

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего
образования
«Ульяновский государственный технический университет»

На правах рукописи

Ал Тамими Таква Флайиих Хасан

**РАЗРАБОТКА И МОДЕЛИРОВАНИЕ ПЕРЕСТАНОВОЧНОГО ДЕКОДЕРА
НЕДВОИЧНОГО ИЗБЫТОЧНОГО КОДА НА БАЗЕ КОГНИТИВНОЙ
МЕТАФОРЫ**

Специальности:

05.13.05 «Элементы и устройства вычислительной техники и систем управления»

05.13.18 «Математическое моделирование, численные методы и комплексы программ»

Диссертация
на соискание ученой степени
кандидата технических наук

Научный руководитель:

Доктор технических наук, профессор
Гладких Анатолий Афанасьевич

Ульяновск – 2018

СОДЕРЖАНИЕ

СОДЕРЖАНИЕ.....	2
СПИСОК СОКРАЩЕНИЙ.....	4
ВВЕДЕНИЕ.....	6
ГЛАВА 1. СИНТЕЗ ЭЛЕМЕНТОВ СИСТЕМ УПРАВЛЕНИЯ С ЦЕЛЬЮ ОПТИМИЗАЦИИ ИХ ТЕХНИЧЕСКИХ ХАРАКТЕРИСТИК	13
1.1. Задача синтеза элементов систем управления	13
1.2. Актуальность применения средств помехоустойчивого кодирования в современных цифровых устройствах.....	17
1.3. Теоретическое обоснование метода перестановочного декодирования.....	22
1.4. Общие принципы мягкого декодирования помехоустойчивых кодов.....	32
1.5. Мягкое декодирование как декодирование в целом.....	38
1.6. Моделирование когнитивной метафоры в технических системах.....	41
1.7. Выводы по главе и постановка задачи на исследование.....	44
ГЛАВА 2. ИССЛЕДОВАНИЕ МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ И МЕТОДОВ ФОРМИРОВАНИЯ МЯГКИХ РЕШЕНИЙ СИМВОЛОВ НЕДВОИЧНЫХ КОДОВ	47
2.1. Особенности применения программируемых логических интегральных схем в системе обработки недвоичных символов.....	47
2.2. Модели формирования мягких решений сложных сигналов.....	53
2.3. Модели формирования мягких решений недвоичных символов методом сравнения гистограмм.....	59
2.4. Вычисление МРС с использованием когнитивной процедуры....	67
2.5. Формирование МРС в системе каскадных кодеков.....	74
2.6. Выводы по главе.....	75
ГЛАВА 3. ЭФФЕКТИВНОЕ ПЕРЕСТАНОВОЧНОЕ ДЕКОДИРОВАНИЕ НЕДВОИЧНЫХ ГРУППОВЫХ КОДОВ	77
3.1. Классические методы декодирования кодов Рида-Соломона.....	77
3.2. Оценка сложности реализации классического подхода к декодированию кодов в системе перестановочного декодирования.....	81

3.3. Декодирование с перестановками недвоичных групповых кодов	83
3.4. Оценка алгоритма декодирования с использованием оператора быстрых матричных преобразований.....	88
3.5. Модифицированный метод перестановочного декодирования на базе когнитивной карты	91
3.6. Выводы по главе.....	101
ЗАКЛЮЧЕНИЕ.....	103
СПИСОК ЛИТЕРАТУРЫ.....	105
ПРИЛОЖЕНИЕ А. Лексикографический декодер каскадного кода.....	116

СПИСОК СОКРАЩЕНИЙ

BER	– вероятность ошибки на бит
OSI	– модель взаимодействия открытых систем
PSK	– фазовая модуляция
QAM	– квадратурная амплитудная модуляция
АБГШ	– аддитивный белый гауссовский шум
АГС	– алгоритм Гурусвами-Судана
АЛУ	– арифметико-логические устройства
АМ	– амплитудная модуляция
АПД	– аппаратуры передачи данных
АЭ	– арифметические элементы
БМА	– алгоритм Берлекэмп-Мессе
БМП	– быстрые матричные преобразования
БЧХ	– код Боуза-Чоудхури-Хоквингема
ИИА	– итеративный интерполяционный алгоритм
ИКС	– искусственная когнитивная система
ИМР	– индекс мягкого решения
ИУК	– информационно-управляющий комплекс
МДК	– максимально декодируемые коды
МРС	– мягкое решение символа
НДК	– недвоичный код
НОД	– наибольший общий делитель
ПД	– перестановочное декодирование
ПЛИС	– программируемая логическая интегральная схема (англ. Programmable Logic Device, PLD)
ПРВ	– плотность распределения вероятностей
РС	– код Рида-Соломона
СОД	– система обмена данными
СПД	– система передачи данных

СУ	– система управления
ТКС	– телекоммуникационные системы
УЦФ	– управляющий целевых функций
УЭ	– управляемый элемент
ФМ	– фазовая модуляция
ЭВК	– энергетический выигрыш кода
ЭМ	– эталонная матрица

ВВЕДЕНИЕ

Актуальность темы исследования

Применение тех или иных методов кодирования способно в значительной степени повысить достоверность принимаемой информации и обеспечить энергетический выигрыш кода (ЭВК) в канале связи до 10 дБ, приблизившись вплотную к порогу Шеннона, например, при использовании турбокодов или кодов с малой плотностью проверок на четность [16, 19, 33, 70]. Недостатками таких мощных кодов являются большая избыточность, вносимая в передаваемое сообщение, а также применение итеративных преобразований, приводящих к существенному увеличению цикла управления на этапе обработки данных, что совершенно недопустимо в условиях реализации современных систем управления для защиты команд управления от влияния деструктивных факторов [23, 30].

Жесткость требований к надежности работы и достоверности получаемой и обрабатываемой информации в управляющих системах кратно возрастает для систем реального времени, от которых требуется еще и повышенная готовность к выполнению программ их действий, что особенно важно для различных категорий автономных транспортных средств [49, 50]. Именно в таких системах наиболее востребованы новые методы синтеза элементов технического зрения, системы связи и навигации, защита цифровых данных от влияния мешающих факторов, гибкие методы обработки оперативной информации и внедрение передовых технологий, связанных с реализацией когнитивных искусственных систем и перспективным применением нейросетевых технологий обработки многочисленных данных.

Внедрение сетевых технологий в процессы управления мобильными объектами предъявляет повышенные требования к характеристикам используемых каналов радиосвязи. Процедура управления в реальном времени мобильными объектами требует не только достижения требуемого уровня энергетической эффективности таких каналов связи, но и повышения их спектральной эффективности [18, 20, 25, 36, 84, 90]. Это вызывает необходимость

использования в таких системах управления сложных видов модуляции в сочетании с недвоичными помехоустойчивыми кодами, специфика обработки которых в системах управления может занимать значительные интервалы времени.

В связи с этим актуальность темы диссертационной работы обусловлена наличием следующих нерешенных задач:

- отсутствие разработанных и научно обоснованных подходов к организации алгоритмов систем управления на базе сокращенных циклов декодирования недвоичных помехоустойчивых кодов;
- отсутствие методов применения когнитивных принципов в искусственных технических системах и, в частности, в системах обмена данными на уровне обработки помехоустойчивых кодов;
- отсутствие моделей когнитивной адаптации в системе формирования мягких решений недвоичных символов;
- отсутствие схемных решений по управлению алгоритмами работы перестановочных декодеров в условиях реализации когнитивной метафоры.

Степень разработанности темы

Концептуальные принципы развития цифровых систем связи заложены в основополагающих работах В.А. Котельникова, К.Е. Шеннона, Р.М. Фано и П. Элайеса. Значительный вклад в разработку теории повышения спектральной и энергетической эффективности систем обмена данными внесли такие зарубежные авторы, как E.R. Berlekamp, R.C. Bose, R.W. Hamming, R.E. Blahut, J. Massey, I.S. Reed, G. Solomon, M. Sudan, G.D. Forney, R.G. Gallager, A.J. Viterbi, а также ряд отечественных ученых: В.И. Коржик, Э.Л. Блох, В.В. Зяблов, К.Ш. Зигангиров, В.В. Золотарев, Г.В. Овечкин, Л.Е. Варакин, в работах которых раскрываются теоретические основы построения различных классов избыточных кодов.

Значительный вклад в разработку теории перестановочного декодирования систематических групповых кодов внесли J.F. MacWilliams и W.W. Peterson, R. Morelos-Zaragoza, B. Sklar. Повышением спектральной и энергетической

эффективности систем обмена данными занимались E.R. Berlekamp, J.L. Massey, I.S. Reed, G. Solomon, G.D. Forney, В.И. Коржик, Э.Л. Блох, В.В. Зяблов, К.Ш. Зигангиров, В.В. Золотарев, Г.В. Овечкин, в работах которых раскрываются теоретические основы построения различных классов избыточных кодов. Вместе с этим применение помехоустойчивых кодов в системах с когнитивной адаптацией в указанных работах даже не рассматривается.

Цели и задачи исследования

Целью работы является сокращение цикла управления перестановочным декодером путем применения процедуры быстрых матричных преобразований в системе когнитивной обработки данных при одновременном снижении объема памяти когнитивной карты декодера.

Для достижения указанной цели требуется решить следующие задачи:

1. Осуществить анализ известных методов построения декодеров избыточных кодов в системе информационно-управляющих комплексов (в том числе реального времени) и выявить их достоинства и недостатки.

2. Разработать систему выработки мягких решений недвоичных символов избыточных кодов и на основе испытаний имитационных моделей и применения численных методов получить вероятностные характеристики системы выработки таких решений.

3. Обосновать корректность системы рационального формирования когнитивной карты декодера подмножеством эталонных матриц эквивалентных кодов и доказать возможность получения из него полного множества матриц таких кодов за счет быстрых матричных преобразований.

4. Оценить возможность снижения цикла работы декодеров недвоичных кодов с использованием процедуры когнитивной обработки данных в системе их перестановочного декодирования.

5. Разработать рекомендации по снижению объема памяти когнитивной карты декодера при использовании циклических свойств нумераторов перестановок символов кодовых векторов.

Объект исследования

Теоретический анализ, моделирование и синтез элементов систем управления и устройств вычислительной техники.

Предмет исследования

Алгоритмы управления мягкой обработкой недвоичных помехоустойчивых кодов с целью улучшения эксплуатационных характеристик декодера избыточного кода.

Соответствие работы рассматриваемым специальностям

Содержание диссертационной работы соответствует следующим пунктам паспорта специальности 05.13.05 «Элементы и устройства вычислительной техники и систем управления»:

– п.п. 1 – разработка научных основ создания и исследования общих свойств и принципов функционирования элементов, схем и устройств вычислительной техники и систем управления;

– п.п. 3 – разработка принципиально новых методов анализа и синтеза элементов и устройств вычислительной техники и систем управления с целью улучшения их технических характеристик;

а также пунктам паспорта специальности 05.13.18 «Математическое моделирование, численные методы и комплексы программ»:

– п.п. 3 – разработка, обоснование и тестирование эффективных вычислительных методов с применением современных компьютерных технологий;

– п.п. 8 – разработка систем компьютерного и имитационного моделирования.

Научная новизна

1. Впервые применен метод когнитивной обработки данных для управления процедурой перестановочного декодирования путем хранения в когнитивной карте декодера результатов поиска порождающих матриц эквивалентных кодов, полученных на предыдущих этапах его работы.

2. Доказана эффективность системы управления декодером на основе введенных быстрых матричных преобразований порождающих матриц эквивалентных кодов с использованием их эталонных аналогов, позволившая на два – четыре порядка и более (в зависимости от параметров кода) снизить объем требуемых матричных вычислений.

3. Предложена принципиально новая методика сокращения общего объема памяти когнитивной карты декодера (от 80% до 90%) за счет использования циклических свойств нумераторов перестановок.

4. Предложена новая структура декодера с элементами лексикографического поиска вектора ошибок, отличающаяся новизной технического решения (патент РФ № 2619533, опубликован 16 мая 2017 г.).

Практическая ценность работы

Предложенные алгоритмы когнитивного декодирования недвоичных кодов оптимальны в смысле минимизации арифметических действий, выполняемых в двоичных полях Галуа заданной степени расширения на кристалле ПЛИС, за счет замены матричных вычислений на тривиальные перестановки строк и столбцов заранее вычисленных эквивалентных матриц в процедуре их обращения в порождающие матрицы систематических блочных кодов, в частности, блоков Рида-Соломона.

Методы исследования

Для решения поставленных задач и достижения намеченной цели использованы методы системного анализа, математического моделирования, теории вероятности, методы математической статистики, теории информационных систем, численные методы, а также методы программирования. Математическое моделирование производилось с использованием пакетов прикладных программ MATCAD, MATLAB и Simulink.

Основные положения, выносимые на защиту

1. Модель перестановочного декодера избыточного кода, использующая результаты преобразований порождающих матриц эквивалентных кодов,

хранимых в памяти когнитивной карты декодера и применяемых в случаях повтора перестановок нумераторов символов принятой кодовой комбинации.

2. Схема формирования мягких решений недвоичных символов в формате коэффициента правдоподобия.

3. Система порождающих матриц эквивалентных кодов в недвоичных полях Галуа, использующая перестановки элементов эталонных матриц без выполнения арифметических операций.

4. Метод снижения объема памяти когнитивной карты декодера, использующий циклические свойства нумераторов перестановок и позволяющий кратно сократить объем памяти когнитивной карты декодера.

5. Программно-аппаратная реализация элемента перестановочного декодера по вычислению порождающих матриц эквивалентных кодов с использованием быстрых матричных преобразований.

Обоснованность и достоверность результатов работы

Результаты исследований получены на основе строгих радиофизических и математических моделей. Использованные при этом методы решения поставленных задач корректны с формальной математической точки зрения. Контроль достоверности результатов осуществлялся анализом физического смысла решений, имитационным моделированием и натурным экспериментом.

Апробация работы

Основные результаты диссертационной работы докладывались на Всероссийской научно-практической конференции (с участием стран СНГ) «Современные проблемы создания и эксплуатации радиотехнических систем». – Ульяновск: УлГТУ, 2015 г.; на 71-й Международной конференции «Радиоэлектронные устройства и системы для инфокоммуникационных технологий (REDS–2016)», посвящённой Дню радио. – Москва, 2016 г.; в сборнике научных трудов «Современные проблемы проектирования, производства и эксплуатации радиотехнических систем». – Ульяновск: УлГТУ, 2016 г.; в докладе на 20-й Международной конференции РНТОРЭС имени А.С. Попова «Цифровая обработка сигналов и её применение – DSPA-2018». – Москва, 2018 г.

Реализация результатов работы

Материалы диссертации использовались в ходе совершенствования учебного процесса при изучении учебной дисциплины «Теория кодирования и защиты информации» при подготовке студентов бакалавриата по направлению 11.03.02 «Инфокоммуникационные технологии и системы связи» на кафедре «Телекоммуникации» УлГТУ.

Публикации по работе

По материалам диссертации опубликовано 9 работ, из них 4 статьи в изданиях, включенных в перечень ВАК, а также один патент РФ на изобретение.

Личный вклад автора

Автору работы принадлежат разработка и программно-аппаратная реализация алгоритма поиска порождающих матриц недвоичных эквивалентных кодов в системе перестановочного декодирования путем линейных преобразований известных декодеру эталонных матриц. В совместных работах автор проводила рассуждения по обоснованию актуальности темы исследования и выработке концептуальных направлений совершенствования аппаратных решений в процедуре поиска эквивалентных кодов, выполняла вывод аналитических соотношений, проведение расчетов, составление математических моделей и проведение испытаний имитационных моделей, обобщение и интерпретацию результатов таких испытаний.

Структура и объем работы

Диссертация состоит из введения, трех глав, заключения, списка литературы и приложений, содержит 126 страниц машинописного текста, в том числе 33 иллюстрации и 11 таблиц. Список литературы включает в себя 117 наименований. В приложении к диссертации представлены: листинг программ имитационных моделей перестановочного декодера, а также акт внедрения результатов работы.

ГЛАВА 1. СИНТЕЗ ЭЛЕМЕНТОВ СИСТЕМ УПРАВЛЕНИЯ С ЦЕЛЬЮ ОПТИМИЗАЦИИ ИХ ТЕХНИЧЕСКИХ ХАРАКТЕРИСТИК

1.1. Задача синтеза элементов систем управления

Задача синтеза классических систем управления (СУ) в общем случае предполагает наличие четырех главных элементов: управляющего и управляемого элементов, прямого канала связи для передачи команд управления $M(c)$ от управляющего элемента (оператора) к управляемому и обратного канала связи для передачи сведений $M(i)$ о степени достижения поставленной цели. При этом справедливо рассматривать совокупность прямого и обратного каналов связи в качестве вполне определенной телекоммуникационной составляющей общей СУ, по которой циркулируют, как правило, команды $M(c)$ в формате цифровых данных (собственно данных, оцифрованного голоса или оцифрованных изображений с командными метками) и сведения $M(i)$ о выполнении команд оператора в виде потока телеметрических данных и цифровых изображений. В случае синтеза СУ роботами, которые предполагают наличие полимодальной сенсорной структуры и базы знаний, структура управления подобными объектами существенно осложняется за счет организации всей когнитивно-регулятивной системы деятельности робота, включая распознавание ситуации, принятие решений и планирование операций по антропоморфному принципу [16, 34, 72]. Таким образом, в задаче синтеза произвольной СУ полагаются определенными множество D рассматриваемых в задаче объектов (допустимых вариантов построения систем), множество U условий функционирования СУ и функционал $F : D \times U \rightarrow R$, выражающий значение $F\{D, U, T, A\}$ степени достижения целевой функции для любых элементов $d \in D$ и $u \in U$, при этом параметр R – суть действительного числа, значение T – временные ограничения, характерные для конкретной СУ, и A – требования по достоверности, предъявляемые к $M(c)$ и $M(i)$ [34]. Возможные варианты построения модели СУ в качественном

отношении полностью зависят от доступных разновидностей пары D и U с вытекающими последствиями в достижении $F\{D, U, T, A\}$ [30, 34, 71, 96].

В работе [30] показано, что задача синтеза СУ в количественном отношении формулируется при выборе некоторого элемента $u_0 \in U$, определяющего конкретные и вполне реализуемые условия функционирования синтезируемой системы. В конечном счете она заключается в максимизации показателя $F\{d, u_0, t, a\}$ для заданных условий $u_0 \in U$, t , a функционирования системы с элементами $d \in D$ и представляется как $F\{d, u_0, t, a\} \rightarrow \max$ при $d \in D$. Отбор наилучшей системы осуществляется по принципу выявления ε -оптимальной системы, когда $d_\varepsilon \in D \Leftrightarrow F\{d, u, t, a\} = F\{d_\varepsilon, u_0, t, a\} + \varepsilon$, где $\varepsilon > 0$ [30, 34, 72]. Очевидно, что оптимизация в зависимости от текущих параметров $F\{\bullet\}$ может носить долговременный или, напротив, кратковременный характер, что вызывает необходимость использования адаптивных систем управления.

Вариации построения системы относительно ε -оптимального варианта ее реализации не могут повысить эффективность ее функционирования в условиях u_0 более чем на величину ε . Необходимость рассмотрения ε -оптимальных решений для случая $\varepsilon > 0$ обусловлена как целесообразностью упрощения методов их поиска и нахождения просто реализуемых решений, так и принципиальным отсутствием оптимальных решений (при $\varepsilon = 0$) для определенных конструкций с $F\{d = d_\varepsilon, u_0, t, a\}$.

Пример 1.1. Пусть u_0 соответствует условиям применения каналов связи для обмена данными $M(c)$ и $M(i)$, отвечающих условиям независимого потока ошибок. Пусть в качестве d_1 выбирается декодер, реализующий алгоритм исправления ошибок путем применения двоичного блочного помехоустойчивого кода $C_{(n,k,d_m)}$, где n – длина кодового вектора, k – число информационных разрядов в нем, а d_m – метрика Хэмминга или минимальное расстояние кода $C_{(\bullet)}$.

Как показано в работах [1, 13, 61, 62, 66, 81, 83], в телекоммуникационных составляющих СУ в качестве критерия эффективности применения в них

помехоустойчивого кодирования выбирают значение получаемого от этой процедуры энергетического выигрыша кода (ЭВК). Известно, что в канале с гауссовским шумом при условии, что отношение $E_b / N_0 \rightarrow \infty$, в котором значение E_b – энергия сигнала, приходящаяся на информационный бит, N_0 – спектральная плотность гауссовского шума, в случае жестких решений и реализации алгоритма исправления $e = \lfloor (d_m - 1)/2 \rfloor$ ошибок ЭВК оценивается выражением $W_{oui} = 10 \lg(\frac{k}{n}(e + 1))$ дБ, что косвенно отвечает параметрам t и a из $F\{d, u_0, t, a\}$. В подобных условиях дается асимптотическая оценка ЭВК [37]. Увеличение кратности исправляемых кодом ошибок неизбежно приводит к повышению сложности декодера и увеличивает параметр t за счет решения большего числа линейных уравнений [8, 9, 26, 79, 88, 100]. Условно обозначим этот процесс через символ $t_{oui} \uparrow$. Естественно, что в рассматриваемых системах из-за требований оперативности управления в СУ целесообразно стремиться к обратному явлению $t_{oui} \downarrow$. В то же время необходимо учитывать, что при $t_{oui} \uparrow$ повышается достоверность приема данных $M(c)$ и $M(i)$, т.е. $a_{oui} \uparrow$. Расчеты показывают: параметр a_m целесообразно увеличивать только до значений, когда отношение $k/n \geq 0,5$.

При использовании алгоритмов исправления стираний (конструкция декодера d_2) ЭВК оценивается выражением $W_{cm} = 10 \lg(\frac{k}{n}(2e + 1))$ дБ [18, 25, 30]. Следовательно, при $E_b / N_0 \rightarrow \infty$ ЭВК при исправлении стираний становится в два раза больше, чем при обработке жестких решений, поскольку параметр $d_m = 2e + 1$, и поэтому в пределе выигрыш составляет около 3 дБ. Указанные соотношения показывают, что безызбыточное кодирование при $n = k$, $t = 0$ и $d_m = 1$ в рассматриваемых системах принципиально не в состоянии обеспечить какой-либо энергетический выигрыш. Поскольку $W_{oui} < W_{cm}$, то вторая система

относительно первой является ε -эффективной, при этом значение ε в терминах данного примера составляет 3 дБ по асимптотической оценке.

Дополнительный выигрыш ЭВК возможно получить в условиях применения максимально декодируемых кодов (МДК) с конструкцией декодера d_3 [4, 30, 39, 85, 87]. В этом случае асимптотической оценкой энергетического выигрыша от применения блочного двоичного кода может служить выражение $W_{мдк} = 10 \lg \left(k \left(1 - \frac{k+1}{n} \right) \right)$ дБ [2]. Для таких кодов значение метрики Хэмминга определяется как $d_m = n - k + 1$, например, для недвоичных кодов Рида-Соломона (РС), которые однозначно достигают значения $W_{мдк}$, но этого нельзя утверждать относительно известных двоичных кодов, которые не являются максимально декодируемыми кодами [3, 4, 44, 61, 91, 93, 104]. В работе [30] показано, что выигрыш ЭВК в последнем случае может составлять дополнительные 2 – 3 дБ к выигрышу $W_{см}$, и третья система использования избыточных кодов для эффективной защиты сигналов $M(c)$ и $M(i)$ оказывается с наибольшим значением ε в системе исправления ошибок и стираний. При этом за счет исключения из алгоритма исправления ошибок шагов по вычислению локаторов ошибок однозначно обеспечивается $a \uparrow$ при $t \downarrow$.

В случае $\varepsilon \leq 0$ для любого $d_i(D, u_0, t, a) = \emptyset$ задача поиска оптимального элемента по существу теряет смысл. Из определения ε -оптимальной системы d_ε вытекает, что при ее применении в условии u_0 обеспечивается значение показателя эффективности, равное $F\{d_\varepsilon, u\} \geq \sup F\{d, u_0\} - \varepsilon$ при $d \in D$.

С точки зрения общего подхода к синтезу СУ множество U целесообразно рассматривать как совокупность двух подмножеств: $U_{он} \in U$, в котором условия функционирования системы априори определены, и подмножества $U_{но} \in U$, в котором подобные условия до реального применения системы остаются неопределенными, но могут быть априори спрогнозированы, $U_{нр} \in U_{но}$. Отсюда

$$U = \begin{cases} U_{on}; \\ U_{no} = \begin{cases} U'_{no}; \\ U_{np}. \end{cases} \end{cases} \quad (1.1)$$

При создании системы в условиях неопределенности полагается неполное задание функционирования проектируемой системы, но, учитывая современные достижения в разработке интеллектуальных систем, возможно использование когнитивных принципов для идентификации новых ситуаций и выработки для них когнитивных адаптивных реакций для перевода части событий из множества U_{no} в множество U_{on} [49, 50, 78]. При этом для формулировки математически корректной задачи так или иначе используются дополнительные сведения об условиях применения системы, содержание которых и порождает различные подходы к ее синтезу.

Таким образом, при разработке принципиально новых методов анализа и синтеза элементов и устройств систем управления с целью улучшения их технических характеристик должны учитываться современные тенденции не только в построении адаптивных систем классического типа, но и использоваться достижения в области построения таких систем на базе применения концепции построения когнитивных систем и систем с когнитивными принципами адаптации.

1.2. Актуальность применения средств помехоустойчивого кодирования в современных цифровых устройствах

В связи с активным развитием современных роботизированных и интеллектуальных устройств (вплоть до развития систем искусственного интеллекта) возникает задача надежного функционирования элементов и устройств вычислительной техники, составляющих основу подобных систем. Цифровые устройства обработки различных видов информации применяются в

сложных системах телеуправления, включая специфические системы связи и радиолокации, системах навигации и цифровой обработки и хранения данных.

Увеличение числа и объемов задач, выполняемых подобными системами, придание им свойств многофункциональности приводят к объективному их усложнению, уменьшению надежности функционирования и снижению достоверности получаемой информации. При этом усложнение методов обработки цифровых данных носит опережающий характер относительно процедуры разработки средств и методов повышения надежности. В этой связи задача реализации высокой надежности сложных систем является актуальной.

Особенно жесткие требования к надежности работы и достоверности обрабатываемых данных предъявляются к управляющим системам, работающим в реальном масштабе времени, от которых дополнительно требуется еще и повышенная готовность к выполнению задач управления.

Обобщенная структурная схема СУ известна [24, 52, 59, 69]. Классический ее вариант содержит управляющую систему (УС), наделенную управляющей целевой функцией (УЦФ) $F(\bullet)$, у которой символ $(\bullet)$ характеризует конечный набор аргументов УЦФ, управляемый элемент (УЭ), предназначенный для реализации конкретных значений из состава $(\bullet)$, каналы прямой и обратной связи для связи УС и УЭ для оценки степени выполнения УЭ требуемых значений $F(\bullet)$ и выработки дополнительных сигналов коррекции в случае расхождения этих значений. Структурная схема обобщенной системы управления представлена на рисунке 1.1.

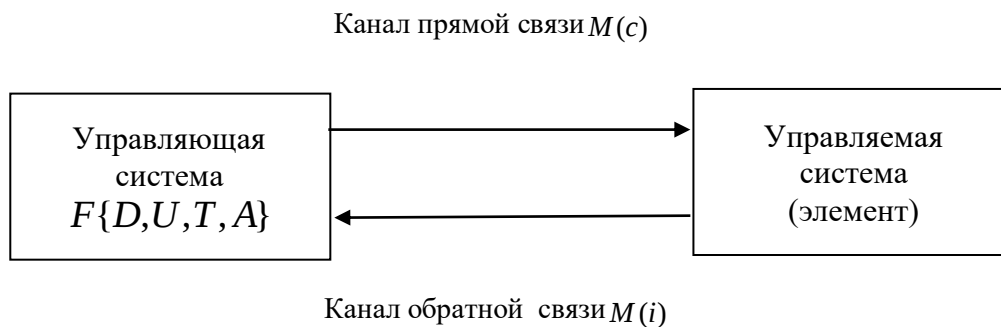


Рисунок 1.1 – Обобщенная структурная схема системы управления

Отсутствие каналов прямой и обратной связи образует моносистему, в которой все процессы, связанные с выполнением функции $F(\bullet)$, организуются в рамках одного устройства (микросхемы, платы, процессора), т.е. внутрисхемно. Наличие указанных каналов в телеметрических и дистанционных системах управления обязательно. С учетом этого системы проверки работоспособности и диагностики отказов систем управления можно классифицировать как внутрисхемные и разнесенные. Наиболее общая классификация таких систем представлена на рисунке 1.2.



