На правах рукописи

Трифонов Петр Владимирович

Методы построения и декодирования многочленных кодов

05.13.17 – Теоретические основы информатики

АВТОРЕФЕРАТ
диссертации на соискание ученой степени

доктора технических наук

Санкт-Петербург – 2018

Работа выполнена в *Федеральном государственном автономном образовательном учреждении высшего образования "Санкт-Петербургский политехнический университет Петра Великого"*

Официальные оппоненты:
доктор технических наук, профессор кафедры вычислительной техники Федерального государственного бюджетного образовательного учреждения высшего образования "Юго-Западный государственный университет"
Егоров Сергей Иванович

доктор физико-математических наук, советник ректора по науке Автономной некоммерческой образовательной организации высшего образования "Сколковский институт науки и технологий"
Кабатянский Григорий Анатольевич

доктор технических наук, профессор кафедры информационных систем Федерального государственного автономного образовательного учреждения высшего образования "Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики"
Кудряшов Борис Давидович

Ведущая организация:
Федеральное государственное автономное образовательное учреждение высшего образования "Санкт-Петербургский государственный университет аэрокосмического приборостроения"

Защита состоится 1 октября 2018 г. в 11:00 часов на заседании диссертационного совета *Д 002.077.05* при *Федеральном государственном бюджетном учреждении науки Институте проблем передачи информации им. А.А. Харкевича Российской академии наук (ИППИ РАН)*, расположенном по адресу: *127051, г. Москва, Большой Каретный переулок, д.19 стр. 1.*

С диссертацией можно ознакомиться в библиотеке *Института проблем передачи информации им. А.А. Харкевича Российской академии наук (ИППИ РАН) и на сайте* `http://www.iitp.ru`.

Автореферат разослан «_____» _____ 2018 г.

Отзывы и замечания по автореферату в двух экземплярах, заверенные печатью, просьба высылать по вышеуказанному адресу на имя ученого секретаря диссертационного совета.

Ученый секретарь
диссертационного совета,

д.ф.-м.н. *Цитович И.И.*

Общая характеристика работы

Актуальность темы исследования. Быстрый рост объема цифровых данных, производимых и обрабатываемых различными техническими системами, требует создания соответствующей инфраструктуры для их передачи и хранения. При этом постоянно ужесточаются требования к скорости обмена данными, задержке передачи информации, энергетической и спектральной эффективности, стоимости оборудования и т. п. Их выполнение невозможно без использования методов помехоустойчивого кодирования.

Несмотря на долгую историю развития теории кодирования, построение корректирующих кодов и методов их декодирования, которые удовлетворяли бы требованиям к перспективным техническим системам, вызывает серьезные затруднения. В частности, современные информационные системы зачастую используют обмен короткими сообщениями, которые должны доставляться с низкой задержкой. Однако оказывается, что широко используемые в настоящее время коды с циклическим замыканием, турбо-коды и коды с малой плотностью проверок на четность (LDPC) требуют внесения весьма высокой избыточности для обеспечения приемлемой вероятности ошибки декодирования таких сообщений. Кроме того, задержка обработки информации в декодере оказывается неудовлетворительной, а высокое энергопотребление приемо-передающей аппаратуры, зависящее в значительной степени от сложности используемых алгоритмов кодирования и декодирования, существенно ограничивает время автономной работы соответствующих устройств.

Причиной этого является отсутствие простых алгоритмов декодирования (почти) по максимуму правдоподобия для известных хороших кодов (например, БЧХ, Рида-Соломона), и недостаточная корректирующая способность тех кодов (например, кодов с малой плотностью проверок на четность), для которых имеются эффективные алгоритмы мягкого декодирования. В частности, предложенные в 2008 г. Э. Ариканом полярные коды достигают предела Шеннона, и для них известны простые алгоритмы построения, кодирования и декодирования. Несмотря на значительный прогресс (А. Варди, И.И. Думер, В.А. Зиновьев, В.В. Зяблов, Г.А. Кабатянский, С. Кудекар, С. Кумар, И. Тал, Т. Танака, Р. Урбанке) в изучении свойств полярных кодов и схожих с ними кодов Рида-Маллера, являющихся частным случаем обобщенных каскадных кодов, на практике оказывается, что корректирующая способность полярных кодов с практически значимыми длинами (до нескольких тысяч) существенно хуже по сравнению с другими известными кодами, алгоритм последовательного исключения не обеспечивает декодирование полярных кодов по максимуму правдоподобия, сложность (размер списка) усовершенствованного списочного алгоритма последовательного исключения чрезмерно высока, а алгоритм Тала-Варди эволюции плотностей требует весьма большого числа уровней квантования, что также приводит к слишком большой сложности построения кодов. Простая структура и замечательные асимптотические свойства полярных кодов делают их весьма привлекательными для использования в перспективных системах передачи информации. Однако для удовлетворения требованиям, предъявляемым к таким системам, должна быть решена задача построения упрощенных алгоритмов декодирования полярных кодов и усовершенствования их конструкции с целью повышения корректирующей способности.

Многие современные системы хранения и передачи информации используют

коды Рида-Соломона. Несмотря на долгую историю исследований (В.Б. Афанасьев, Э.М. Габидулин, С.И. Егоров, Е.Т. Мирончиков, С.В. Федоренко, Э. Берлекэмп, Р. Кёттер, Дж. Месси, Р. Рот), даже классические процедуры их декодирования зачастую оказываются слишком сложными для практического использования. Кроме того, известные алгоритмы с полиномиальной сложностью не обеспечивают их декодирование по максимуму правдоподобия. Одним из возможных путей повышения практической корректирующей способности кодов Рида-Соломона является использование списочного декодирования. Однако алгоритмы Гурусвами-Судана и Ву списочного декодирования имеют весьма высокую (хотя и полиномиальную) сложность, что ограничивает их практическое применение. В связи с этим, для повышения помехозащищенности современных и перспективных систем хранения и передачи информации должны быть разработаны простые алгоритмы декодирования кодов Рида-Соломона с улучшенной корректирующей способностью, а также снижена сложность известных алгоритмов их декодирования.

В системах хранения данных применение длинных МДР-кодов, обеспечивающих оптимальную избыточность при заданной вероятности потери информации, сдерживается высокой сложностью их кодирования и значительным объемом данных, которые приходится считывать и/или передавать в процессе восстановления. Хотя недавно были предложены эффективные решения последней проблемы для кодов Рида-Соломона, недостаточная производительность операции кодирования, регулярно применяемой в штатном режиме работы СХД, заставляет разработчиков применять субоптимальные с точки зрения избыточности решения. Таким образом, для повышения производительности и полезной емкости систем хранения данных должна быть решена задача построения упрощенных алгоритмов систематического кодирования кодов Рида-Соломона.

Коды Рида-Соломона, Рида-Маллера, полярные, БЧХ используют весьма схожую конструкцию. Более конкретно, кодовые слова этих кодов получаются как векторы значений некоторых (различным образом определенных) многочленов в различных точках. Вместе с тем, формально эти коды друг к другу не сводятся. В связи с этим возникает задача создания единого математического аппарата для описания указанных классов кодов. Это позволило бы не только упростить их декодирование за счет расширения области применимости известных эффективных алгоритмов, но и построить новые коды, которые сочетали бы в себе хорошую корректирующую способность и возможность простого декодирования. Кроме того, необходимо разработать такую кодовую конструкцию, которая позволяла бы выбирать корректирующую способность с учетом ограничений на сложность декодирования. Решению этих проблем посвящена данная работа.

Цели и задачи диссертационной работы. Целью работы является разработка математического аппарата, который позволил бы упростить декодирование корректирующих кодов, а также построить новые коды, обеспечивающие повышение помехозащищенности и производительности систем передачи и хранения информации. При этом *объектом исследований* являются линейные блоковые коды, а *предметом исследований* — методы их построения и декодирования.

Для достижения указанных целей в работе решаются следующие задачи:

1. Разработка математической модели линейных блоковых кодов, основанной на представлении их кодовых слов как векторов значений (векторных) многочленов от нескольких переменных в различных точках, позволяющей использовать

для декодирования метод последовательного исключения и его обобщения.

2. Разработка на основе созданной модели метода построения кодов, называемых в работе полярными подкодами, который допускал бы возможность выбора корректирующей способности с учетом ограничений на сложность декодирования.

3. Применение предложенной модели для построения новых алгоритмов декодирования полярных кодов, кодов БЧХ, Рида-Соломона, Голея и полярных подкодов.

4. Разработка быстрых алгоритмов кодирования и декодирования кодов Рида-Соломона.

5. Разработка на основе предложенных подходов методов помехозащиты для перспективных систем передачи и хранения информации.

Методология и методы исследования. Результаты работы основываются на аппарате алгебраической теории кодирования, теории информации, коммутативной алгебры, теории вероятностей.

Научная новизна. В работе введено обобщение полиномиальных и мономиальных кодов, называемое многочленными кодами. Оно основано на представлении линейного блокового кода в виде системы линейных ограничений динамического замораживания (ОДЗ) на входные символы поляризующего преобразования. С помощью предложенного обобщения показана возможность использования метода последовательного исключения и его аналогов для декодирования кодов БЧХ, Голея и Рида-Соломона. Впервые представлена конструкция полярных подкодов, основанная на предложенном обобщении и обеспечивающая существенно лучшую корректирующую способность по сравнению с полярными кодами с CRC и известными кодами с малой плотностью проверок на четность. Впервые предложен последовательный алгоритм декодирования полярных (под)кодов. Впервые предложен рандомизированный алгоритм построения базиса Грёбнера произведения нульмерных идеалов и описано применение двоичного метода возведения в степень к задаче построения базиса Грёбнера идеала/модуля интерполяционных многочленов в алгоритмах Гурусвами-Судана и Ву списочного декодирования кодов Рида-Соломона. Впервые представлен асимптотически быстрый вариант циклотомического алгоритма быстрого преобразования Фурье и основанный на нем быстрый алгоритм систематического кодирования кодов Рида-Соломона.

Все полученные результаты на момент их публикации являлись новыми.

Положения, выносимые на защиту:

1. Представление линейных блоковых кодов в виде системы ограничений динамического замораживания (ОДЗ) на элементы входного вектора поляризующего преобразования позволяет осуществлять декодирование некоторых линейных блоковых кодов (в частности, БЧХ, Голея и Рида-Соломона) с использованием алгоритма последовательного исключения и его списочного/последовательного обобщения.

2. Метод построения полярных подкодов, основанный на построении системы ОДЗ, обеспечивающей исключение ненулевых кодовых слов малого веса, и наложении ограничений статического замораживания на символы, передаваемые по

ненадежным подканалам поляризующего преобразования, позволяет получить коды с улучшенной корректирующей способностью по сравнению с известными LDPC и турбо-кодами.

3. Последовательный алгоритм обеспечивает снижение средней сложности декодирования полярных подкодов по сравнению со списочным и стековым алгоритмами с аналогичной корректирующей способностью.

4. Быстрый алгоритм двумерной интерполяции, основанный на рандомизированном алгоритме построения базиса Грёбнера произведения нульмерных идеалов и двоичном методе возведения в степень, обеспечивает снижение сложности алгоритмов Гурусвами-Судана и Ву списочного декодирования кодов Рида-Соломона.

5. Циклотомический алгоритм БПФ обеспечивает быстрое систематическое кодирование кодов Рида-Соломона и повышение производительности операции кодирования в системах хранения данных.

Теоретическая и практическая значимость. Предложенный в работе метод представления линейных блоковых кодов в виде системы ограничений динамического замораживания может быть использован для создания новых методов декодирования корректирующих кодов, а также для создания новых корректирующих кодов. Быстрый алгоритм построения базиса Грёбнера произведения нульмерных идеалов может быть использован в системах компьютерной алгебры.

Представленные в работе быстрые алгоритмы декодирования кодов БЧХ и Рида-Соломона могут быть использованы в существующих и перспективных системах хранения и передачи информации, в которых применяются соответствующие коды. Предложенные в работе полярные подкоды могут быть использованы в перспективных системах мобильной и фиксированной связи. В частности, предложенная конструкция рандомизированных полярных подкодов положена в основу процедуры кодирования для контрольного канала, предусмотренной в стандарте мобильной связи 5 поколения[1], и продемонстрировала лучшую корректирующую способность по сравнению с кодами с циклическим замыканием, применяемыми в системах предшествующих поколений. Предложенный быстрый алгоритм систематического кодирования кодов Рида-Соломона может быть использован в системах хранения данных.

Публикации. Материалы диссертации опубликованы в 26 печатных работах, из них 12 статей в рецензируемых журналах [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12], 14 статей в сборниках трудов конференций [13, 14, 15, 16, 17, 18, 19, **?**, 20, 21, 22, 23, 24, 25].

Личный вклад автора. Содержание диссертации и основные положения, выносимые на защиту, отражают персональный вклад автора в опубликованные работы. Некоторые результаты получены совместно с соавторами (С.В. Федоренко, В.Д. Милославской, Г.А. Трофимюком, К.Г. Ивановым, Е. Коста, А. Варди, Ю. Ма, М.Х. Ли), которым автор выражает искреннюю благодарность. В работе [1] автору принадлежит метод разложения многочленов на сумму полиномов, кратных аффинным. В работе [2] автору принадлежит идея представления полинома

[1] TS 38.212 v2.0.0(2017-12). Technical specification group radio access network; NR; multiplexing and channel coding (Release 15) / 3GPP: 2017, п. 5.3.1.2

в виде суммы линеаризованных многочленов и разложения матрицы дискретного преобразования Фурье на двоичную и блочно-диагональную матрицы. В работе [13] автору принадлежит матричная интерпретация итеративного интерполяционного алгоритма, в то время как доказательство теоремы 3 было получено соавторами независимо друг от друга. В работе [3] автору принадлежит конструкция обратного циклотомического алгоритма БПФ, а также идея варьирования порядка элементов в нормальном базисе с целью снижения сложности получаемого алгоритма. В работе [6] автору принадлежит новая интерпретация алгоритма Ву, оценка размера получаемого списка, а также обобщение двоичного интерполяционного алгоритма. В работе [16] автору принадлежит идея использования кодов БЧХ для построения ограничений динамического замораживания, а также идея использования эвристической функции для ускорения декодирования полярных кодов. В работе [9] автору принадлежит идея использования эвристической функции для ускорения декодирования полярных кодов. В работах [**?**, 22] автору принадлежит идея использования обобщенного разложения Плоткина для декодирования рассматриваемых кодов. В работах [18, 11] автору принадлежит идея использования кодов БЧХ для построения ограничений динамического замораживания, теоремы 1 и 2, а также конструкции полярных подкодов с ядрами БЧХ и Рида-Соломона. В работе [12] автору принадлежит обобщение быстрого алгоритма кодирования кодов Рида-Соломона на случай полярных кодов. В работе [23] автору принадлежит конструкция динамически замороженных символов типа Б и идея использования псевдослучайных ограничений динамического замораживания.

