривается 2^m значений, а для замороженного только одно. Вычисление вероятности $R_{2^m}(u_0^i, y_0^{n-1}) = \max\limits_{u_{i+1}^{n-1}\in\mathbb{F}_{2^m}^{n-i-1}} P(u_0^{n-1}|y_0^{n-1})$ сводится к рекурсивному применению выражений (3) и (4), при этом поиск максимума в выражении (3) должен осуществляться по $u_i \in \mathbb{F}_{2^m}$. Для вычисления метрики $\hat{T}(u_0^i, y_0^{n-1})$ необходимо найти оценки вероятностей $P_j^{(2^m)}$ для $0 \leq j < i$, где $P_j^{(2^m)}$ является вероятностью ошибки декодирования алгоритмом последовательного исключения символа $u_j \in \mathbb{F}_{2^m}$ при условии того, что известны правильные значения символов $u_{j'}$, $0 \leq j' < j$. В случае аддитивного Гауссовского канала задача вычисления $P_j^{(2^m)}$ может быть сведена к задаче вычисления математических ожиданий логариф-

мических отношений правдоподобия (ЛОПП) $l_{u_i} = \log \frac{P(u_0^{i-1},0|y_0^{n-1})}{P(u_0^i|y_0^{n-1})}$ для случая передачи нулевого кодового слова, то есть $u_0^{i-1} = \mathbf{0}$, $u_i \in \mathbb{F}_{2^m}$, при применении Гауссовской аппроксимации. ЛОПП l_{u_i} рассматриваются как зависимые Гауссовские случайные величины с заданной ковариационной матрицей. Предлагается аппроксимировать числитель $P(u_0^{i-1}, 0|y_0^{n-1})$ и знаменатель $P(u_0^i|y_0^{n-1})$ наибольшими слагаемыми, что позволяет свести задачу поиска математического ожидания ЛОПП l_{u_i} к задаче поиска математического ожидания максимума среди зависимых Гауссовских случайных величин с различными распределениями. Это математическое ожидание максимума предлагается оценить посредством построения верхней и нижней границ, являющихся математическими ожиданиями максимумов из новых независимых Гауссовских случайных величин с различными распределениями. Сложность декодирования расширенных кодов Рида-Соломона можно оценить как $O(Ln^3 \log n)$ операций над вещественными числами. Необходимо отметить, что при увеличении длины кода n требуемый размер списка L растет экспоненциально.

В случае передачи двоичного образа кода Рида-Соломона по каналу без памяти можно показать, что $R_{2^m}(u_0^i, y_0^{n-1}) = \prod_{j=0}^{m-1} R\left(u_0^i[j], y_0^{n-1}[j]\right)$, где $u_0^i[j] = (u_0[j], \ldots, u_i[j])$, $u_s = \sum_{j=0}^{m-1} u_s[j]a_j$, $u_s[j] \in \mathbb{F}_2$, $(a_0, \ldots, a_{m-1})$ — некоторый базис $\mathbb{F}_{2^m}$, и $y_0^{n-1}[j]$ — подвектор вектора y_0^{n-1}, соответствующий j-ым битам принятых символов. Таким образом, декодирование кода над $\mathbb{F}_{2^m}$ может быть реализовано посредством m синхронизированных запусков декодера для двоичных кодов. Синхронизация необходима для вычисления $R_{2^m}(u_0^i, y_0^{n-1})$ по найденным $R\left(u_0^i[j], y_0^{n-1}[j]\right)$, $0 \leq j < m$, на слое поляризующего преобразования, соответствующем входной последовательности, а также вычисления значений динамически замороженных символов согласно выражению (1) с использованием арифметики поля $\mathbb{F}_{2^m}$. Применение этого подхода в случае передачи двоичного образа приводит к значительному снижению сложности декодирования.