Рисунок 1.2 – Классификация систем контроля и диагностики систем управления

Основным методом решения проблем высокой надежности, достоверности и коэффициента готовности является использование структурной (аппаратной) и информационной (сигнальной) избыточности. В большинстве случаев работы по исследованию структурной избыточности относятся к математической оценке надежности различных моделей резервирования безотносительно к их структуре, а работы по информационной избыточности развивались в основном применительно к теории кодов для каналов связи [68].

Структурно избыточные СУ подразумевают резервирование важных элементов и их схемное построение. В этом случае под системой понимается

любое устройство, состоящее из частей (элементов), надежность которых задана. Структура СУ и характер ее работы должны быть известны настолько, чтобы для любого элемента было определено, вызывает ли отказ такого элемента отказ всей СУ. В простейшем случае предполагается, что элементы отказывают независимо друг от друга [38, 67].

В общем случае СУ состоит из n элементов с известными функциями надежности $p_1(t), p_2(t), \dots, p_n(t)$, т.е. безотказной работы элемента в течение времени t . При последовательном соединении таких элементов функции надежности перемножаются. Выражая функцию надежности через вероятности отказа

$$\exp\left(-\int_0^t \lambda(s) ds\right) = \exp\left(-\int_0^t \lambda_1(s) ds + \int_0^t \lambda_2(s) ds + \dots + \int_0^t \lambda_n(s) ds\right), \quad (1.2)$$

получают $\lambda(t) = \lambda_1(t) + \lambda_2(t) + \dots + \lambda_n(t)$. Здесь λ_i – локальная характеристика надежности, определяющая надежность элемента СУ в каждый данный момент времени. По сути, это параметр плотности условной вероятности отказа в момент t при условии, что до этого момента элемент работал безотказно.

При параллельном соединении элементы вероятности отказов перемножаются. В частности, когда все элементы равнонадежны, то получают

$$Q(t) = 1 - P(t) = q^n(t). \quad (1.3)$$

Если надежность каждого элемента подчиняется экспоненциальному закону, то надежность системы не будет подчиняться этому закону. Например, для случая элементов с равными вероятностями отказа (что является сильным допущением) получают

$$Q(t) = (1 - e^{-\lambda t})^n. \quad (1.4)$$

В этом случае можно найти среднее время жизни системы

$$T_0 = \int_0^{\infty} P(t) dt = \int_0^{\infty} [1 - (1 - e^{-\lambda t})^n] dt. \quad (1.5)$$

Заменяя $1 - e^{-\lambda t} = x$, получают $t = (1/\lambda) \ln(1/(1-x))$, при этом $dt = dx/\lambda(1-x)$.

$$T_0 = \frac{1}{\lambda_0} \int_0^1 \frac{1-x^n}{1-x} dx = \frac{1}{\lambda_0} \int_0^1 (1+x+\dots+x^{n-1}) dx = \frac{1}{\lambda} \left(1 + \frac{1}{2} + \dots + \frac{1}{n}\right). \quad (1.6)$$

В реальных системах допущение о равновероятности отказов всех элементов системы не выполняется, поэтому модель оценки таких систем сводится к разбиению отдельных частей СУ на пересекающиеся группы, в которых выделяются классы связанных групп. Тогда, например, первый класс образуют группы $G_1, G_2, \dots, G_{s_1}$, а второй класс – группы $G_{s_1+1}, G_{s_1+2}, \dots, G_{s_2}$. Считая события A_i из разных классов независимыми, заключающимися в том, что группа G_i не отказала за время t , надежность системы выражается в формате

$$P(t) = P\{A_1 \times A_2 \times \dots \times A_n\} = P\{A_1 \dots A_{s_1}\} \times P\{A_{s_1+1} \dots A_{s_2}\} \dots \quad (1.7)$$

Таким образом, аппарат аналитических моделей для оценки структурно зависимых СУ считается разработанным и достаточно хорошо апробированным на практике [38].

С развитием средств микроэлектроники в сложных СУ все чаще используются внутрисхемные системы диагностики, функционирующие за счет встроенных систем исправления ошибок и сбоев с использованием избыточных кодов. Для решения указанных задач в таких СУ могут быть использованы избыточные коды, которые находят широкое применение в системах обмена данными на канальном уровне семиуровневой модели OSI. Однако, в арифметических элементах (АЭ) таких СУ чаще используются арифметические коды, структура которых хорошо согласуется с архитектурой самих АЭ, выполненных на ПЛИС [27, 28].

Системы тестирования и контроля применяют специальные тестирующие последовательности, с помощью которых оценивается работоспособность элементов тестируемой схемы. Непосредственное использование кодов, разработанных применительно к каналам связи для нужд дискретных устройств обработки информации, ведет к неоправданно большой избыточности и, как следствие, к описанным выше затруднениям. Учет структуры устройств и особенностей их функционирования позволяет более полно и эффективно

использовать вводимую избыточность. При этом часто удобно комбинировать методы структурной и сигнальной избыточности, что позволяет обеспечить требуемую корректирующую способность при меньших затратах оборудования.

Важное значение для проверки работоспособности сложных систем и диагностики отказов имеет тестовый контроль. Построение минимальных или оптимальных в каком-либо отношении тестовых сигналов позволяет существенно сократить время восстановления аппаратуры, сохраняя тем самым ресурс надежности и повышая коэффициент готовности систем.

В разнесенных системах каналы прямой связи и обратной связи между УС и УЭ являются обязательным атрибутом. В подобных системах главное внимание уделяется защите данных, циркулирующих в таких каналах, с использованием кодовых или алгоритмических методов защиты данных от ошибок. Вопрос эксплуатации таких систем близок к проблемам передачи данных по системам связи со всем многообразием деструктивных факторов [10, 22, 37, 92, 101, 115].

Современные подходы к построению СУ выделяют два основных способа организации управления такими системами: диалоговое управление и супервизорное управление. В первом варианте используется голосовая или манипуляционная система передачи команд. В таких системах вероятность ошибки в передаче команд управления в основном зависит от корректности речепреобразующих устройств и действий оператора. Во втором варианте актуальной становится именно защита данных в дискретных последовательностях $M(c)$ и $M(i)$ от ошибок. С точки зрения построения ε -эффективной СУ решение именно этой задачи представляется актуальной.

1.3. Теоретическое обоснование метода перестановочного декодирования

Синтез СУ с использованием принципа супервизирования несомненно должен опираться на ε -эффективные решения в области передачи данных по каналам произвольной физической природы. Наиболее важными элементами разнесенных СУ являются каналы прямой и обратной связи. В этом случае такие

СУ создаются как взаимоувязанные системы информационного потока сигналов управления и телекоммуникаций с использованием элементной базы нового поколения. Становится ясно, что использование перестановочного декодирования отвечает вышеназванному требованию, поскольку позволяет исправлять ошибки, кратность которых равна значению $(n - k)$.

Основой способа перестановочного декодирования является свойство линейных блочных систематических избыточных кодов сохранять свою весовую структуру для различных наборов информационных символов длины k [2, 6, 17, 58, 63, 82, 102].

Если G – порождающая матрица систематического (n, k, d) -кода, то такая матрица по определению имеет k строк и n столбцов, при этом существует всего q^k различных типов возможных столбцов с равным количеством нулей и единиц в отдельно взятом столбце, здесь q – основание кода (наличие нулевого вектора в данном случае учитывается) [57]. Выбирая произвольный порядок перестановки столбцов, можно убедиться в сохранении весовой структуры кода, поскольку в самих столбцах сдвиги по вертикали не производились. Естественно, что в первых k столбцах любого набора перестановок при таком подходе всегда окажется полный набор информационных символов, присущих данному корректирующему коду. Это положение известно из литературы как модулярное представление линейных блочных кодов [47, 59, 63, 93, 106].

В общем случае для двоичных кодов формируется специальная матрица M размерности $k \times (2^k - 1)$. Столбцами этой матрицы являются возможные векторы из k двоичных элементов, исключая нулевой вектор. Тогда отдельно взятый i -й столбец матрицы M рассматривается как столбец типа i , а код может быть задан вектором, образованным $2^k - 1$ возможными в данной информационной системе разрядами (естественно, без учета нулевого вектора). Принципиально перестановки элементов кодовой комбинации осуществляются на основе той или иной концепции. Например, приоритет отдается символам, которые имеют наиболее высокие градации оценок надежности. Чем ближе принятое значение

мягкого решения к математическому ожиданию, тем выше индекс мягкого решения символа. Переставляя символы с наиболее надежными оценками на позиции информационных разрядов, можно сформировать комбинацию эквивалентного кода. Вес такой комбинации будет адекватен весу комбинации исходного кода, и если в комбинации эквивалентного кода произвести обратные перестановки, то комбинация исходного кода и комбинация обратно переставленного кода в точности совпадут. Поразрядное сложение таких комбинаций обеспечит получение нулевого вектора.

Поскольку комбинация исходного кода передается по каналу с помехами, то вероятность искажения символа в такой комбинации зависит от уровня помех в таком канале связи. Комбинация переставленного (эквивалентного) кода не испытывает подобных влияний, и поэтому уровень ошибочных решений символов для нее практически находится на уровне внутренних сбоев процессора приемника. Сравнение двух комбинаций обеспечивает с высокой вероятностью получение вектора ошибок, действовавшего в канале связи.

В работах [30, 58, 63] показано, что если S – любая невырожденная матрица размерности $k \times k$, и если $\mathbf{v}_i$ и $\mathbf{v}_j$ – векторы с k компонентами каждый, то $\mathbf{v}_i S \oplus \mathbf{v}_j S = (\mathbf{v}_i \oplus \mathbf{v}_j) S$, S – есть линейная комбинация строк этой матрицы. Поскольку строки матрицы S линейно зависимы, то $(\mathbf{v}_i \oplus \mathbf{v}_j) S = 0$ тогда и только тогда, когда $(\mathbf{v}_i \oplus \mathbf{v}_j) = 0$ [63]. Поэтому если векторы $\mathbf{v}_i$ и $\mathbf{v}_j$ не совпадают, то не совпадают и векторы $\mathbf{v}_i S$ и $\mathbf{v}_j S$. Следовательно, все $q^k - 1$ строк матрицы $M^T S$ будут различны [56]. Это положение указывает на линейную зависимость порождающих матриц эквивалентных кодов, формируемых на основе порождающей матрицы исходного, основного кода. Задача заключается в том, чтобы выявить закономерности структурных изменений порождающей матрицы исходного кода при ее трансформации в порождающую матрицу эквивалентного кода.

Так как имеется ровно $q^k - 1$ различных ненулевых векторов, то матрица $M^T S$ должна отличаться от матрицы M^T только расстановкой строк [30, 63]

$$M^T S = R M^T, \quad (1.8)$$

где R – некоторая матрица перестановки.

Если S и U – невырожденные матрицы размерности $k \times k$, то

$$M^T S U = R M^T U = R_S R_U M^T, \quad (1.9)$$

т.е. произведению SU соответствует перестановка $R_S R_U$. Отсюда следует, что рассматриваемые перестановки образуют группу, изоморфную (т.е. обладающую той же самой структурой) группе невырожденных матриц размерности $k \times k$ [30, 63]. Выявление подобных закономерностей позволит снизить сложность реализации декодера с O^3 , характерной для подавляющего большинства матричных вычислений, до значения сложности O , соответствующей линейным преобразованиям данных. Актуальность подобного перехода подчеркивается возможностями использования перестановочного декодирования в современных когерентных сетях, для которых характерны противоречия относительно все более и более возрастающих скоростей обмена данными в оптических системах с некоторым запаздыванием технологий по скорости обработки данных в процессорах кодеков таких систем. Одновременно с этим следует указать, что в перспективных когерентных сетях проявляется тенденция использования недвоичных корректирующих кодов, что вызывает необходимость исследования таких кодов для решения задач повышения спектральной и энергетической эффективности указанных систем. В этой связи рассмотрим технологию перестановочного декодирования линейных систематических кодов на примере недвоичного кода Рида-Соломона (РС) более подробно.

В соответствии с теорией линейных преобразований в системе перестановочного декодирования различные порождающие матрицы приводят к модулярным представлениям, которые отличаются той или иной перестановкой [61, 63]. Все операции по преобразованию матрицы того или иного исходного кода выполняются с использованием арифметических действий в двоичных полях Галуа заданной степени расширения. Особенностью таких операций в двоичном поле является однотипность выполнения операций сложения и вычитания по

модулю два. При этом сложение в расширенном поле Галуа выполняется с использованием специальных таблиц сложения [7, 12, 30, 63, 66, 111]. В качестве основного кода РС, на базе которого в работе выполняются все примеры и доказательства, выбран систематический код РС с параметрами (7,3,5). Используя свойства линейности таких кодов, можно утверждать, что все доказанные теоремы для указанного кода будут справедливы для кодов РС с другими параметрами.

Код РС (7,3,5) в качестве порождающей матрицы имеет матрицу следующего вида

$$G = \begin{pmatrix} \alpha^0 & 0 & 0 & \alpha^4 & \alpha^0 & \alpha^4 & \alpha^5 \\ 0 & \alpha^0 & 0 & \alpha^2 & \alpha^0 & \alpha^6 & \alpha^6 \\ 0 & 0 & \alpha^0 & \alpha^3 & \alpha^0 & \alpha^1 & \alpha^3 \end{pmatrix}, \quad (1.10)$$

1 2 3 4 5 6 7

где α^j – примитивный элемент поля $GF(2^3)$, при этом вводятся нумераторы столбцов, которые показаны ниже матричного поля.

Пусть задана произвольная перестановка вида

$$r = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 7 & 2 & 3 & 1 & 5 & 6 \end{pmatrix}. \quad (1.11)$$

Перестановке вида (1.11) соответствует матрица перестановок R .

$$R = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}. \quad (1.12)$$

Для выполнения обратной перестановки нумераторов используется транспонированная матрица R^T . Из структуры матриц R и R^T заметно, что

сложность выполнения процедуры умножения вектора нумераторов на матрицу перестановки из-за размерности нулевого пространства указанных матриц может быть оценена на уровне O . Результатом перестановки матрицы G является переставленная матрица G_{nep} вида

$$G_{nep} = \begin{pmatrix} \alpha^4 & \alpha^5 & 0 & 0 & \alpha^0 & \alpha^0 & \alpha^4 \\ \alpha^2 & \alpha^6 & \alpha^0 & 0 & 0 & \alpha^0 & \alpha^6 \\ \alpha^3 & \alpha^3 & 0 & \alpha^3 & 0 & \alpha^0 & \alpha^1 \end{pmatrix}. \quad (1.13)$$

4 7 2 3 1 5 6

Дальнейшая технология преобразования матрицы G_{nep} в систематическую форму будет описана схематически. В последующих разделах конкретные примеры позволят выявить тонкую структуру технологии.

В выражении (1.13) выделяют первые три столбца с нумераторами 4, 7 и 2. Указанные столбцы формируют промежуточную квадратную матрицу Q . В общем случае размерность такой матрицы $k \times k$. Далее для матрицы Q отыскивается обратная матрица Q^{-1} , и, поскольку $Q \times Q^{-1} = E$, то именно матрица Q^{-1} становится ключевой для формирования систематической формы матрицы G_{nep} . Другими словами, по структуре матрицы Q^{-1} выполняются арифметические действия с элементами G_{nep} для получения $G_{nep}^{cис}$. Именно эта последовательность вычислений по сложности реализации оценивается на уровне O^3 . Действительно, необходимо найти определитель Δ матрицы Q , после чего для этой матрицы вычислить матрицу миноров U_Q . Затем вычислить частное $Q^{-1} = U_Q^T / \Delta$. Учитывая, что все арифметические действия выполняются в расширенном двоичном поле Галуа, становится ясно, почему перестановочное декодирование не используется в реальных системах.

Пример 1.2. Пусть источник информации передает вектор $\alpha^1 \ \alpha^2 \ \alpha^3$. В результате умножения этого вектора на порождающую матрицу кода РС из выражения (1.10) будет получен вектор $\alpha^1 \ \alpha^2 \ \alpha^3 \ \alpha^2 \ \alpha^6 \ \alpha^3 \ \alpha^1$. Пусть

надежными символами оказались недвоичные символы комбинации с нумераторами 2, 4 и 6. Пусть оставшиеся символы распределились в порядке 1, 3, 5 и 7. Декодер на основании этого формирует переставленную матрицу вида

$$G_{nep} = \begin{pmatrix} 0 & \alpha^4 & \alpha^4 & \alpha^0 & 0 & \alpha^0 & \alpha^5 \\ \alpha^0 & \alpha^2 & \alpha^6 & 0 & 0 & \alpha^0 & \alpha^6 \\ 0 & \alpha^3 & \alpha^1 & 0 & \alpha^0 & \alpha^0 & \alpha^3 \end{pmatrix}.$$

2 4 6 1 3 5 7

Матрица Q в этом случае имеет вид

$$Q = \begin{pmatrix} 0 & \alpha^4 & \alpha^4 \\ \alpha^0 & \alpha^2 & \alpha^6 \\ 0 & \alpha^3 & \alpha^1 \end{pmatrix}.$$

Определитель этой матрицы $\Delta = \alpha^5 \oplus \alpha^0 = \alpha^4$. Далее в соответствии с концепцией поиска обратной матрицы Q^{-1} необходимо вычислить матрицу миноров A_M .

$$A_M = \begin{pmatrix} \begin{vmatrix} \alpha^2 & \alpha^6 \\ \alpha^3 & \alpha^1 \end{vmatrix} & \begin{vmatrix} \alpha^0 & \alpha^6 \\ 0 & \alpha^1 \end{vmatrix} & \begin{vmatrix} \alpha^0 & \alpha^2 \\ 0 & \alpha^3 \end{vmatrix} \\ \begin{vmatrix} \alpha^4 & \alpha^4 \\ \alpha^3 & \alpha^1 \end{vmatrix} & \begin{vmatrix} 0 & \alpha^4 \\ 0 & \alpha^1 \end{vmatrix} & \begin{vmatrix} 0 & \alpha^4 \\ 0 & \alpha^3 \end{vmatrix} \\ \begin{vmatrix} \alpha^4 & \alpha^4 \\ \alpha^2 & \alpha^6 \end{vmatrix} & \begin{vmatrix} 0 & \alpha^4 \\ \alpha^0 & \alpha^6 \end{vmatrix} & \begin{vmatrix} 0 & \alpha^4 \\ \alpha^0 & \alpha^2 \end{vmatrix} \end{pmatrix} = \begin{pmatrix} \alpha^5 & \alpha^1 & \alpha^3 \\ \alpha^4 & 0 & 0 \\ \alpha^4 & \alpha^4 & \alpha^4 \end{pmatrix}.$$

Тогда

$$A_M^T = \begin{pmatrix} \alpha^5 & \alpha^4 & \alpha^4 \\ \alpha^1 & 0 & \alpha^4 \\ \alpha^3 & 0 & \alpha^4 \end{pmatrix}.$$

Отсюда

$$Q^{-1} = \frac{Q}{\Delta} = \begin{pmatrix} \alpha^1 & \alpha^0 & \alpha^0 \\ \alpha^4 & 0 & \alpha^0 \\ \alpha^6 & 0 & \alpha^0 \end{pmatrix}.$$

Вид матрицы Q^{-1} говорит о том, что для получения порождающей матрицы эквивалентного кода в систематической форме необходимо умножить поочередно строки матрицы $G_{пер}$ на соответствующие элементы строк вычисленной матрицы Q^{-1} . Первую строку из матрицы $G_{пер}$ необходимо умножить на элемент α^1 , вторую строку матрицы $G_{пер}$ – умножить на элемент α^0 и по аналогии третью строку необходимо умножить на α^0 , полученные таким образом результаты необходимо сложить [60, 65].

$$\oplus \begin{array}{cccccccc} 0 & \alpha^4 & \alpha^4 & \alpha^0 & 0 & \alpha^0 & \alpha^5 & \times \alpha^1 \\ \alpha^0 & \alpha^2 & \alpha^6 & 0 & 0 & \alpha^0 & \alpha^6 & \times \alpha^0; \\ 0 & \alpha^3 & \alpha^1 & 0 & \alpha^0 & \alpha^0 & \alpha^3 & \times \alpha^0 \end{array}$$

$$\oplus \begin{array}{cccccccc} 0 & \alpha^5 & \alpha^5 & \alpha^1 & 0 & \alpha^1 & \alpha^6 & \\ \alpha^0 & \alpha^2 & \alpha^6 & 0 & 0 & \alpha^0 & \alpha^6 & \\ 0 & \alpha^3 & \alpha^1 & 0 & \alpha^0 & \alpha^0 & \alpha^3 & . \\ \text{Итого} & \alpha^0 & 0 & 0 & \alpha^1 & \alpha^0 & \alpha^1 & \alpha^3 \end{array}$$

Для получения второй строки порождающей матрицы переставленного кода в систематической форме необходимо умножить первую строку матрицы $G_{пер}$ на α^4 из матрицы Q^{-1} , а третью строку из $G_{пер}$ необходимо умножить на α^0 из второй строки и третьего столбца матрицы Q^{-1} , результаты сложить.

$$\oplus \begin{array}{cccccccc} 0 & \alpha^1 & \alpha^1 & \alpha^4 & 0 & \alpha^4 & \alpha^2 & \\ 0 & \alpha^3 & \alpha^1 & 0 & \alpha^0 & \alpha^0 & \alpha^3 & \\ \text{Итого} & 0 & \alpha^0 & 0 & \alpha^4 & \alpha^0 & \alpha^5 & \alpha^5 . \end{array}$$

Для образования последней третьей строки матрицы эквивалентного кода в систематической форме необходимо первую строку переставленной матрицы $G_{пер}$ умножить на α^6 , третью строку взять без изменений ($\alpha^0 = 1$), результаты сложить.

$$\begin{array}{rccccccc}
& & 0 & \alpha^3 & \alpha^3 & \alpha^6 & 0 & \alpha^6 & \alpha^4 \\
\oplus & & 0 & \alpha^3 & \alpha^1 & 0 & \alpha^0 & \alpha^0 & \alpha^3 \\
Итого & & 0 & 0 & \alpha^0 & \alpha^6 & \alpha^0 & \alpha^2 & \alpha^6
\end{array}$$

По результатам приведенных вычислений получается матрица эквивалентного кода $G_{пер}^{сис}$

$$G_{пер}^{сис} = \begin{pmatrix} \alpha^0 & 0 & 0 & \alpha^1 & \alpha^0 & \alpha^1 & \alpha^3 \\ 0 & \alpha^0 & 0 & \alpha^4 & \alpha^0 & \alpha^5 & \alpha^5 \\ 0 & 0 & \alpha^0 & \alpha^6 & \alpha^0 & \alpha^2 & \alpha^6 \end{pmatrix}.$$

Умножение информационной части переставленного вектора $\alpha^1 \ \alpha^2 \ \alpha^3$ на выше приведенную матрицу приводит к вектору эквивалентного кода РС вида $\alpha^2 \ \alpha^2 \ \alpha^3 \ \alpha^1 \ \alpha^3 \ \alpha^6 \ \alpha^2$. Обратная перестановка нумераторов столбцов приводит к исходному вектору, отправленному по каналу связи. Заметно, что в системе перестановочного декодирования не используется одно замечательное свойство. В этой системе существует два типа процессов: во-первых, случайная составляющая процесса, которая зависит от произвольного выбора источником сообщений той или иной комбинации используемого в системе кода, и природа помех в канале связи носит стохастический характер и не может быть определена априори. Во-вторых, детерминированный процесс, который заключается в том, что допустимые перестановки надежных символов могут быть вычислены заранее, и соответствующие матрицы $G_{пер}^{сис}$ для таких выявленных перестановок допустимо хранить в памяти декодера. В общем случае процесс перестановочного декодирования для блочных кодов можно представить в виде выражения

$$Pd(t) = \begin{cases} Rn(t) = I(t) + C(t); \\ P(t). \end{cases} \quad (1.14)$$

В выражении (1.14) введены следующие обозначения: $Rn(t)$ – случайная составляющая процедуры декодирования, которая включает в себя случайный процесс $I(t)$ выбора источником информации кодового слова, семантически

отвечающего передаваемому сообщению, и случайный процесс $C(t)$ влияния помех в используемом системой передачи данных канале связи на физическом уровне. Параметр $P(t)$ соответствует детерминированной составляющей процесса декодирования.

Суть процесса $P(t)$ заключается в следующем. Пусть в ходе работы процессора приемника в момент времени t_1 образовалась перестановка нумераторов столбцов вида $p1(t_1)$, и для такой перестановки декодер выполнил все действия, связанные с поиском обратной матрицы $Q^{-1}(t_1) = U_Q^T / \Delta$ с последующим вычислением матрицы $G_{nep}^{cuc}(t_1)$, при этом на производство вычислений было затрачено время Δt_1 . В ходе передачи данных может возникнуть ситуация, когда перестановка нумераторов столбцов может повториться в некоторый произвольный и дискретный момент времени t_i при $i > 1$. В соответствии с существующей концепцией перестановочного декодирования систематических блочных кодов декодер выполняет действия $Q^{-1}(t_i) = U_Q^T / \Delta \equiv Q^{-1}(t_1)$ с образованием $G_{nep}^{cuc}(t_i) \equiv G_{nep}^{cuc}(t_1)$. В подобной ситуации процессор приемника работает крайне непроизводительно [31].

На этом фоне возникает несколько научных задач:

- возможно ли запомнить результат вычисления матрицы $G_{nep}^{cuc}(t_1)$ в оперативной памяти процессора приемника и использовать его в случае повторения перестановки нумераторов столбцов в i -й момент времени;
- возможно ли использование когнитивных методов обработки данных в декодере приемника, когда перестановочный декодер на первых этапах обработки данных действует в соответствии с классической концепцией, но запоминает результаты обработки текущих перестановок нумераторов столбцов и гибко использует эти результаты по мере их накопления в оперативной памяти;

- возможно ли получение результатов перестановок нумераторов столбцов за счет внешних вычислительных ресурсов и введение их в память декодера на этапе его предварительной подготовки к работе;
- возможно ли хранить в оперативной памяти процессора приемника весь объем возможных результатов оценки перестановок нумераторов столбцов;
- каким образом должна быть организована память хранения результатов перестановок в целях быстрого и результативного поиска требуемой в текущий момент времени перестановки.

1.4. Общие принципы мягкого декодирования помехоустойчивых кодов

Одной из актуальных задач современных средств робототехники, контроля сложных технологических процессов и дистанционного управления необитаемыми аппаратами является обеспечение качества управления. В СУ, предназначенных для подобных целей, применение длинных кодов ограничивается продолжительностью цикла управления. Поэтому для достижения требуемых характеристик в системах реального времени при использовании коротких кодов необходимо комплексное применение средств обработки сигналов, способных формировать индексы надежности в формате мягких решений символов (MPC), комбинирования кодов и использования итеративных процедур декодирования для полного использования введенной в код избыточности, что особенно важно не только для однонаправленных систем обмена данными. Мягкие методы обработки данных активно используются в когерентных сетях для реализации каскадных методов повышения достоверности данных, когда на первой ступени декодирования данных применяется сверточный код, а на второй ступени код РС [15, 42, 70, 76, 80]. Для сверточного декодера применяется мягкий алгоритм Витерби, позволяющий снизить вероятность ошибки 10^{-2} - 10^{-3} на бит до значения 10^{-4} - 10^{-7} на бит [61]. Применение кода РС на второй ступени декодирования доводит этот показатель до значения 10^{-12} .