Степень достоверности и апробация результатов. Основные результаты диссертации докладывались на следующих конференциях:

1. IEEE Int. Symposium on Information Theory (2004, 2014, 2017);
2. IEEE Information Theory Workshop (2012, 2013);
3. Int. Symposium on Information Theory and its Applications (2014);
4. Polar Coding for Future Networks: Theory and Practice, Polar Coding in Wireless Communications: Theory and Implementation (2017, 2018);
5. Int. ITG Conference on Systems, Communications and Coding (2017);
6. Int. Symposium on turbo codes and iterative information processing (2016);
7. Int. Symposium on Wireless Communication Systems (2015).
8. Iran Workshop on Communication and Information Theory (2018).

Кроме того, они были представлены на следующих семинарах:

1. по теории кодирования Института проблем передачи информации РАН (Москва, руководитель — Л.А. Бассалыго);
2. по теории информации и ее приложениям Калифорнийского университета в Сан-Диего (США, руководитель — А. Варди);
3. лаборатории связи и построения сигналов Пхохангского университета (Южная Корея, руководитель — К. Янг);

4. кафедры безопасности информационных систем Санкт-Петербургского государственного университета аэрокосмического приборостроения (руководитель — Е. А. Крук);

5. кафедры распределенных вычислений и компьютерных сетей Санкт-Петербургского политехнического университета (руководитель — Ю.Г. Карпов).

Все предложенные алгоритмы были реализованы программно, их поведение было исследовано методами статистического моделирования, результаты которого были сопоставлены с ранее опубликованными.

Структура и объем диссертации. Диссертация состоит из введения, шести глав, заключения и библиографии. Общий объем диссертации 254 страницы, включая 63 рисунка и 12 таблиц. Библиография включает 196 наименований.

Содержание работы

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

В первой главе представлен обзор требований, предъявляемых в перспективных системах передачи и хранения информации к средствам помехоустойчивого кодирования. Показано, что различные приложения требуют построения корректирующих кодов с различными соотношениями скорости, относительного минимального расстояния, вероятности ошибки декодирования, сложности и задержки кодирования и декодирования и других параметров.

В частности, системы мобильной связи 5 поколения требуют существенного повышения корректирующей способности используемых кодов по сравнению с применяемыми в настоящее время решениями. Ввиду большой распространенности мобильных устройств, при этом также требуется значительно снизить энергопотребление кодеров и декодеров. Кроме того, такие системы должны обеспечивать эффективную поддержку межмашинной коммуникации, что требует обеспечения хорошей помехозащиты коротких сообщений.

Показано, что современные системы хранения данных требуют использования кодов с большим числом проверочных символов. Например, в системах Hadoop File System и EMC Atmos предусмотрено использование кодов Рида-Соломона, соответственно, с 4 и 6 проверочными символами. Производительность таких систем определяется сложностью операции кодирования, выполняемой при записи данных, числом операций (в т.ч. ввода/вывода), выполняемых при частичном обновлении данных, числом устройств, с которых производится считывание данных в процессе восстановления информации, хранившейся на отказавших устройствах, объемом данных, передаваемых по сети (в случае сетевых систем хранения) в процессе восстановления информации, хранившейся на отказавших устройствах и др. Отмечено, что за последние годы опубликовано большое число работ, посвященных построению локально восстановимых и регенерирующих кодов, использование которых позволяет существенно повысить эффективность операции восстановления данных. Однако в литературе уделено недостаточно внимания производительности операции кодирования, хотя она регулярно выполняется в штатном режиме работы систем хранения.

Далее в главе введены основные понятия теории кодирования и теории информации, используемые в работе, представлен обзор некоторых кодовых конструкций и алгоритмов декодирования, проведен анализ их недостатков.

В частности, рассмотрены классические конструкции полиномиальных и мономиальных кодов. Отмечено, что коды БЧХ, Рида-Соломона и выколотые коды Рида-Маллера могут быть получены как полиномиальные коды, в то время как полярные коды, расширенные коды Рида-Соломона и коды Рида-Маллера могут быть получены как мономиальные коды. Несмотря на схожесть конструкции, формально полиномиальные и мономиальные коды друг к другу не сводятся.

Таким образом, разработка перспективных систем передачи информации и хранения данных требует создания методов помехоустойчивого кодирования, обладающих простыми процедурами построения, кодирования и декодирования, а также высокой корректирующей способностью. Полярные коды обладают первыми тремя качествами и способны достигать предела Шеннона, но демонстрируют неудовлетворительную корректирующую способность на практически значимых длинах. Кроме того, декодирование полярных кодов почти по максимуму правдоподобия требует применения достаточно сложного списочного алгоритма, в котором, однако, существует потенциальная возможность существенного упрощения. Следует также отметить, что полярные коды являются частным случаем мономиальных кодов, структура которых близка к структуре полиномиальных кодов, многие из которых обладают хорошими дистантными свойствами. Проведенный анализ показывает, что возможно создание кодовой конструкции, объединяющей преимущества полиномиальных и полярных кодов, а также расширение области применимости алгоритмов декодирования полярных кодов на иные кодовые конструкции.

Во многих приложениях (например, системах хранения данных, стеганографии) большое значение имеет гарантированная способность кода исправлять ошибки и/или стирания. В этом смысле оптимальными являются коды Рида-Соломона. Несмотря на долгую историю их исследований, существующие методы их систематического кодирования и декодирования остаются чрезмерно сложными. Кроме того, даже при использовании списочных методов не удается реализовать декодирование кодов Рида-Соломона по максимуму правдоподобия.

Во второй главе введено понятие многочленных кодов, обобщающее конструкции полиномиальных и мономиальных кодов. Пусть $\mathcal{P}_m = \mathbb{F}_q[X_0, \dots, X_{m-1}]$ — множество многочленов, степень которых относительно каждой из переменных меньше некоторого числа l. Для произвольного множества $\mathcal{E} \subset \mathbb{F}_q^m$ и многочлена $f \in \mathcal{P}_m$ определим функцию

$$v(f, \mathcal{E}) = (f(e_0), \dots, f(e_{|\mathcal{E}|-1})),$$

результатом которой является вектор значений многочлена f в различных точках $e_i \in \mathcal{E}$. Эта функция может быть обобщена на случай вектора многочленов следующим образом:

$$\mathcal{V}\left((f^{(0)}, \dots, f^{(z-1)}), (\mathcal{E}_0, \dots, \mathcal{E}_{z-1})\right) = (v(f^{(0)}, \mathcal{E}_0), \dots, v(f^{(z-1)}, \mathcal{E}_{z-1})),$$

где $\mathcal{E}_i \subset \mathbb{F}_q^{m_i}$, $f^{(i)} \in \mathcal{P}_{m_i}$.

Определение 1. *Рассмотрим конечное множество $\mathcal{P} \subset \mathcal{P}_{m_0} \times \dots \times \mathcal{P}_{m_{z-1}}$ линейно независимых над $\mathbb{F}_q$ векторов многочленов. Пусть E — некоторое l-элементное*

подмножество $\mathbb{F}_q$. *Многочленным кодом длины* $n = \sum_{s=0}^{z-1} l^{m_s}$ *над* $\mathbb{F}_q$ *называется*

$$C(\mathcal{P}) = \left\{ \mathcal{V}(f, (E^{m_0}, \ldots, E^{m_{z-1}})) \,\middle|\, f = \sum_i f_i P^{(i)}, f_i \in \mathbb{F}_p \right\}, \mathbb{F}_p \subset \mathbb{F}_q$$

где $P^{(i)} = (p_0^{(i)}(X_0, \ldots, X_{m_0-1}), \ldots, p_{z-1}^{(i)}(X_0, \ldots, X_{m_{z-1}-1}))$ — *i-ый многочлен из* $\mathcal{P}$.

К классу многочленных кодов можно отнести многие классические корректирующие коды, в т.ч. Рида-Соломона, Рида-Маллера, полярные и БЧХ. Заметим, что вычисление значений многочлена от одной переменной в различных точках соответствует умножению вектора его коэффициентов на матрицу Вандермонда или, что то же самое, ядро Рида-Соломона

$$F_l = \begin{pmatrix} \alpha_{l-1}^{l-1} & \alpha_{l-2}^{l-1} & \ldots & \alpha_2^{l-1} & \alpha_1^{l-1} & \alpha_0^{l-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ \alpha_{l-1}^{1} & \alpha_{l-2}^{1} & \ldots & \alpha_2^{1} & \alpha_1^{1} & \alpha_0^{1} \\ \alpha_{l-1}^{0} & \alpha_{l-2}^{0} & \ldots & \alpha_2^{0} & \alpha_1^{0} & \alpha_0^{0} \end{pmatrix},$$

где α_i — различные элементы $\mathbb{F}_q$. Вычисление значений многочлена от m переменных соответствует умножению вектора его коэффициентов на матрицу $F_l^{\otimes m}$. Таким образом, кодирование в (n, k) многочленном коде может быть выполнено как

$$c_0^{n-1} = xW \underbrace{\operatorname{diag}(A_{m_0}, \ldots, A_{m_{z-1}})}_{A}, \tag{1}$$

где W — $k \times n$ *матрица прекодирования*, i-ая строка которой содержит коэффициенты многочлена $\mathcal{P}^{(i)}$, A — матрица смешанного поляризующего преобразования, $A_m = B_{l,m} F_l^{\otimes m}$ — матрица поляризующего преобразования с ядром Рида-Соломона F_l, и $B_{l,m}$ — матрица, задающая перестановку "обращения цифр" $R_{l,m}(\sum_{j=0}^{m-1} i_j l^j) = \sum_{j=0}^{m-1} i_j l^{m-1-j}$, $0 \le i_j < l$.

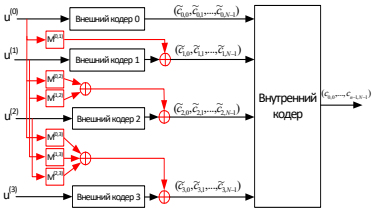


Рис. 1. Кодер ОККПС

В силу обратимости матрицы A такое представление может быть найдено для произвольного линейного блокового кода из уравнения $WA = G$, где G — порождающая матрица. Это позволяет представить рассматриваемый код в виде, аналогичном полярному коду, и воспользоваться алгоритмами декодирования, разработанными для полярных кодов.

Кроме того, предлагается расширение концепции обобщенных каскадных кодов (ОКК), называемое обобщенными каскадными кодами с перекрестными связями (ОККПС). Структура кодера ОККПС повторяет структуру кодера обобщенных каскадных кодов. Единственным отличием является то, что в случае ОККПС кодирование вектора $u^{(i)} \in \mathbb{F}_q^{K_i}$ осуществляется не во внешнем коде $\mathbb{C}_i$, как в классических ОКК, но в его смежном классе $\mathbb{C}_i + \left(\sum_{s=0}^{i-1} u^{(i)} M^{(s,i)}\right)$, где $M^{(s,i)} \in \mathbb{F}_q^{K_s \times N}$ — некоторая матрица, как показано на рис. 1. Таким образом, получается линейный блоковый код длины Nn и размерности $\sum_{i=0}^{n-1} K_i$. Это расширение позволяет использовать для декодирования широкого класса линейных блоковых

кодов методы (в частности, многошаговое декодирование), разработанные для декодирования ОКК и многоуровневых кодов. Такой подход, однако, не гарантирует хорошую (и даже сравнимую с другими известными методами декодирования) корректирующую способность в общем случае.

В качестве примера ОККПС, соответствующего внутренним кодам, порождаемым строками $\mathcal{G} = F_2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, предложено обобщение классической конструкции Плоткина и доказана

Теорема 1. *Любой линейный* $(2n, k, d)$ *код* $\mathcal{C}$ *имеет порождающую матрицу вида*

$$G = \begin{pmatrix} I_{k_1} & 0 & \tilde{I} \\ 0 & I_{k_2} & 0 \end{pmatrix} \begin{pmatrix} G_1 & 0 \\ G_2 & G_2 \\ G_3 & G_3 \end{pmatrix}, \tag{2}$$

где I_l *—* $l \times l$ *единичная матрица,* $G_i, 1 \le i \le 3$, *— матрицы размерности* $k_i \times n$, $k = k_1 + k_2$, *и* $\tilde{I}$ *получается путем дописывания нулевой матрицы размерности* $(k_1 - k_3) \times k_3$ *к матрице* I_{k_3}, *причем* $k_3 \le k_1$.

На основе предложенных конструкций многочленных кодов и ОККПС предложен метод представления линейных блоковых кодов в виде системы линейных ограничений динамического замораживания (ОДЗ). Рассмотрим $(n = l^m, k, d)$ код $\mathcal{C}$ над $\mathbb{F}_q$ с проверочной матрицей H. Пусть A — матрица $n \times n$ поляризующего преобразования. Т.к. A обратима, любой вектор длины n может быть получен как результат $c_0^{n-1} = u_0^{n-1}A$ применения поляризующего преобразования к подходящему вектору u_0^{n-1}. Ограничения, которые должны быть наложены на u_0^{n-1}, чтобы результат его применения принадлежал коду $\mathcal{C}$, задаются уравнением $u_0^{n-1}AH^T = 0$. Путем элементарных преобразований строк можно получить *матрицу ограничений* $V = QHA^T$, где Q — такая обратимая матрица, что последние ненулевые элементы всех строк V расположены в различных столбцах, т.е. значения $j_i = \max\{t | V_{i,t} \ne 0\}, 0 \le i < n-k$ различны и $V_{i,j_i} = -1$. Пусть $\mathcal{F} = \{j_i | 0 \le i < n-k\}$ — множество номеров замороженных символов. Тогда получим

$$u_{j_i} = \sum_{s=0}^{j_i - 1} u_s V_{i,s}, 0 \le i < n-k. \tag{3}$$

Эти уравнения могут рассматриваться как обобщение ограничений, налагаемых на замороженные символы в полярных кодах $u_{j_i} = 0, j_i \in \mathcal{F}$. Заметим, что символы $u_{j_i}, j_i \in \mathcal{F}$ могут принимать произвольные значения, которые, однако, зависят от значений символов с меньшими номерами. Таким образом, символы u_{j_i}, задаваемые (3), будем называть динамически замороженными (ДЗС). Если все коэффициенты $V_{i,s}$ в правой части (3) являются нулевыми, будем называть соответствующие символы u_{j_i} статически замороженными.