Вероятность ошибки для символа u_i может быть вычислена как $P_i^{(2^m)} = 1 - (1 - P_i)^m$, где P_i — вероятность ошибки декодирования i-го бита двоичной входной последовательности при использовании алгоритма последовательного исключения. Таким образом, $\hat{\Omega}_{2^m}(i) = \prod_{j \in \mathcal{F}, j>i} (1 - P_j^{(2^m)})$ может быть вычислена с помощью методов, разработанных для двоичных полярных кодов. На Рис. 3 приведен график зависимости вероятности ошибки декодирования от отношения сигнал/шум для предлагаемого алгоритма декодирования и метода направленного поиска, корректирующая способность которого такая же, как у стекового алгоритма последовательного исключения. При той же корректирующей способности предлагаемый алгоритм декодирования обеспечивает значительное снижение сложности по сравнению со стековым алгоритмом последовательного исключения и декодированием методом направленного поиска. Также приведены данные для метода Кёттера-Варди.

В четвертой главе предложен комбинаторно-алгебраический алгоритм

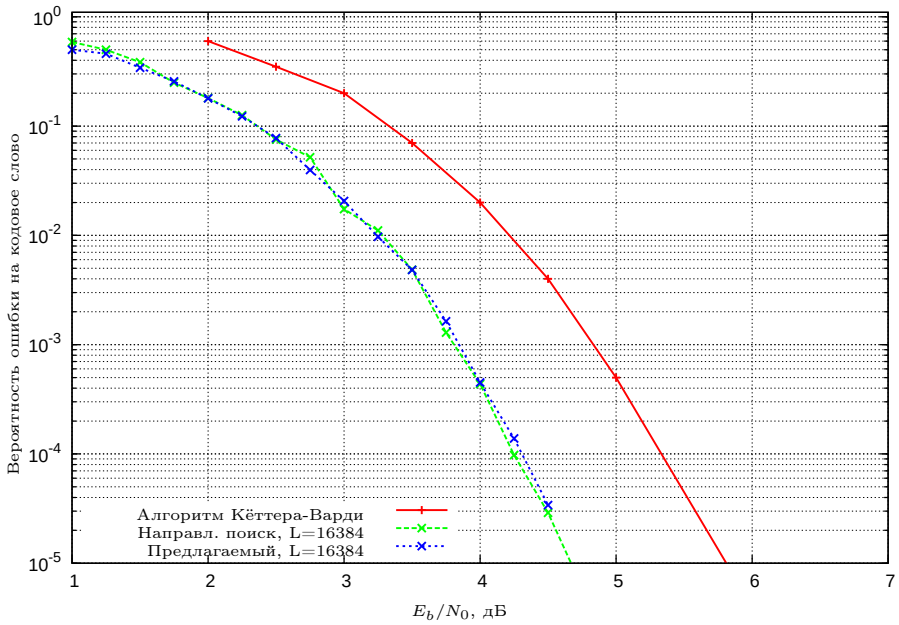

Рис. 3. Вероятность ошибки декодирования кода Рида-Соломона $(31, 15)$ в случае передачи двоичного образа по аддитивному Гауссовскому каналу

декодирования длинных (n, k) кодов Рида-Соломона. Данный алгоритм построен на базе метода Кёттера-Варди и метода Чейза. Для реализации интерполяционного шага метода Кёттера-Варди разработан быстрый алгоритм двумерной интерполяции. Результаты четвертой главы опубликованы в работах [2, 4, 5].

На интерполяционном шаге метода Кёттера-Варди решается задача построения интерполяционного полинома по множеству точек (x_i, y_j), $0 \leq i < n$, $0 \leq j < q$. При этом интерполяционный полином должен иметь минимально возможную $(1, k-1)$-взвешенную степень и корни кратности как минимум $M_{i,j}$ во всех точках (x_i, y_j). Точка (x_i, y_j) является корнем полинома $Q(x, y)$ кратности $M_{i,j}$, если соответствующие производные Хассе $Q(x, y)$ удовлетворяют условию $Q^{[\alpha,\beta]}(x_i, y_j) = 0$, $\alpha + \beta < M_{i,j}$. Интерполяционный шаг является наиболее трудоемким. Известно, что искомый полином $Q(x, y)$ содержится в базисе Грёбнера идеала многочленов, имеющих корни (x_i, y_j) кратности $M_{i,j}$. Предлагаемый алгоритм двумерной интерполяции предполагает итеративное построение требуемого идеала многочленов, при этом кратности корней увеличиваются согласно двоичному методу возведения в степень. Применение метода перекодирования позволяет обеспечить дополнительное снижение сложности. Сложность предлагаемого алгоритма декодирования составляет $O(n^2\mu^4)$, где μ — наибольшее значение кратности $M_{i,j}$. Кроме того, предложен комбинаторно-алгебраический алгоритм декодирования, использующий метод Чейза для снижения вероятности ошибки. Более конкретно, осуществляется перебор двух наиболее вероятных значений для заданного числа наименее надежных символов принятой последовательности. Переиспользование результатов промежуточных вычислений позволяет избежать многократное увеличение сложности.