Недостатком указанного подхода к повышению достоверности данных является продолжительность процедуры декодирования сверточного кода по алгоритму Витерби, когда декодер просматривает принятую последовательность на несколько десятков шагов вперед и только после этого, возвращаясь назад, на основе мягких решений декодирует просмотренные биты в последовательность недвоичных символов кода РС [98, 109]. Противоречие заключается в том, что скорость поступления информации из когерентного канала достигает высоких значений (в субканале порядка 25 Гбит/с для системы с групповой скоростью 100 Гбит/с), а скорость обработки данных в декодере имеет ограничения, связанные с технологией практического применения программируемых логических интегральных схем (ПЛИС). Традиционное использование кодов РС на второй ступени декодирования только усиливает высказанное противоречие [106, 109]. Кроме того, мягкие методы формирования мягких решений в основном ориентированы на двоичные сигналы, а в когерентных сетях однозначно используются сложные виды модуляции QPSK и КАМ, для которых система выработки МРС требует своего разрешения. Кроме того, выработка МРС для сложных сигналов ограничивает применение алгоритма Витерби, поскольку эффективные алгоритмы декодирования сверточных кодов главным образом ориентированы на двоичные последовательности. Таким образом, возникает актуальная задача согласования все возрастающих скоростей передачи данных в оптических системах с некоторыми ограничениями по скорости обработки данных в ПЛИС. Без рациональной технологии ранжирования жестких решений двоичных и недвоичных символов по показателям МРС методы перестановочного декодирования теряют свой смысл. Поэтому совершенствование мягких методов обработки помехоустойчивых кодов является наиболее перспективной тенденцией в данном направлении. Требуется такой арсенал алгоритмов мягкого декодирования, который бы удовлетворял требованиям и возможностям не только двоичных избыточных кодов, но и носил бы универсальный характер применительно к сложным видам модуляции.

Кроме систем обмена данными в современных условиях методы мониторинга окружающей среды объективно приобретают возрастающее значение. По мере освоения этой предметной области указанные технологии становятся важным приложением для развития технологий информационно-измерительных и управляющих систем на базе сенсорных сетей. Обеспечение естественных пространств разнородными микродатчиками становится материальным носителем информационной среды, которую трудно или даже невозможно оценить традиционными средствами. Непосредственная связь датчиков с физической средой позволяет получать от них локализованную и подробную информацию в реальном масштабе времени, что является важным во многих практических приложениях.

За редким исключением элементы сенсорных сетей оказываются энергозависимыми из-за ограниченного срока действия питающих элементов. Средства радиоинтерфейса элементов сенсорных сетей с хорошо продуманными стеками протоколов позволяют реализовать передачу данных с использованием подходящих сетевых технологий. Это позволяет продлить ресурс элементов питания. Тем не менее неизбежная процедура замены таких элементов на сенсорных датчиках представляется трудной задачей, растянутой во времени, что непродуктивно.

По этой причине в ряде работ предлагается использовать датчики, которые работают в режиме накопления информации. При этом они способны статистически обрабатывать полученные данные, хранить их в своей памяти и быть готовыми передать информацию по команде с мобильного модуля сбора подобных данных на его борт. Наиболее очевидным решением подобной задачи является использование беспилотных средств, действующих по заданной программе. Сокращение ресурсов на трансляцию данных, реализация режима краткой работы передатчика сенсорного узла на передачу накопленных данных и гибкость протокола обмена данными решают задачу продления срока действия элементов питания таких узлов. В этом случае использование помехоустойчивых

кодов обеспечивает повышение энергетической эффективности систем обмена данными в сенсорных сетях.

Вместе с этим по многим причинам возникает задача защиты данных от ошибок при использовании радиоинтерфейса. Использование в подобных ситуациях помехоустойчивых кодов становится объективной реальностью. Известно, что именно восстановление данных в декодере избыточного кода является наиболее сложной задачей. Поэтому либо на мобильной платформе, либо на сервере сенсорной сети эта задача может быть решена наиболее эффективным методом без учета ограничений на ресурсы по питанию. В любом случае физический уровень системы обмена данными (по сути непрерывный канал связи в структурной схеме такой системы) считается тем элементом, на базе которого формируются МРС.

В основе математической модели непрерывного канала связи находятся множество наборов передаваемых сигналов (алфавит) $v \in V$ и множество случайных или преднамеренных помеховых факторов (помех) $e \in E$, которые расширяют мощность алфавита V до значений множества Z и условного распределения вероятностей $P(v|z)$. При этом основой топологического пространства представленных моделей является множество вещественных чисел [75, 105]. Для большинства моделей СУ из алфавита Z необходимо выделить алфавит разрешенных сигналов. При $z \notin Z$ сигналы необходимо считать неопределенными. Алгоритм фиксации символов в такой системе интерпретируется как канонический канал со стиранием элементов. На выходе этого канала создаются дополнительные решения вида s_i . Для идеального стирающего канала решения, представленные как s_i , сопровождаются условиями, определяющими, что $z \notin Z$. Эти условия могут меняться по усмотрению конструктора для достижения требуемого уровня вероятности ошибки на бит. Модель такого канала является примитивным примером мягкого декодирования и подробно рассмотрена во многих научных трудах [23, 30, 38, 52, 66, 92]. В условиях развития системы цифровой обработки сигналов модель стирающего

канала связи трансформировалась в модель не с одним альтернативным решением: стирать или не стирать, а с несколькими решениями λ_i , указывающими на сколько z уклонилось от установленных граничных значений. Степень уклонения оценивают через МРС, которое формируется на выходе физического уровня и передается на дальнейшую обработку через первый (нижний) подуровень канального уровня эталонной модели взаимодействия открытых систем. Они являются более тонкими оценками в сравнении с решениями, представленными в виде $s_i \cup \bar{s}_i$, что соответствует условиям формирования ε -оптимальных систем. Характеристики оценок s_i и λ_i напрямую зависят от свойств физического уровня, определяемых конкретной системой каналообразования: оптика, радио в широком смысле или проводной канал связи.

Главными рабочими характеристиками системы обмена данными являются высокая скорость трафика (основная характеристика для конечного пользователя) и минимальная временная задержка транслируемых данных. При этом в обязательном порядке требуется достижение необходимого уровня по достоверности обрабатываемой в нем информации. На основе решений вида s_i или показаний λ_i может быть сформирована функция вида $F\{\bullet\}$. Итеративные преобразования значений λ_i совместно с кодовыми методами повышения достоверности позволяют добиться необходимого эффекта по обеспечению требуемых значений вероятности ошибки на бит, но это требует временных затрат как для кодов с малой плотностью проверок на четность [43, 166, 188, 191, 205], так и для методов многопорогового декодирования [82, 83, 84, 85]. При этом достигается не только необходимая корректирующая способность системы обмена данными, но и объективная простота реализации системы декодирования.

В любом случае по асимптотическим оценкам мягкое декодирование любых избыточных кодов дает энергетический выигрыш кода в пределах 3 дБ [30]. При этом важное значение уделяется принципам формирования мягких решений как в системе двоичного кодирования, так и в системе применения недвоичных кодов. Центральной задачей формирования МРС является хорошая корреляция низких

значений МРС с ошибочными символами. При равенстве указанного параметра единице в системе формируется классический стирающий канал связи, который обеспечивает снижение сложности декодирования данных, поскольку не требуется осуществлять операцию по вычислению локаторов ошибок. Известные способы формирования МРС не обеспечивают данного требования. Например, в гауссовском канале связи формирование МРС в пределах от математического ожидания до значения, по крайней мере, равного 3σ не обеспечивает низких ожидаемых значений вероятности ошибки при формировании МРС с высоким показателем. Действительно, вероятность ошибки на бит в таком канале связи может быть определена как

$$p(\lambda_i) = \frac{1}{\sqrt{2\pi\sigma^2}} \int_{\sqrt{E_b}}^{3\sigma} e^{-\frac{(x-\sqrt{E_b})^2}{2\sigma^2}} dx \neq 0, \quad (1.15)$$

где E_b – энергия сигнала на бит, σ – среднее квадратическое отклонение значения обрабатываемого демодулятором случайного из-за гауссовских помех сигнала x [30, 66]. Аналитическое моделирование подобного процесса показывает, что при очень высоких отношениях сигнал-шум порядка 10 дБ вероятность ошибочной регистрации символа с высоким значением МРС составляет 10^{-9} , т.е. не является бесконечно малой величиной. При очень низких отношениях параметра сигнал-шум вероятность регистрации жесткого решения, сопровождаемого высоким значением МРС, возрастает до значения 10^{-3} . Именно это явление снижает результативность применения мягких методов обработки помехоустойчивых кодов. Указанная модель справедлива для двоичных кодов, и переход к моделированию процедуры формирования МРС для недвоичных кодов принимает более сложный характер, поскольку в сложных системах модуляции возрастает сложность реализации устройств, формирующих МРС. Таким образом, существует вероятность неправильного декодирования принятой приемником информации в условиях, когда в группу надежных символов будет отобран ошибочный символ с высоким значением МРС. Вероятность подобного исхода для двоичных кодов и описанных условий будет определяться выражением (1.15)

с учетом значений параметра отношения сигнал-шум (ОСШ). Задача выработки адекватных принципов вычисления МРС для недвоичных кодов, в частности кодов РС, становится более сложной в условиях применения модуляции типа QPSK и КАМ. Решение подобной задачи требует специального изучения и построения специальных моделей формирования МРС в таких системах.

Несколько усложняя процесс перестановочного декодирования, можно использовать комбинированные методы оценки надежности переставленных символов за счет, например, списочного декодирования на основании лексикографических разбиений пространства кодовых векторов, но глубокая проработка подобной задачи представляет отдельную проблему, решение которой выходит за рамки целевой установки данной работы.

1.5. Мягкое декодирование как декодирование в целом

В работах по общей теории связи [66, 69, 72], относящихся к описанию процедуры декодирования комбинаций блоковых кодов или последовательностей непрерывных помехоустойчивых кодов, подчеркивается, что методы мягкого декодирования избыточных кодов обеспечивают более низкие значения вероятности ошибочного декодирования относительно систем без кодирования данных или систем с классическим жестким декодированием на основе алгебраических подходов к выявлению ошибок.

В любом случае сопровождение жестких решений полученными на физическом уровне значениями МРС позволяет использовать не просто систему уравнений, связанных с проверочной матрицей конкретного кода, а применять вариативную схему повышения достоверности данных, получившую название метод «распространения доверия» от английского «belief propagation» [61]. Не определяя методику образования МРС для символов недвоичного кода, можно указать, что в системе перестановочного декодирования возможно образование двух последовательностей в результате сортировки таких символов по значениям

МРС. Пусть в результате приема данных на канальном уровне была сформирована последовательность МРС вида

$$\lambda_1 \lambda_2 \bar{\lambda}_3 \lambda_4 \lambda_5 \dots \lambda_k \dots \lambda_{k+1} \dots \bar{\lambda}_{n-1} \lambda_n, \quad (1.16)$$

в которой данные, представленные с надсимвольной чертой, приняты ошибочно. На втором этапе в результате сортировки МРС пусть выполняется условие, когда образуется последовательность

$$\lambda_4 \geq \lambda_5 \geq \lambda_{k+2} \geq \lambda_6 \geq \lambda_k \geq \dots \geq \bar{\lambda}_3 \geq \dots \geq \bar{\lambda}_{n-1} \geq \dots \geq \bar{\lambda}_7 \geq \lambda_2. \quad (1.17)$$

Пусть по результатам сортировки данных из выражения (1.17) среди k первых символов оказались надежными символы вида $\lambda_4 \geq \lambda_5 \geq \lambda_{k+2} \geq \lambda_6 \geq \lambda_k$. В этот набор не попал ни один ошибочный символ. Естественно, что процедура перестановочного декодирования при данной сортировке будет завершена успешно.

Пусть в новых условиях сортировка данных привела к результату, когда среди k разрядов оказались ошибочные символы. В этом случае перестановочный декодер оценивает ситуацию вида $\lambda_4 \geq \lambda_5 \geq \lambda_{k+2} \geq \bar{\lambda}_3 \geq \lambda_k$, что однозначно приведет к ошибочному результату декодирования. Для минимизации вероятности подобного исхода принципиально важно корректно формировать значения МРС, а в принятом кодовом векторе целесообразно формировать максимальное число стертых позиций по результатам анализа значений λ_i .

Пусть P_{oui} – вероятность ошибочного декодирования принятого кодового вектора. Тогда

$$P_{oui} = \sum_{i=j=0}^S P_i \bar{P}_j + \sum_{i=S+1}^n P_i, \quad (1.18)$$

где P_i – вероятность появления таких значений МРС, которые в алгоритме перестановочного декодирования считаются ненадежными и стираются, а $\bar{P}_j$ – вероятность появления ошибочных решений при наличии ровно i стираний. Принципиально декодер может формировать различное число стираний.

Представим систему, в которой число стираний всегда формируется на границе метрики Хэмминга и равно $S = d_{\min} - 1$, где $d_{\min}$ – минимальное расстояние используемого в системе кода. Пусть в этих условиях вероятность ошибочного декодирования имеет значение P_{d-1} , тогда $P_{oui} > P_{d-1}$. Действительно, в подобных условиях формирование максимально возможного числа стираний на длине кодового вектора приводит к тому, что большая часть ненадежных решений коррелирует с ошибочными символами, что приводит к повышению вероятности правильного приема данных. Именно такой способ обработки данных реализуется в системе перестановочного декодирования, когда отбор ровно k надежных символов автоматически приводит к выполнению условия $P_{oui} > P_{d-1}$, что соответствует условиям формирования ε -оптимальных систем, но методы формирования МРС в этом случае требуют тщательного анализа и изучения [21, 53]. Это особенно важно для вычислительных процессов, в результате которых формируются МРС для недвоичных символов.

По сути, любой метод формирования МРС и их последующее использование в двоичном симметричном канале связи приводит к модели классического канала связи со стиранием элементов. Действительно, использование значений из выражения (1.16) по принципу выявления локаторов ошибок в последующем приводит к использованию в процедуре декодирования только надежных символов.

Исключение составляют итеративные методы повышения достоверности, которые, используя байесовский принцип оценки апостериорных вероятностей, позволяют повысить значения отдельных МРС исходя из заданных кодом проверочных соотношений жестких решений символов [30, 61, 97, 104]. Подобный метод оказался продуктивным в системе турбокодов [61], но не может быть использован в системах с ограниченным циклом управления, поскольку окончательный результат зависит от числа выполненных итераций.

В ряде работ для систем недвоичных кодов предлагается использовать комплекс оценок, включающих проверку на четность в системе внутреннего кода

при использовании каскадных схем кодирования, оценку математического ожидания МРС, принятых на длине одного символа, и значений дисперсии этих МРС. В данном случае используется принцип $\max\min$ для выработки комплексной оценки МРС недвоичного символа [30, 33, 48]. Принципиально такой подход не требует больших временных затрат, поскольку указанные параметры могут быть оценены на длине недвоичного символа практически вслед за его обработкой в демодуляторе. Недостатками метода являются его применение преимущественно к двоичным методам модуляции и сложность выработки комплексного решения по этим параметрам на длине всего кодового вектора.

Выработка предложений для реализации относительно простых методов вычисления МРС недвоичных символов применительно к сложным видам модуляции, оценка их вероятностных характеристик и методов реализации требуют специального исследования.

1.6. Моделирование когнитивной метафоры в технических системах

Наличие в системе перестановочного декодирования условий вида (1.14) позволяет утверждать, что детерминированную составляющую в системе обработки данных целесообразно запоминать. По сути эту составляющую декодер может вычислять в ходе своей работы и запоминать результат, что соответствует принципам обучения системы декодирования полученным данным и соответствует концепции когнитивной обработки данных [50].

К искусственным когнитивным системам (ИКС) (небиологическим системам) принято относить технические структуры большей сложности, обладающие группой специфических функций. К таким функциям целесообразно отнести:

- целевую функцию – обмен данными между выраженными частями технической структуры средствами цифровых или аналоговых форматов для быстрого и эффективного решения практических задач;

- функцию регулирования – сравнение данных реального времени с данными диагностики и реализации процедуры когнитивного регулирования и когнитивной адаптации;
- функцию моделирования – система взаимоувязанных семантических моделей для усваивания новых связей между актуальными событиями внешней среды;
- функцию адаптации – для реализации процедуры когнитивной адаптации.

Структура ИКС может быть представлена в отдельных взаимоувязанных блоках, реализующих указанные функции. На рисунке 1.3 показан объект, которым, применительно к теме диссертации, является мягкий декодер, реализующий принцип перестановочного декодирования вместе с непрерывным каналом связи. Сенсорная плоскость получает данные от объекта и на основе этого через блок диагностики и блок адаптации формирует когнитивную модель поведения. Принципиально это означает, что указанный блок отыскивает аналоги ситуации, встречавшиеся ранее в работе системы, и на основе этого принимает решение о структуре когнитивной модели.

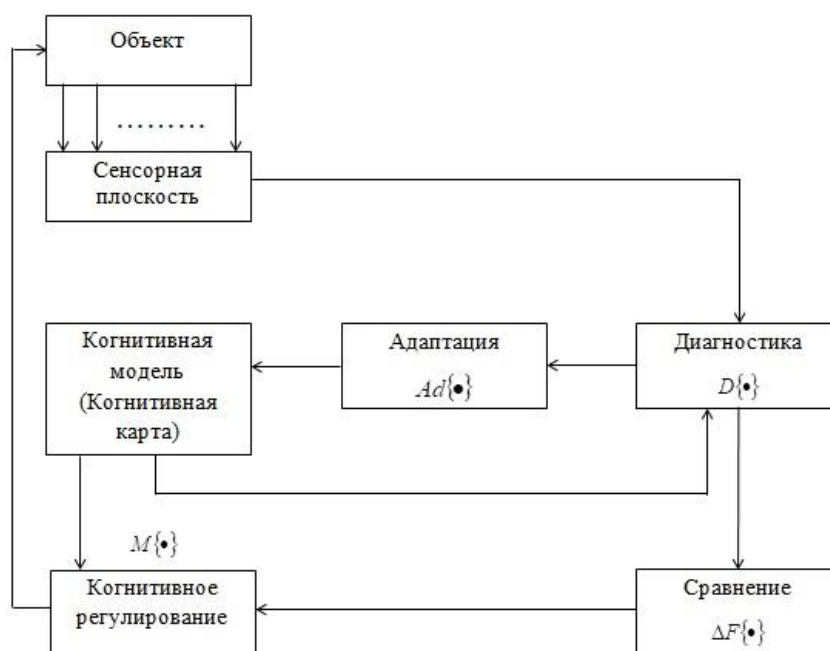


Рисунок 1.3 – Структура искусственной когнитивной системы

В случае отсутствия аналогов блок адаптации вырабатывает совершенно новое решение, которое запоминается когнитивной картой ИКС. Если объем

решений ограничен, то данные записываются и хранятся в когнитивной карте. В системе перестановочного декодирования такими решениями могут быть вычисленные образцы порождающих матриц эквивалентных кодов $G_{пер}^{cuc}$, соответствующих тем или иным перестановкам нумераторов столбцов порождающей матрицы исходного кода G .

Блоки сравнения и когнитивного регулирования ИКС оценивают степень достижения системой заданной целевой функции.

Архитектура ИКС находится в полной зависимости от среды ее функционирования и связывается с этой средой через сенсорную плоскость, при этом результат обработки данных этой плоскости отражается в когнитивной карте КС, являющейся неотъемлемой частью когнитивной модели. В данном случае знания следует трактовать как связь между событиями.

Пример 1.1 убедительно показывает, что результат вычисления матрицы, который по идеологии построения ИКС должен храниться в памяти когнитивной карты системы, избавляет декодер от проведения серии матричных вычислений сложности O^3 , и если с сенсорной плоскости поступают данные о перестановке нумераторов столбцов матрицы G в формате 2 4 6 1 3 5 7, то из когнитивной карты извлекается готовый результат в виде $G_{пер}^{cuc}$. В последующем целесообразно вместо обозначения вида $G_{пер}^{cuc}$ использовать символику в формате $G_{246\ 1357}$, чтобы отличать одну перестановку нумераторов от другой с иным расположением нумераторов. При этом обозначение матрицы вида $G_{xxx\ xxxx}$ всегда связывается с систематической матрицей эквивалентного кода.

Таким образом, предложенная схема впервые в практике построения систем помехоустойчивого кодирования описывает когнитивный процесс на канальном уровне, который отличается от известных систем с когнитивной метафорой, используемых, например, в когнитивном радио [50]. Одновременно с этим предложенная схема не отрицает применения когнитивных принципов на физическом уровне. Поскольку перестановочное декодирование оперирует МРС,

получаемыми на основе непрерывного канала связи, то целесообразность реакции процедуры формирования таких МРС на изменения параметра сигнал-шум или процесса группирования ошибок сохраняется.

Когнитивная модель функционирования технической системы основывается на принципах процедуры обучения, предполагающей, что различные факторы внешней среды и сопутствующие им признаки развиваются в результате реакции сенсоров системы (сенсорной плоскости) на внешние условия [50]. В общем случае происходит последовательная обработка сенсорной информации с последующим ее перекомпилированием и закреплении «удачных» гипотез, и удалением «неудачных» вариантов таковых по частоте их успешного применения [1]. «Неудачные» варианты могут появиться в системе перестановочного декодирования двоичных кодов, для которых выделенная матрица Q не всегда отвечает условиям невырожденности. Недвоичные коды РС являются максимально декодируемыми, поэтому подобное условие для них не проверяется.

1.7. Выводы по главе и постановка задачи на исследование

1. Идея использования средств помехоустойчивого кодирования для контроля качества работы отдельных функциональных элементов, схем и устройств вычислительной техники носит давний характер, но практического развития не получила из-за высокой себестоимости и роста дополнительных схемных издержек на систему контроля. Однако, в системах с разнесенными управляющим и управляемым элементами приобретает особую актуальность в связи с развитием робототехники. Именно это направление требует новых методов анализа и синтеза систем управления с целью улучшения их технических характеристик.

2. Вероятность внутрисистемных сбоев элементов СУ по сравнению с влиянием деструктивных факторов в каналах связи СУ чрезвычайно мала. Поэтому применение избыточных кодов в системах защиты данных от ошибок оправдано с прагматической точки зрения. При этом наибольший эффект

достигается от применения системы эквивалентных кодов, обеспечивающих наибольший ЭВК.

3. В основе перестановочного декодирования лежат мягкие методы обработки данных. В этой связи актуальной остается задача формирования мягких решений двоичных символов, максимально коррелированных с помехой. Это позволит снизить ошибку декодирования комбинаций эквивалентного кода и избежать ошибочных решений в процедуре перестановочного декодирования.

4. Требуется детализация технологии формирования МРС для недвоичных кодов, которая должна основываться на дополнительном изучении и апробации различных аналитических и имитационных моделей.

В связи со сказанным актуальность темы диссертационной работы обусловлена наличием следующих нерешенных задач:

- отсутствием разработанных научных подходов к организации алгоритмов систем управления на базе сокращенных циклов декодирования недвоичных помехоустойчивых кодов;
- отсутствием методов применения когнитивных принципов в искусственных технических системах и, в частности, в системах управления;
- отсутствием моделей когнитивной адаптации в системе формирования мягких решений недвоичных символов.

Для достижения указанной цели в диссертационной работе необходимо решить следующие задачи:

- выполнить анализ известных методов защиты команд управления в системе информационно-управляющих комплексов (в том числе реального времени) и выявить их достоинства и недостатки;
- доказать исключительную возможность когнитивной обработки данных команд управления в системе их защиты от влияния мешающих факторов в системе перестановочного декодирования;
- решить задачу моделирования разработанных алгоритмов формирования мягких решений символов блочных кодов недвоичных избыточных кодов и на

основе испытаний имитационных моделей доказать целесообразность использования метода правдоподобий;

– доказать корректность разработанной системы быстрых матричных преобразований порождающей матрицы эквивалентных кодов, предложить структурную схему декодера таких кодов и разработать функциональную схему узла преобразованных эталонных матриц в матрицу эквивалентного кода.

ГЛАВА 2. ИССЛЕДОВАНИЕ МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ И МЕТОДОВ ФОРМИРОВАНИЯ МЯГКИХ РЕШЕНИЙ СИМВОЛОВ НЕДВОИЧНЫХ КОДОВ

2.1. Особенности применения программируемых логических интегральных схем в системе обработки недвоичных кодов

В современных телекоммуникационных системах за счет реальных возможностей получения высоких скоростей обмена данными стали интенсивно развиваться когерентные оптические системы связи, которые на современном этапе их развития обеспечивают передачу мультимедийной информации со скоростью более 100 Гбит/с. В перспективных когерентных сетях предполагается использование систем со скоростью обмена данными до 400 Гбит/с. В наибольшей степени подобные скорости передачи данных востребованы в области супервизорных управляющих систем, когда своевременная обработка качественных изображений или дистанционное управление робототехникой, способствуют адекватной выработке целевой функции управления за счет анализа видеоряда и соответствующей реакции оператора на текущую ситуацию в реальном масштабе времени [1].

Кроме того, объективно возрастающие потребности в таких системах стимулируют специалистов реализовывать высокоскоростные каналы не только на магистральных участках сетей, но и в городских metro-системах, а также в центрах обработки данных, где от телекоммуникационной составляющей требуется большая производительность [102]. Во многом применение подобных технологий способствует эффективной реализации процедуры восстановления утраченных данных в условиях выхода из строя отдельных хранилищ, резервируемых той или иной системой структурированной избыточности данных.

В подавляющем большинстве когерентные системы связи используют сложные многоуровневые форматы модуляции (DP-QPSK, DP-mQAM), которые считаются достаточно требовательными к величине шумов в оптической линии.

Главным мешающим фактором в таких системах является неустойчивое восстановление фазы сигнала, когда оптические системы, в частности лазеры, работают нестабильно и вызывают дрожание канонических точек многоуровневого сигнала на векторной диаграмме, внося шум в процедуру распознавания отсчетов исходного сигнала [82, 88, 106]. Как указывалось, компенсация помех в таких системах обеспечивается за счет применения помехоустойчивых кодов, организованных по каскадной схеме. Пример структуры приемника когерентной системы для обеспечения скорости в 100 Гбит/с показан на рисунке 2.1 [1].

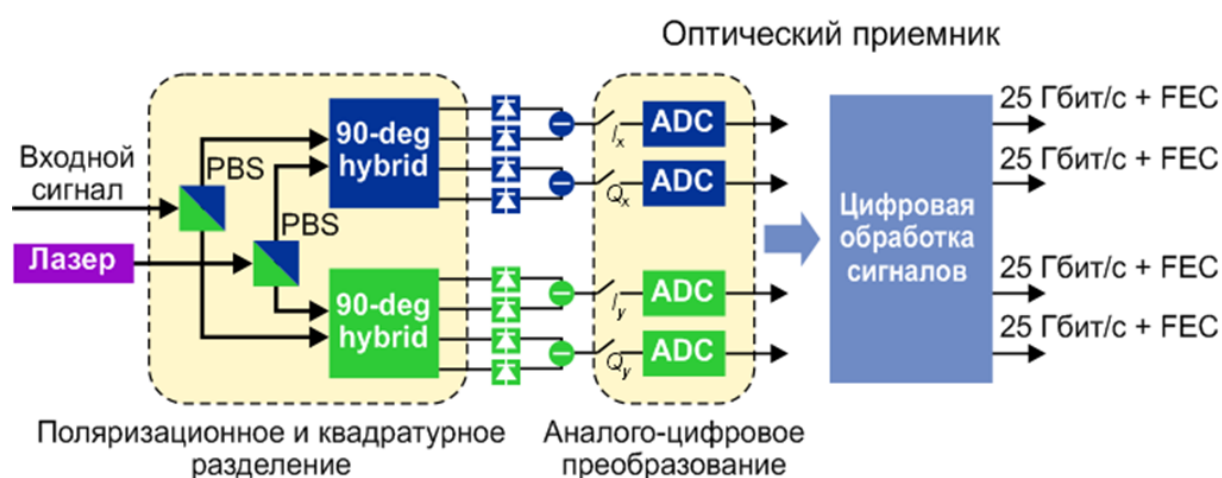


Рисунок 2.1 – Схема приемника когерентной системы

На приемной стороне осуществляется поэтапное преобразование сигнала из оптического излучения в электрический сигнал с последующей цифровой его обработкой. При этом электронная компенсация хроматической дисперсии в современном оборудовании DWDM позволяет организовывать линии более 4000 километров без использования компенсаторов дисперсии.

Содержание основных этапов цифровой обработки сигнала включает:

- оценку и восстановление синхронизации;
- выполнение адаптивной подстройки;
- компенсацию нелинейных искажений;
- компенсацию хроматической дисперсии;
- компенсацию поляризационно-модовой дисперсии.

Однако указанные действия в принципе не обеспечивают требуемой достоверности цифровых данных, поэтому на заключительном этапе их обработки

приемником применяются кодовые методы повышения достоверности, которые в общем случае связываются с повышением энергетической эффективности системы передачи данных. Принципиально использование сложных видов модуляции способствует повышению спектральной эффективности системы связи, в частности, оптической когерентной системы.