Заметим, что любой линейный код длины n может быть представлен в виде системы линейных уравнений (3). Это позволяет применить метод последовательного исключения и его обобщения для декодирования произвольных линейных кодов длины n. Таким образом, декодирование кода длины $n = l^m$ может производиться путем последовательного принятия решений

$$\widehat{u}_i = \begin{cases} \arg\max_{u_i \in \mathbb{F}_q} \mathcal{W}_m^{(i)} \left\{ \widehat{u}_0^{i-1}, u_i | y_0^{n-1} \right\}, & i \notin \mathcal{F} \\ \sum_{s=0}^{i-1} \widehat{u}_s V_{t_i,s}, & \text{иначе,} \end{cases} \tag{4}$$

где t_i — такое целое, что $j_{t_i} = i$, $\mathcal{W}_m^{(i)}\left\{u_0^i | y_0^{l^m-1}\right\} = \frac{\mathcal{W}_m^{(i)}(y_0^{n-1}, u_0^{i-1}|u_i)P\{u_i\}}{\mathcal{W}(y_0^{n-1})}$, $P\{u_i\} = \frac{1}{q}$, $u_i \in \mathbb{F}_q$, и $\mathcal{W}_m^{(i)}(y_0^{n-1}, u_0^{i-1}|u_i)$ — функция переходных вероятностей i-го подканала поляризующего преобразования A_m. Аналогичный подход, подробно рассмотренный в главе 4, может быть использован и для декодирования кодов иных длин, представление которых в виде ОДЗ требует использования смешанного поляризующего преобразования. Заметим, что если $\widehat{u}_0^{i-1}$ являются истинными значениями входных символов поляризующего преобразования, вероятность ошибки P_i на каждом шаге этого алгоритма совпадает с таковой (т.е. с вероятностью ошибки в $\mathcal{W}_m^{(i)}$) для классических полярных кодов. Таким образом, вероятность ошибки декодирования кода методом последовательного исключения может быть оценена как $P_{SC} \leq \sum_{i \notin \mathcal{F}} P_i$.

Существенно лучшая корректирующая способность может быть получена при использовании списочного метода Тала-Варди. Анализ корректирующей способности этого метода до настоящего времени остается открытой проблемой. В работе показано, что в случае ядра Арикана ($l = 2$) при использовании упрощенного (практически нереализуемого) варианта списочного метода, использующего не более k точных "подсказок" относительно значений входных символов поляризующего преобразования, вероятность ошибки декодирования кода длины N со скоростью R в двоичном стирающем канале с параметром Бхаттачарьи Z удовлетворяет

$$P_e(N, R, Z, k) \geq \left(\frac{3}{16}\right)^{2^k - 1} (AZ^\delta)^{2^k} + o(Z^{\delta 2^k}),$$

где A — некоторый коэффициент, $\delta = 2^w$, $w = \min_{i \notin \mathcal{F}} \mathrm{wt}(i)$. Отсюда следует, что декодирование с помощью (списочного) алгоритма последовательного исключения линейных блоковых кодов с использованием предложенного представления может быть эффективным только для кодов, характеризующихся достаточно большими значениями δ (т.е. представимых в виде векторов значений многочленов достаточно малой степени).

Представление линейного блокового кода с помощью матрицы ограничений эквивалентно его представлению в виде многочленного кода. Очевидно, что матрицы ограничений и прекодирования при этом связаны соотношением $WV^T = 0$. В главе охарактеризованы множества замороженных символов для расширенных примитивных двоичных кодов БЧХ в узком смысле (РБЧХ) и кодов Рида-Соломона. Доказаны

Теорема 2. *Рассмотрим $(2^m, k, d)$ код РБЧХ над $\mathbb{F}_2$ и поляризующее преобразование $A_m = B_{2,m}F_2^{\otimes m}$. Пусть $S = \{i \in \mathcal{Q} | 0 \leq i < d-1\}$, где $\mathcal{Q}$ — множество наименьших представителей циклотомических классов над $\mathbb{F}_2$ по модулю $2^m - 1$. Пусть N_t — число номеров і ДЗС u_i этого кода таких, что $\mathrm{wt}(i) = t$. Тогда $N_t = \sum_{s \in S_t} m_s$, где $S_t = \{s \in S | \mathrm{wt}(s) = t\}$, и m_s — мощность циклотомического класса над $\mathbb{F}_2$ по модулю $2^m - 1$, порождаемого s.*

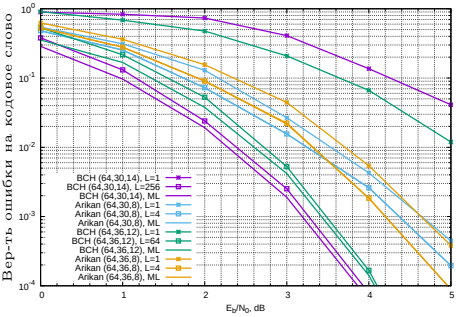
Теорема 3. *$(2^m, k, 2^m - k + 1)$ расширенный код Рида-Соломона над $\mathbb{F}_{2^m}$ может быть представлен в виде системы ОДЗ с множеством номеров замороженных символов $\mathcal{F} = \{0, \ldots, 2^m - 1\} \setminus \{2^m - 1 - R_{2,m}(i) | 0 \leq i < k\}$.*

Обе теоремы предполагают, что элементы $x_i, 0 \leq i < 2^m$ первой строки проверочной матрицы кодов выписаны в стандартном битовом порядке, т.е. $x_i =$

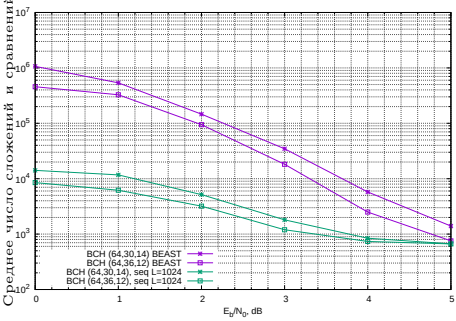
$\sum_{j=0}^{m-1} i_j\beta_j, i = \sum_{j=0}^{m-1} i_j 2^j, i_j \in \{0,1\}$, где $\beta_0, \ldots, \beta_{m-1}$ — некоторый базис $\mathbb{F}_{2^m}$. Доказательство теорем основывается на представлении кодовых слов рассматриваемых кодов в виде векторов значений некоторых многочленов $f(x)$ в различных $x \in \mathbb{F}_{2^m}$ и представлении $x = \sum_{i=0}^{m-1} x_i\beta_i$, $x_i \in \{0,1\}$. Из вышеприведенного анализа следует, что эти коды допускают относительно простое декодирование списочным методом последовательного исключения и его аналогами.

Кроме того, на основе конструкции Турина получено представление расширенного кода Голея в виде системы ограничений динамического замораживания.

Предложенное представление позволяет использовать для декодирования линейных блоковых кодов метод последовательного исключения и его обобщения. На рис. 2 представлены[2] корректирующая способность и сложность последовательного алгоритма ПИ, предложенного в главе 4, в случае кодов РБЧХ. Для сравнения приведены результаты для классических полярных кодов Арикана. Видно, что последние существенно превосходят коды РБЧХ в случае размера списка $L = 1$ (т.е. алгоритма ПИ). Однако большее минимальное расстояние обеспечивает значительный энергетический выигрыш кодов РБЧХ при декодировании почти по максимуму правдоподобия. Для декодирования почти по максимуму правдоподобия коды РБЧХ требуют существенно большего размера списка по сравнению с полярными кодами Арикана. Тем не менее, предлагаемый подход обеспечивает существенное снижение средней сложности декодирования по сравнению с алгоритмом BEAST, особенно в области малых отношений сигнал/шум.



($а$) Вероятность ошибки



($б$) Средняя сложность декодирования

Рис. 2. Декодирование кодов РБЧХ, представленных в виде системы ОДЗ

Результаты второй главы опубликованы в работах [11, 18, 16].

В третьей главе рассматривается задача построения кодов, которые допускали бы простое декодирование с помощью обобщений метода последовательного исключения и обладали бы при этом хорошей корректирующей способностью. Предлагаемая конструкция основана на введенном выше представлении линейных блоковых кодов в виде системы ограничений динамического замораживания.

Определение 2. *Рассмотрим q-ичный симметричный канал $\mathcal{W}(y|c)$ и $(n = l^m, k', d)$ код $\mathcal{C}'$ над $\mathbb{F}_q$, называемый протокодом. Пусть $\mathcal{F}'$ — множество номе-*

[2] Здесь и далее, если не указано иное, приведены результаты для 2-АМ и канала с АБГШ.

ров замороженных символов $\mathcal{C}'$ относительно ядра F_l. $(n, k, \geq d)$ полярный подкод в узком смысле $\mathcal{C}$ кода $\mathcal{C}'$ — множество векторов $c_0^{n-1} = u_0^{n-1} B_{l,m} F_l^{\otimes m}$, где u_0^{n-1} удовлетворяет как ОДЗ кода $\mathcal{C}'$, так и дополнительным ограничениям $u_s = 0$ для $k' - k$ номеров $s \notin \mathcal{F}'$ с наибольшими вероятностями ошибки P_s в соответствующих подканалах поляризующего преобразования, задаваемого $B_{l,m} F_l^{\otimes m}$.

Определение 3. *Пусть дано ядро F_l, натуральные числа z, r, $m_0, \ldots, m_{z-1}$. Полярным подкодом в широком смысле называется множество векторов*

$$c = xW \operatorname{diag}(B_{l,m_0} F_l^{\otimes m_0}, \ldots, B_{l,m_{z-1}} F_l^{\otimes m_{z-1}}), x \in \mathbb{F}_q^k,$$

где матрица W имеет нулевые столбцы в позициях, соответствующих r подканалам $\mathcal{W}_{m_t}^{(j)}, 0 \leq t < z$, с наибольшей вероятностью ошибки.

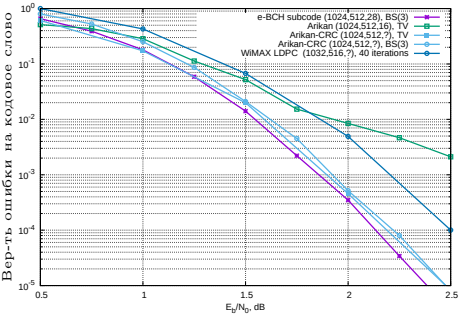


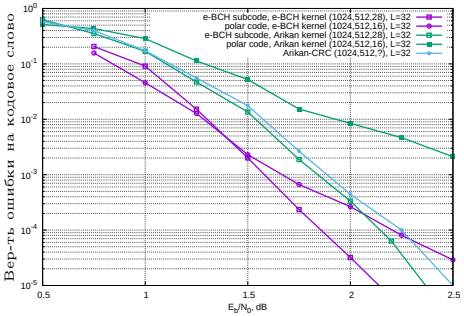
Рис. 3. Полярные подкоды с ядром Арикана

При декодировании методом ПИ полярные подкоды не имеют никаких преимуществ перед классическими полярными кодами, построенными для соответствующего канала. Это связано с тем, что вероятность ошибки декодирования методом ПИ однозначно определяется множеством номеров замороженных символов, и классическая конструкция полярных кодов явным образом ее минимизирует. Однако полярные подкоды демонстрируют существенный выигрыш при использовании списочного и последовательного алгоритмов декодирования.

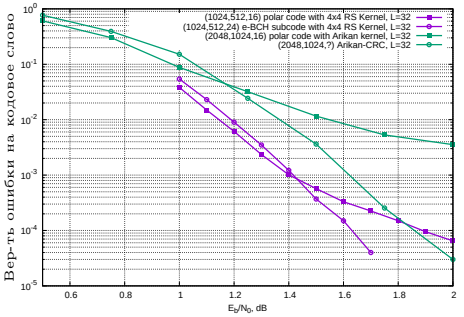
Предложена алгебраическая конструкция полярных подкодов в узком смысле для случая ядер Арикана, РБЧХ и Рида-Соломона. В качестве протокода предложено использовать код РБЧХ (l^m, k', d) над $\mathbb{F}_q$, где $\mathbb{F}_q$ — алфавит, над которым задано ядро, и d — конструктивное расстояние кода. На рис. 3 представлены результаты статистического моделирования для кодов длины ≈ 1024 для случая передачи по каналу с АБГШ и двоичной фазовой модуляцией. Для сравнения приведены также результаты для полярных кодов (Arikan) и полярных кодов с CRC-16 (Arikan-CRC), а также LDPC кода из стандарта WiMAX. Декодирование полярных (под)кодов выполнялось, соответственно, с помощью блочного последовательного алгоритма декодирования (BS(s)), описанного в главе 4, где 2^s — длина внешних кодов в представлении рассматриваемого кода как ОККПС, и списочного алгоритма Тала-Варди (TV) с размером списка 32. Можно заметить, что полярный подкод обеспечивает значительный энергетический выигрыш по сравнению с LDPC-кодом (0.25 дБ), классическим полярным кодом и полярным кодом с CRC.

На рис. 4, *а* представлены результаты моделирования для полярных (под)кодов с ядрами РБЧХ и Арикана, а также полярного кода с ядром Арикана и CRC-16. Декодирование производилось с помощью последовательного алгоритма, описанного в [26]. Видно, что использование ядра РБЧХ обеспечивает выигрыш более 0,3 дБ по сравнению со случаем ядра Арикана.