В пятой главе представлен метод кодирования информации для отказо-

устойчивых систем хранения данных, основанный на теории полярных кодов. Изложен разработанный алгоритм систематического кодирования полярных кодов с произвольным двоичным ядром поляризации, в основе которого лежит алгоритм, предложенный Э.Л. Блохом и В.В. Зябловым для обобщенных каскадных кодов. Идея предлагаемого алгоритма заключается в сведении задачи систематического кодирования полярного кода длины l^m с $l \times l$ ядром поляризации M к l задачам систематического кодирования полярного кода длины l^{m-1}. Алгоритм предполагает, что ядро M является нижнетреугольной матрицей с единичной диагональю. Показано, что это предположение не влияет на вероятность ошибки декодирования, достижимую используемыми полярными кодами. В случае полярного кода с ядром Арикана асимптотическая сложность предлагаемого алгоритма равна $O(n \log n)$ и совпадает со сложностью алгоритма Арикана, где n — длина кода. В случае $l \times l$ ядра БЧХ сложность предлагаемого алгоритма $O\left(n \log(n) \log^{1+a}(l)\right)$, где $a \leq 2$.

Рассмотрено применение предложенного подхода в отказоустойчивых системах хранения данных, включающих в себя совокупность высокопроизводительных твердотельных дисков. Необходимость кодирования данных в таких системах возникает вследствие недостаточной надежности дисков. Было показано, что предложенный метод позволяет построить кодер с производительностью, превышающей производительность кодера кода Рида-Соломона в 1.6 раза при сопоставимых параметрах кодов. Заметим, что при обновлении даже небольшого числа информационных символов кодового слова может потребоваться обновление почти всех проверочных символов, что ведет к перегрузке дисков, на которых хранятся проверочные символы. В классических архитектурах RAID-5 и RAID-6 для решения этой проблемы используется циклический метод балансировки нагрузки. Однако он не может быть использован в сочетании с кодами, не являющимися кодами с максимальным достижимым расстоянием. Предлагаемый метод балансировки нагрузки предназначен для двоичных обобщенных каскадных кодов с внутренними полярными кодами с ядром Арикана и внешними двоичными линейными кодами, в частности, он может быть использован для полярных кодов с ядром Арикана, представленных в виде обобщенных каскадных. Метод включает две составляющие: балансировка нагрузки для внешних кодов и балансировка нагрузки для внутренних кодов. Для внешних кодов выполняется построение семейства вложенных множеств информационных совокупностей, используемых для размещения информационных символов. Это обеспечивает балансировку нагрузки среди группы дисков, соответствующих заданному внешнему коду. Балансировка нагрузки между различными группами дисков обеспечивается благодаря записи половины кодовых слов внутреннего кода в обратном порядке. Показано, что если внутренний код является полярным кодом с ядром Арикана, то получаемые при кодировании последовательности являются кодовыми словами исходного обобщенного каскадного кода. Численные результаты показывают, что обеспечивается степень сбалансированности нагрузки на носители данных, близкая к

случаю системы хранения данных с тем же числом дисков, организованных в несколько групп RAID-4, и избыточностью.

В **Заключении** обобщены основные результаты диссертационной работы.

Основные результаты работы

Предложена конструкция кодов, называемых полярными подкодами БЧХ, декодирование которых может быть эффективно выполнено с помощью списочного/стекового алгоритма последовательного исключения и его аналогов.

Разработан алгоритм построения полярных кодов с произвольным двоичным ядром поляризации, обеспечивающий оптимальный выбор множества замороженных битовых подканалов для случая двоичного стирающего канала и декодирования методом последовательного исключения. Полученные численные результаты свидетельствуют о том, что построенные полярные коды демонстрируют хорошую корректирующую способность и в случае Гауссовского канала.