Использование средств помехоустойчивой защиты данных на базе недвоичных кодов и реализации процессоров кодеров таких кодов с применением ПЛИС требуют анализа их возможностей по обработке данных, представленных символами из расширенных полей Галуа. Учитывая общие тенденции развития современных телекоммуникационных технологий, целесообразно подвергнуть анализу двоичные поля вида $GF(2^4)$ и $GF(2^8)$. При этом в качестве примеров в работе будут использованы двоичные поля расширения степени три $GF(2^3)$, которые позволят сохранять наглядность тех или иных теоретических положений, используя небольшой объем информационного пространства. В силу линейности кодов РС сведения, полученные для кодов в пространстве символов из поля $GF(2^3)$, всегда будут верны и для символов из пространств полей $GF(2^4)$ и $GF(2^8)$.

Следует отметить, что процессор декодера в рассматриваемом случае будет оперировать не действительными числами, а системой данных, выраженных через показатель α как некоторый примитивный элемент поля $GF(2^i)$, где $i \in \mathbb{N}$. Важность этого положения подчеркивается тем, что сам примитивный элемент α и его степени представляются последовательностью бит, комбинации которых не являются целыми числами, выраженными в двоичной системе счисления.

Элементы любого поля $GF(2^i)$, и в частности поля $GF(2^3)$, определяются через структуру неприводимого (примитивного) полинома, характерного для каждого поля. Например, для поля $GF(2^3)$ полином имеет вид $f_3(\alpha) = 1 + \alpha + \alpha^3$, а для поля вида $GF(2^4)$ примитивный полином принимает вид $f_4(\alpha) = 1 + \alpha + \alpha^4$. Для поля $GF(2^8)$ полином принимает вид $f_8(\alpha) = 1 + \alpha^2 + \alpha^3 + \alpha^4 + \alpha^8$ [66].

Поскольку в теории помехоустойчивого кодирования рассматриваются конечные поля, то элементы такого поля учитывают, что $\alpha^g \equiv \alpha^{\text{mod}(2^K-1)}$, K – число информационных разрядов в выбранном коде РС. Таким образом, для кода РС с параметрами (7,3,5) следует учитывать, что $\alpha^7 \equiv \alpha^0$ или, например, $\alpha^{16} \equiv \alpha^2$. Исходя из этого, элементами конечного поля будут последовательности, представленные в таблице 2.1.

Таблица 2.1 – Элементы двоичного поля Галуа третьей степени расширения

Элементы поля	α^0	α^1	α^2	α^3	α^4	α^5	α^6
Двоичное представление элементов	001	010	100	011	110	111	101
Элементы поля	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}

Из таблицы заметно, что значения степеней примитивного элемента α не соответствуют двоичному представлению чисел, что существенно затрудняет выполнение операции сложения в технологии ПЛИС. Действительно, если сложить два элемента по mod 2, то новый элемент из конечномерного пространства кода не будет равен сумме показателей степеней слагаемых. Таким образом, сложение элементов в поле требует создания специальной таблицы, указывающей на результат сложения элементов поля. Это требует от процессора приемника выделения ресурсов памяти для идентификации результатов сложения двух операндов, выраженных в двоичном виде. Легко посчитать, что таблица сложения для поля $GF(2^3)$ содержит $(2^K - 1)^2 K = 147$ битов. Для поля $GF(2^4)$ объем таблицы вырастает незначительно и составляет всего 900 битов, однако для поля $GF(2^8)$ таблица должна содержать около 508 кбит данных или 0,5 Мбит, что составляет заметную долю в оперативной памяти ПЛИС. Хранение данных вне структуры ПЛИС приведет к задержкам вычислительного процесса при декодировании кодовых векторов.

Декодер выполняет только арифметические операции, при этом операция умножения на первый взгляд выполняется относительно операции сложения

несколько проще, поскольку действует обычное правило сложения показателей степеней при умножении чисел с одинаковыми основаниями. Однако, для применения этого правила необходимо выполнять процедуру поиска показателей степеней сомножителей, представляемых в структуре ПЛИС двоичными последовательностями. Это требует определенного объема памяти для хранения кодовой книги, позволяющей идентифицировать степени операндов в процедуре умножения. Объем такой памяти можно характеризовать выражением 2^K с учетом нулевого вектора длины K бит.

Подобные проблемы арифметической обработки комбинаций недвоичных кодов создают определенные технологические трудности при программировании ПЛИС и их интеграции в процессор приемника на аппаратном уровне. Структура ПЛИС включает логические конъюнкторы, дизъюнкторы, инверторы – буферные элементы, схемы с логикой «Исключающее ИЛИ», триггеры D- и T-типа, а также другие элементы, которые на основе заданных алгоритмов кодирования и декодирования реализуют программно-аппаратную часть кодеков.

В зависимости от особенностей используемых алгоритмов может меняться структура ПЛИС, поэтому степень предоставления таких возможностей делает ПЛИС наиболее привлекательными. Подобная технология реализуется на системе логических матриц и способах их коммутации. В современных условиях наибольшее распространение находят программируемые логические матрицы (ПЛМ), программируемая матричная логика (ПМЛ), программируемая макрологика (ПМ), программируемые коммутируемые матричные блоки (ПКМБ), программируемые вентильные матрицы (ПВМ) [1, 97, 116]. Конечно же значительную роль играют постоянные запоминающие устройства, которые могут служить идентификаторами степеней в системе умножения примитивных элементов. На рисунке 2.2 представлен принцип объединения макроячеек в системе ПЛИС. На схеме аббревиатурой БВВ обозначены блоки ввода – вывода данных.

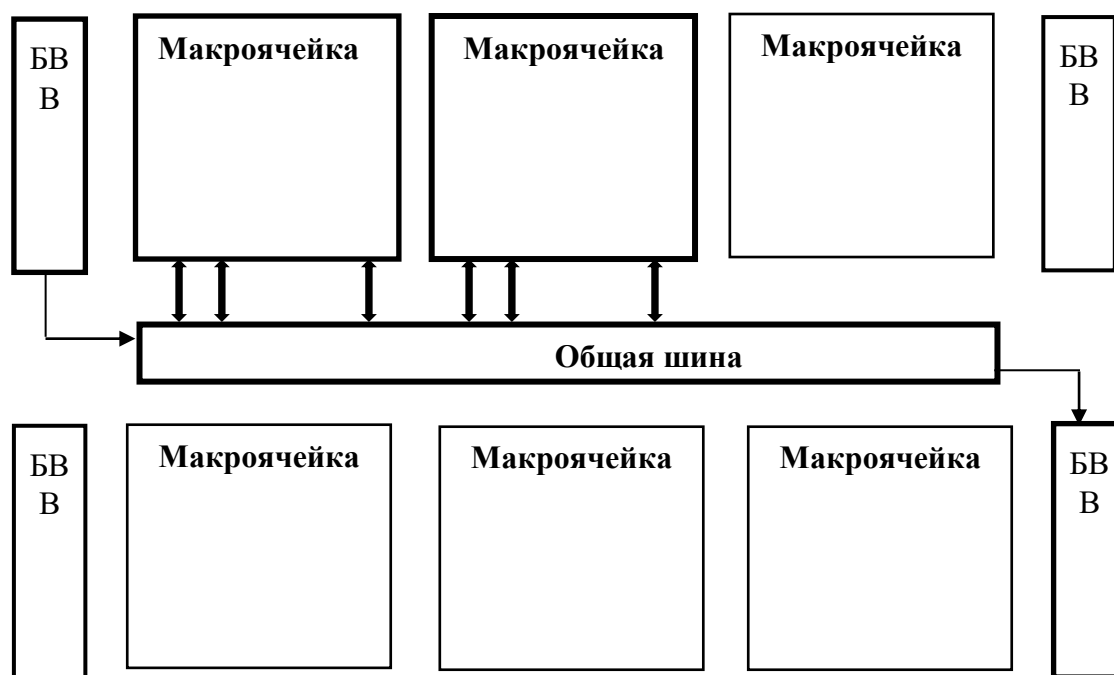


Рисунок 2.2 – Схема взаимодействия макроячеек в ПЛИС

В последующем будет показана схема эффективного использования приведенной структуры для решения задачи поиска порождающей матрицы эквивалентного кода.

Таким образом, целесообразность применения ПЛИС при разработке кодеков, требующая нестандартных схемотехнических решений, а также при проектировании малогабаритных устройств, не вызывает сомнений. Вместе с этим перестановочное декодирование требует от процессора приемника выработку, хранение и обработку мягких решений символов кодовых комбинаций, и если для двоичных последовательностей этот вопрос считается относительно решенным, то в процедуре обработки недвоичных символов возникают особенности, которые требуют дополнительного изучения. Исследование и детализацию статистических особенностей методов формирования мягких решений для недвоичных символов в условиях применения

сложных видов модуляции целесообразно осуществить на базе разработанных имитационных моделей получения таких решений.

2.2. Модели формирования мягких решений сложных сигналов

Передача данных в современных телекоммуникационных системах стала возможной благодаря развитию технологий применения в каналах различной физической природы сложных видов модуляции. Это позволило существенно повысить спектральную эффективность систем связи, но одновременно увеличило сложность вычислительного процесса при обработке таких сигналов. Основные трудности появились из-за перехода от одномерной модели формирования МРС, характерной для системы передачи двоичных сигналов с их условными ПРВ и нулевым порогом принятия решения, к двумерным моделям с множеством канонических точек на плоскости, отвечающих конкретному набору бит в символе [30]. Последнее обстоятельство обусловило применение в таких системах недвоичных кодов, в частности кодов РС. Это привело к необходимости формировать МРС не для отдельных битов, а для группы битов, определяющих символ сложного сигнала, связанного с конкретной канонической точкой на комплексной плоскости, как показано на рисунке 2.3.

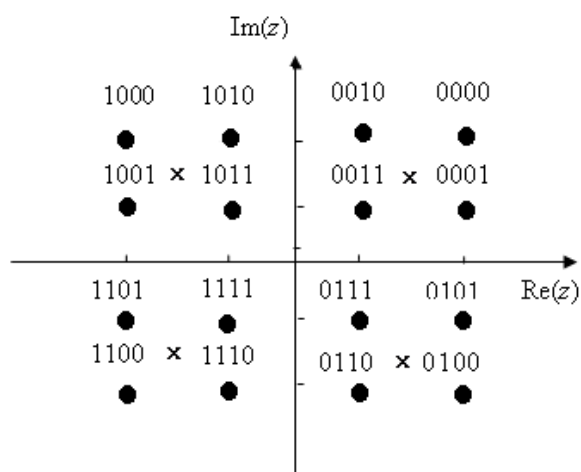


Рисунок 2.3 – Конфигурация сигналов КАМ-16

В последнее время появились работы, указывающие на возможности перехода от комплексной плоскости к обработке пространственных сигналов, что приводит к еще большей вычислительной сложности формирования МРС [1, 30]. В любом случае мерой снижения уровня надежности принятого сложного сигнала является удаление его от канонической точки на плоскости или взаимоувязанная оценка принятого сигнала относительно ближайших точек на сигнальной плоскости (в объеме). Подобная обработка сигнала для плоскости показана на рисунке 2.4.

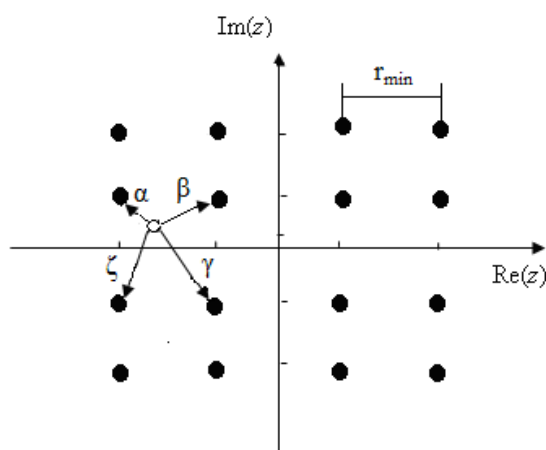


Рисунок 2.4 – Векторный метод принятия решения о сигнале

В случае применения векторного метода оценки сигнала сравниваются вектора в соответствии со строгим неравенством $\alpha < \beta < \zeta < \gamma$. По минимальному значению α принимается решение о фиксации сложного сигнала в двоичном представлении 1001 (см. рисунок 2.3), однако сформулировать значение МРС в данной технологии без введения дополнительных параметров не представляется возможным. Кроме того, в случае фиксации нестрогого неравенства, например, $\alpha \leq \beta < \zeta < \gamma$, возникает неопределенность относительно решения о сигнале, и такой сигнал целесообразно представить в виде стирания и присвоить ему минимальное из возможных значений МРС.

В случае формирования неравенства вида $\alpha < \beta < \zeta < \gamma$ и введения дополнительного параметра в виде радиусов концентрических окружностей, как показано на рисунке 2.5, для формирования МРС приемник должен сформировать дополнительное неравенство $R_i < \alpha < R_j$. В этом случае по номеру промежутка

между значениями i и j концентрических окружностей определяют значение МРС. На рисунке 2.5 радиусы окружностей соотносятся с формой двумерной условной ПРВ. Чем меньше значение радиуса окружности, тем выше значение МРС, верхняя окружность практически примыкает к точке математического ожидания сигнала, совпадающей с номинальной точкой этого сигнала на комплексной плоскости.

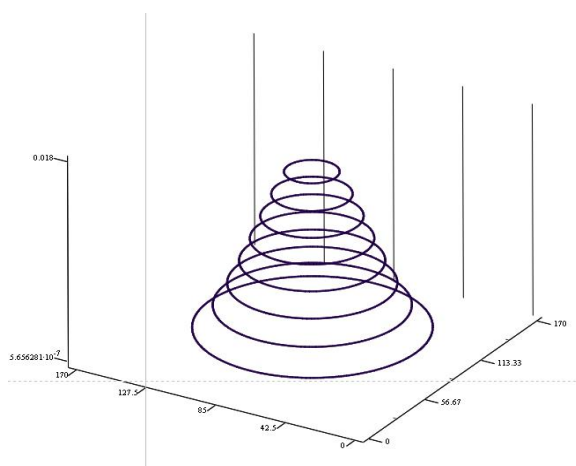


Рисунок 2.5 – Схема формирования границ для оценки МРС

Заметно, что применение концентрических окружностей не учитывает уникальность крайних номинальных точек созвездий, для которых в ряде случаев можно не учитывать соседние точки, поскольку позиция принятого сигнала оказывается на плоскости, граничащей с открытым интервалом. Подобная точка не может конкурировать с соседними сигналами, и поэтому может быть оценена как надежная с высоким МРС.

При фазовой модуляции значение символа зависит только от фазы принятого сигнала. В этом случае квантование целесообразно осуществлять только по углу отклонения принятого сигнала от номинальной точки сигнального созвездия. В таком случае концентрические окружности допускается заменить на области в виде угловых величин. Такое созвездие по результатам моделирования представлено на рисунке 2.6. В качестве примера приведена система с QPSK-модуляцией при соотношении сигнал-шум 10 дБ. Более светлые области на сигнальном созвездии соответствуют наиболее надежным символам, поскольку они в большей степени удалены от соседних номинальных точек созвездия.

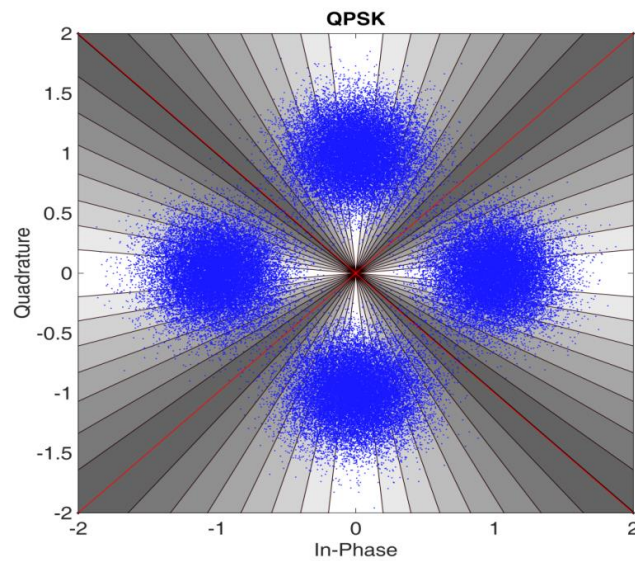


Рисунок 2.6 – Созвездие сигналов QPSK с угловыми зонами квантования

Гистограмма распределения индексов достоверности символов MPC для указанной схемы представлена на рисунке 2.7.

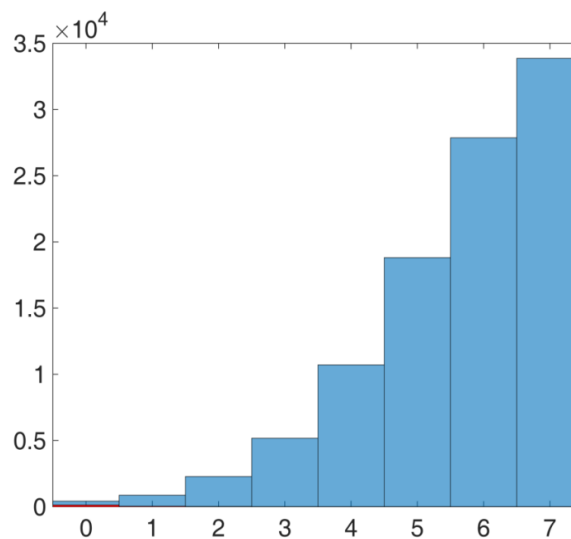


Рисунок 2.7 – Гистограмма распределения MPC принятого сигнала при QPSK

Из гистограммы следует существенное преобладание MPC с высокими показателями за счет использования открытых сигнальных зон. Ясно, что граничные окружности не используют указанные зоны, и поэтому метод концентрических окружностей проигрывает методу секторов.

При QAM-модуляции значение символа зависит не только от фазы, но и от амплитуды принимаемого сигнала, поэтому квантование сигнала осуществляется

по прямоугольным зонам, площади всех зон при этом строятся равными. В работе также предложено оставлять открытыми границы зон, в которых с увеличением амплитуды сигнала конкурирующие точки будут отсутствовать. Вид сигнального созвездия, иллюстрирующего данный подход, представлен на рисунке 2.8.

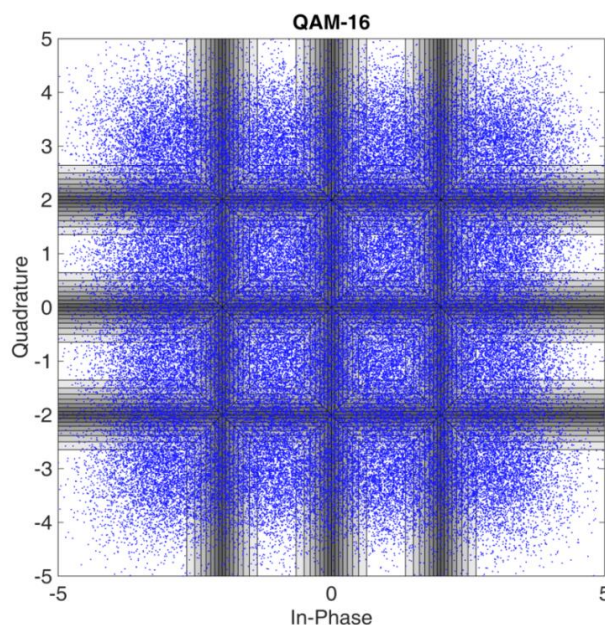


Рисунок 2.8 – Созвездие сигналов при QAM-16 модуляции

В качестве примера рассматривается система с QAM-16 модуляцией и квантованием каждого принимаемого символа на восемь уровней при соотношении сигнал-шум в канале связи 10 дБ. Заметно, что в таком созвездии 12 сигнальных точек имеют открытые зоны. Гистограмма распределения МРС принятого сигнала представлена на рисунке 2.9. В нижней части диаграммы выделена частота появления ошибочных решений по значениям МРС. Это говорит о том, что формирование стертых позиций (по сути ненадежных символов недвоичных кодов) требует определенной осторожности в зависимости от характеристик канала связи. Суть предлагаемого подхода заключается в том, чтобы для каждого принятого из канала связи символа получать мягкие решения от детектора. Сочетание описанного выше метода определения МРС с кодами РС позволяет избежать выполнения алгоритма поиска полинома ошибок (алгоритм Берлекэмп-Мессе). Из анализа гистограммы следует, что вероятность

ошибочных решений для высоких значений МРС не является бесконечно малой величиной, поэтому требуется поиск новых подходов к системе выработки МРС.

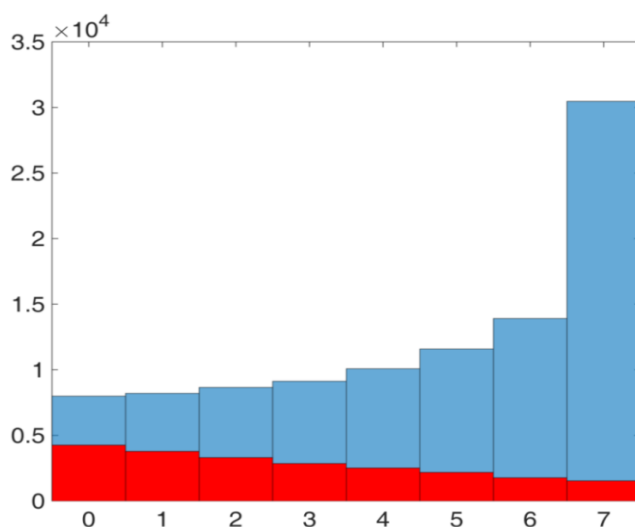


Рисунок 2.9 – Частоты распределения МРС принятого сигнала при QAM-16

В ходе выполнения работы были рассмотрены различные методы упразднения процедуры поиска локаторов ошибок по алгоритму Берлекэмп – Месси (АБМ). Все предложенные подходы сводятся к получению стираний из канала связи и дальнейшему поиску их значений. Из этого следует, что отказываться от процедуры АБМ и полностью положиться на стирания нецелесообразно. Необходимо искать пути оптимизации этой процедуры, например, на пути перестановочного декодирования недвоичных кодов. В ряде работ показано, что алгоритм декодирования кодов РС нельзя непосредственно обобщить таким образом, чтобы использовать мягкие решения демодулятора [84, 93]. Разработаны технологии, в которых несколько раз производится декодирование с жесткими решениями о символах, например, по принципу турбокодов, когда информация от источника передается по каналу дважды в разные периоды времени и затем сравнивается и восстанавливается по принципу «распространения доверия». Эти решения сравниваются и на позициях, где символы не совпадают, формируются стирания. Затем последовательно используются алгоритмы Ченя и Форни для исправления выделенных стираний [95, 101, 116].

2.3. Модели формирования мягких решений недвоичных символов методом сравнения гистограмм

Очевидная сложность выработки МРС недвоичных символов методом концентрических окружностей, методом выделения угловых границ, методом площадей равных квадратов и выделением открытых зон приводит к необходимости поиска более простых в вычислительном плане способов сопровождения жестких решений мягкими оценками. Кроме того, указанные методы не являются универсальными и не могут быть использованы для различных видов созвездий сигналов. Например, методы, пригодные для использования совместно с QPSK, не подходят для систем, применяющих QAM.

Исследования показали, что универсальными свойствами для решения поставленной задачи облают методы сравнения гистограмм на предмет их совпадения, близости и корреляционной зависимости сравниваемых показателей. Математический аппарат подобного сравнения считается достаточно развитым [16]. Оценка некой эталонной гистограммы H_s с произвольной гистограммой H_d может осуществляться: на базе оценки корреляционных связей; с использованием критерия χ^2 (Хи-квадрат); по методу пересечений гистограмм; с использованием метода Бхаттачария [60].

За эталонную гистограмму принимается такой набор данных, который соответствует набору максимальных значений МРС $\lambda_{\max} = 7$. Этот подход обеспечивает универсальность выработки МРС для различных методов обработки сложных сигналов на физическом уровне и одинаковую нормализацию сравниваемых гистограмм по бинам. При двоичной модуляции и основании недвоичного кода m значение эталонной гистограммы будет определяться как $H_s = 7 \times 2^m$. В случае применения модуляции вида QPSK значение этого параметра будет равно, по аналогии для QAM-16, $H_s = 7 \times 2^{m-2}$. Унификация позволяет повысить скорость обработки данных процессором приемника, что важно для когерентных сетей.

Аналитическая модель корреляционного метода или метода оценки коэффициента корреляции по Пирсону имеет вид, в котором через i обозначается номер сравниваемого бина

$$\left[\lambda_k(H_g, H_d) \right] = \frac{\sum_i (H_g(i) - \bar{H}_g)(H_d(i) - \bar{H}_d)}{\sqrt{\sum_i (H_g(i) - \bar{H}_g)^2 * (H_d(i) - \bar{H}_d)^2}}. \quad (2.1)$$

Применение выражения (2.1) в системе оценки МРС двоичных символов по условиям, приведенным выше, не имеет смысла из-за равенства нулю первой скобки под знаком суммы в числителе и знаменателе этого выражения.

Применение критерия χ^2 определяется аналитическим выражением вида

$$\left[\lambda_\chi(H_g, H_d) \right] = \sum_i \frac{(H_g(i) - H_d(i))^2}{H_g(i)} = \sum_i \frac{(7 - H_d(i))^2}{7}. \quad (2.2)$$

Значение МРС в выражении (2.2) изменяется от 0 до ∞ , что создает определенные трудности при программировании ПЛИС, поскольку верхняя оценка практически не определена. Нижняя граница определяет плохое совпадение сравниваемых гистограмм, верхняя – хорошее их совпадение. Однако, относительная простота получения данных по этому критерию условно говорит в пользу его практического применения.

Аналитическая модель метода пересечения диаграмм имеет еще более простой вид, обеспечивающий несложный вычислительный процесс. В этом методе нижняя граница равна нулю, а верхняя граница равна единице при условии дополнительного нормирования оценки. Это обстоятельство является отрицательным фактором.

$$\left[\lambda_{cr}(H_g, H_d) \right] = \sum_i \min(H_g(i), H_d(i)) = \sum_i H_d(i), \quad (2.3)$$

поскольку $H_g(i) \geq H_d(i)$ всегда.

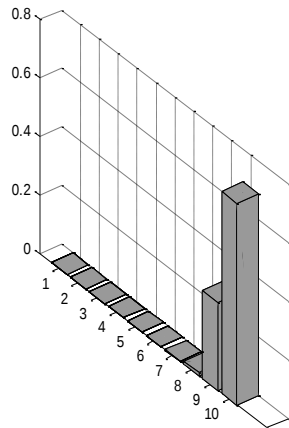
Верхняя граница этого критерия соответствует хорошему совпадению гистограмм. Учитывая простоту реализации, в работе проведено имитационное

моделирование процесса получения МРС на основе этого критерия с получением статистических данных для различных ОСШ.

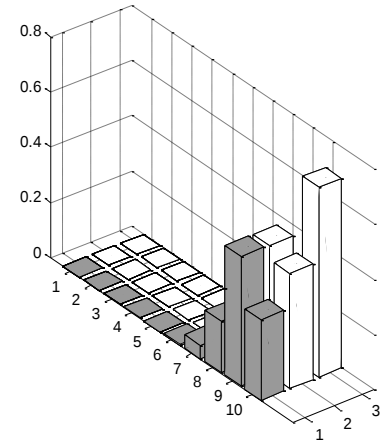
Пусть некоторый код РС рассматривается над полем Галуа $GF(2^2)$. Тогда за эталонную модель системы оценок по выражению (2.3) принимается структура МРС вида $n_{PC} \Rightarrow 7777$. В такой модели при двоичной модуляции нормированный множитель равен значению $N_{нор} = \lambda_{\max} \times 4$, т.е. $N_{нор} = 28$. Если приемник зафиксировал для каждого двоичного символа последовательность вида $n_{PC} \Rightarrow 7 = 6574$, то $\lambda_{cr} = 22$. Нормированный вид $\lambda_{cr}^H = 22/28 = 0,7857$. Но если $n_{PC} \Rightarrow 7653$ (отличие общей суммы оценок от предыдущего значения всего на единицу), то $\lambda_{cr}^H = 21/28 = 0,7500$. Разница между нормированными значениями достаточно заметная. Контрастность оценок способствует повышению скорости сортировки МРС в процессоре приемника.