В обоих случаях конструкция полярных подкодов позволяет существенно повысить корректирующую способность в области высоких отношений сигнал/шум. На рис. 4, *б* представлены результаты моделирования для случая передачи двоичного образа полярного (под)кода с 4×4 ядром РС над полем $\mathbb{F}_{2^2}$ по каналу с АБГШ и двоичной фазовой модуляцией. Декодирование полярных (под)кодов выполнялось с помощью обобщения метода Тала-Варди на случай недвоичных кодов. Как и в ранее рассмотренных случаях, полярный подкод обеспечивает значительный выигрыш в области высоких отношений сигнал/шум по сравнению с полярным кодом с тем же ядром.



(*а*) Ядро РБЧХ



(*б*) Ядро РС

Рис. 4. Полярные (под)коды кодов РБЧХ

Предложена рандомизированная конструкция полярных подкодов в широком смысле. Конструкция описана для случая кодов с ядром Арикана. Идея конструкции основана на построении классического полярного кода размерности $k + t$ с последующим выбором его случайного подкода размерности k. При равновероятном выборе подкодов матожидание числа ненулевых кодовых слов в получаемом коде равно $\mathbf{M}[w_s] = w'_s \frac{2^k - 1}{2^{k+t}-1} \approx w'_s 2^{-t}$, $s > 0$, где w'_s — число кодовых слов веса s в исходном полярном коде. Эксперименты показывают, что с увеличением t ошибочный коэффициент w'_d, где d — минимальное расстояние, классического полярного кода растет достаточно медленно, вследствие чего $\mathbf{M}[w_i]$ быстро убывает с увеличением t. Кроме того, предлагается формировать ОДЗ таким образом, чтобы они могли быть учтены на возможно более ранних фазах декодирования, а также ввести дополнительные ОДЗ, обеспечивающие быстрое убывание весов неправильных путей при списочном/последовательном декодировании. Это позволяет снизить вероятности потери правильного пути списочным/последовательным декодером на ранних фазах декодирования.

Конструкция предполагает использование двух типов ограничений динамического замораживания. Построение кода начинается с нахождения множества $\mathcal{N}$ номеров $k + t$ наиболее надежных подканалов поляризующего преобразования. Затем налагаются t ограничений динамического замораживания (ОДЗ) типа А на последние входные символы поляризующего преобразования $u_i, i \in \mathcal{N}$, с номерами i наименьшего веса[3]. Далее формируются q ОДЗ типа Б на символы $u_i, i \notin \mathcal{N}$,

[3] Вес числа равен числу ненулевых битов в его двоичном представлении.

соответствующие наиболее надежным подканалам. Коэффициенты ОДЗ типа А и Б выбираются псевдослучайным образом. Ограничения типа А и Б обеспечивают, соответственно, исключение из получаемого кода ненулевых кодовых слов малого веса и снижение вероятности потери списочным/последовательным декодером правильного пути на ранних фазах декодирования. Представлены рекомендации по выбору параметров t и q предложенной конструкции, а также описана процедура укорочения, которая позволяет получить коды произвольной длины. Сложность предложенного алгоритма построения $(2^m, k)$ полярного подкода в широком смысле составляет $O(k(t+q))$ обращений к генератору псевдослучайных чисел, в то время как построение матрицы ограничений полярного подкода $(n, \tilde{k}, d)$ в узком смысле кода РБЧХ с $(n-k') \times n$ проверочной матрицей $\tilde{H}$ предполагает применение метода Гаусса к матрице $\tilde{H}A_m^T$, что требует $(n-k')^2 n$ операций сложения.

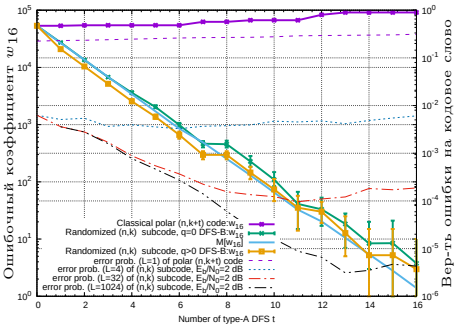


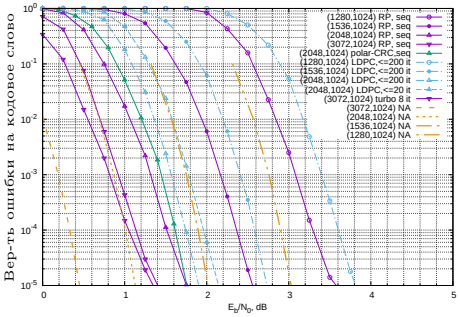
Рис. 5. Ошибочный коэффициент w_{16} и вероятность ошибки декодирования рандомизированных полярных подкодов

На рис. 5 представлены значения среднего, максимального и минимального значений ошибочного коэффициента w_{16} (т.е. числа кодовых слов веса 16) рандомизированных полярных $(n = 1024, k = 512)$ подкодов, построенных для $E_b/N_0 = 1.5$ дБ, а также вероятности ошибки их декодирования методом последовательного исключения и с помощью последовательного алгоритма с различными значениями размера списка L. Для каждого t и q были построены 50 кодов. Во всех случаях минимальное расстояние кодов было не менее 16. Видно, что среднее значение ошибочного коэффициента весьма близко к математическому ожиданию $\mathbf{M}[w_{16}]$ ошибочного коэффициента кода, получаемого путем равновероятного выбора k-мерных линейных подпространств классического $(n, k+t)$ полярного кода.

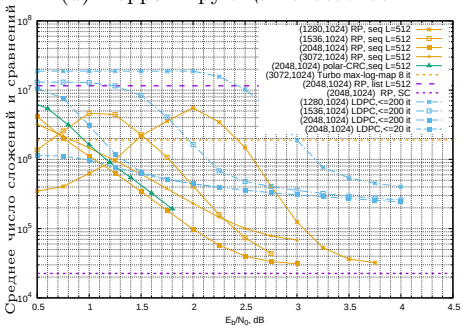
Видно, что матожидание ошибочного коэффициента $\mathbf{M}[w_{16}]$ полярного подкода быстро убывает с t. Однако увеличение t требует размораживания символов, передаваемых по ненадежным подканалам поляризующего преобразования, что приводит к увеличению вероятности ошибки декодирования методом последовательного исключения, и вероятности потери декодером правильного пути. Для компенсации вызываемого этим ухудшения корректирующей способности декодера должен быть увеличен его размер списка L, который влияет на сложность декодирования. Из рис. 5 видно, что при различных значениях L минимум вероятности ошибки последовательного алгоритма достигается при различных значениях параметра кодовой конструкции t. Таким образом, предложенный подход позволяет строить коды с учетом требований к сложности декодирования.

На рис. 6 представлена вероятность ошибки декодирования рандомизированных полярных подкодов (RP), полярных подкодов кодов РБЧХ (PBCH) и полярного кода с CRC-16. Для сравнения приведены результаты для кодов AR4JA LDPC, определенных в стандарте CCSDS и декодируемых алгоритмом распространения доверия с чередованием, и турбо-кода LTE.

Для некоторых полярных (под)кодов представлены результаты как в случае последовательного (seq), так и списочного (list) декодирования с размером списка $L = 512$. Кроме того, представлены значения нормальной аппроксимации (NA) нижней границы вероятности ошибки декодирования линейных кодов Полянского-Пура-Верду. Можно заметить, что предложенные рандомизированные полярные подкоды обеспечивают выигрыш до 0,3 дБ по сравнению с полярным кодом с CRC, кодом LDPC и турбо-кодом. При использовании последовательного алгоритма средняя сложность декодирования полярных подкодов оказывается существенно меньше по сравнению со средней сложностью декодирования LDPC кодов. Таким образом, предложенная конструкция и алгоритм декодирования обеспечивают одновременное повышение корректирующей способности и снижение сложности декодирования по сравнению с LDPC кодами. На практике при декодировании LDPC-кодов, как правило, ограничиваются значительно меньшим числом итераций алгоритма распространения доверия. Из рис. 6 видно, что это приводит к росту вероятности ошибки, причем для кода $(2048, 1024)$ при $E_b/N_0 > 1.1$ дБ сложность последовательного алгоритма декодирования полярного подкода остается меньшей по сравнению с алгоритмом декодирования LDPC кода с 20 итерациями.



($а$) Корректирующая способность



($б$) Сложность декодирования

Рис. 6. Последовательное декодирование рандомизированных полярных подкодов

Представлена конструкция цепных полярных подкодов, позволяющая получить коды произвольной длины без использования механизмов выкалывания и укорочения. Она позволяет не только упростить декодер, отказавшись от обработки в нем заведомо абсолютно надежных или ненадежных символов, но и упростить расчет надежности подканалов при построении кодов. Рассмотрим построение кода длины $n = \sum_{i=0}^{z-1} 2^{m_i}$, $m_i > m_{i+1}, 0 \le i \le z-2$ и размерности k, кодовые слова которого образованы конкатенацией выходных векторов поляризующих преобразований A_{m_i}, причем входные вектора этих преобразований

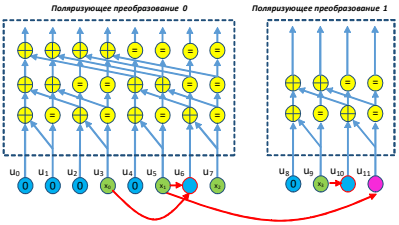


Рис. 7. Кодер цепного полярного подкода

имеют некоторые линейные зависимости, как показано на рис. 7. Кодовые слова предлагаемых кодов также могут быть получены в соответствии с (1). В работе описаны два метода построения матрицы прекодирования W для случая ядра Арикана.

Алгебраический метод, основанный на конструкциях X4 и XX и кодах РБЧХ, позволяет получить цепные полярные подкоды с заданным минимальным расстоянием и состоит в следующем. Пусть d — конструктивное расстояние рассматриваемого кода. Выберем $2^{m_i} \times 2^{m_i}$ матрицы $G^{(i)}$, первые κ строк которых порождают $(2^{m_i}, \kappa, d_{i,\kappa})$ коды, $d_{i,\kappa} \geq d_{i,\kappa+1}$. Далее $G^{(i)}$ будут называться компонентными матрицами. Пусть $\delta(i,d) = \max_{\kappa: d_{i,\kappa} < d} d_{i,\kappa}$. Не ограничивая общности будем считать, что первые ненулевые элементы строк матрицы $W^{(i)} = G^{(i)} A_{m_i}$ расположены в различных столбцах. Пусть $l_{i,j}$ — позиция первого ненулевого элемента в $W^{(i)}_{j,-}$, где $X_{j,-}$ обозначает j-ый столбец матрицы X. Будем строить порождающую матрицу (n,k,d) цепного полярного подкода как $G = \begin{pmatrix} \tilde{G} \\ \overline{G} \end{pmatrix}$. Здесь матрицы $\tilde{G}$ и $\overline{G}$ являются блочными, причем блоки имеют 2^{m_i} столбцов. Матрица $\tilde{G}$ является блочно-диагональной с блоками $G(i,d)$, где $G(i,d)$ — матрица, состоящая из некоторых строк $G^{(i)}_{s,-}, 0 \leq s < 2^{m_i}$, причем $d_{i,s+1} \geq d$. Матрица $\overline{G}$ содержит ровно два ненулевых блока в каждой строке. Если первый ненулевой блок в строке имеет номер i, тогда он равен некоторой строке $G^{(i)}_{s,-}$, где $d_{i,s+1} \geq \delta(i,d)$. Если второй ненулевой блок в той же строке имеет номер $j > i$, то он равен некоторой строке $G^{(j)}_{t,-}$, причем $d_{i,t+1} \geq d - \delta(i,d)$. Выбор строк из компонентных матриц осуществляется таким образом, чтобы каждая строка использовалась в матрице G не более одного раза. Это гарантирует, что в результате описанных действий будет получена матрица полного ранга. Для обеспечения возможности эффективного декодирования предлагаемых кодов с помощью списочного/последовательного алгоритма декодирования, должны использоваться следующие дополнительные правила выбора строк матрицы G:

1. k строк $G^{(i)}_{s,-}$, использованные в $\tilde{G}$ или в качестве первых ненулевых блоков матрицы $\overline{G}$, должны соответствовать наименьшим значениям вероятности ошибки $P_{m_i, l_{i,s}}$ в подканалах $\mathcal{W}^{(l_{i,s})}_{m_i}$ поляризующего преобразования, для которых выполняются вышеприведенные неравенства для $d_{i,s}$.

2. Строки $G^{(j)}_{t,-}$, используемые в качестве вторых ненулевых блоков матрицы $\overline{G}$, выбираются из соображений минимизации $P_{m_j, l_{j,t}}$.

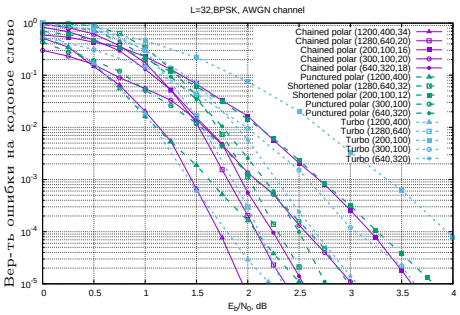
3. τ строк $G^{(i)}_{s,-}$ с $d_{i,s+1} \geq d$ и наивысшими значениями $P_{m_i,s}$ используются в качестве первых ненулевых блоков $\overline{G}$. Здесь τ является параметром конструкции.

4. Для любой пары строк матрицы $\overline{G}$, содержащих ненулевые блоки $G^{(i)}_{s,-}$, $G^{(j)}_{t,-}$ и $G^{(i)}_{s',-}$, $G^{(j)}_{t',-}$, из $l_{i,s} < l_{i,s'}$ следует $l_{j,t} < l_{j,t'}$.