Предложен метод построения укороченных полярных кодов, в основе которого лежит совместная оптимизация шаблона укорочения и множества замороженных символов с целью минимизации вероятности ошибки декодирования методом последовательного исключения.

Разработан алгоритм последовательного декодирования полярных кодов с ядром Арикана. Показано, что этот алгоритм обладает существенно меньшей сложностью по сравнению с существующими списочными и стековыми алгоритмами декодирования полярных кодов. Снижение сложности достигается за счет незначительного ухудшения корректирующей способности.

Выполнено обобщение предлагаемого метода последовательного декодирования на случай полярных кодов с произвольным двоичным ядром. Численные результаты показывают, что предлагаемый подход позволяет выполнять декодирование полярных кодов с ядром БЧХ почти по максимуму правдоподобия. На базе предложенного метода последовательного декодирования построен алгоритм декодирования коротких кодов Рида-Соломона над полем $\mathbb{F}_{2^m}$. Показано, что предлагаемый подход обеспечивает меньшую вероятность ошибки декодирования, чем метод Кёттера-Варди.

Предложен комбинаторно-алгебраический алгоритм декодирования кодов Рида-Соломона, построенный на базе метода Кёттера-Варди. Для реализации интерполяционного шага метода Кёттера-Варди разработан эффективный алгоритм двумерной интерполяции.

Представлен алгоритм систематического кодирования полярных кодов с произвольным двоичным ядром поляризации. На основе данного алгоритма предложен высокопроизводительный метод кодирования укороченными полярными подкодами для отказоустойчивых систем хранения данных, включающий в себя метод балансировки нагрузки на носители информации.

Список публикаций

[1] *Милославская В.* Генератор двоичных полярных кодов с ядром большой размерности. — Свидетельство о государственной регистрации программы для ЭВМ 2012614815. — 2012.

[2] *Милославская В., Трифонов П.* Гибридный алгоритм мягкого декодирования кодов Рида-Соломона // *Научно-технические ведомости СПбГПУ. Информатика. Телекоммуникации. Управление.* — 2011. — № 2. — С. 169–174.

[3] *Заявка 2014114215 Российская Федерация, МПК G 06 F 11/00.* Способ и устройство кодирования и декодирования данных в скрученном полярном коде / Милославская В., Трифонов П.; заявитель Самсунг Электроникс Ко., Лтд.; пат. поверенный Миц А.В. — №364; заявл. 10.04.2014. — 36 с.: ил.

[4] *Miloslavskaya V., Trifonov P.* Fast interpolation in algebraic soft decision decoding of Reed-Solomon codes // Proceedings of IEEE R8 International Conference on Computational Technologies in Electrical and Electronics Engineering. — 2010. — Pp. 65–69.

[5] *Miloslavskaya V., Trifonov P.* Hybrid interpolation algorithm for algebraic soft decision decoding of Reed-Solomon codes // Proceedings of 8th IEEE International Symposium on Wireless Communication Systems. — 2011. — Pp. 131–135.

[6] *Miloslavskaya V., Trifonov P.* Design of polar codes with arbitrary kernels // Proceedings of IEEE Information Theory Workshop. — 2012. — Pp. 119–123.

[7] *Miloslavskaya V., Trifonov P.* Performance of binary polar codes with high-dimensional kernel // Proceedings of International Workshop on Algebraic and Combinatorial Coding Theory. — 2012. — Pp. 263–268.

[8] *Miloslavskaya V., Trifonov P.* Sequential decoding of polar codes // *IEEE Communications Letters.* — 2014. — Vol. 18, no. 7. — Pp. 1127–1130.

[9] *Miloslavskaya V., Trifonov P.* Sequential decoding of polar codes with arbitrary binary kernel // Proceedings of IEEE Information Theory Workshop. — 2014. — Pp. 377–381.

[10] *Miloslavskaya V., Trifonov P.* Sequential decoding of Reed-Solomon codes // Proceedings of International Symposium on Information Theory and Applications. — 2014. — Pp. 424–428.

[11] *Trifonov P., Miloslavskaya V.* Polar codes with dynamic frozen symbols and their decoding by directed search // Proceedings of IEEE Information Theory Workshop. — 2013. — September. — Pp. 1 – 5.