В ходе имитационного моделирования системы формирования МРС по методу пересечений для получения представительной выборки передавалось не менее 10^6 недвоичных символов из поля $GF(2^8)$ при использовании различных видов модуляции при различных ОСШ. Энергия сигнала на бит принималась во всех испытаниях имитационной модели одинаковой и равной значению $E_b = 2$. Результаты испытаний имитационной модели формирования МРС системы с АМ показаны на рисунке 2.10. На всех графиках этого рисунка по оси ОХ отложены значения МРС с поправочным коэффициентом 0,1. По оси ОУ представлены значения ОСШ, определяемые по формуле $h = \frac{E_b}{N_0} = \frac{E_b}{2\sigma^2} (\partial Б)$, где $N_0 = 2\sigma^2$ – спектральная аддитивная мощность белого гауссовского шума (АБГШ). На оси ОZ представлены нормированные частоты появления тех или иных значений МРС. На рисунке 2.10 а) показана гистограмма коэффициента пересечения в условиях хорошего канала связи ($h = 10 \partial Б$). В этих условиях значения МРС в подавляющем большинстве располагаются в диапазоне от 0,8 до 1. Сортировка таких оценок не представляет трудностей. При ухудшении параметров канала

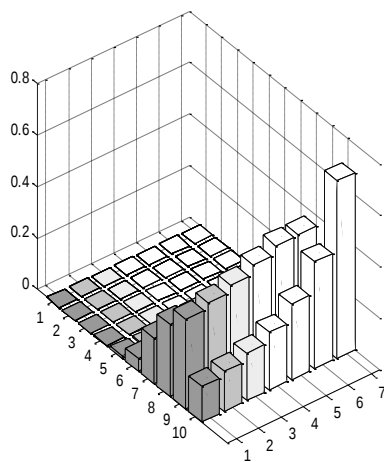
связи (рисунок 2.10 б) появляются оценки от 0,7 до 0,8, количество таких оценок незначительно, и в общей массе они мало влияют на определение надежности недвоичного символа.



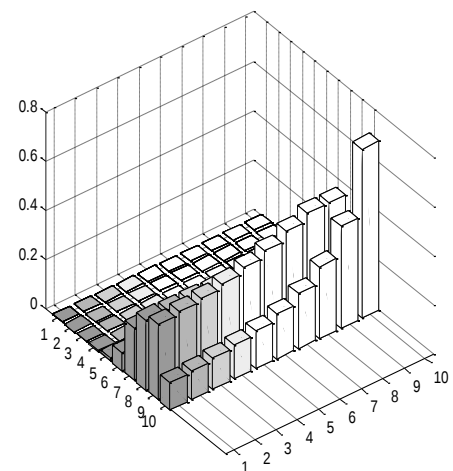
а) Модуляция АМ, $E_b=2$, $n=8$, $h=10$ дБ



б) Модуляция АМ, $E_b=2$, $N=8$, $h=5,2$ дБ



в) Модуляция АМ, $E_b=2$, $n=8$, $h=1,5$ дБ



г) Модуляция АМ, $E_b=2$, $n=8$, $h=0$ дБ

Рисунок 2.10 – Результаты испытаний имитационной модели системы с АМ при различных отношениях сигнал-шум

На рисунке 2.11 представлены результаты имитационного моделирования в системе обмена данными с ФМ. В целях получения более ясной информации о степени совпадений системы принятых МРС с эталонной системой на рисунке 2.11 г) начало осей координат развернуто по часовой стрелке на 90° (отношение сигнал-шум откладывается по оси OX).

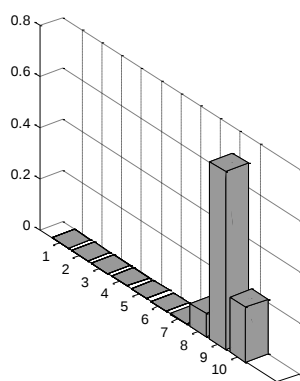
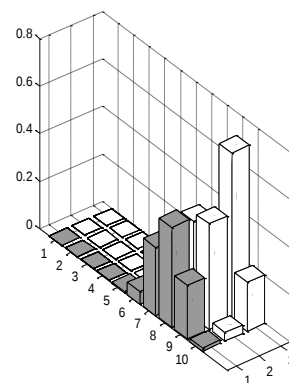
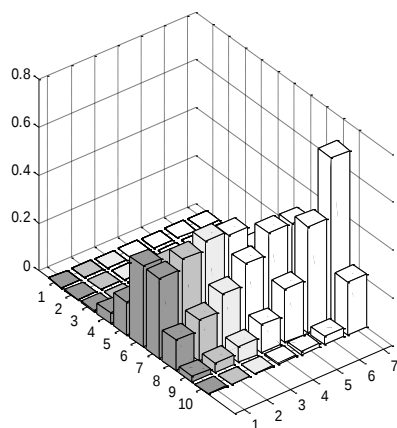
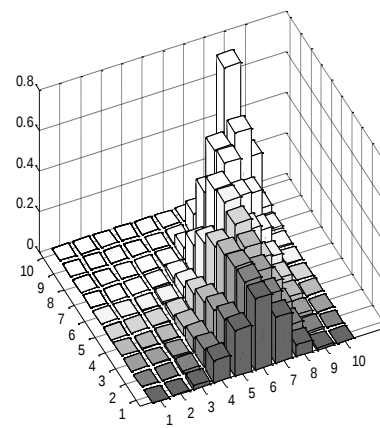
а) Модуляция ФМ, $E_b=2$, $n=8$, $h=10$ дБб) Модуляция ФМ, $E_b=2$, $n=8$, $h=5,2$ дБв) Модуляция ФМ, $E_b=2$, $n=8$, $h=1,5$ дБг) Модуляция ФМ, $E_b=2$, $n=8$, $h=0$ дБ

Рисунок 2.11 – Результаты испытаний имитационной модели системы с ФМ

Заметно, что диапазон оценок расширился, и до значения параметра ОСШ 4 дБ оценки убывают и становятся более различимыми. В этом видна позитивная роль ФМ. Дальнейшая деградация параметра отношения сигнал-шум приводит к тому, что оценки надежности занимают интервалы включительно до 0,5. Из рисунка 2.11 г) понятно, что в широком интервале диапазона параметр отношения ОСШ мало изменяется (мало различим), и оценка надежностей недвоичных символов в этом диапазоне оказывается затруднительной. На рисунке 2.12 представлены диаграммы испытаний имитационной модели ФМ в условиях, аналогичных испытаниям системы с АМ.

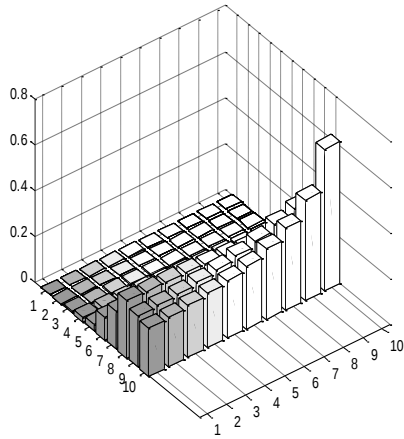
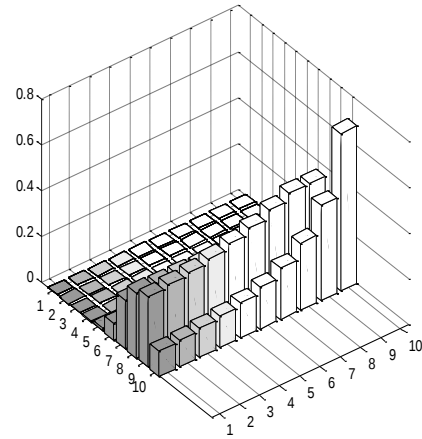
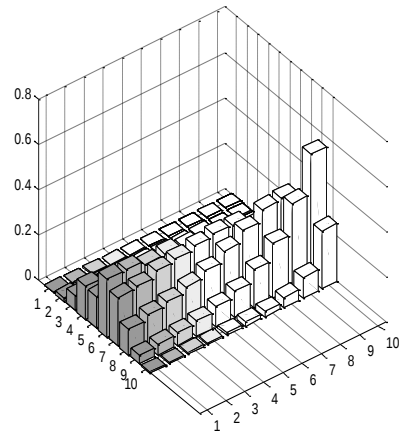
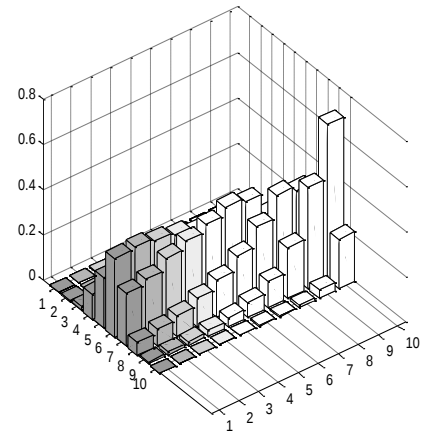
а) Модуляция АМ, $E_b=2$, $n=4$, $h=0$ дБб) Модуляция АМ, $E_b=2$, $n=8$, $h=0$ дБв) Модуляция ФМ, $E_b=2$, $n=4$, $h=0$ дБг) Модуляция ФМ, $E_b=2$, $n=8$, $h=0$ дБ

Рисунок 2.12 – Сравнительные характеристики метода пересечения

Аналитическое выражение для модели Бхаттачария имеет вид

$$[\lambda_{Bh}(H_s, H_d)] = \sqrt{1 - \sum_i \frac{\sqrt{H_s(i) * H_d(i)}}{\sqrt{\sum_i H_s(i) * \sum_i H_d(i)}}}. \quad (2.4)$$

Неудобство этой модели заключается в смысловой инверсии нижней и верхней границ. Нижняя граница равна нулю и означает хорошее совпадение сравниваемых гистограмм. Верхняя граница равна единице и соответствует плохому совпадению сравниваемых объектов.

Можно показать, что расстояние Бхаттачария имеет меньшую чувствительность к изменению структуры принятых МРС. Кроме того, необходимость выполнять действия с иррациональными выражениями существенно усложняет работу процессора декодера. Отсюда следует, что использование выражения (2.3) для оценки МРС недвоичных кодов остается приоритетным. Возникает целесообразность сравнения первого и второго подхода при различных условиях передачи данных в канале связи как внутри каждого метода, так и между собой.

Для сравнения статистических особенностей выбранных методов сравнения эталонной комбинации с комбинациями, принятыми по каналу связи с помехами, были выбраны одни и те же методы при различных длинах кодовых комбинаций, переданных по каналам связи с идентичным уровнем помех. В соответствии с этим на рисунке 2.19 представлены сравнительные характеристики метода пересечения. Полученные данные показывают, что при любых видах модуляции и хорошем состоянии канала связи количество оценок надежности монотонно возрастает для оценок от 8 до 10. Количество оценок, меньших чем 8, напротив, монотонно убывает, что соответствует физическим процессам, происходящим в канале связи с помехами. В силу открытости интервала максимальной оценки системы с АМ количество хороших оценок превосходит количество подобных оценок для системы с ФМ.

Для проверки гипотезы несоответствия средних значений требуемой достоверности символов в случае ошибочного решения о проверке четности была разработана имитационная модель СОД с каскадным кодом на основе кода РС над полем $GF(2^4)$. В качестве проверочного соотношения в модели использовалась единственная проверка на четность для символов кода РС.

Испытания проводились для отношений сигнал-шум, определяемых как E_b/N_0 , для диапазона значений от 0 дБ до 10 дБ. Выборка в 10^6 недвоичных символов при испытании модели обеспечивала требуемую погрешность

полученных результатов. Итоги статистических испытаний модели приведены на рисунке 2.13.

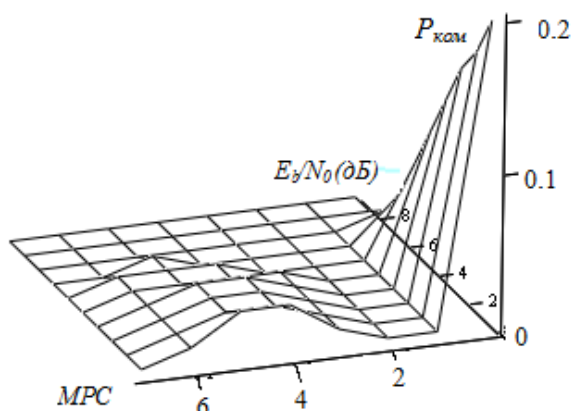


Рисунок 2.13 – Оценка ошибочной регистрации не двоичных символов

Заметно, что ряд значений МРС при низких ОСШ хорошо коррелирует с ошибочными решениями. Это особенно проявляется для МРС λ_4 и λ_5 . Причиной подобного явления становится высокая вероятность двойных ошибок при указанных ОСШ. Подобные оценки без дополнительных преобразований данных следует применять с осторожностью. Решениями возникшего противоречия могут явиться использование в качестве внутреннего кода системы с большей исправляющей способностью или итеративные преобразования символов кодовых комбинаций внутреннего кода, что отрицательно скажется на скорости обработки данных в высокоскоростных системах когерентных сетей.

Рассмотренный метод выработки мягких решений не двоичных символов на базе двоичных видов модуляции или с использованием сигнальных созвездий обладает универсальностью. Из известных методов сравнения гистограмм среди приведенных аналитических моделей в наибольшей степени подходит метод пересечения, который прост в реализации. Однако, отсутствие монотонности в изменениях МРС при последовательном изменении параметра ОСШ требует дополнительных вычислительных ресурсов для реализации его на ПЛИС. Проверка статистических характеристик метода в гауссовском канале связи при использовании двоичных видов модуляции показала эффективность метода только при достаточно высоких значениях ОСШ. В случае деградации этого

параметра требуются дополнительные ресурсы от системы обмена данными в виде повторов данных или снижения скорости их передачи из-за применения итеративных методов повышения значений, выработанных МРС, как это выполняется в системах многопорогового декодирования, в системах с турбокодированием или с применением кодов с малой плотностью проверки на четность [42, 43, 74, 86, 95, 103, 105, 108, 110, 116, 117]. Большим недостатком метода (2.3) является требование дополнительной нормировки полученных данных.

Применение критерия (2.4) при реализации мягкого декодера на ПЛИС не является целесообразным из-за необходимости вычислять радикалы. В этой связи требуется поиск рационального подхода к формированию МРС недвоичных символов на базе вычислительных возможностей ПЛИС.

2.4. Вычисление МРС с использованием когнитивной процедуры

Предлагается новый подход к организации работы перестановочного декодера недвоичного избыточного кода, в котором используется двухэтапная процедура когнитивной обработки данных. Интерес к методам обработки недвоичных кодов объясняется широким внедрением в телекоммуникационные системы технических решений, связанных с одновременным повышением их спектральной и энергетической эффективности, использованием недвоичных кодов в системах хранения данных. Поиск приемлемых совместных решений указанных задач возможен на пути мягкого декодирования избыточных кодов с применением сигнально-кодовых конструкций или тривиальной двоичной обработки данных.

В работе предлагается метод оценки МРС недвоичных избыточных кодов, описывается методика ранжирования таких символов по мягким решениям в составе кодового вектора с целью надежной реализации принципа ПД. Показывается уникальная приспособленность алгоритма ПД применительно к эффективной реализации процедуры когнитивной обработки данных как в ходе

формирования мягких решений, так и в ходе обработки кодовых векторов. Оценивается объем памяти декодера для формирования его полноценной когнитивной карты в ходе работы или в ходе предварительного его обучения с применением внешних вычислительных средств. Формулируются правила снижения сложности вычислительного процесса за счет регулярных преобразований эталонных матриц (ЭМ) эквивалентных кодов.

Концептуальная модель любой когнитивной системы включает в себя две тесно связанных сентенции одного и того же процесса. Первый вопрос носит прагматический характер и звучит как: «Что делать?». Второй вопрос отражает материальную сторону реализации модели и формулируется как: «Какими средствами?». Когнитивная модель функционирования технической системы основывается на принципах процедуры обучения, предполагающей, что различные факторы внешней среды и сопутствующие им признаки развиваются в результате реакции сенсоров системы (сенсорной плоскости) на внешние условия. В общем случае происходит последовательная обработка сенсорной информации с последующим ее перекомпилированием, закреплении «удачных» гипотез (решений) и удалением «неудачных» вариантов таковых, например, по частоте их успешного применения [3, 6, 34, 35]. При этом хорошо известные принципы построения адаптивных систем предполагают выполнение части из этих функций в усеченном виде, поскольку адаптация является только элементом перцептивного цикла, включающего схему обучения как главный элемент когнитивной структуры. Поэтому введение в алгоритм адаптивной системы операторов сравнения текущей ситуации с заданными порогами можно трактовать как решение задачи по заданному извне шаблону. В когнитивных системах названные этапы рассматриваются значительно шире и трактуются как способность различать внешние факторы функциональной дезадаптации, приводящие к нарушениям работы технической системы в целом.

Анализ современных методов построения устройств помехоустойчивого кодирования показывает, что подавляющее большинство из них принципиально создается под те или иные системы связи, в которых предварительно и достаточно

полно изучена статистика потока ошибок как элемент внешнего обучения. Такие устройства не приспособлены к реализации функций обучения. Однако, при использовании весьма эффективных алгоритмов ПД такая возможность появляется, поскольку для кортежа данных можно указать конечное множество вариантов перестановок символов комбинаций, найти и сохранить для них готовые решения, которые можно хранить в памяти декодера и не вычислять их заново при повторях конкретных перестановок [5, 6, 35, 54, 57]. Важными составляющими перестановочного декодирования являются вычисление и отбор МРС, которые лежат в основе процедуры сортировки символов принятой комбинации и организации их последующих перестановок и поэтому должны адекватно соответствовать текущему состоянию используемого канала связи. Применение сложных видов модуляции ставит вопрос об использовании алгоритмов перестановочного декодирования недвоичных избыточных кодов [6]. Некоторые сведения о таком подходе известны из работ [6, 35, 36, 77]. Вместе с этим из известных источников не всегда ясно, каким образом применять когнитивные процедуры к поиску наиболее вероятных векторов переставленных недвоичных кодов, как, используя свойства переставленных матриц, сократить объем хранимых данных, полученных в результате обучения декодера.

Целями данной части исследования являются изложение основных аспектов, связанных с оценкой мягких решений недвоичных символов избыточных кодов, и описание методов сокращения объема хранимых в декодере данных для переставленных порождающих матриц эквивалентных кодов. Анализ выражения (1.14) показывает, что для реализации когнитивной модели на канальном уровне в системе построения декодера должна быть детерминированная составляющая. Такой составляющей является всегда известное число перестановок нумераторов столбцов порождающей матрицы кода, даже если они составляют очень большое, но конечное множество. На физическом уровне подобное множество указать невозможно, поскольку все многообразие изменений в непрерывном канале связи системы обмена данными формирует бесконечное множество событий. В последнем случае приходится

ориентироваться на параметр ОСШ, который указывает некоторое ограниченное подмножество трансформаций физического уровня, которые укладываются в некоторую статистически определенную картину. По ней допустимо формирование МРС, соответствующих реальному состоянию непрерывного канала связи. Удобной формой представления МРС является их целочисленное выражение, которое по ЭВК незначительно (всего 0,2 дБ) уступает действительным оценкам ЭВК, но способствует повышению скорости вычислительного процесса [36, 37, 64]. Аналитическое выражение для вычисления целочисленных МРС при использовании двоичных видов модуляции имеет вид

$$\lambda_i(z) = \left\lfloor \frac{\lambda_{\max}}{\rho M_z} \times z \right\rfloor, \quad (2.5)$$

где $\lambda_{\max}$ – максимальное значение МРС, принятое для данной системы, $M_z = \pm\sqrt{E_b}$ – математическое ожидание значений принимаемых сигналов, ρ – интервал стирания (обычно $0 \leq \rho < 1$), а z – значение принятого сигнала, учитывающее влияние мешающих факторов [30, 45, 76]. Оценку надежности недвоичного символа в поле $GF(2^n)$ удобно осуществлять по совокупности λ_i , где $i = \overline{1, n}$, в формате коэффициента правдоподобия

$$K_{np} = \sum_{i=1}^n \lambda_i / \sum_{i=1}^n \lambda_{\max}. \quad (2.6)$$

Выражение (2.6) выгодно отличается от моделей (2.3) и (2.4). Во-первых, всегда выполняется условие $0 \leq K_{np} \leq 1$, что позволяет использовать его в вычислительном процессе без специальной нормировки как в случае попытки использования критерия пересечения гистограмм (2.3). Во-вторых, простота вычислительного процесса при оценке K_{np} не вызывает сомнений, поскольку знаменатель в выражении (2.6) для данной системы есть число постоянное.

Следовательно, суммирование текущих значений МРС λ_i осуществляется только в числителе указанной дроби. Поиск частного при реализации процедуры (2.6) несколько уступает поиску суммы в процессе (2.3) по простоте реализации, но не требует нормировки окончательного результата. В последующем в ходе исследований для поиска МРС использовалось выражение (2.6). Частота F появления различных оценок для параметра K_{np} при использовании различных степеней расширения двоичного поля n представлена на рисунках 2.14 – 2.17. Для удобства чтения гистограмм на указанных рисунках по оси абсцисс введен поправочный коэффициент, равный 10.

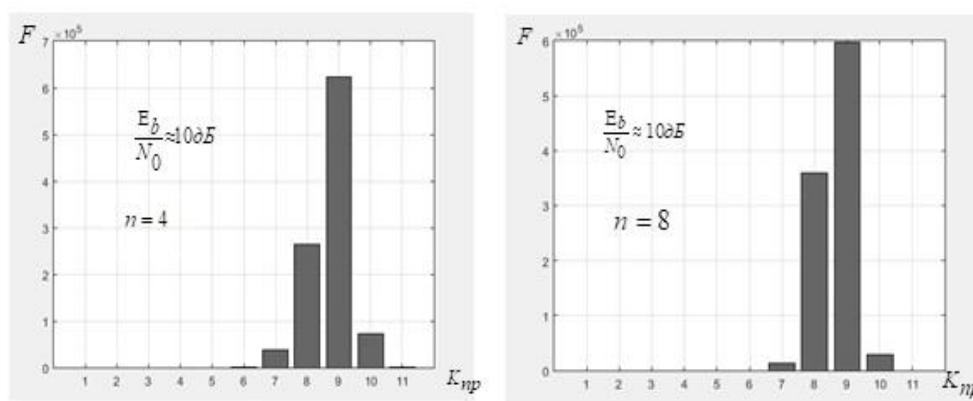


Рисунок 2.14 – Частота показателей коэффициента правдоподобия для различных длин недвоичных символов в битах при высоком значении ОСШ

Анализ представленных результатов имитационного моделирования дает неожиданный результат в условиях хорошего значения параметра ОСШ. Максимумы параметра F на приведенных выше гистограммах при различных расширениях двоичного поля Галуа не совпадают с ожидаемым значением на позиции 10.

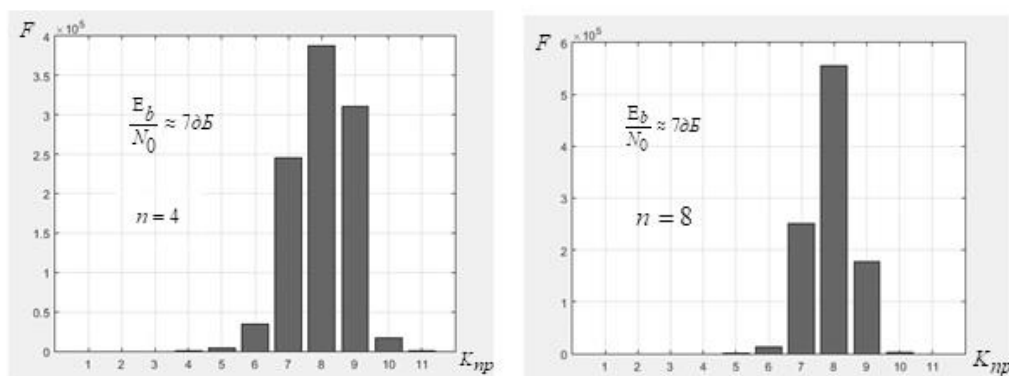


Рисунок 2.15 – Частота значений K_{np} при понижении параметра ОСШ

Некоторое снижение параметра ОСШ приводит к изменению положения максимума на оси абсцисс и явному увеличению дисперсии оценок МРС.

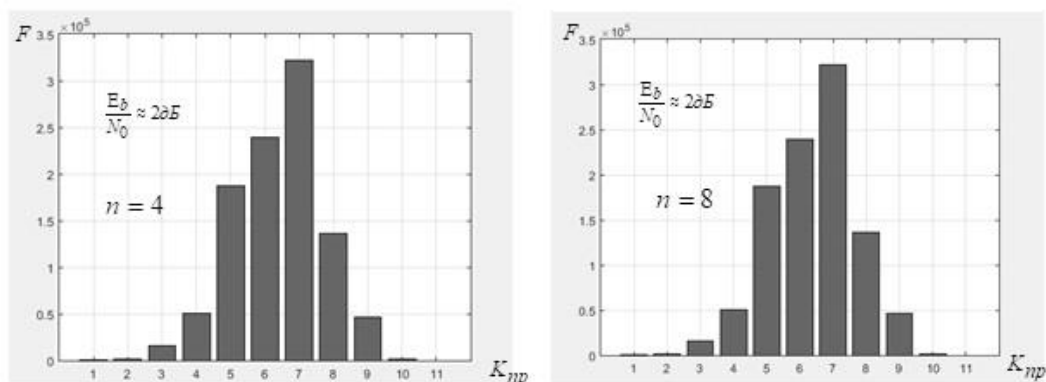


Рисунок 2.16 – Частота значений K_{np} при $h = 2 \text{ dB}$

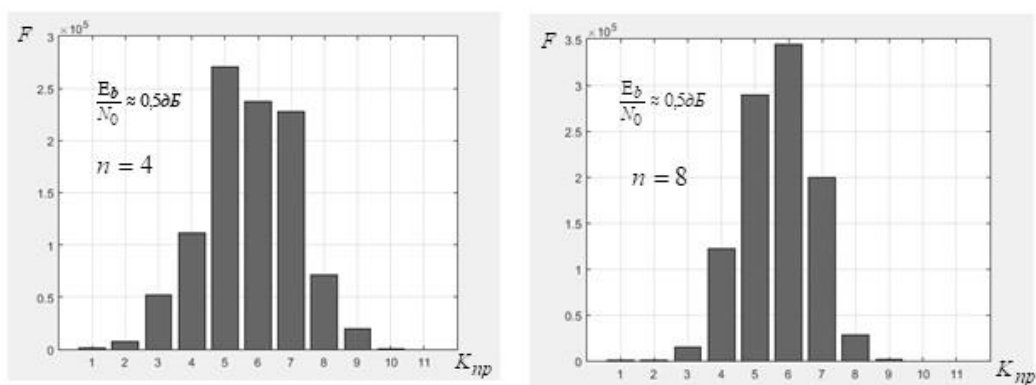


Рисунок 2.17 – Частота значений K_{np} при очень низком ОСШ

Анализ результатов имитационного моделирования канала с независимым потоком ошибок для различных отношений сигнал-шум в формате E_b/N_0 показал, что частота F значений K_{np} для различных оценок во многом зависит от показателя E_b/N_0 и не является монотонной, что вызывает трудности при определении лучших оценок. Это приводит к целесообразности применения когнитивной процедуры определения коэффициента правдоподобия по заранее известным для декодера гистограммам, характерным различным значениям ОСШ. Такие характеристики предварительно могут быть получены в ходе тестовых испытаний заданного канала связи или оцениваться в ходе оперативной работы направления связи. На стационарных каналах связи подобные испытания входят в обязательные регламенты, которые проводятся регулярно.

Задачами когнитивного подхода на физическом уровне обработки данных являются сбор и пополнение статистики изменения параметра K_{np} для конкретного направления связи в целях гибкого формирования наилучших оценок системы обмена данными. Учитывая изменение координаты максимального значения параметра $F(h)$ при изменении ОСШ и двух других ближайших к нему максимумов второго и третьего планов, удалось выявить закономерности изменений максимальной оценки, которые могут быть использованы в когнитивной карте для оценки параметра ОСШ.

По результатам испытаний имитационных моделей на рисунках 2.18 и 2.19 приведен разброс максимальных оценок второго и третьего планов относительно оценок K_{np} , максимумов первого плана. При этом с изменением параметра ОСШ оценки максимумов второго и третьего планов не стабильны относительно друг друга и поэтому не могут служить ориентирами для выработки когнитивной модели. Целесообразно использовать характеристику изменений только глобального максимума значений K_{np} , поскольку эти изменения носят монотонный характер по мере увеличения (уменьшения) параметра ОСШ. Возможна оценка по среднему между всеми тремя названными максимумами, однако такой анализ в работе не проводился.