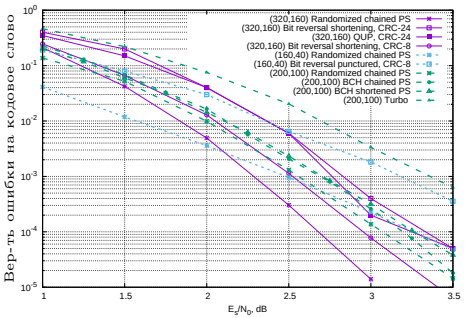
Предложена рандомизированная конструкция цепных полярных подкодов, основанная на рекурсивном построении ОКК с внутренними полярными кодами с ядром Арикана и внешними удлиненными ОКК, и удлинении полученных ОКК на один символ. Для удлинения кода длины n на один символ предлагается дополнительно передать один из входных символов поляризующего преобразования,

используемого в конструкции этого кода. Для получения кода длины $(n+1)2^m$ в случае ядра Арикана предлагается воспользоваться конструкций обобщенных каскадных кодов с внутренними полярными кодами длины 2^m и внешними кодами, получаемыми с помощью вышеописанной процедуры удлинения. Рекурсивное применение такого подхода позволяет получить коды произвольной длины. В работе описано обобщение вышеописанной процедуры построения ОДЗ типа А и Б, позволяющее улучшить дистантные характеристики получаемых таким образом кодов.

На рис. 8 представлено сравнение корректирующей способности цепных полярных подкодов и различных укороченных и выколотых кодов. Видно, что цепные полярные подкоды обеспечивают лучшую корректирующую способность по сравнению с укороченными и выколотыми полярными (под)кодами и турбо-кодами. При этом рандомизированная конструкция демонстрирует лучшие результаты по сравнению с алгебраической (BCH).



($а$) Алгебраическая конструкция



($б$) Рандомизированная конструкция

Рис. 8. Цепные полярные подкоды

На рис. 9 представлена зависимость отношения сигнал/шум на символ, требуемого для достижения вероятности ошибки 10^{-2} рандомизированными цепными полярными подкодами, от их скорости и размерности. Для сравнения приведены результаты для укороченных кодов, полученных с помощью вышеописанной рандомизированной конструкции, и LDPC-кодов, предложенных для включения в стандарт 5G, декодируемых с помощью алгоритма распространения доверия с 15 итерациями. Видно, что предлагаемые цепные рандомизированные полярные подкоды обеспечивают примерно такую же корректирующую способность как и укороченные рандомизированные полярные подкоды, в то время как LDPC коды существенно им проигрывают.

Как видно из вышепредставленных результатов, полярные подкоды при фиксированной сложности декодирования особо эффективны для блоков малой длины. В связи с этим они представляют значительный интерес для использования в управляющем канале систем передачи информации. На рис. 10 представлено сравнение корректирующей способности полярных подкодов и кодов с циклическим замыканием, используемых в системах мобильной связи 3–4 поколений. Декодирование последних осуществлялось по максимуму правдоподобия. Видно, что полярные подкоды обеспечивают значительный энергетический выигрыш. В связи с этим рандомизированные полярные подкоды были положены в основу метода кодирова-

ния данных для управляющего канала в стандарте мобильной связи 5 поколения[4].

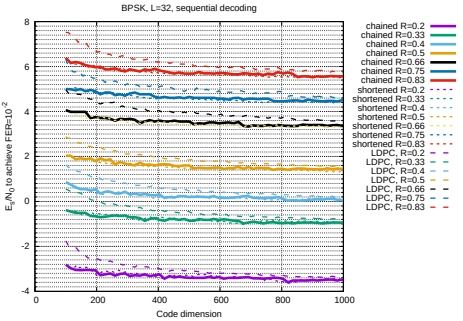


Рис. 9. Отношение сигнал/шум, требуемое для достижения вероятности ошибки 10^{-2}

Однако ключевым требованием к управляющему каналу является обеспечение вероятности ложного приема данных не более 10^{-5}. В связи с этим данные должны снабжаться перед кодированием контрольной суммой CRC, которая может использоваться также и для выбора пути из списка, формируемого списочным алгоритмом Тала-Варди. При этом CRC выполняет ту же функцию, что и ОДЗ типа A, т.е. обеспечивает исключение кодовых слов малого веса из исходного полярного кода путем выбора его псевдослучайного подкода. В связи с этим, а также малой длиной кодируемых блоков данных, общее число динамически замороженных символов ограничено для управляющих каналов величиной $q + t \leq 3$.

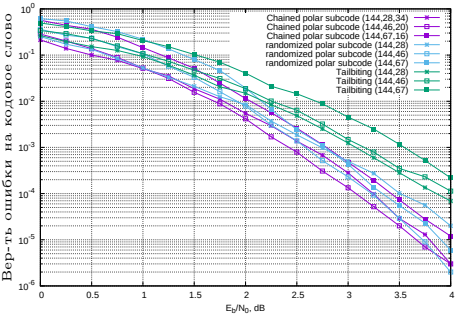


Рис. 10. Полярные подкоды и коды с циклическим замыканием в канале с АБГШ

Существенным недостатком полярных (под)кодов является значительная задержка декодирования при использовании алгоритма последовательного исключения и его аналогов. Для преодоления этой проблемы предложена конструкция звездных полярных подкодов, предполагающая использование нескольких поляризующих преобразований. Использование нескольких поляризующих преобразований позволяет выполнить декодирование звездных полярных подкодов с помощью нескольких параллельно работающих экземпляров списочного декодера Тала-Варди (ЭСДТВ), что и обеспечивает снижение задержки декодирования.

Определение 4. (n, k) *звездный полярный подкод — множество векторов* $c = (u^{(0)}A^{(0)}, \ldots, u^{(s-1)}A^{(s-1)})$, *где* s *— число лучей,* $A^{(i)} = B_{2,m_i}F_2^{\otimes m_i}$, $u^{(i)} \in \mathbb{F}_2^{2^{m_i}}$, *выполняются уравнения* $u^{(i)}(V^{(i)})^T = 0, 0 \leq i < s$, *и ограничения перекрестных проверок* $u^{(j)}(S^{(j,i)})^T = u^{(i)}(S^{(i,j)})^T, 0 \leq j < i$. *Здесь* $n = \sum_{i=0}^{s-1} 2^{m_i}$ *— длина кода,* $V^{(i)}$ *—* $\rho_i \times 2^{m_i}$ *матрицы локальных (лучевых) ограничений,* $S^{(i,j)}$ *—* $\mu_{ij} \times 2^{m_i}$ *матрицы перекрестных проверок, причем* $\mu_{ij} = \mu_{ji}$. *Вектор* $u^{(i)}$ *и подвектор* $u^{(i)}A^{(i)}$ *кодового слова называются, соответственно, i-ым лучом и блоком.*

С целью упрощения описания кодов, а также алгоритмов кодирования и деко-

[4] TS 38.212 v2.0.0(2017-12). Technical specification group radio access network; NR; multiplexing and channel coding (Release 15) / 3GPP: 2017, п. 5.3.1.2.

дирования, предлагается использовать симметричные ограничения перекрестных проверок, т.е. $S^{(0,j)} = S^{(0,1)}, 1 \le j < s$. Описан метод построения симметричных звездных полярных подкодов, основанный на кодах РБЧХ и конструкции X4. Декодирование таких кодов может быть выполнено с помощью s синхронно работающих ЭСДТВ для поляризующих преобразований $A^{(i)}, 0 \le i < s$. Синхронизация между ними осуществляется с помощью перекрестных проверок. При сортировке путей в каждом ЭСДТВ используются оценки снизу для корреляционной невязки кодового слова, которое может быть получено путем конкатенации векторов, найденных различными ЭСДТВ и удовлетворяющими перекрестным проверкам. Таким образом, декодирование кода длины $2^m s$ может быть выполнено за 2^m шагов списочного декодирования, а не за $\ge 2^m s$ шагов, как в случае обычных полярных (под)кодов.

На рис. 11 представлено сравнение корректирующей способности звездных полярных подкодов, полярных подкодов кодов РБЧХ, т.е. звездных кодов с $s = 1$ лучом, и полярного кода с CRC. Видно, что звездные коды с $s = 2, 3$ демонстрируют выигрыш по сравнению со случаем $s = 1$. Однако при $s = 4$ наблюдается значительное снижение корректирующей способности. При этом, однако, обеспечивается 4-кратное снижение задержки декодирования.

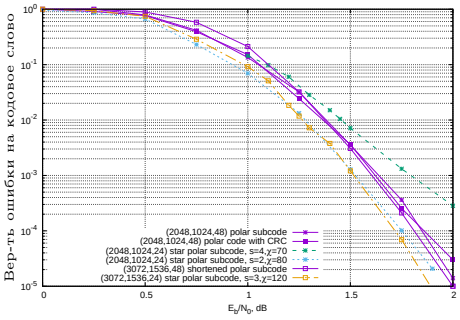


Рис. 11. Звездные полярные подкоды

Представлены упрощенные методы расчета надежности подканалов поляризующего преобразования Арикана в случае аддитивного гауссовского канала и канала с релеевскими замираниями. В первом случае предложено аппроксимировать распределения логарифмических отношений правдоподобия в подканалах поляризующего преобразования нормальным. Показано, что данный подход позволяет производить расчет "надежности" подканалов поляризующего преобразования без использования вычислительно сложного адаптивного метода квантования Тала-Варди. В случае неукороченных кодов ее предлагается характеризовать матожиданием логарифмических отношений правдоподобия (ЛОПП) на выходе подканалов поляризующего преобразования, которые удовлетворяют

$$\mathcal{L}_{\lambda}^{(2i)} = \Xi\left(\mathcal{L}_{\lambda-1}^{(i)}\right) = \phi^{-1}\left(1-\left(1-\phi\left(\mathcal{L}_{\lambda-1}^{(i)}\right)\right)^2\right) \tag{5}$$

$$\mathcal{L}_{\lambda}^{(2i+1)} = 2\mathcal{L}_{\lambda-1}^{(i)}, \tag{6}$$

$0 \le i < 2^{\lambda-1}$, где $\mathbf{M}\left[L_0^{(0)}\right] = \mathcal{L}_0^{(0)} = \frac{2}{\sigma^2}$, $\phi(x) = \begin{cases} 1 - \frac{1}{\sqrt{4\pi x}} \int_{-\infty}^{\infty} \tanh\frac{u}{2} e^{-\frac{(u-x)^2}{4x}} du, & x > 0 \\ 1, & x = 0, \end{cases}$

и

$$\Xi(x) \approx \begin{cases} 0.98611x - 2.31515 & x > 12 \\ x(9.0047 \cdot 10^{-3}x + 0.76943) - 0.95068, & 3.5 < x \le 12 \\ x(0.062883x + 0.36784) - 0.16267 & 1 < x \le 3.5 \\ x(0.22024x + 0.06448) & \text{иначе,} \end{cases} \tag{7}$$

Вероятность ошибки в подканалах $\mathcal{W}_m^{(i)}$ поляризующего преобразования Арикана может быть найдена как $P_i \approx Q\left(\sqrt{\mathcal{L}_m^{(i)}/2}\right), 0 \le i \le 2^m - 1$. Для построения полярных (под)кодов достаточно лишь вычислить и отсортировать значения $\mathcal{L}_m^{(i)}$ Таким образом, предлагаемый подход сводится к вычислению кусочно-квадратичных функций и имеет ту же сложность, что и метод Арикана расчета параметров Бхаттачарьи в случае двоичного стирающего канала. Показано, что предложенная кусочно-квадратичная аппроксимация обеспечивает достаточно высокую точность при $m \le 16$. При этом, в отличие от аппроксимации Ха-Кима-МакЛафлина, вычисление (7) не использует трансцендентных функций, т.е. предлагаемый подход намного проще в реализации.

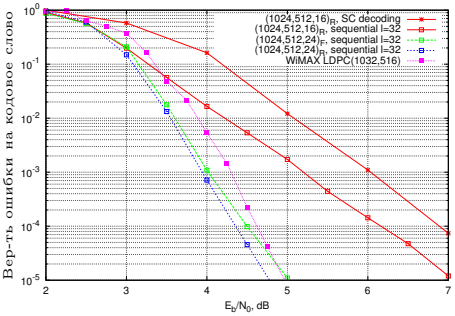


Рис. 12. Корректирующая способность полярных (под)кодов в релеевском канале

В случае канала с независимыми релеевскими замираниями предложено представить подканалы поляризующего преобразования Арикана как обобщенные релеевские каналы с передаточными коэффициентами, распределенными по закону χ, и представлены методы расчета параметров этого распределения. На рис. 12 представлены результаты статистического моделирования для полярных подкодов кодов РБЧХ в канале с независимыми замираниями Релея. Коды были построены с помощью описанных выше методов гауссовской аппроксимации (F) и χ-аппроксимации (R). Видно, что применение последней приводит к кодам с лучшей корректирующей способностью. Выигрыш особенно велик в случае классических полярных кодов (соответствуют $d = 16$). В то же время полярный подкод кода РБЧХ, построенный для гауссовского канала, демонстрируют незначительный проигрыш по корректирующей способности по сравнению с аналогичным кодом, построенным для релеевского канала.

Результаты третьей главы опубликованы в работах [11, 23, 20, 21, 25, 7, 19].

В четвертой главе представлены алгоритмы декодирования многочленных кодов, основанные на их представлении в виде системы ограничений динамического замораживания. Предложено обобщение последовательного (стекового) алгоритма декодирования на случай полярных кодов. Предлагаемый алгоритм работает следующим образом:

1. Поместить в приоритетную очередь[5] (ПО) путь нулевой длины с весом 0. Пусть $t_0^{n-1} = 0$. В дальнейшем вектор t_0^{n-1} используется для подсчета числа проходов декодера через различные фазы.

2. Извлечь из ПО вектор (путь) $v_0^{\phi-1}$ с наибольшим весом. Пусть $t_\phi \leftarrow t_\phi + 1$.

[5] В литературе по последовательному декодированию ПО часто называется стеком. Однако реализация предлагаемого алгоритма основывается на структурах данных Тала-Варди, которые используют “настоящие” стеки. В связи с этим, далее будет использоваться стандартная терминология компьютерных наук.

3. Если $\phi = n$, возвратить кодовое слово $v_0^{n-1}A_m$ и завершить работу.

4. Если число допустимых (с учетом ОДЗ) продолжений вектора $v_0^{\phi-1}$ превышает количество свободных ячеек в ПО, удалить из нее элемент с наименьшим весом.

5. Вычислить веса $M(v_0^{\phi}, y_0^{n-1})$ допустимых потомков v_0^{ϕ} извлеченного вектора и поместить их в ПО.

6. Если $t_\phi \geq L$, удалить из ПО все векторы $v_0^{j-1}, j \leq \phi$.

7. Перейти к шагу 2.

Под итерацией понимается один проход этого алгоритма по шагам 2–7.

Предлагаемая весовая функция обобщает метрику Фано, используемую при декодировании сверточных кодов, и имеет вид

$$M(v_0^{\phi-1}, y_0^{n-1}) = \underbrace{\sum_{i=0}^{\phi-1} \tau(S_m^{(i)}(v_0^{i-1}|y_0^{n-1}), v_i)}_{R(v_0^{\phi-1}|y_0^{n-1})} - \underbrace{\mathbf{M}_{Y_0^{n-1}}\left[\sum_{i=0}^{\phi-1} \tau(S_m^{(i)}(u_0^{i-1}|Y_0^{n-1}), u_i)\right]}_{\Psi(\phi)}, \quad (8)$$

где

$$\tau(S, v) = \begin{cases} 0, & \operatorname{sgn}(S) = (-1)^v \\ -|S|, & \text{иначе} — \end{cases}$$

штрафная функция, Y_0^{n-1} — случайные величины, соответствующие выходным символам симметричного канала без памяти $W_{Y|C}$, C — случайная величина, соответствующая его входным символам, и $S_m^{(i)}(v_0^{i-1}, y_0^{n-1})$ — модифицированные логарифмические отношения правдоподобия (ЛОПП)

$$S_\lambda^{(2i)}(v_0^{2^{i-1}}|y_0^{2^{\lambda}-1}) = Q(a, b) = \operatorname{sgn}(a)\operatorname{sgn}(b)\min(|a|, |b|), \quad (9)$$

$$S_\lambda^{(2i+1)}(v_0^{2^i}|y_0^{2^{\lambda}-1}) = P(v_{2i}, a, b) = (-1)^{v_{2i}}a + b. \quad (10)$$

Вычитаемое в (8), называемое эвристической функцией, представляет собой математическое ожидание первого слагаемого в предположении, что $v_0^{\phi-1} = u_0^{\phi-1}$, т.е. в случае, если декодер следует по пути, соответствующему истинному вектору u_0^{n-1}, использованному передатчиком. Оно может быть вычислено как

$$\Psi(\phi) = -\sum_{i=0}^{\phi-1} \int_{-\infty}^{0} F_m^{(i)}(x)dx,$$

где

$$F_\lambda^{(2i)}(x) = \begin{cases} 2F_{\lambda-1}^{(i)}(x)(1 - F_{\lambda-1}^{(i)}(-x)), & x < 0 \\ 2F_{\lambda-1}^{(i)}(x) - (F_{\lambda-1}^{(i)}(-x))^2 - (F_{\lambda-1}^{(i)}(x))^2, & x > 0 \end{cases} \quad (11)$$

$$F_\lambda^{(2i+1)}(x) = \int_{-\infty}^{\infty} F_{\lambda-1}^{(i)}(x - y)dF_{\lambda-1}^{(i)}(y), \quad (12)$$

и $F_0^{(0)}(x)$ — функция распределения ЛОПП на выходе канала при условии передачи по нему нулевых символов.

Дальнейшее снижение сложности декодирования может быть достигнуто за счет рекурсивного представления полярного (под)кода как обобщенного каскадного кода с перекрестными связями (или обобщенного разложения Плоткина). Рекурсивное разбиение кода должно быть остановлено при получении внешних кодов, допускающих простое списочное декодирование. Примерами таких кодов являются код с повторениями, каскадные коды с внешним кодом Рида-Маллера порядка 1 и внутренним кодом с повторениями, коды со скоростью 1, коды с проверкой на четность, расширенный код Хемминга (16,11,4). Доказана

Теорема 4. *Пусть i', i — номера двух смежных блоков в дереве рекурсивного обобщенного разложения Плоткина, т.е. $\phi_i = \phi_{i'} + n_i$ и $n_i = 2^{m_i}$. Тогда*

$$R(u_0^{\phi_i}|y_0^{n-1}) = R(u_0^{\phi_{i'}}|y_0^{n-1}) - E(u_{\phi_{i'}+1}^{\phi_i} A_{m_i}, \mathbf{S}),$$

где $\mathbf{S}$ *— вектор значений* $S_{m-m_i}^{(\phi_i/2^{m_i})}$*, задаваемых* (9)–(10) *и* $E(c_0^{n-1}, S_0^{n-1}) = -\sum_{i=0}^{n-1} \tau(S_i, c_i)$ *— корреляционная невязка вектора* $c_0^{n-1} \in \mathbb{F}_2^n$

Декодирование может быть выполнено следующим образом. Пусть $\mathcal{L} = \{\phi_i\}$ — множество границ выявленных блоков. На каждой итерации из приоритетной очереди извлечем путь $v_0^{\phi_i}, \phi_i \in \mathcal{L}$, с наибольшим весом. Для него вычислим вектор ЛОПП $S_{m-m_i}^{(\phi_i/2^{m_i})}$ и подготовимся[6] к декодированию кода $\mathcal{C}_i$. Далее найдем наиболее вероятное кодовое слово $v_{\phi_i+1}^{\phi_i+n_i} A_{m_i}$, соответствующее вычисленным ЛОПП, его корреляционную невязку e_0 и корреляционную невязку e_1 следующего кодового слова. Поместим в ПО пути $v_0^{\phi_i+n_i}$ и $v_0^{\phi_i}$. В качестве веса первого будем использовать значение $R(v_0^{\phi_i}|y_0^{n-1}) - e_0 - \Psi(\phi_i + n_i)$, а в качестве веса второго — $R(v_0^{\phi_i}|y_0^{n-1}) - e_1 - \Psi(\phi_i + n_i)$. Кроме того, сопоставим пути $v_0^{\phi_i}$ переменную состояния декодера $\mathcal{C}_i$. Если при последующих итерациях путь $v_0^{\phi_i}$ будет извлечен из ПО в j-ый раз, $1 \le j \le L$, воспользуемся сохраненным состоянием декодера $\mathcal{C}_i$ для нахождения j-го кодового слова $\widetilde{v}_{\phi_i+1}^{\phi_i+n_i} A_{m_i}$, его корреляционной невязки e_j и корреляционной невязки $(j+1)$-го слова e_{j+1}. Поместим в приоритетную очередь пути $v_0^{\phi_i}.\widetilde{v}_{\phi_i+1}^{\phi_i+n_i}$ с весом $R(v_0^{\phi_i}|y_0^{n-1}) - e_j - \Psi(\phi_i + n_i)$ и $v_0^{\phi_i}$ с весом $R(v_0^{\phi_i}|y_0^{n-1}) - e_{j+1} - \Psi(\phi_i + n_i)$. Будем выполнять описанные действия до получения пути длины n, который и задает результат декодирования.

На рис. 13 представлена зависимость вероятности ошибки и среднего числа итераций, выполняемых последовательным алгоритмом декодирования, от отношения сигнал шум для предложенной весовой функции M, весовой функции Нию-Ченя $M_1(v_0^{\phi-1}, y_0^{n-1}) = \mathcal{W}_m^{(\phi-1)}\{v_0^{\phi-1}|y_0^{n-1}\}$, и ее аппроксимации минимум-сумма $M_2(v_0^{\phi-1}, y_0^{n-1}) = R(v_0^{\phi-1}, y_0^{n-1})$. Представлены результаты для полярных кодов с CRC-16 (polar-CRC) и рандомизированных полярных подкодов (ps), описанных выше. Напомним, что предложенная весовая функция может быть представлена как $M_3(v_0^{\phi-1}, y_0^{n-1}) = M_2(v_0^{\phi-1}, y_0^{n-1}) - \Psi(\phi)$. Следует также отметить, что при достаточно большом Θ алгоритм Нию-Ченя обеспечивает ту же корректирующую способность, что и декодер Тала-Варди.

[6] Содержание подготовки зависит от кода $\mathcal{C}_i$. Она включает в себя все действия, которые необходимы для последующего эффективного нахождения кодовых слов в порядке увеличения их корреляционных невязок.

Можно заметить, что использование весовой функции M_2 приводит к незначительному увеличению вероятности ошибки и весьма существенному снижению среднего числа итераций, выполняемых декодером. Еще более значительное снижение сложности достигается при использовании предложенной весовой функции M. Предложенная весовая функция дает возможность корректно сравнивать пути $v_0^{\phi-1}$ различных длин ϕ. В результате достигается многократное снижение среднего числа итераций. Заметим, что корректирующая способность декодера, использующего весовую функцию M, остается примерно такой же, как и в случае весовой функции M_2. Как было показано на рис. 6, предложенный последовательный алгоритм декодирования в сочетании с конструкцией рандомизированных полярных подкодов одновременно обеспечивает меньшую сложность и лучшую корректирующую способность по сравнению с LDPC-кодами.

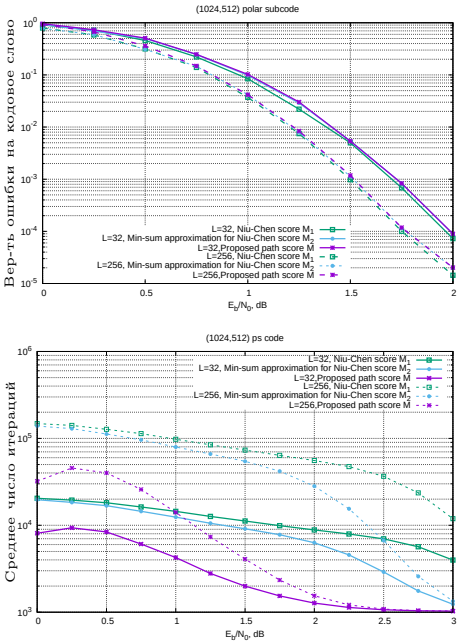


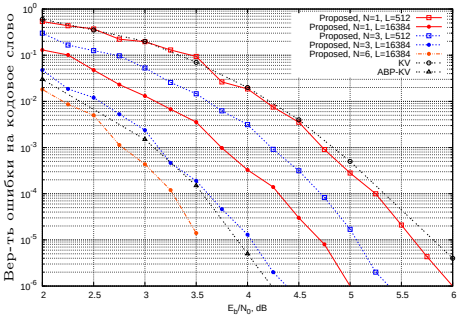
Рис. 13. Влияние весовой функции на корректирующую способность и сложность последовательного декодера

Представлено обобщение алгоритма последовательного исключения на случай цепных полярных подкодов. Оно основывается на некотором упорядочении входных символов используемых поляризующих преобразований, называемом расписанием. Расписание должно учитывать зависимости между символами, задаваемыми как ОДЗ, так и процедурой расчета ЛОПП в подканалах поляризующего преобразования. Это обобщение допускает естественное расширение на случай списочного и последовательного декодирования. Показано, что корректирующая способность списочного/последовательного алгоритмов существенно зависит от используемого расписания. Предложен жадный алгоритм построения расписания, который помещает замороженные символы различных поляризующих преобразований на наиболее ранние фазы декодирования с учетом зависимостей между символами, задаваемыми ОДЗ.

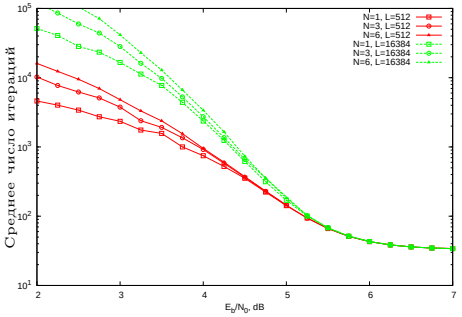
Показано, что применение этого подхода к расширенному коду Голея с использованием его представления в виде (1), полученного в главе 2, позволяет выполнить его декодирование по максимуму правдоподобия со средней сложностью, близкой к сложности алгоритма Варди, наилучшего известного метода декодирования этого кода.

Введенное в главе 2 представление кодов Рида-Соломона в виде системы ОДЗ позволяет использовать для их декодирования списочный или вышеописанный последовательный алгоритм. При этом в случае передачи двоич-

ного образа кода над $\mathbb{F}_{2^m}$ по каналу без памяти с двоичным входом декодер может быть реализован с помощью m устройств, параллельно вычисляющих логарифмические отношения правдоподобия $S_m^{(i)}$ для отдельных битов входных символов $u_i \in \mathbb{F}_{2^m}$ поляризующего преобразования, с единым модулем расчета значений динамически замороженных символов. Из теоремы 3 вытекает, что множество $\mathcal{F}$ номеров замороженных символов (но не коэффициенты ОДЗ) не зависит от используемого базиса $\beta_0, \ldots, \beta_{m-1}$ конечного поля. Различные базисы задают различные перестановки декодируемого зашумленного вектора. При этом успешность декодирования с помощью предложенного алгоритма конкретного зашумленного вектора зависит от используемого базиса. Таким образом, корректирующая способность предложенного алгоритма может быть повышена путем многократного запуска с перестановками зашумленного вектора, задаваемыми различными базисами конечного поля.



($а$) Вероятность ошибки



($б$) Среднее число итераций последовательного алгоритма

Рис. 14. Декодирование двоичного образа кода Рида-Соломона $(31, 15, 16)$

На рис. 14, $а$ представлены результаты статистического моделирования для случая передачи двоичного образа кода $(31, 15, 16)$ над $\mathbb{F}_{2^5}$ по аддитивному гауссовскому каналу. Приведены результаты для предложенного метода последовательного декодирования с различным размером списка L и числом используемых базисов N, метода Кёттера-Варди (KV) и адаптивного алгоритма распространения доверия в сочетании с мягким алгебраическим декодированием(ABP-KV). Таким образом, предложенный метод при достаточно большом размере списка может обеспечить большую корректирующую способность по сравнению с адаптивным алгоритмом распространения доверия в сочетании с мягким алгебраическим декодированием, а также методом Кёттера-Варди. Как видно из рис. 14, $б$, с увеличением отношения сигнал/шум средняя сложность предложенного алгоритма быстро уменьшается и стремится к сложности классического алгоритма последовательного исключения.

Результаты главы опубликованы в работах [17, 16, 9, 8].