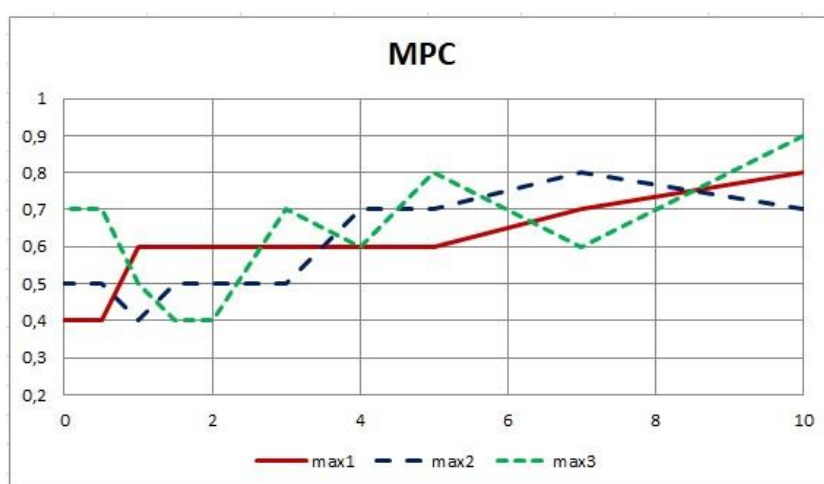


Рисунок 2.18 – Частота значений трех максимумов K_{np} при различных ОСШ (M=4)

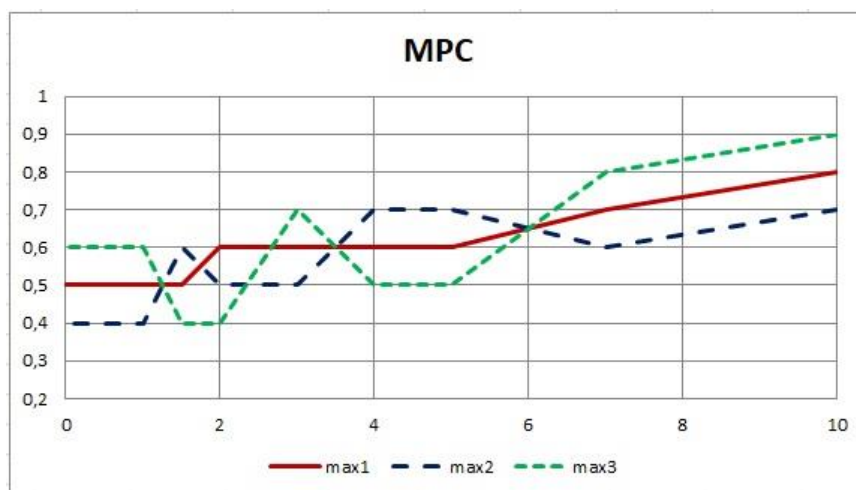


Рисунок 2.19 – Частота значений трех максимумов K_{np} при различных ОСШ ($M=8$)

Анализ показывает, что кроме двоичных видов модуляции использование указанной методики допустимо при применении сложных видов преобразований сигналов с учетом формирования MPC не для одного бита данных, а для группы битов в зависимости от кратности сложного сигнала.

2.5. Формирование MPC в системе каскадных кодеков

Коды РС в системах обмена данными могут использоваться самостоятельно или в составе произведения кодов (каскадных конструкциях) на внешней ступени декодирования [11, 46, 66, 70]. Как правило, в качестве внутреннего кода в таких конструкциях используется код с проверкой на четность. Тогда гистограммы когнитивной карты декодера на этапе формирования мягких решений должны учитывать статистику возникновения нечетных или четных ошибок. Нечетные ошибки будут выявлены на внутренней ступени декодирования, и на этой основе сформированы стерты позиции, которым однозначно присваивается наименьший индекс MPC. Четные ошибки таким декодером не будут выявлены вообще. На рисунке 2.20 представлены гистограммы при условии проверки символов кода РС на четность внутренним декодером. Первый ряд показывает частоту появления четных ошибок (темновыделенные бины), а второй ряд указывает на появление нечетных ошибок (светлосерое выделение бинов). Третий ряд соответствует

безошибочной фиксации символов кода РС. Именно четные ошибки проявляются в качестве ошибочных недвоичных символов на второй ступени декодирования.

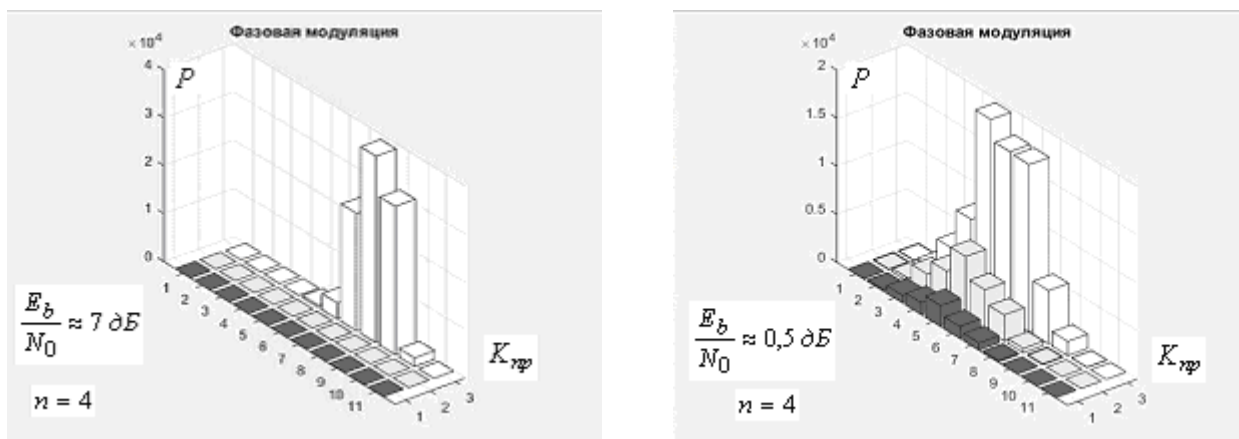


Рисунок 2.20 – Гистограммы оценки ошибочных решений приема недвоичного символа

Именно эти ошибки необходимо исправлять на внешней ступени декодирования. В ряде систем на внутренней ступени декодирования применяют сверточные коды, но, как отмечалось выше, процедура декодирования таких кодов не всегда оптимальна по времени для процесса защиты данных в целом [40]. На примере кодов РС можно показать, что перестановочное декодирование каскадных кодов приводит к снижению вычислительной сложности декодера за счет образования детерминированных структур в вычислительном процессе декодирования. Это позволяет тратить на получение окончательного результата от 28% до 40% арифметических операций меньше в расширенном поле Галуа относительно классических методов декодирования [36]. Применение когнитивных процедур дает дополнительный выигрыш в процедуре минимизации вычислительной сложности декодера.

2.6. Выводы по главе

1. Метод формирования мягких решений недвоичных символов за счет оценки выборочных средних МРС двоичных символов не позволяет адекватно оценить надежность недвоичных символов из-за увеличения неопределенности итоговой оценки при выполнении процедуры усреднения.

2. Выборочное среднее в условиях стабильных показателей отношения сигнал/шум сохраняет линейную зависимость с угловым коэффициентом, который практически не изменяется от объема кортежа данных. Это свойство может быть использовано в системах с когнитивной адаптацией для переключения режимов помехоустойчивого кодирования.

3. Использование метода пересечений для оценки степени совпадения принятой последовательности мягких решений двоичных символов не отвечает целям исследования из-за явного нарушения монотонности величин оценок недвоичных символов в рабочем диапазоне ОСШ. Метод прост в реализации, но требует нормирования полученных результатов из-за открытости верхней границы получаемой оценки. По причине поиска иррациональных выражений метод Бхаттачария повышает сложность вычислительного процесса, особенно при его реализации на ПЛИС.

4. Исследование показало, что применение мягких методов в процессе декодирования недвоичных кодов при использовании двоичных видов модуляции требует гибкого сочетания процедуры оценки МРС в полунепрерывном канале связи и оценки на этой основе символа недвоичного кода. При этом наиболее рациональным подходом к вычислению оценок надежности недвоичных символов следует считать метод отношения правдоподобий полученной серии значений МРС в пределах символа недвоичного кода к эталонной оценке недвоичного символа. Подобный подход имеет наиболее простую реализацию и адекватно отвечает требованиям перестановочного декодирования.

ГЛАВА 3. ЭФФЕКТИВНОЕ ПЕРЕСТАНОВОЧНОЕ ДЕКОДИРОВАНИЕ НЕДВОИЧНЫХ ГРУППОВЫХ КОДОВ

3.1. Классические методы декодирования кодов Рида-Соломона

Коды РС были открыты в 1960 году. В настоящее время эти коды являются одним из наиболее востребованных инструментов помехоустойчивого кодирования [97]. Коды РС эффективно справляются с исправлением группирующихся ошибок, которые возникают при воздействии на канал связи импульсной помехи или при наличии памяти в канале связи [45, 46, 89, 99].

Алгебраические способы декодирования недвоичных кодов РС известны и широко применяются в разнообразных системах обмена данными. Обработка комбинаций этих кодов осуществляется в несколько этапов. Как правило, половина исправляющей мощности кода расходуется на вычисление локаторов ошибок, которые при правильно выполненной процедуре этого этапа декодирования указывают на позиции недвоичных символов в принятой кодовой комбинации, в которых выявлены ошибки. Для исправления ошибок требуется вторая половина мощности кода, когда за счет решения системы линейных уравнений по выявленным локаторам ошибок осуществляется их исправление. Схемы декодирования кодов РС достаточно полно разработаны в теоретическом смысле и в плане их реализации и до настоящего времени представляют собой довольно сложную вычислительную задачу [7, 81]. Типовая схема декодирования, получившая название авторегрессионного спектрального метода декодирования, состоит из следующих шагов [9, 81, 82]:

- вычисление синдрома ошибки (синдромный декодер);
- построение полинома локаторов ошибок, осуществляемое либо посредством высокоэффективного, но сложно реализуемого алгоритма АБМ, либо посредством простого, но медленного алгоритма Евклида;
- нахождение корней данного полинома переборным методом, выполняемым обычно полным перебором возможных значений (алгоритм Ченя);

– определение характера ошибки, сводящееся к построению битовой маски, вычисляемой на основе обращения алгоритма Форни или любого другого алгоритма обращения матрицы;

– исправление ошибочных символов путем наложения битовой маски на информационное слово и последовательного инвертирования всех искаженных битов. Таким образом, можно использовать несколько алгоритмов декодирования кодов РС, которые приведены на рисунках 3.1 – 3.3.

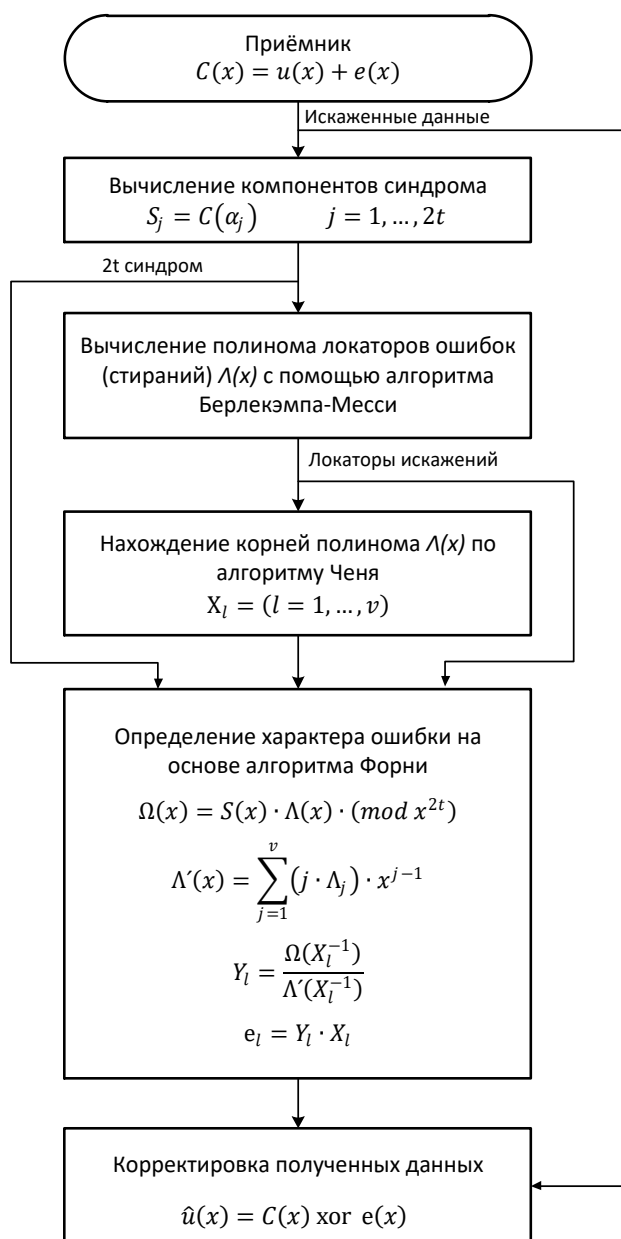


Рисунок 3.1 – Схема быстрого декодирования кодов Рида-Соломона

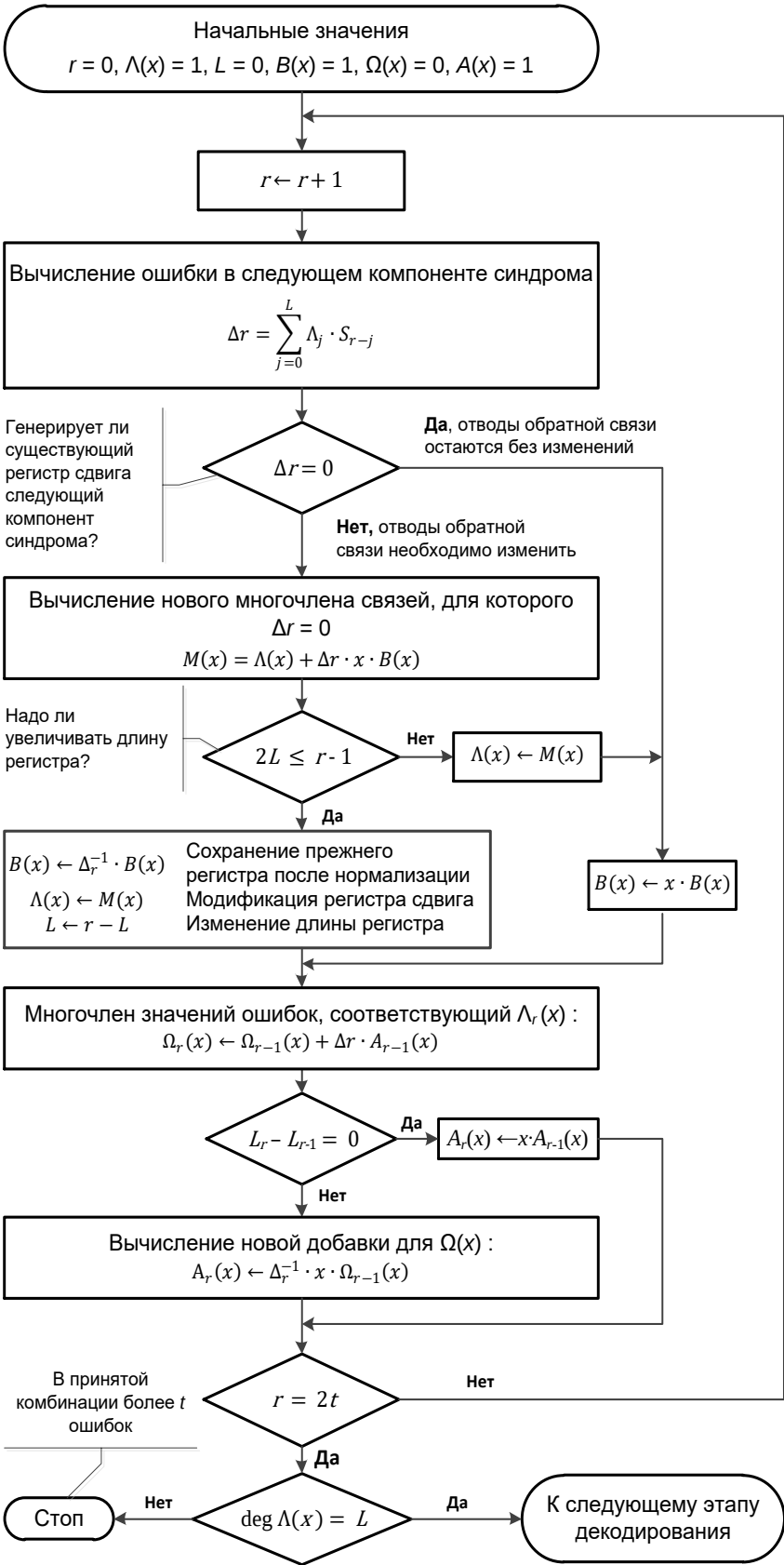


Рисунок 3.2 – Алгоритм Берлекэмпа – Мессии

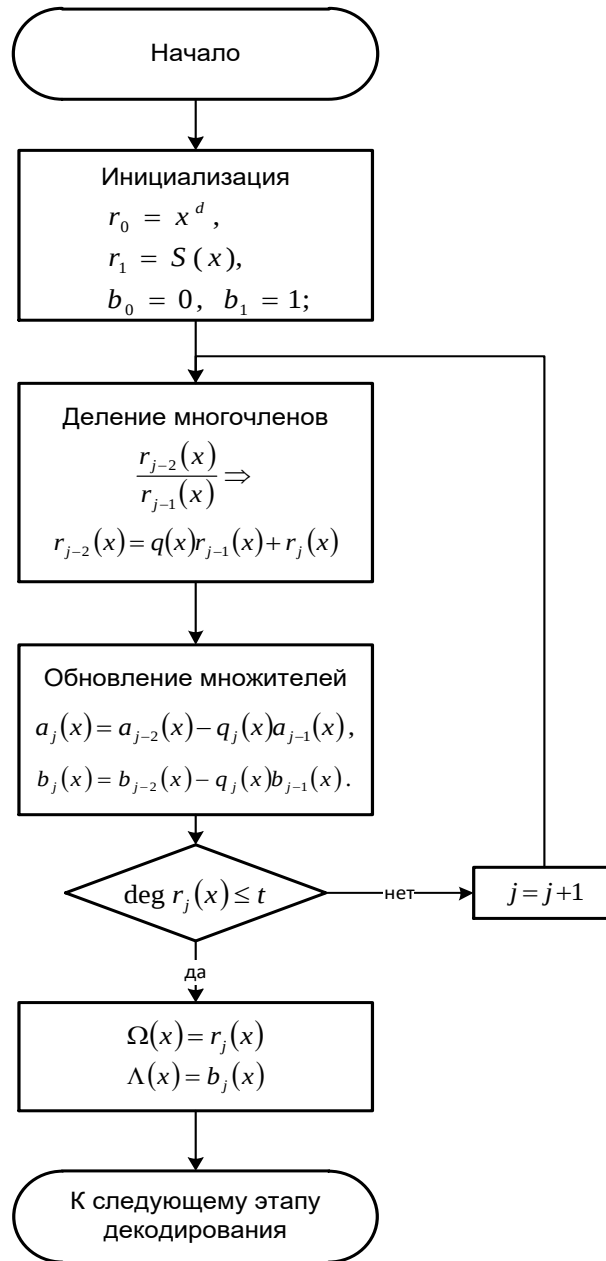


Рисунок 3.3 – Алгоритм Евклида

В научно-технической литературе достаточно много уделено внимания алгоритму Гурсвами-Судана (АГС), который позволяет произвести списочное декодирование кодов РС за полиномиальное время, которое может оказаться чрезмерно большим для практического применения. При этом наиболее трудоемким шагом является построение интерполяционного многочлена от двух переменных, проходящего с некоторой кратностью точке, соответствующей принятым символам [20, 22, 103]. Оригинальный метод списочного декодирования кодов РС приведен в **Приложении А**.

3.2. Оценка сложности реализации классического подхода к декодированию кодов в системе перестановочного декодирования

Для выявления преимуществ предлагаемого метода перестановочного декодирования кодов РС необходимо выявить его возможности по экономии бюджета вычислительного процесса по числу выполняемых декодером такого кода, реализованным на ПЛИС, арифметических операций. Для этого рассмотрим тонкую структуру классического алгоритма декодирования по шагам с оценкой числа элементарных арифметических операций, требуемых для реализации процедуры декодирования.

Прием переданного по каналу кодового вектора V_{np} осуществляется на физическом и канальном уровнях эталонной модели. Для реализации полного цикла вычислений на физическом уровне формируются оценки надежности λ_i в формате целочисленных МРС. Этот процесс в классическом алгоритме и в исследуемом процессе декодирования носит одинаковый характер и поэтому не включается в систему подсчета числа операций.

По этой же причине процедура сортировки принятых жестких решений по абсолютным значениям λ_i на канальном уровне в оценку сложности алгоритма не включается. При этом декодер формально не использует жесткие решения, а оперирует с нумераторами этих решений. Итогом этого этапа обработки принятых данных становится соответствие жестких решений и их МРС в формате биекции $f: V_{np} \rightarrow V_{nep}$, где V_{nep} – вектор переставленных нумераторов принятого вектора V_{np} . На основании этой биекции декодером формируется перестановочная матрица P . В силу адекватности этого шага работы декодера в сравниваемых процессах целесообразно не включать в бюджет подсчета числа операций этот шаг декодирования. Как показывалось в примере 1.2, матрица P носит разреженный характер с числом единиц, равным длине n вектора, используемого в системе помехоустойчивого кода. Поэтому декодер, умножая вектор нумераторов символов из V_{np} на матрицу P , выполнит всего n действий.

Эта операция по числу арифметических вычислений одинакова для кодов с любым основанием. Итогом этого этапа выполнения общего алгоритма является выделение по сформированным приемником МРС λ_i первых k надежных символов, которые будут в дальнейшем представлять информационные символы переставленного кодового вектора формируемого приемником эквивалентного кода.

Пример 3.1. Пусть каноническая последовательность нумераторов принятого вектора кода РС (7,3,5) в результате выполненных действий, описанных выше, получила вид

$$4 \ 5 \ 2 \quad 3 \ 6 \ 7 \ 1.$$

В этой последовательности символы с нумераторами 4 5 2 оказались с наиболее высокими значениями параметра λ_i . В соответствии с этими значениями порождающая матрица исходного кода РС будет представлена как

$$G_{пер} = \begin{pmatrix} \alpha^4 & \alpha^0 & 0 & 0 & \alpha^4 & \alpha^5 & \alpha^0 \\ \alpha^2 & \alpha^0 & \alpha^0 & 0 & \alpha^6 & \alpha^6 & 0 \\ \alpha^3 & \alpha^0 & 0 & \alpha^0 & \alpha^1 & \alpha^3 & 0 \end{pmatrix}$$

В общем случае оценка определителя Δ матрицы $Q_{k \times k}$ потребует 12 операций умножения и 5 операций сложения, выполняемых с элементами поля $GF(2^3)$. Общий итог составляет 17 арифметических операций.

Пример 3.2. Вид матрицы миноров

$$M = \begin{vmatrix} \begin{vmatrix} \alpha^0 & \alpha^0 \\ \alpha^0 & 0 \end{vmatrix} & \begin{vmatrix} \alpha^2 & \alpha^0 \\ \alpha^3 & 0 \end{vmatrix} & \begin{vmatrix} \alpha^2 & \alpha^0 \\ \alpha^3 & \alpha^0 \end{vmatrix} \\ \begin{vmatrix} \alpha^0 & 0 \\ \alpha^0 & 0 \end{vmatrix} & \begin{vmatrix} \alpha^4 & 0 \\ \alpha^3 & 0 \end{vmatrix} & \begin{vmatrix} \alpha^4 & \alpha^0 \\ \alpha^3 & \alpha^0 \end{vmatrix} \\ \begin{vmatrix} \alpha^0 & 0 \\ \alpha^0 & \alpha^0 \end{vmatrix} & \begin{vmatrix} \alpha^4 & 0 \\ \alpha^2 & \alpha^0 \end{vmatrix} & \begin{vmatrix} \alpha^4 & \alpha^0 \\ \alpha^2 & \alpha^0 \end{vmatrix} \end{vmatrix} = \begin{pmatrix} \alpha^0 & \alpha^3 & \alpha^5 \\ 0 & 0 & \alpha^6 \\ \alpha^0 & \alpha^4 & \alpha^1 \end{pmatrix}.$$

Поиск матрицы миноров M для $Q_{k \times k}$ потребует $3 \times 9 = 27$ арифметических операций, а операция транспонирования M в M^T требует 3 действий, не

связанных с вычислениями в поле $GF(2^3)$. Поиск обратной матрицы $Q_{k \times k}^{-1}$ путем деления элементов из M^T на Δ потребует 9 операций.

В соответствии с основным алгоритмом по виду полученной матрицы $Q_{k \times k}^{-1}$ декодер вычисляет переставленную порождающую матрицу кода $G_{пер}^{сис}$, для чего в общем случае максимально потребуется 189 операций умножения и 42 операции сложения, а всего на этом этапе обработки данных потребуется 231 арифметическая операция. Таким образом, окончательно для анализируемого кода в процедуре обработки одного кодового вектора этого кода требуется выполнить 270 операций с элементами поля $GF(2^3)$. С учетом умножения переставленного вектора кода РС на полученную матрицу $G_{пер}^{сис}$ и обратных преобразований кодового вектора эквивалентного кода потребуется дополнительно 66 операций. В итоге необходимо выполнить 336 операций. Из-за матричных вычислений реализация подобного декодера на ПЛИС оценивается как O^3 , что требует дополнительных непроизводительных временных затрат. Предлагаемый метод когнитивной метафоры способствует минимизации объема вычислений. Причем получаемый выигрыш оказывается тем больше, чем больше степень расширения двоичного поля Галуа.

3.3. Декодирование с перестановками недвоичных групповых кодов

Получение сравнительных характеристик различных способов обработки принятых кодовых векторов целесообразно проводить на отдельных примерах с последующим обобщением полученных результатов на все пространство кодовых векторов выбранного кода. При этом, учитывая линейность пространства групповых кодов РС, полученные результаты на отдельном коде РС допустимо переносить на все пространство данного класса кодов. Суть когнитивной метафоры была приведена в первой главе. Применительно к системе перестановочного декодирования можно утверждать, что все допустимые

перестановки теоретически могут быть вычислены для любого кода, и на этой основе порождающие матрицы эквивалентных кодов могут быть вычислены заранее, что, предположительно, снижает сложность реализации процедуры декодирования на ПЛИС. Задачей данного раздела диссертационной работы является выявление таких свойств линейных групповых систематических кодов РС, которые позволят не только оптимизировать процедуру декодирования таких кодов в смысле минимизации объема вычислений, но и найти дополнительные резервы для рациональной организации памяти когнитивной карты декодера, реализуемой на ПЛИС. Основная сложность перестановочного декодирования заключается именно в реализации процесса преобразования $G_{пер} \Rightarrow G_{пер}^{сис}$ с минимальными вычислительными затратами за счет выявления закономерностей матричных преобразований по алгоритмам перестановок [4, 6, 32]. Если результаты таких преобразований сохранить в памяти декодера, то при повторе известных декодеру перестановок нумераторов символов кодовых векторов просто воспользоваться этим результатом. Таким образом, сложный процесс $G_{пер} \Rightarrow G_{пер}^{сис}$ становится обычной базой данных в формате справочной системы или кодовой книги. На вход системы передается последовательность ранжированных нумераторов, в соответствии с которой выбирается соответствующее решение вида $G_{пер} \Rightarrow G_{пер}^{сис}$. В случае двоичных кодов не всякое преобразование указанного вида может явиться основанием для формирования эквивалентного кода. В этом случае нужно просто проверить, относится ли вновь образованная комбинация нумераторов к запрещенному виду. Для двоичных кодов не всякая комбинация нумераторов обеспечивает формирование невырожденной матрицы $Q_{k \times k}$. Если отрицательный ответ подтверждается, то необходима коррекция перестановки. Следует указать, что для кодов РС эта процедура является лишней, поскольку такие коды являются максимально декодируемыми [35, 51, 56, 63].

Анализ показывает, что в наборе нумераторов символов любого кодового вектора следует отличать две группы нумераторов: в первую группу входит ровно

k надежных символов, и нумераторы этой группы в общем случае обеспечивают получение $k!$ перестановок, во вторую группу входят $(n - k)$ нумераторов. При этом для ограниченного множества всех нумераторов выполняется условие $k \notin (n - k)$. Вторая группа потенциально формирует $(n - k)!$ перестановок. Возникает вопрос: в каком отношении находятся нумераторы из подмножества $\{k!\}$ к перестановкам из подмножества $\{(n - k)!\}$? Существуют ли какие-либо закономерности в образовании эквивалентных кодов для таких подмножеств? Первоначально установим закономерности образования порождающих матриц эквивалентных кодов при изменении следования нумераторов в подмножестве $\{k!\}$ при неизменном порядке следования нумераторов во второй части набора номеров. Пусть произвольно выбранными номерами из первого подмножества будут нумераторы 2 5 4, и пусть нумераторы второго подмножества составляют последовательность вида 3 6 7 1. Тогда с использованием выражения (1.11) получают

$$G_{nep} = \begin{vmatrix} 0 & \alpha^0 & \alpha^4 & 0 & \alpha^4 & \alpha^5 & \alpha^0 \\ \alpha^0 & \alpha^0 & \alpha^2 & 0 & \alpha^6 & \alpha^6 & 0 \\ 0 & \alpha^0 & \alpha^3 & \alpha^0 & \alpha^1 & \alpha^3 & 0 \end{vmatrix}.$$

Обратная матрица для матрицы $Q_{3 \times 3}$, найденная с использованием классики матричных преобразований, имеет вид

$$Q_{3 \times 3}^{-1} = \begin{pmatrix} \alpha^6 & \alpha^0 & \alpha^2 \\ \alpha^4 & 0 & \alpha^5 \\ \alpha^1 & 0 & \alpha^1 \end{pmatrix}.$$

Как было показано в главе 1, для реализации процедуры $G_{nep} \Rightarrow G_{nep}^{cic}$ нужно первую строку матрицы G_{nep} умножить на α^6 , вторую строку матрицы G_{nep} умножить на α^0 , а третью строку этой матрицы умножить на элемент G_{nep} . Полученные результаты необходимо сложить для получения первой строки матрицы G_{nep}^{cic} . Таким образом, матрица $Q_{3 \times 3}^{-1}$ является ключевой для реализации

процедуры $G_{nep} \Rightarrow G_{nep}^{cuc}$, поскольку для образования второй строки матрицы G_{nep}^{cuc} необходимо первую строку из G_{nep} умножить на α^4 , а третью строку из G_{nep} умножить на α^5 , затем результаты сложить. Соответственно, для образования третьей строки матрицы G_{nep}^{cuc} необходимо первую и третью строки матрицы G_{nep} последовательно умножить на элемент α^1 и полученные результаты сложить. Только в таком случае на позициях матрицы $Q_{3 \times 3}$ из G_{nep} формируется единичная матрица, как показано ниже

$$G_{nep}^{cuc} = \begin{pmatrix} \alpha^0 & 0 & 0 & \alpha^2 & \alpha^6 & \alpha^2 & \alpha^6 \\ 0 & \alpha^0 & 0 & \alpha^5 & \alpha^5 & \alpha^4 & \alpha^4 \\ 0 & 0 & \alpha^3 & \alpha^1 & \alpha^3 & \alpha^3 & \alpha^1 \end{pmatrix}.$$

Возникает предпосылка к утверждению, что четвертый столбец α^5 полученной матрицы G_{nep}^{cuc} по этой причине всегда будет соответствовать третьему нумератору из состава нумераторов $(n - k)$. Пятый столбец будет соответствовать нумератору 6, и оставшиеся столбцы – нумераторам 7 и 1. Отсюда следует, что изменение порядка следования нумераторов в этой части матрицы не меняет структуру столбцов, и этот фактор можно использовать в целях экономии вычислительного ресурса. Например, при неизменном следовании нумераторов

2 5 4 изменение следования нумераторов второй части, например, с первоначальной последовательности 3 6 7 1 на последовательность 6 7 1 3 обеспечит получение матрицы вида

$$G_{nep}^{cuc} = \begin{pmatrix} \alpha^0 & 0 & 0 & \alpha^6 & \alpha^2 & \alpha^6 & \alpha^2 \\ 0 & \alpha^0 & 0 & \alpha^5 & \alpha^4 & \alpha^4 & \alpha^5 \\ 0 & 0 & \alpha^3 & \alpha^3 & \alpha^3 & \alpha^1 & \alpha^1 \end{pmatrix}.$$

Проверка, проведенная в соответствии с классическим методом поиска обратной матрицы, показывает справедливость этого утверждения. Вместе с этим

возникает предпосылка ко второму важному утверждению. Если задана последовательность нумераторов из множества надежных символов, то любые допустимые перестановки этих нумераторов будут соответствовать перестановкам строк не единичной части матрицы G_{cuc} . Возникает идея введения специального оператора, который назовем оператором быстрых матричных преобразований (БМП).

Пусть в когнитивной карте декодера хранится эталонный образец преобразования вида 2 4 5 и 1 3 6 7. Как видно, нумераторы в обеих частях имеют лексикографический упорядоченный вид. Поиск переставленной матрицы в систематической форме после исключения из ее состава единичной матрицы имеет вид

$$\begin{array}{ccccc} \alpha^6 & \alpha^2 & \alpha^6 & \alpha^2 & 2 \\ \alpha^1 & \alpha^1 & \alpha^3 & \alpha^3 & 4 \\ \alpha^4 & \alpha^5 & \alpha^5 & \alpha^4 & 5 \\ 1 & 3 & 6 & 7 & \end{array}$$

Получим из приведенного выше лексикографически упорядоченного оператора систематическую матрицу, в которой нумераторы столбцов были расположены в формате 2 5 4 и 3 6 7 1. Получаем последовательность действий

$$\begin{array}{ccccccccc} \alpha^6 & \alpha^2 & \alpha^6 & \alpha^2 & 2 & \alpha^6 & \alpha^2 & \alpha^6 & \alpha^2 & 2 & \alpha^2 & \alpha^6 & \alpha^2 & \alpha^6 & 2 \\ \alpha^1 & \alpha^1 & \alpha^3 & \alpha^3 & 4 & \Rightarrow & \alpha^4 & \alpha^5 & \alpha^5 & \alpha^4 & 5 & \Rightarrow & \alpha^5 & \alpha^5 & \alpha^4 & \alpha^4 & 4 \\ \alpha^4 & \alpha^5 & \alpha^5 & \alpha^4 & 5 & \Rightarrow & \alpha^1 & \alpha^1 & \alpha^3 & \alpha^3 & 4 & \Rightarrow & \alpha^1 & \alpha^3 & \alpha^3 & \alpha^1 & 5 \\ 1 & 3 & 6 & 7 & & & 1 & 3 & 6 & 7 & & & 3 & 6 & 7 & 1 \end{array}$$

Полученный результат соответствует результату, полученному выше, с использованием классической процедуры формирования порождающей матрицы эквивалентного кода. Заметно, что для получения искомой матрицы из эталонной формы было затрачено всего n шагов, не связанных с выполнением арифметических действий в поле Галуа $GF(2^3)$. Очевидно, что последовательность перестановки строк и столбцов можно изменить без последствий для окончательного результата. При этом по любому вычисленному

оператору в произвольной форме всегда можно определить за счет обратных упорядоченных действий оператор в лексикографической форме.

Лексикографическая форма необходима для ускорения поиска образца эталонной матрицы в системе когнитивной карты. Приведенный оператор необходимо вычислять для всех образцов сочетаний номеров нумераторов, определяющих семейство надежных символов. Таких перестановок будет ровно $\binom{n}{k}$. Остается открытым вопрос о необходимости хранения всех таких образцов.

Учитывая, что групповые коды обычно обладают свойством цикличности, целесообразно использовать это свойство для снижения объема хранимых в когнитивной карте декодера данных.

3.4. Оценка алгоритма декодирования с использованием оператора быстрых матричных преобразований

Оценка впервые предложенного способа применения к алгоритмам перестановочного декодирования оператора БМП может быть на данном этапе исследований дана только относительно известного классического метода обработки кодовых векторов путем перестановок. Известный метод формирования матрицы эквивалентного кода не является производительным и не может быть использован в современных когерентных системах. Даже в условиях применения высокопроизводительных процессоров, но при использовании в системе обработки данных кодов РС с практически значимыми параметрами не обеспечивается требуемая сложность реализации процесса декодирования. Именно это обстоятельство препятствовало применению метода перестановок в реальных системах связи [3, 4, 6, 14, 107]. Метод БМП существенно улучшает ситуацию по снижению вычислительной сложности процессора приемника. Его эффективность основана на применении когнитивной карты, где хранятся результаты вычислений не только обратных матриц, требуемых для формирования эквивалентных кодов, но и разработана оригинальная система

упаковки данных о таких матрицах, которая резко сокращает объем памяти, требуемый для хранения подобных матриц. Основанием для подобного рассуждения является введенное в работе понятие эталонной матрицы, из которой может быть получено все семейство эталонных матриц, связанное с вариациями конкретного набора нумераторов как надежных символов перестановки, так и восстанавливаемых данных. При сравнении указанных методов целесообразно вычислить число элементарных арифметических операций (умножение и сложение). В процедуре вычисления эквивалентной матрицы в классической методике мы для этого выбираем различные коды РС и вычисляем число арифметических операций.

Таблица 3.1 – Число арифметических операций в процедуре классического вычисления матрицы эквивалентного кода

$PC(7,3,5)$	$PC(15,5,11)$	$PC(15,9,7)$	$PC(15,13,3)$
336	2410	2912994	68584334026
$6720 \cdot 10^{-9}$ с	$48200 \cdot 10^{-9}$ с	$58259880 \cdot 10^{-9}$ с	$1371686680520 \cdot 10^{-9}$ с
Число операций при реализации предлагаемого метода			
(3+4) 7	(5+10) 15	(9+6) 15	(13+2) 15
$140 \cdot 10^{-9}$ с	$300 \cdot 10^{-9}$ с	$300 \cdot 10^{-9}$ с	$300 \cdot 10^{-9}$ с
Выигрыш в 48 раз	Выигрыш в $1,6 \cdot 10^2$ раза	Выигрыш в $1,9 \cdot 10^6$ раза	Выигрыш в $4,6 \cdot 10^9$ раза

В таблице 3.1 в последней строке получено число операций, которые не являются арифметическими, а представляют собой обычное копирование элементов эквивалентной матрицы и перенос этих данных в модель новой матрицы. Технология копирования и переноса данных показана на рисунке 3.4.

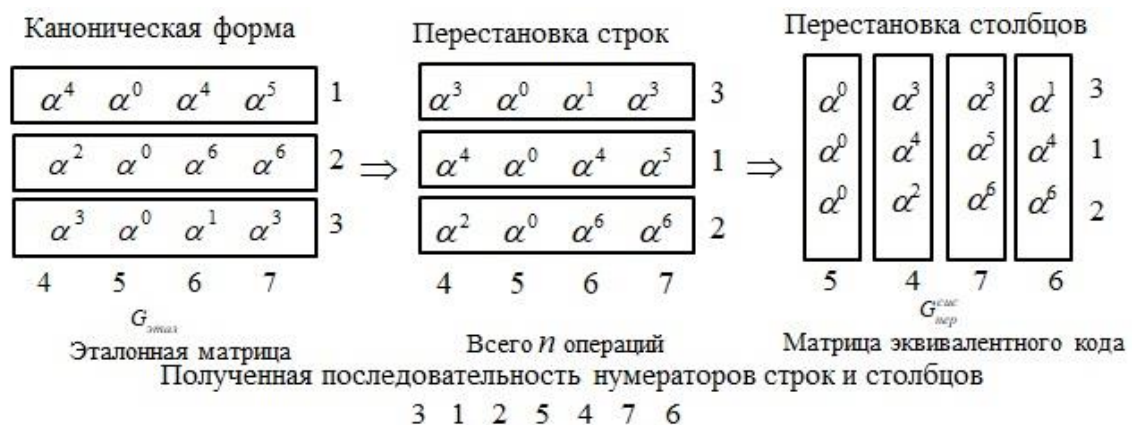


Рисунок 3.4 – Технология перестановки данных

Программа реализации процедуры перестановки данных представлена на рисунке 3.5.

```

clc
Go = [1,0,0,4,0,4,5;
      0,1,0,2,0,6,6;
      0,0,1,3,0,1,3,];
G = [4,0,4,5;
      2,0,6,6;
      3,0,1,3,];
[M, N] = size(G);
disp('Исходная матрица');
disp(Go);
disp(G);
disp('перестановка столбцы ')
B(:,1)= G (:,4,1);
B(:,2)= G (:,1,1);
B(:,3)= G (:,2,1);
B(:,4)= G (:,3,1);
disp(B);
disp('перестановка строчки ')
B1(1,:)= G (3, :,1);
B1(2,:)= G (1, :,1);
B1(3,:)= G (2, :,1);
disp(B1);
disp('перестановка столбцы и строчки ')

B2(:,1)= G (:,4,1);
B2(:,2)= G (:,1,1);
B2(:,3)= G (:,2,1);
B2(:,4)= G (:,3,1);
Bn(1,:)= B2 (3, :,1);
Bn(2,:)= B2 (1, :,1);
Bn(3,:)= B2 (2, :,1);
disp(Bn);
disp('циклический сдвиг столбцы и строчки');
Y = circshift(G,[1,1]);
disp(Y);
disp('циклический сдвиг строчки');
W = circshift(G,2,1);
disp(W);

```

Рисунок 3.5 – Реализация технологии переноса данных в MATLAB

Важно отметить, что перенос данных не является арифметической операцией, следовательно, в процедуре декодирования данных в расширенных двоичных полях Галуа нет необходимости в ходе вычислений обращаться к таблицам сложения и умножения. Это является мощным ресурсом в организации вычислительного процесса в системе обработки недвоичных кодов.

Детальное изучение тонкой структуры предложенного алгоритма и исследование возможностей использования циклических свойств кодов РС вскрыли ряд факторов, при использовании которых возможно дополнительное

повышение эффективности вычислительного процесса в смысле снижения его сложности. Модификация метода рассматривается ниже.

3.5. Модифицированный метод перестановочного декодирования на базе когнитивной карты

Использование в системе обработки кодовых векторов метода перестановок надежно принятых символов на позиции информационных разрядов оператора БМП позволяет сократить время, необходимое для поиска вектора ошибок. Указанное сокращение временного интервала обеспечивается за счет хранения в когнитивной карте декодера готового результата матрицы $G_{пер}^{сис}$, являющейся матрицей эквивалентного кода, которая однозначно отвечает конкретной перестановке нумераторов ранжированного кодового вектора. Рассматривая структуру ПЛИС, можно заметить, что оперативная память таких процессоров не предоставляет больших возможностей по хранению данных. Отсюда возникает задача организации вычислительного процесса на базе ПЛИС таким образом, чтобы наряду с сокращением времени, необходимого для поиска матрицы $G_{пер}^{сис}$ (за счет оператора БМП), добиться сокращения объема памяти когнитивной карты. Желательно хранить эталонные матрицы именно в оперативной памяти ПЛИС, чтобы исключить временные потери для поиска требуемых на данном временном отрезке эталонов в системах хранения данных, размещенных вне оперативной памяти ПЛИС.

Анализируя циклические свойства комбинаций кодов РС, можно отметить, что их допустимо продуктивно использовать в вычислительном процессе. В ходе проведения численных экспериментов было установлено, что циклический сдвиг нумераторов символов, устанавливаемых на позиции информационных разрядов, приводит однозначно к одной и той же матрице вида $G_{пер}^{сис}$. Пусть в результате сортировки принятых символов по значениям МРС сформировались две группы нумераторов, относящихся к надежным и ненадежным символам. Для удобства

последующих рассуждений представим эти группы нумераторов в виде 4 5 2 и 3 6 7 1. Учитывая структуру первой группы нумераторов, требуется найти начало цикла для указанной перестановки с таким расчетом, чтобы в трехзначной группе оказались нумераторы с минимальными по абсолютной величине значениями. Такой последовательностью нумераторов будет блок 1 2 6 и соответствующий ему блок нумераторов символов с низкими значениями МРС 7 3 4 5. Оценка матрицы вида $G_{пер}^{cис}$ для указанной системы блоков нумераторов с использованием классической схемы поиска обратной матрицы $Q_{3 \times 3}^{-1}$ привела к результату

$$\begin{array}{cccc} \alpha^1 & \alpha^3 & \alpha^3 & \alpha^1 & 1 \\ \alpha^5 & \alpha^5 & \alpha^4 & \alpha^4 & 2 \\ \alpha^2 & \alpha^6 & \alpha^2 & \alpha^6 & 6 \\ 7 & 3 & 4 & 5 \end{array}.$$

Однако подобный результат может быть получен и для последовательностей 4 5 2 и 3 6 7 1, являющихся циклическим продолжением последовательностей нумераторов вида 1 2 6 и 3 6 7 1, которые могут быть получены с использованием оператора БМП из соответствующей эталонной матрицы, как показано ниже

$$\begin{array}{ccccccccc} \alpha^6 & \alpha^2 & \alpha^6 & \alpha^2 & 2 & \alpha^1 & \alpha^1 & \alpha^3 & \alpha^3 & 4 & \alpha^1 & \alpha^3 & \alpha^3 & \alpha^1 & 4 \\ \alpha^1 & \alpha^1 & \alpha^3 & \alpha^3 & 4 & \Rightarrow & \alpha^4 & \alpha^5 & \alpha^5 & \alpha^4 & 5 & \Rightarrow & \alpha^5 & \alpha^5 & \alpha^4 & \alpha^4 & 5 \\ \alpha^4 & \alpha^5 & \alpha^5 & \alpha^4 & 5 & & \alpha^6 & \alpha^2 & \alpha^6 & \alpha^2 & 2 & & \alpha^2 & \alpha^6 & \alpha^2 & \alpha^6 & 2 \\ 1 & 3 & 6 & 7 & & & 1 & 3 & 6 & 7 & & & 3 & 6 & 7 & 1 \end{array}$$

Аналогичная проверка по другим циклическим сдвигам, которые приведены в таблице 3.2, подтвердила версию о том, что любые упорядоченные циклические сдвиги нумераторов в пределах длины кодового вектора соответствуют единственным образом только одному виду эталонной матрицы. При этом объем хранимых в когнитивной карте эталонных матриц сокращается в n раз, с учетом всех возможных перестановок для выбранной структуры цикла объем памяти когнитивной карты может быть сокращен на $(n \times k! \times (n - k)!) - 1 = 143$ эталонные

матрицы, что является достаточно эффективным с точки зрения экономии оперативной памяти ПЛИС. Проверка сочетания номеров нумераторов вида 7 1 5 и 6 2 3 4 однозначно приводит к известному оператору БМП первого типа

$$\begin{array}{cccccc} \alpha^1 & \alpha^3 & \alpha^3 & \alpha^1 & 7 \\ \alpha^5 & \alpha^5 & \alpha^4 & \alpha^4 & 1 \\ \alpha^2 & \alpha^6 & \alpha^2 & \alpha^6 & 5 \\ 6 & 2 & 3 & 4 \end{array}.$$

Таблица 3.2 – Циклические сдвиги нумераторов образца 126

126	7345
237	1456
341	2567
452	3671
563	4712
674	5123
715	6234

Для рассматриваемого в разделе сравнительно короткого кода (7,3,5) можно сформировать еще четыре образца циклов, поэтому общий объем высвобождаемой оперативной памяти ПЛИС для рассматриваемого кода составляет примерно

$$\{[(n \times k! \times (n - k)!)] \times q - 5\} \times 36 = 715 \times 36 \approx 25 \text{ кбит}.$$

Все возможные сочетания перестановок в системе циклических сдвигов представлены в таблице 3.3. В этой связи целесообразно для данного кода представить все возможные циклические сдвиги нумераторов и оценить трансформацию операторов БМП, представив их в отдельной таблице. При этом следует учитывать, что полученные данные не упорядочены лексикографически и по этой причине не приспособлены для быстрого их поиска в оперативной памяти ПЛИС. Лексикографическое упорядочение можно проводить как по первой группе нумераторов, относящихся к кортежу надежных символов, или по обеим группам одновременно для быстрой трансформации оператора БМП в требуемую

перестановку и отыскания соответствующего образа оператора. Применение этих принципов позволит сократить время поиска необходимой информации.

Таблица 3.3 – Сочетания номеров надежных символов комбинаций кода РС с однотипными порождающими матрицами в каноническом виде

G_{cuc}^1	G_{cuc}^2	G_{cuc}^3	G_{cuc}^4	G_{cuc}^5
123 – 4567	124 – 3567	125 – 6734	126 – 7345	135 – 6724
234 – 5671	235 – 4671	236 – 7145	237 – 1456	246 – 7135
345 – 6712	346 – 5712	347 – 1256	341 – 2567	357 – 1246
456 – 7123	457 – 6123	451 – 2367	452 – 3671	461 – 2357
567 – 1234	561 – 2347	562 – 3471	563 – 4712	572 – 3461
671 – 2345	672 – 3451	673 – 4512	674 – 5123	613 – 4572
712 – 3456	713 – 4562	714 – 5623	715 – 6234	724 – 5613

В таблице 3.3 закрашены позиции, в которых первые три нумератора не являются каноническими. Иначе говоря, такие позиции лексикографически не упорядочены. Ранжирование всех нумераторов и размещение их в списке по возрастанию их значений позволят оперативно отыскивать соответствующий оператор БМП. Прежде чем проводить подобную трансформацию данных, необходимо убедиться в том, что все операторы БМП, принадлежащие одному столбцу таблицы 3.3, имеют одинаковую структуру.

В соответствии с приведенными выше рассуждениями можно предварительно предположить, что оператором БМП будет являться собственно порождающая матрица кода, на что указывает верхняя строка первой колонки данных наборов нумераторов. Проверка этого утверждения осуществлялась на примере набора 4 5 6 и 7 1 2 3. Прямое вычисление матрицы $G_{пер}^{cuc}$ для этого набора нумераторов показало, что оператор БМП для него в точности

повторяет структуру проверочной части порождающей матрицы кода. Предположение нашло свое подтверждение, т.е. оператор БМП равен

$$\begin{array}{ccccc} \alpha^4 & \alpha^0 & \alpha^4 & \alpha^5 & 4 \\ \alpha^2 & \alpha^0 & \alpha^6 & \alpha^6 & 5 \\ \alpha^3 & \alpha^0 & \alpha^1 & \alpha^3 & 6 \\ 7 & 1 & 2 & 3 & \end{array}.$$

Для второй колонки набора нумераторов оператор БМП принимает значение

$$\begin{array}{ccccc} \alpha^1 & \alpha^3 & \alpha^1 & \alpha^0 & 1 \\ \alpha^6 & \alpha^2 & \alpha^6 & \alpha^0 & 2 \\ \alpha^4 & \alpha^4 & \alpha^5 & \alpha^0 & 4 \\ 3 & 5 & 6 & 7 & \end{array}.$$

Для наборов нумераторов третьей колонки значение оператора БМП оценивалось по комбинациям нумераторов вида

$$\begin{array}{ccccc} \alpha^6 & \alpha^2 & \alpha^0 & \alpha^6 & 2 \\ \alpha^5 & \alpha^4 & \alpha^0 & \alpha^5 & 3 \\ \alpha^1 & \alpha^3 & \alpha^0 & \alpha^3 & 6 \\ 7 & 1 & 4 & 5 & \end{array}.$$

Для четвертой колонки данных оператор БМП получен выше.

Для пятой колонки нумераторов оператор БМП равен

$$\begin{array}{ccccc} \alpha^3 & \alpha^1 & \alpha^0 & \alpha^1 & 1 \\ \alpha^5 & \alpha^4 & \alpha^0 & \alpha^5 & 3 \\ \alpha^6 & \alpha^6 & \alpha^0 & \alpha^2 & 5 \\ 6 & 7 & 2 & 4 & \end{array}.$$

Таким образом, вместо 35 различных операторов БМП в системе оперативной памяти ПЛИС требуется в 7 раз меньше объема памяти.

Вскрытое свойство циклических перестановок нумераторов надежных символов и символов, подлежащих коррекции, объединенных системой циклических перестановок, в общем случае требует в n раз меньше объема

памяти, что существенно влияет на процедуру реализации перестановочного декодера на ПЛИС.

Вместе с этим доказанное свойство циклических перестановок нумераторов не отвечает на вопрос: каким образом рационально организовать память когнитивной карты с целью быстрого извлечения из памяти этой карты необходимого оператора БМП? Если такой оператор из памяти когнитивной карты извлечен, то порождающая матрица вида $G_{пер}^{cис}$ будет немедленно найдена за счет добавления слева соответствующей единичной матрицы.

Будем считать, что декодер сформировал произвольный набор нумераторов, ранжированных по значениям соответствующих МРС. Использование таблицы 3.3 оказывается крайне нерациональным, поскольку необходимы временные затраты на перебор данных этой таблицы с целью отыскания необходимого образа оператора БМП. Этот стохастический интервал времени (декодер может практически сразу встретить нужный набор, а может идентифицировать требуемый набор в конце цикла перебора) крайне не желателен в системе обработки данных процессором. С целью устранения указанного недостатка в организации алгоритма декодирования предлагается следующая процедура поиска необходимого оператора БМП. Когнитивная карта организуется как система ярлыков. Отдельно взятый ярлык состоит из двух типов данных.

Во-первых, ярлык содержит строчку данных, упорядоченных по возрастанию значений нумераторов, что позволяет реализовать лексикографический поиск нужного продолжения алгоритма.

Во-вторых, с канонической формой представления нумераторов (упорядоченной по возрастанию значений нумераторов) всегда увязывается конкретная матрица из таблицы 3.3, а значение соответствующих индексов в операторе БМП берется напрямую из второй строки ярлыка. Проверочные части матриц эквивалентных кодов совместно с их циклическими нумераторами показаны в таблице 3.4.

Таблица 3.4 – Сочетания номеров надежных символов комбинаций кода РС с однотипными порождающими матрицами в циклическом виде (матрицы и ее циклы)

G_{cuc}^1	G_{cuc}^2	G_{cuc}^3	G_{cuc}^4	G_{cuc}^5
123 – 4567 $\begin{pmatrix} \alpha^4 & \alpha^0 & \alpha^4 & \alpha^5 \\ \alpha^2 & \alpha^0 & \alpha^6 & \alpha^6 \\ \alpha^3 & \alpha^0 & \alpha^1 & \alpha^3 \end{pmatrix}$	124 – 3567 $\begin{pmatrix} \alpha^1 & \alpha^3 & \alpha^1 & \alpha^0 \\ \alpha^6 & \alpha^2 & \alpha^6 & \alpha^0 \\ \alpha^4 & \alpha^4 & \alpha^5 & \alpha^0 \end{pmatrix}$	125 – 6734 $\begin{pmatrix} \alpha^6 & \alpha^2 & \alpha^0 & \alpha^6 \\ \alpha^5 & \alpha^4 & \alpha^0 & \alpha^5 \\ \alpha^1 & \alpha^3 & \alpha^0 & \alpha^3 \end{pmatrix}$	126 – 7345 $\begin{pmatrix} \alpha^1 & \alpha^3 & \alpha^3 & \alpha^1 \\ \alpha^5 & \alpha^5 & \alpha^4 & \alpha^4 \\ \alpha^2 & \alpha^6 & \alpha^2 & \alpha^6 \end{pmatrix}$	135 – 6724 $\begin{pmatrix} \alpha^3 & \alpha^1 & \alpha^0 & \alpha^1 \\ \alpha^5 & \alpha^4 & \alpha^0 & \alpha^5 \\ \alpha^6 & \alpha^6 & \alpha^0 & \alpha^2 \end{pmatrix}$
234 – 5671	235 – 4671	236 – 7145	237 – 1456	246 – 7135
345 – 6712	346 – 5712	347 – 1256	341 – 2567	357 – 1246
456 – 7123	457 – 6123	451 – 2367	452 – 3671	461 – 2357
567 – 1234	561 – 2347	562 – 3471	563 – 4712	572 – 3461
671 – 2345	672 – 3451	673 – 4512	674 – 5123	613 – 4572
712 – 3456	713 – 4562	714 – 5623	715 – 6234	724 – 5613

Для быстрого поиска необходимой матрицы используют расширенный формат когнитивной карты, представленный в таблице 3.5. В соответствии с этим форматом в карту заносятся сведения о перестановке столбцов порождающей матрицы, и указывается цикл, к которому относится та или иная перестановка. Поскольку в приводимых примерах циклов всего пять, объем когнитивной карты существенно сокращается. Кроме того, алгоритм поиска проверочной части порождающей матрицы эквивалентного кода существенно упрощается за счет простых перестановок строк и столбцов эталонных матриц, извлекаемых из памяти когнитивной карты.