В пятой главе предложен быстрый алгоритм интерполяции в алгоритмах Гурусвами-Судана и Ву списочного декодирования (n, k) кода Рида-Соломона. Наиболее сложным этапом алгоритма Гурусвами-Судана является построение многочлена $Q(x, y)$ с наименьшей $(1, k-1)$-взвешенной степенью, имеющего некоторые корни

(x_i, y_i) кратности r, где x_i — различные элементы конечного поля $\mathbb{F}$. Для краткости будем обозначать это условие как $Q(x_i, y_i) = 0^r, 0 \le i < n$. Такой многочлен может быть найден в базисе Грёбнера соответствующего идеала I_r относительно $(1, k-1)$-взвешенного лексикографического упорядочения. В работе доказана

Лемма 1. *Пусть* $I_r = \{Q(x,y) \in \mathbb{F}[x,y] | Q(x_i, y_i) = 0^r, 0 \le i < n\}$. *Тогда* $I_{r_1+r_2} = I_{r_1} \cdot I_{r_2}$.

Из этой леммы вытекает, что $I_r = \underbrace{I_1 \cdot I_1 \cdots I_1}_{r\text{раз}} = I_1^r$, где $I_1 = \langle \phi(x), y - T(x) \rangle$, $T(x_i) = y_i, 0 \le i < n$, и $\phi(x) = \prod_{i=0}^{n-1}(x - x_i)$. Очевидно, что для избежания повторяющихся вычислений можно воспользоваться двоичным методом возведения в степень, т.е. вычислить

$$I_r = I_1^r = (\ldots((I_1^2 \cdot I_1^{r_{m-1}})^2 \cdot I_1^{r_{m-2}})^2 \cdot I_1^{r_{m-3}} \cdots I_1^{r_1})^2 \cdot I_1^{r_0}$$

где $r = \sum_{j=0}^{m} r_j 2^j, r_m = 1$, $I^2 = I \cdot I$, $I^0 = \mathbb{F}[x,y]$, и $I \cdot \mathbb{F}[x,y] = I$. Таким образом, возникает задача быстрого нахождения базиса Грёбнера произведения $I_{a+b} = I_a \cdot I_b$ идеалов $I_a = \langle P_0(x,y), \ldots, P_u(x,y) \rangle$ и $I_b = \langle S_0(x,y), \ldots, S_v(x,y) \rangle$. Стандартный подход состоит в вычислении

$$I_a \cdot I_b = \langle P_i(x,y) S_j(x,y), 0 \le i \le u, 0 \le j \le v \rangle, \tag{13}$$

т.е. попарном перемножении всех элементов базисов рассматриваемых идеалов с последующим нахождением базиса Грёбнера. Это требует $(u+1)(v+1)$ перемножений многочленов от двух переменных, а базис $I' \cdot I''$, получаемый таким образом, обладает крайне высокой избыточностью. Отметим, что рассматриваемые идеалы являются нульмерными.

Предлагаемый подход к построению базиса Грёбнера произведения нульмерных идеалов состоит в нахождении просто вычислимого базиса некоторого подыдеала искомого идеала-произведения с последующей его коррекцией. При этом удобно рассматривать множество элементов искомого идеала с ограниченной степенью относительно переменной y, которое образует модуль. Доказана

Лемма 2. *Пусть даны такие многочлены* $P_j(x,y) : P_j(x_i, y_i) = 0^s, 0 \le i < n, 0 \le j \le m$, *что* $\mathrm{LT}\, P_j(x,y) = a_j x^{p_j} y^j$, $\mathrm{wdeg}_{(0,1)} P_j(x,y) \le m$, $p_m = 0$, *u*

$$\Delta\left((P_0(x,y), \ldots, P_m(x,y))\right) = \sum_{j=0}^{m} p_j = \frac{ns(s+1)}{2}. \tag{14}$$

Тогда $I_s = \langle P_j(x,y), 0 \le j \le m \rangle$, *и многочлены* $P_j(x,y)$ *образуют базис Грёбнера* I_s.

Предлагаемый подход состоит в построении последовательности базисов

$$\mathcal{Q}'_{j+1} = Reduce\left(\mathcal{Q}'_j, \left(\sum_{i=0}^{u} \alpha_{ij} P_i(x,y)\right)\left(\sum_{i=0}^{v} \beta_{ij} S_i(x,y)\right)\right),$$

где $j \ge u + v$, α_{ij}, β_{ij} являются случайными величинами, равномерно распределенными в $\mathbb{F}$, и $Reduce(\mathcal{Q}'_j, T(x,y))$ — алгоритм Малдерса-Сторжохана, используемый для построения базиса Грёбнера модуля

$$M = \left\{ \sum_i a_i(x) Q'_{ji}(x,y) + b(x) T(x,y) | a_i(x), b(x) \in \mathbb{F}[x] \right\}.$$

Эта последовательность строится до тех пор, пока не выполнится условие (14), т.е. $\Delta(\mathcal{Q}'_j) = n\frac{(a+b)(a+b+1)}{2}$. Предлагается также построить начальный базис $\mathcal{Q}'_{u+v} = (Q_0(x,y),\ldots,Q_{u+v}(x,y))$ как $Q_i(x,y) = P_{i-j}(x,y)S_j(x,y)$, причем для каждого i выбирается такое j, что $\mathrm{LT}\,Q_i(x,y) = a_i x^{q_i} y^i$, и величины $q_i, 0 \le i \le u+v$, выбираются минимально возможными. Будем называть описанный рандомизированный метод умножения идеалов алгоритмом $Merge$. В работе доказана

Теорема 5. *Пусть $\mathcal{P} = (P_0(x,y),\ldots,P_u(x,y))$ и $\mathcal{S} = (S_0(x,y),\ldots,S_v(x,y))$ — базисы Грёбнера идеалов I_a и I_b. Результатом $Merge$ является базис Грёбнера I_{a+b}.*

Таким образом, двоичный интерполяционный алгоритм в сочетании с предложенным рандомизированным методом умножения идеалов позволяют построить базис Грёбнера идеала I_r, который содержит искомый многочлен $Q(x,y)$. В работе с использованием аппарата собственных чисел матричных многочленов показано, что предложенный подход имеет сложность $O(nr^3(a\log(r\sqrt{n/k})\log(nr) + b(n - \sqrt{nk})))$ для некоторых величин a, b, в то время как классический итеративный интерполяционный алгоритм имеет сложность $O(n^2r^5)$. В работе также представлено описание модификации этого метода, позволяющей использовать его в сочетании с преобразованием перекодирования, которое позволяет существенно уменьшить степени рассматриваемых многочленов.

Предложена новая интерпретация алгоритма By списочного декодирования кодов Рида-Соломона, которая выражена в виде следующей теоремы:

Теорема 6. *Пусть $\overline{y} = (y_1,\ldots,y_n)$ — некоторый вектор из $\mathbb{F}^n$. Рассмотрим многочлены $Q'(x,y) = q_{00}(x) + yq_{10}(x), Q''(x,y) = q_{01}(x) + yq_{11}(x)$, образующие базис Грёбнера модуля $\mathcal{M} = [\phi(x), y - T(x)]$ относительно $(1, k-1)$-взвешенного лексикографического упорядочения, где $T(x) : T(x_i) = y_i, 1 \le i \le n, \phi(x) = \prod_{i=1}^{n}(x - x_i)$. Если $t < n - \sqrt{n(k-1)}$ и параметры r, ρ удовлетворяют*

$$r > \frac{\left(n - t + \sqrt{n^2 - 2tn + wn}\right)w}{2(t^2 - wn)}, \tag{15}$$

$$\rho > \frac{n}{t} - 1 \tag{16}$$

при $w = 0$ и

$$\rho_l = \frac{2rt - w - \sqrt{D}}{2w} < \rho < \frac{2rt - w + \sqrt{D}}{2w} = \rho_h \tag{17}$$

при $w > 0$, где $D = (w + 2rt)^2 - 4wnr(r+1) > 0$ и $w = 2t + (k-1) - n$, то все кодовые слова $\overline{c} = (c_1,\ldots,c_n)$ $(n, k, n-k+1)$ кода РС над $\mathbb{F}$, удовлетворяющие $d_H(\overline{c},\overline{y}) = t' \le t$, могут быть найдены из многочленов $\sigma(x) = a(x)q_{10}(x) + b(x)q_{11}(x)$, причем $c_i \ne y_i \Leftrightarrow \sigma(x_i) = 0$, $S(x, a(x), b(x)) = 0$. Здесь $S(x,y,z) = \sum_{i=0}^{\rho} s_i(x)y^i z^{\rho-i}$ является таким многочленом, что для всех $\alpha \in \mathbb{F}$ точки $(x_i, \alpha q_{11}(x_i), -\alpha q_{10}(x_i)), 1 \le i \le n$, являются его корнями кратности r, и $\mathrm{wdeg}_{(1,w_1,w_2)} S(x,y,z) < rt$, где $w_1 = t + k - 1 - \deg q_{00}(x), w_2 = t - \deg q_{11}(x)$.

На основе этой теоремы в работе получены уточненные оценки кратности корней для алгоритма By

$$r > \left\lceil \frac{(1 - \tau + \sqrt{R})(2\tau + R - 1)}{2(\tau^2 - 2\tau - R + 1)} \right\rceil$$

и максимального размера списка

$$\rho_l = \frac{r\tau - \sqrt{(\tau(r+1)+\frac{R-1}{2})^2 - (2\tau+R-1)r(r+1)}}{2\tau+R-1} - \frac{1}{2},$$

где $\tau = \frac{t}{n}$ — нормализованный радиус декодирования, $R = \frac{k-1}{n}$ и $t < n - \sqrt{n(k-1)}$ — радиус декодирования. Применение этих оценок позволяет упростить декодирование по сравнению со случаем использования оценок, приведенных в работе Ву.

Представлено обобщение вышеописанного быстрого интерполяционного алгоритма на случай метода Ву списочного декодирования кодов Рида-Соломона. Алгоритм Ву предполагает использование бесконечно удаленных корней, что не позволяет воспользоваться аппаратом идеалов коммутативных колец. Для преодоления этой трудности введены частично однородные многочлены вида $S(x,y,z) = \sum_{j=0}^{\rho} s_j(x) z^{\rho-j} y^j$. При этом искомый интерполяционный многочлен может быть найден в базисе Грёбнера модуля $\mathbf{M}_{\rho,r} = \left\{S(x,y,z) | \operatorname{wdeg}_{0,1,1} S(x,y,z) = \rho, S(x_i,y_i,z_i) = 0^r\right\}$. Предлагаемый подход включает алгоритмы построения базиса Грёбнера модуля $\mathbf{M}_{\rho_1+\rho_2,r_1+r_2}$ из базисов $\mathbf{M}_{\rho_1,r_1}$ и $\mathbf{M}_{\rho_2,r_2}$ и $\mathbf{M}_{\rho+1,r}$ из $\mathbf{M}_{\rho,r}$. Оба алгоритма основаны на вычислении случайных линейных комбинаций многочленов и применении алгоритма Малдерса-Сторжохана. Сложность предложенного обобщения составляет $O(n^2 r^3)$. При программной реализации применение данного подхода обеспечивает повышение скорости декодирования в 5 и более раз по сравнению с итеративным интерполяционным алгоритмом в случае алгоритма Ву и в 12–157 раз в случае алгоритма Гурусвами-Судана.

Результаты главы опубликованы в работах [5, 6, 13, 4].

В шестой главе рассматривается задача быстрого систематического кодирования кодов Рида-Соломона и полярных кодов с ядром Рида-Соломона. Предлагаемый подход основан на циклотомическом алгоритме быстрого преобразования Фурье. Сгруппируем элементы вектора компонентов ДПФ по циклотомическим классам. Тогда оно может быть представлено как

$$F_{k_i 2^s} = \sum_{j=0}^{n-1} f_j \alpha^{j k_i 2^s}, 0 \le i < l, \tag{18}$$

где k_i — представители различных циклотомических классов над $\mathbb{F}_2$ по модулю n, $\alpha^n = 1$. Известно, что элементы $\alpha^{k_i 2^s}$ образуют класс сопряженности над $\mathbb{F}_{2^m}$, и их минимальный многочлен равен $\mu_i(x) = \prod_{s=0}^{m_i-1}(x - \alpha^{k_i 2^s})$. Следовательно, (18) может быть переписано как $F_{k_i 2^s} = f(\alpha^{k_i 2^s}) = r_i(\alpha^{k_i 2^s})$, где $r_i(x) \equiv f(x) \bmod \mu_i(x)$. После нахождения $r_i(x)$, значения $F_{k_i 2^s}$ могут быть найдены как

$$F_{k_i 2^s} = r_i(\alpha^{k_i 2^s}) = \sum_{t=0}^{m_i-1} \gamma_i^{2^{s+t}} \sum_{j=0}^{n-1} a_{itj} r_{ij}, \tag{19}$$

где γ_i — образующий элемент нормального базиса $\mathbb{F}_{2^{m_i}}$ Таким образом, ДПФ может быть вычислено как $F = LA'A''f$, где L — блочно-диагональная матрица, блоки которой являются $m_i \times m_i$ циркулянтами, образованными γ_i, вычисление $A''f$ эквивалентно нахождению остатков от деления $f(x)$ на $\mu_i(x)$ и A' — блочно-диагональная матрица, состоящая из блоков $A'_i = (a_{itj}), 0 \le t,j < m_i$. Умножение на L сводится к вычислению циклических сверток (умножению многочленов). Для вычисления

$A''f$ может использоваться быстрый рекурсивный алгоритм одновременного приведения по модулю, используемый в классической процедуре одновременного вычисления значений многочлена в различных точках, со сложностью $2D(n)\lfloor \log l \rfloor$ операций сложения, где $D(n)$ — сложность используемого алгоритма деления многочленов с остатком. Полагая, что $D(n) = 2M(n) + n$, где $M(n) = O(n \log^{\gamma} n), \gamma \le 2$ — сложность перемножения многочленов степени n, получим, что сложность предлагаемого обратного циклотомического алгоритма равна $O(n \log^{\gamma+1} n)$. Предложенный алгоритм может быть использован для вычисления неполного ДПФ, возникающего в задаче вычисления синдрома при декодировании кодов Рида-Соломона.

Предложен быстрый алгоритм систематического кодирования кодов Рида-Соломона над $\mathbb{F}_{2^m}$, основанный на вышеописанном циклотомическом алгоритме БПФ, а также классическом алгоритме Форни вычисления значений ошибок и стираний при декодировании кодов БЧХ. Пусть проверочные и информационные символы располагаются в позициях кодового слова, задаваемых, соответственно, множествами $U = \{u_0, \ldots, u_{n-k-1}\}$ и $V = \{v_0, \ldots, v_{k-1}\}$, $V \cap U = \varnothing, U \cup V \subset \{0, \ldots, 2^m - 2\}$.

Предлагаемый алгоритм быстрого кодирования укороченного (n, k) кода Рида-Соломона над $\mathbb{F}_q, n < N = q - 1$, включает следующие шаги:

1. Подготовка: построить многочлен локаторов проверочных символов $\Lambda^{(c)}(x) = \sum_{i=0}^{n-k} \Lambda_i^{(c)} x^i = \prod_{i=0}^{n-k-1}(1 - \alpha^{u_i} x)$. Вычислить коэффициенты Форни $\phi_i^{(c)} = \frac{\alpha^{(1-b)u_i}}{\sum_{s=0}^{\lfloor (n-k-1)/2 \rfloor} \Lambda_{2s+1}^{(c)} \alpha^{-2u_i s}}$.

2. Вычислить синдром вектора информационных символов: $S_i = \sum_{j=0}^{k-1} m_j \alpha^{v_j(b+i)}, 0 \le i < n - k$.

3. Вычислить многочлен значений проверочных символов $\Gamma^{(c)}(x) \equiv S(x)\Lambda^{(c)}(x) \bmod x^{n-k}$.

4. Вычислить проверочные символы c_{u_i} как

$$c_{u_i} = \phi_i^{(c)} \Gamma^{(c)}(\alpha^{-u_i}), 0 \le i < n - k. \tag{20}$$

Для вычисления синдрома информационных символов может быть использован вышеописанный циклотомический алгоритм БПФ. Для упрощения расчета проверочных символов множество U может быть построено как объединение нескольких циклотомических классов[7]. В этом случае (20) также может быть вычислено с помощью обратного циклотомического алгоритма БПФ, а $\Lambda^{(c)}(x)$ оказывается многочленом с двоичными коэффициентами.

Заметим, что вычисление $\Gamma^{(c)}(x)$ эквивалентно умножению $(S_0, \ldots, S_{n-k-1})$ на двоичную матрицу, задаваемую коэффициентами $\Lambda^{(c)}(x)$. Первый этап обратного циклотомического алгоритма БПФ также состоит в умножении на двоичную матрицу. Эти операции могут быть объединены, и построена единая оптимизированная процедура вычисления значений $\Gamma^{(c)}(x)$ по $(S_0, \ldots, S_{n-k-1})$. В случае $(n-k)|(2^m-1)$ множество U может быть построено так, что $\Lambda^{(c)}(x) = x^{n-k} - 1$, т.е. $\Gamma^{(c)}(x) = -S(x)$, а (20) сводится к полному $(n-k)$-точечному ДПФ.

[7] Такое представление возможно для любых $n - k$ при m, равном степени 2.

Таблица 1. Производительность библиотеки Jerasure и программной реализации предложенного метода систематического кодирования кодов Рида-Соломона, ГБ/с

k	$r = n - k$	Jerasure 2.0	Предложенный метод
9	3	4.7	10.3
16	3	4.9	14.1
30	5	2.8	10.0
10	6	2.3	3.3
10	8	1.7	2.2
20	11	1.2	2.5

Сложность этапа вычисления синдрома в предлагаемом методе систематического кодирования составляет $O((n-k)\log^{\gamma}\log n), \gamma \le 2$, умножений. При использовании асимптотически быстрого варианта обратного циклотомического алгоритма БПФ требуемое число сложений равно $O(n\log^{\gamma+1} n)$. Число умножений и сложений, выполняемых при вычислении значений проверочных символов, равно соответственно $O((n-k)\log^{\gamma}\log n)$ и $O((n-k)\log^{\gamma+1}(n-k))$.

В таблице 1 представлено сравнение производительности программной реализации предложенного метода и библиотеки Jerasure, широко используемой в программно определяемых системах хранения данных. Кодирование данных осуществлялось блоками размером λk байт, где $\lambda = 4096$. Видно, что использование предложенного метода систематического кодирования обеспечивает повышение производительности до 3.6 раз, причем наиболее значительный выигрыш достигается при больших k.

В работе представлен метод быстрого систематического кодирования полярных кодов с ядром Рида-Соломона F_l, основанный на вышеописанном методе систематического кодирования кодов Рида-Соломона, представлении полярного кода как обобщенного каскадного и обобщающий алгоритм Арикана систематического кодирования полярных кодов с ядром F_2. Предлагаемый подход состоит в том, что проверочные символы объявляются стертыми, после чего рекурсивно задействуется предложенный алгоритм систематического кодирования для компонентных кодов Рида-Соломона, возникающих в представлении рассматриваемого полярного кода как обобщенного каскадного.

Представлен упрощенный подход к реализации процедуры Ченя поиска корней многочленов над полями характеристики 2, основанный на представлении многочлена в виде суммы некоторых многочлнов кратных аффинным, и упорядочении элементов поля в соответствии с кодом Грея.

Результаты шестой главы опубликованы в [2, 3, 1, 10].

Заключение и основные результаты работы

В диссертационной работе решена научная проблема построения кодов, допускающих простое декодирование с хорошей корректирующей способностью, имеющая важное теоретическое и прикладное значение. Получены следующие основные результаты.

1. Разработана математическая модель линейных блоковых кодов, основанная на

системе линейных ограничений динамического замораживания на входные символы поляризующего преобразования. Охарактеризованы такие системы ограничений для расширенных примитивных кодов БЧХ и Рида-Соломона в узком смысле, а также расширенного кода Голея. Показано, что применение предложенного подхода позволяет выполнить декодирование коротких кодов из указанных семейств со сложностью меньшей (до 40 раз по сравнению с алгоритмом BEAST на рассмотренных примерах) или сопоставимой с другими известными алгоритмами декодирования.

2. На основе предложенной математической модели разработан метод построения полярных подкодов, который позволяет получить коды произвольной длины, допускающие декодирование с помощью списочного или последовательного алгоритмов последовательного исключения. Было показано, что предложенные коды обеспечивают лучшую корректирующую способность (выигрыш до 1 дБ на рассмотренных примерах) по сравнению с известными турбо- и LDPC кодами и кодами с циклическим замыканием, а при использовании последовательного алгоритма декодирования одновременно обеспечивается и меньшая сложность декодирования.

3. Для решения проблемы высокой задержки декодирования полярных (под)кодов была предложена конструкция звездных полярных подкодов и соответствующее обобщение списочного алгоритма Тала-Варди. Было показано, что данный подход позволяет сократить число шагов (списочного) алгоритма последовательного исключения в l раз, где l — параметр конструкции.

4. Предложен последовательный алгоритм декодирования полярных подкодов и иных кодов, представленных в виде системы ОДЗ. Предложенный алгоритм позволяет упростить декодирование коротких кодов БЧХ, а для кодов Рида-Соломона обеспечивает повышение корректирующей способности до 0.4 дБ по сравнению с другими известными алгоритмами декодирования.

5. Для решения проблемы эффективного декодирования длинных кодов Рида-Соломона, был разработан быстрый алгоритм со сложностью $O(n^2 r^3)$, реализующий интерполяционный шаг в алгоритмах Гурусвами-Судана и Ву.

6. Предложен быстрый алгоритм вычисления дискретного преобразования Фурье над полями характеристики 2 со сложностью $O(n \log^{\gamma} \log n)$ умножений и $O(n \log^{\gamma+1} n)$ сложений, $\gamma \leq 2$.

7. Предложен быстрый алгоритм систематического кодирования кодов Рида-Соломона, основанный на предложенном циклотомическом алгоритме быстрого преобразования Фурье. Показано, что программная реализация разработанного алгоритма обеспечивает существенно лучшую производительность до 3.6 раз) по сравнению с библиотекой Jerasure, широко используемой в современных системах хранения данных.

8. Предложен быстрый алгоритм систематического кодирования полярных кодов с ядром Рида-Соломона.

Список публикаций

1. Fedorenko, S. V. Finding roots of polynomials over finite fields [Text] / S. V. Fedorenko, P. V. Trifonov // IEEE Transactions on Communications. — 2002. — Vol. 50, no. 11. — P. 1709–1711.
2. Трифонов, П. В. Метод быстрого вычисления преобразования Фурье над конечным полем [Текст] / П. В. Трифонов, С. В. Федоренко // Проблемы передачи информации. — 2003. — Т. 39, № 3. — С. 3–10.
3. Costa, E. On computing the syndrome polynomial in Reed-Solomon decoder [Text] / E. Costa, S. V. Fedorenko, P. V. Trifonov // European Transactions on Telecommunications. — 2004. — May/June. — Vol. 15, no. 4. — P. 337–342.
4. Трифонов, П. Интерполяция в списочном декодировании кодов Рида-Соломона [Текст] / П.В. Трифонов // Проблемы передачи информации. — 2007. — Т. 43, № 3. — С. 28–38.
5. Trifonov, P. Efficient interpolation in the Guruswami-Sudan algorithm [Text] / P. Trifonov // IEEE Transactions on Information Theory. — 2010. — September. — Vol. 56, no. 9. — P. 4341–4349.
6. Trifonov, P. Efficient interpolation in Wu list decoding algorithm [Text] / P. Trifonov, M. H. Lee // IEEE Transactions on Information Theory. — 2012. — September. — Vol. 58, no. 9. — P. 5963–5971.
7. Trifonov, P. Efficient design and decoding of polar codes [Text] / Peter Trifonov // IEEE Transactions on Communications. — 2012. — November. — Vol. 60, no. 11. — P. 3221 – 3227.
8. Трифонов, П. Декодирование кодов Рида-Соломона методом последовательного исключения [Текст] / П.В. Трифонов // Проблемы передачи информации. — 2014. — Т. 50, № 4. — С. 3–14.
9. Miloslavskaya, V. Sequential decoding of polar codes [Text] / V. Miloslavskaya, P. Trifonov // IEEE Communications Letters. — 2014. — Vol. 18, no. 7. — P. 1127–1130.
10. Trifonov, P. Low-complexity implementation of RAID based on Reed-Solomon codes [Text] / P. Trifonov // ACM Transactions on Storage. — 2015. — February. — Vol. 11, no. 1. — P. 1:1–1:25.
11. Trifonov, P. Polar subcodes [Text] / P. Trifonov, V. Miloslavskaya // IEEE Journal on Selected Areas in Communications. — 2016. — February. — Vol. 34, no. 2. — P. 254–266.
12. Fast encoding of polar codes with Reed-Solomon kernel [Text] / P. Trifonov, V. Miloslavskaya, Ch. Chen, Y. Wang // IEEE Transactions on Communications. — 2016. — July. — Vol. 64, no. 7. — P. 2746–2753.
13. Ma, J. Divide-and-conquer interpolation for list decoding of Reed-Solomon codes [Text] / J. Ma, P. Trifonov, A. Vardy // Proceedings of IEEE International Symposium on Information Theory. — Chicago, USA : IEEE, 2004. — June 27 – July 2. — P. 387.
14. Trifonov, P. Another derivation of Wu list decoding algorithm and interpolation in rational curve fitting [Text] / P. Trifonov // Proceedings of IEEE R8 International Conference on Computational Technologies in Electrical and Electronics Engineering. — Irkutsk, Russia : IEEE, 2010. — P. 59–64.
15. Trifonov, P. On the additive complexity of the cyclotomic FFT algorithm [Text] /

P. Trifonov // Proceedings of IEEE Information Theory Workshop. — Lausanne, Switzerland : IEEE, 2012. — P. 537 – 541.
16. Trifonov, P. Polar codes with dynamic frozen symbols and their decoding by directed search [Text] / P. Trifonov, V. Miloslavskaya // Proceedings of IEEE Information Theory Workshop. — Sevilla, Spain : IEEE, 2013. — September. — P. 1 – 5.
17. Trifonov, P. Binary successive cancellation decoding of polar codes with Reed-Solomon kernel [Text] / P. Trifonov // Proceedings of IEEE International Symposium on Information Theory. — Honolulu, USA : IEEE, 2014. — P. 2972 – 2976.
18. Trifonov, P. Twisted polar codes [Text] / P. Trifonov, V. Miloslavskaya // Proceedings of International Symposium on Information Theory and Its Applications. — Melbourne, Australia : IEEE, 2014. — P. 456–460.
19. Trifonov, P. Design of polar codes for Rayleigh fading channel [Text] / P. Trifonov // Proceedings of International Symposium on Wireless Communication Systems. — Brussels, Belgium : IEEE, 2015. — P. 331–335.
20. Trifonov, P. Chained polar subcodes [Text] / P. Trifonov // Proceedings of 11th International ITG Conference on Systems, Communications and Coding. — Hamburg, Germany : ITG, 2017. — P. 1–6.
21. Trifonov, P. Star polar subcodes [Text] / P. Trifonov // Proceedings of IEEE Wireless Communications and Networking Conference Workshops. — San-Francisco, USA : IEEE, 2017. — P. 1–6.
22. Ivanov, K. Hybrid decoding of interlinked generalized concatenated codes [Text] / K. Ivanov, P. Trifonov // Proceedings of 9th International Symposium on Turbo Codes and Iterative Information Processing. — Brest, France : IEEE, 2016. — P. 41–45.
23. Trifonov, P. A randomized construction of polar subcodes [Text] / P. Trifonov, G. Trofimiuk // Proceedings of IEEE International Symposium on Information Theory. — Aachen, Germany : IEEE, 2017. — P. 1863–1867.
24. Trifonov, P. Chained successive cancellation decoding of the extended Golay code [Text] / P. Trifonov // Proceedings of Iran Workshop on Communication and Information Theory. — Tehran, Iran : Sharif University of Technology, 2018.
25. Trifonov, P. Randomized chained polar subcodes [Text] / P. Trifonov // Proceedings of IEEE Wireless Communications and Networking Conference Workshops. — Barcelona, Spain : IEEE, 2018. — P. 292–297.
26. Miloslavskaya, V. Sequential decoding of polar codes with arbitrary binary kernel [Text] / V. Miloslavskaya, P. Trifonov // Proceedings of IEEE Information Theory Workshop. — Hobart, Australia : IEEE, 2014. — P. 377–381.