Для реализации алгоритма требуется принять стохастический набор значений нумераторов и привести их в каноническую форму, затем найти в когнитивной карте декодера соответствующий ярлык и по второй строке ярлыка

отыскать образ оператора БМП в каноническом виде. Далее напрямую заменить в нем соответствующие нумераторы строк и столбцов и выполнить соответствующие перестановки строк и столбцов по реальному набору нумераторов с последующим формированием требуемой матрицы вида $G_{пер}^{сис}$.

Таблица 3.5 – Сводная таблица ярлыков

$G_{сис}^1$	$G_{сис}^2$	$G_{сис}^3$	$G_{сис}^4$	$G_{сис}^5$
123 – 4567 – 1 123 – 4567	124 – 3567 – 2 124 – 5673	125 – 3467 – 3 125 – 6734	126 – 3457 – 4 126 – 7345	127 – 3456 – 1 712 – 3456
134 – 2567 – 1 341 – 2567	135 – 2467 – 5 135 – 6724	136 – 2457 – 5 613 – 4572	137 – 2456 – 2 713 – 4562	145 – 2367 – 3 451 – 2367
146 – 2357 – 5 461 – 2357	147 – 2356 – 3 714 – 5623	156 – 2347 – 2 561 – 2347	157 – 2346 – 4 715 – 6234	167 – 2345 – 1 671 – 2345
234 – 1567 – 1 234 – 5671	235 – 1467 – 2 235 – 6714	236 – 1457 – 3 236 – 7145	237 – 1456 – 4 237 – 1456	245 – 1367 – 4 452 – 3671
246 – 1357 – 5 246 – 7135	247 – 1356 – 5 724 – 5613	256 – 1347 – 3 562 – 3471	257 – 1346 – 5 572 – 3461	267 – 1345 – 2 672 – 3451
345 – 1267 – 1 345 – 6712	346 – 1257 – 2 346 – 7125	347 – 1256 – 3 347 – 1256	356 – 1247 – 4 563 – 4712	357 – 1246 – 5 357 – 1246
367 – 1245 – 3 673 – 4512	456 – 1237 – 1 456 – 7123	457 – 1236 – 2 457 – 1236	467 – 1235 – 4 674 – 5123	567 – 1234 – 1 567 – 1234

Архитектура устройства управления, реализующего алгоритм быстрых матричных преобразований на ПЛИС, показана на рисунках 3.6 и 3.7, представляет систему регистров, которые в исходном состоянии готовы к приему новых данных из выбранной декодером эталонной матрицы. Содержание проверочной части матрицы по конфигурации заданной перестановки извлекается из памяти когнитивной карты декодера и заносится в верхний ряд регистров через устройство контроля. В оставшейся свободной части устройства среди регистров нижнего ряда создается образ будущей переставленной матрицы, характерной для

трансляции строк, в которую заносятся по адресу перестановки надежных символов строки из эталонной матрицы (группа верхних регистров).

После этой операции группа верхних регистров оказывается свободной от оперативной информации. Именно в эту группу вносятся изменения из нижнего регистра. В отличие от первого шага в верхние регистры заносятся столбцы данных из нижней группы регистров.

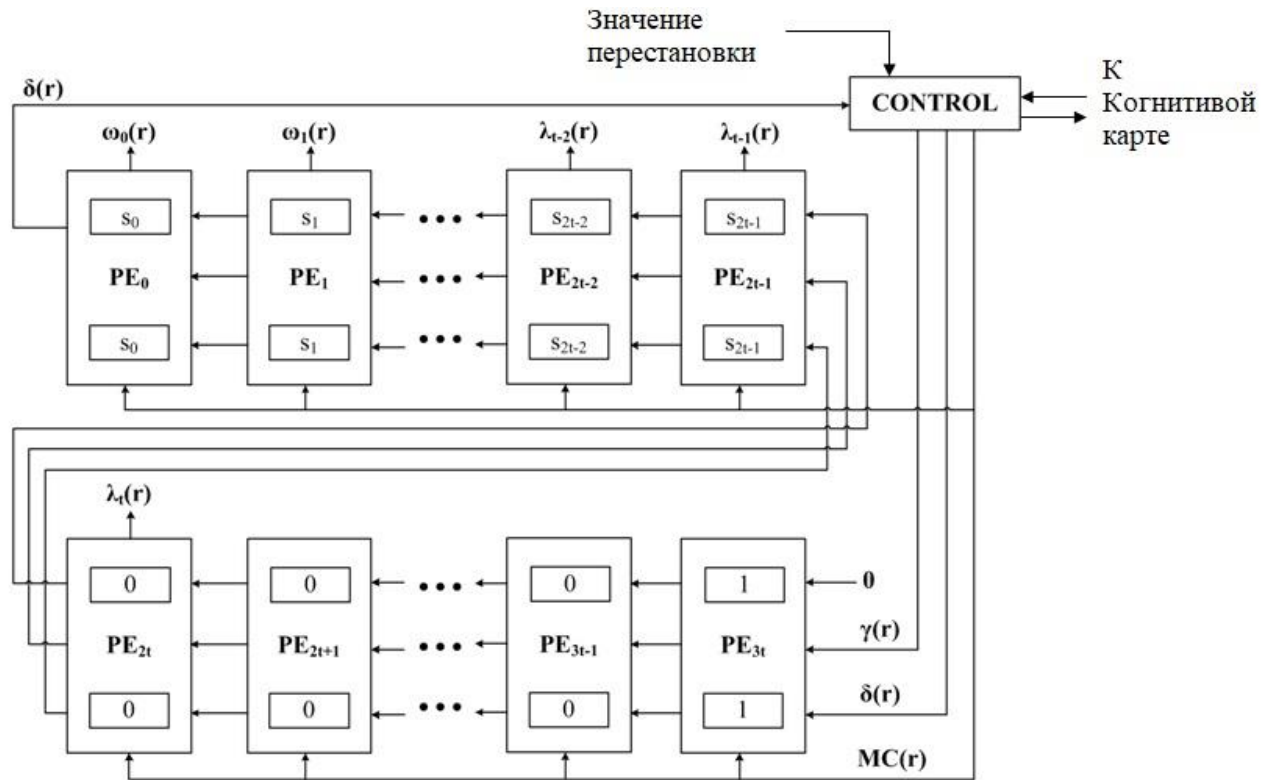


Рисунок 3.6 – Схема устройства, работающего по алгоритму быстрого преобразования матриц

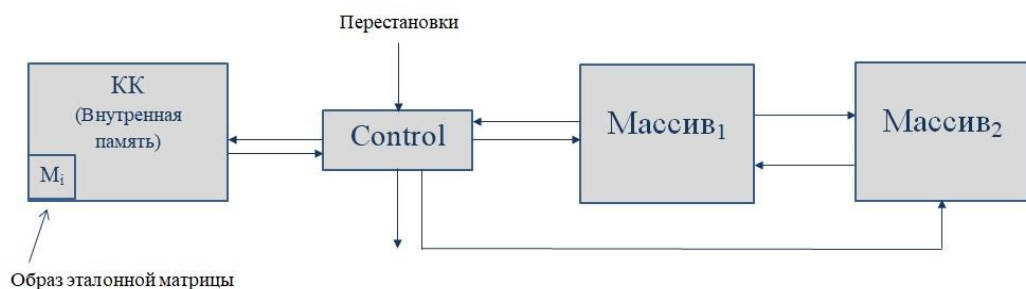


Рисунок 3.7 – Принцип реализации на ПЛИС

Пример реализации на ПЛИС "Альтера" показан в таблице 3.6 для различных видов матриц.

Таблица 3.6 – Возможность реализации когнитивной карты декодера относительно внутренней памяти ПЛИС "Альтера"

Коды	1 система (общ) полное множества матриц	2 система (БМП) система эталонных матриц	3 система (ЦС) циклические свойства эталонных матриц
РС (7,3,5) полигон	$V_{kk} \ll 1\%$ $(9 * 10^{-4})$ Мбайт	$V_{kk} \ll 1\%$ $(1,5 * 10^{-4})$ Мбайт	$V_{kk} \ll 1\%$ $(2,1 * 10^{-5})$ Мбайт
РС (15,11,5)	5715950%	1,5%	0,1%
РС (15,7,9)	43300%	8,6%	0,5%
РС (255,251,5) РС (40,36,5)	Очень большой объем	625%	15%

Таким образом, формируется итоговый результат, к которому в последующих шагах добавляется единичная матрица для получения переставленной порождающей матрицы эквивалентного кода. Вся процедура управления работой декодера выполняется в двухходовом цикле. Подобная структура устройства управления позволяет динамически перестраивать его в зависимости от параметров кода. Блок CONTROL управляет динамической перестройкой устройства за счет переключения связей внутри сдвигового регистра. При этом все основные параметры устройства такие, как критический путь, аппаратные затраты, скорость работы, будут соответствовать параметрам наиболее избыточного кода.

Выигрыш в логарифмическом масштабе для различных кодов РС представлен на рисунках 3.8 и 3.9.

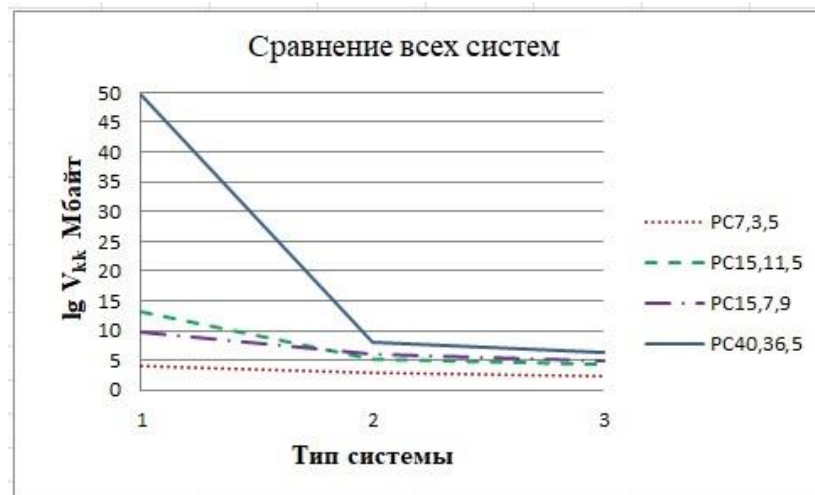


Рисунок 3.8 – Сравнение между тремя системами

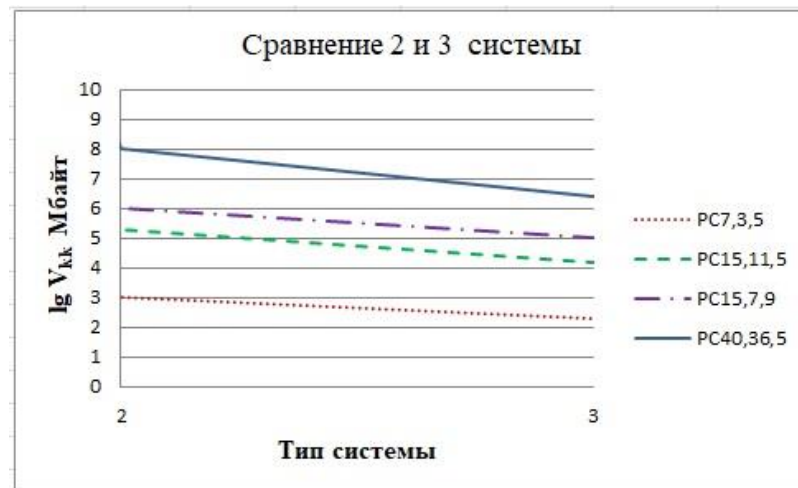


Рисунок 3.9 – Сравнение между двумя системами

3.6. Выводы по главе

1. Применение в системах управления недвоичных кодов связано с необходимостью повышения скорости передачи управляющей информации от управляющего объекта к управляемому модулю или объекту. Кроме того, такие коды в наибольшей степени приспособлены для обработки видеоданных, которые в современных системах управления все чаще используются в качестве интегральной оценки достижения целевой функции. При этом наибольшую нагрузку по обработке данных испытывает управляющая система, которая по ряду объективных причин имеет для реализации подобной процедуры лучшие условия и возможности.

2. Применение недвоичных кодов в системах управления оправдано с точки зрения конструктивных возможностей системы обмена управляющими командами и собственно информационной составляющей системы управления за счет использования хорошо апробированных на практике систем каскадного кодирования на базе недвоичных кодов РС.

3. Главным недостатком классических методов декодирования кодов РС является использование процедуры подбора полинома ошибок по алгоритму Берлекэмп-Мессе. Это снижает скорость обработки данных управляющей информации даже в условиях возникновения ошибок небольшой кратности. Указанный метод не является эффективным при возникновении большого числа ошибок в кодовом векторе. Принципиально метод Судана имеет аналогичные недостатки и в основном направлен на вычисление локаторов ошибок небольшой кратности.

4. Применение метода перестановочного декодирования открывает новые возможности по снижению сложности реализации декодеров недвоичных кодов за счет организации когнитивной карты декодера и использования быстрых матричных преобразований в системе поиска эквивалентных кодов. Показано преимущество разработанного метода относительно классического подхода при реализации алгоритма перестановочного декодирования. Разработана программа реализации разработанного алгоритма в системе программно-аппаратной реализации декодера.

5. В целях сокращения объема памяти когнитивной карты декодера предложен и разработан метод лексикографической организации памяти когнитивной карты, основанный на циклических свойствах групповых кодов и, в частности, кодов РС. Доказана целесообразность использования процедуры последовательных преобразований эталонных матриц когнитивной карты за счет тривиальных перестановок строк и столбцов таких матриц.

ЗАКЛЮЧЕНИЕ

Постановка и решение задач оптимизации управления, в том числе и автоматического, отличаются большим разнообразием. Алгоритмы оптимального и субоптимального управления целесообразно осуществлять с учетом решаемых задач и условий, для которых предназначен тот или иной алгоритм. Подобные задачи могут решаться системой в целом, включающей не только аппаратные и программные модули формирования управляющих воздействий, но и модули оценивания, идентификации, адаптации, реконфигурации. Алгоритмы оптимального (субоптимального) автоматического управления целесообразно классифицировать по объему необходимой априорной и текущей (апостериорной) информации, минимизируемому функционалу, необходимой вычислительной производительности и возможностям адаптации к воздействию деструктивных факторов. Главной трудностью решения современных проблем систем управления остается необходимая вычислительная производительность. Преодоление этой трудности возможно только на пути сочетания развитой системы моделирования алгоритмического обеспечения с численными методами как формой реализации указанных алгоритмов.

Основные научные результаты диссертационной работы состоят в следующем:

1. Впервые разработана модель декодера избыточного кода, использующая методы когнитивной обработки при реализации процедуры перестановочного декодирования для защиты команд дистанционного управления от влияния деструктивных факторов управляющих и управляемых объектов.

2. Математически обоснован сокращенный алгоритм декодирования избыточных кодов по упорядоченным статистикам с использованием когнитивной карты декодера, в котором реализуется процедура когнитивного формирования мягких решений символов с системой выявления достоверных оценок на длине кодового вектора.

3. Разработан метод снижения объема памяти когнитивной карты декодера от двух до трех порядков в зависимости от параметров кода за счет использования подмножества эталонных матриц эквивалентных кодов, которые на базе предложенных быстрых матричных преобразований позволяют выбрать любой вариант матриц основного множества.

4. Доказаны циклические свойства нумераторов эталонных матриц, которые за счет некоторого увеличения вычислительной нагрузки на процессор декодера позволяют дополнительно снизить объем когнитивной карты до трех порядков для наиболее востребованных кодов.

5. Представлена логистика функционирования схемы перестановочного декодера и системы быстрых преобразований матриц на базе копирования и перестановок строк и столбцов эталонных матриц без выполнения арифметических операций, позволившая снизить число операций процессора от одного до трех порядков в зависимости от параметров избыточного кода.

6. Приведены схемные решения для реализации исследованного метода перестановочного декодирования недвоичных избыточных кодов на ПЛИС.

СПИСОК ЛИТЕРАТУРЫ

1. Аджемов, А.С. Общая теория связи. Учебник для вузов / А.С. Аджемов, В.Г. Санников. – М.: Горячая линия – Телеком, 2018. – 624 с.
2. Акимов, О.Е. Дискретная математика: логика, группы, графы, фракталы / О.Е. Акимов – М.: издатель АКИМОВА, 2005. – 656 с.
3. Ал Тамими, Т.Ф.Х. Эффективное декодирование недвоичных кодов / Ал Тамими Т.Ф.Х. // Сборник научных трудов девятой Всероссийской научно-практической конференции (с участием стран СНГ) «Современные проблемы создания и эксплуатации радиотехнических систем». – Ульяновск: УлГТУ, 2015. – С. 146–147.
4. Ал Тамими, Т.Ф.Х. Списочное декодирование недвоичных кодов / Ал Тамими Т.Ф.Х. // Доклады 71-й Международной конференции «Радиоэлектронные устройства и системы для инфокоммуникационных технологий (REDS–2016)», посвящённая Дню радио. – Москва, 2016. – С. 370–374.
5. Ал Тамими, Т.Ф.Х. Методы выработки мягких решений в системе с недвоичными кодами / Ал Тамими Т.Ф.Х. // «Современные проблемы проектирования, производства и эксплуатации радиотехнических систем»: сборник научных трудов. – Ульяновск: УлГТУ, 2016. – С. 188–192.
6. Ал Тамими, Т.Ф.Х. Система быстрых матричных преобразований в процедуре перестановочного декодирования недвоичных избыточных кодов / Ал Тамими Т.Ф.Х. // Доклады 20-й Международной конференции РНТОРЭС имени А.С. Попова «Цифровая обработка сигналов и её применение – DSPA-2018». – Москва, 2018. – С. 164–169.
7. Арнольд, В. И. Динамика, статистика и проективная геометрия полей Галуа / В.И. Арнольд. – М.: МЦНМО, 2005. – 72 с.
8. Архипкин, А.В. Экономный алгоритм декодирования двоичных блочных турбокодов / А.В. Архипкин // Цифровая обработка сигналов и её применение. – Москва, 2006.

9. Березкин, А.А. Оценка сложности реализации декодирования кодов Рида-Соломона при исправлении стираний / А.А. Березкин, В.М. Охорзин // 57-я НТК: материалы / СПб.: Изд-во СПбГУТ, 2005. С. 6.
10. Берлекэмп, Э.Р. Алгебраическая теория кодирования / Э.Р. Берлекэмп; пер.с англ. / под ред. Бермана С.Д. – М.: Мир, 1971. – 384 с.
11. Берлекэмп, Э.Р. Техника кодирования с исправлением ошибок / Э.Р. Берлекэмп // ТИИЭР. – 1980. – Т. 68, №5, – С. 24–58.
12. Биркгоф, Г. Современная прикладная алгебра: Пер. с англ./ Г. Биркгоф, Т. Бартти. – М.: Мир, 1976. – 400 с.
13. Блейхут, Р. Теория и практика кодов, контролирующих ошибки. – М.: Мир, 1986. – 267 с.
14. Блиновский, В.М. Пропускная способность произвольно меняющегося канала при списочном декодировании / В.В. Блиновский, П. Нарайан, М.С. Пинскер // Проблемы передачи информации. – 1995. – Т.31. №2. – С. 3–19.
15. Бородин, Л.Ф. Введение в теорию помехоустойчивого кодирования / Л.Ф. Бородин. – М.: Советское радио, 1968. – 408 с.
16. Бузов, А.Л. Специальная радиосвязь. Развитие оборудования и объектов / Под. ред. А.Л. Бузова, С.А. Букашкина. – М.: Радиотехника, 2017. – 448 с.
17. Ван дер Вандер, Б.Л. Алгебра / Б.Л. Ван дер Вандер.– М.: Наука, 1976.– 648 с.
18. Варгаузин, В.А. Методы повышения энергетической и спектральной эффективности цифровой радиосвязи / В.А. Варгаузин, И.А. Цикин - СПб: БХВ-Петербург, 2013 – 352 с.
19. Васильев, К.К. Методы обработки сигналов: учебное пособие / К.К. Васильев. – Ульяновск: УлГТУ, 2001. – 78 с.
20. Васильев, К.К. Математическое моделирование систем связи / К.К. Васильев, М.Н. Служивый. – Ульяновск: УлГТУ, 2010. – 128 с.
21. Вентцель, Е.С. Теория вероятностей и ее инженерные приложения / Е.С. Вентцель, Л.А. Овчаров: / Учеб. пособие для вузов. 2-е изд., стер. – М.: Высш.шк. – 2000. – 480 с.
22. Вернер, М. Основы кодирования / М. Вернер. – М.: Техносфера, 2004. – 288 с.

23. Вечканов, В.В. Адаптивная система нечеткого управления мобильным роботом / В.В. Вечканов, Д.В. Киселев, А.С. Ющенко // Мехатроника. – 2002. – №1. – С.20–26.
24. Возенкрафт, Дж. Последовательное декодирование / Дж. Возенкрафт и М. Рейффен: Иностр. лит-ра, 1963.– 152 с.
25. Волков, Л.Н., Немировский М.С., Шинаков Ю.А. Системы цифровой радиосвязи: базовые методы и характеристики. М.: Экотрендз, 2005.
26. Галлагер, Р. Теория информации и надежная связь / Р. Галлагер; пер. с англ, под ред. Пинскера М.С. и Цыбакова Б.С. – М.: Сов. радио, 1974. – 568 с.
27. Гантмахер, Ф.Р. Теория матриц / Ф.Р. Гантмахер. – М.: Гл. ред. Физ.-мат. лит-ры, 1967, – 575 с.
28. Гасанов, Э.Э. Теория хранения и поиска информации / Э.Э. Гасанов, В.Б. Кудрявцев. – М.: Физмалит, 2002. – 288 с.
29. Гихман, И.И. Введение в теорию случайных процессов / И.И. Гихман, А.В. Скороход. – М.: Наука, 1965. – 654 с.
30. Гладких, А.А. Основы теории мягкого декодирования избыточных кодов в стирающем канале связи / А.А. Гладких – Ульяновск: УлГТУ, 2010. – 379 с.
31. Гладких, А.А. Модифицированный принцип формирования оценок надежности на основе стирающего канала связи / А.А. Гладких, А.Ю. Пуцев, П.Г. Кожанов // Современные проблемы создания и эксплуатации радиотехнических систем. Труды шестой всероссийской научно-практической конференции (с участием стран СНГ), Ульяновск, 2009. – С. 196–198.
32. Гладких, А.А., Климов Р.В. Численное моделирование обобщенной процедуры формирования индексов мягких решений // ИТК, Том 12, №2, 2013 – С. 22–28.
33. Гладких, А.А. Методы эффективного декодирования избыточных кодов и их современные приложения / А.А. Гладких, Р.В. Климов, Н.Ю. Чилихин // Ульяновск : УлГТУ, 2016. – 258 с.

34. Гладких, А.А. Математическая модель телекоммуникационных систем, используемых в интегрированных информационно-управляющих комплексах / А.А. Гладких, Ал Тамими Таква Флайиих Хасан // Автоматизация процессов управления. – № 3 (45). – 2016, С. 38–43.
35. Гладких, А.А. Структура быстрых матричных преобразований в процедуре формирования эквивалентных избыточных кодов / А.А. Гладких, Ал Тамими Таква Флайиих Хасан // Радиотехника. – № 6, 2017, С. 41–44.
36. Гладких, А.А. Концепция когнитивной обработки данных в системе перестановочного декодирования недвоичного избыточного кода / А.А. Гладких, Ал Тамими Таква Флайиих Хасан // Электросвязь. – № 9. – 2018, С. 69–74.
37. Гладких, А.А. Перестановочное декодирование как инструмент повышения энергетической эффективности систем обмена данными / А.А. Гладких // Электросвязь. – № 8. – 2017, С. 52–56.
38. Гладких, А.А. Обеспечение достоверности данных в измерительных системах на базе сенсорных сетей / А.А. Гладких, Н.Ю. Чилихин, Ал Тамими Таква Флайиих Хасан // Информационно-измерительные и управляющие системы. – № 12, т. 15. – 2017, С. 4–9.
39. Гладких, А.А. Лексикографический декодер каскадного кода / А.А. Гладких, А.А. Шагарова, Ал Тамими Т.Ф.Х. // Патент РФ. № 2619533, опубликован 16 мая 2017.
40. Злотник, Б. М. Помехоустойчивые коды в системах связи / Б.М. Злотник // Статистическая теория связи. – М.: Радио и связь, Вып. 31, 1989. – 232 с.
41. Зигангиров, К.Ш. К теории списочного декодирования сверточных кодов / К.Ш. Зигангиров, Р. Йоханнесон // Проблемы передачи информации. – 1996. – Е.32. – №1. – С. 122–130.
42. Золотарев, В.В. Помехоустойчивое кодирование. Методы и алгоритмы. Справочник / В.В. Золотарев, Г.В. Овечкин; под редакцией чл.-кор. РАН Зубарева Ю.Б. – М.: Горячая линия-Телеком, 2004. – 126 с.

43. Золотарев, В.В. Теория и алгоритмы многопорогового декодирования. – М.: «Радио и связь», «Горячая линия-Телеком», 2006. – 276 с.
44. Ибрагимов, И.А. Асимптотическая теория оценивания / И.А. Ибрагимов, Р.З. Хасьминский. – М.: Наука, 1979. – 528 с.
45. Карташевский, В.Г. Итерационное декодирование турбо-кодов в канале с памятью / В.Г. Карташевский, Д.В. Мишин // 3-я Международная конференция и выставка «Цифровая обработка сигналов и ее применение». – М, 2000. – С. 65–68.
46. Карташевский, В.Г. Прием кодированных сигналов в каналах с памятью / В.Г. Карташевский, Д.В. Мишин. – М.: Радио и связь, 2004. – 239 с.
47. Кларк, Дж. Кодирование с исправлением ошибок в системах цифровой связи / Дж. мл. Кларк, Дж. Кейн; пер. с англ. – М.: Радио и связь, 1987. – 392 с.
48. Кловский, Д.Д. Передача дискретных сообщений по радиоканалам / Д.Д. Кловский. – М.: Связь, 1969. – 375 с.
49. Комашинский, В.И. Когнитивные системы и телекоммуникационные сети / В.И. Комашинский, Н.А. Соколов // Вестник связи. – 2011. – № 10. – С. 4–8.
50. Комашинский, В.И. Когнитивная метафора в развитии телекоммуникационных и индустриальных сетевых инфраструктур, или первые шаги к постинформационной эпохе / В.И. Комашинский, Д.В. Комашинский // Технологии и средства связи. – 2015. – № 1. С. 62–66.
51. Конопелько, В.К. Теория норм синдромов и перестановочное декодирование помехоустойчивых кодов / В.К. Конопелько, В.А. Липницкий . – Изд. 3-е. – М.: Едиториал УРСС, 2012. – 176 с.
52. Коржик, В.И. Помехоустойчивое кодирование дискретных сообщений в каналах со случайной структурой / В.И. Коржик, Л.М. Финк. – М.: Связь, 1975. – 272 с.
53. Кремер, Н.Ш. Теория вероятностей и математическая статистика: Учебник для вузов. – 2-е изд., перераб. и доп. / Н.Ш. Кремер. – М.: Юнити-Дана, 2004. – 573 с.

54. Ларкин, Е.В. Определение временных параметров управления роботами / Е.В. Ларкин, А.Н. Привалов // Телекоммуникации – № 6. – 2017, С. 10–19.
55. Лагутин М.Б. Наглядная математическая статистика. Учебное пособие / М.Б. Лагутин. – М.: Бином. Лаборатория знаний, 2018. – 472 с.
56. Липницкий, В.А. Норменное декодирование помехоустойчивых кодов и алгебраические уравнения / В.А. Липницкий, В.К. Конопелько. – Минск, 2007. – 325 с.
57. Магазов, С.С. Когнитивные процессы и модели / С.С. Магазов. – М.: УРСС, 2007. – 237 с.
58. Мак-Вильямс, Ф. Дж. Перестановочное декодирование систематических кодов / Ф. Дж. Мак-Вильямс // Кибернетический сборник. Новая серия, 1965, Вып. 1. – С. 35–57.
59. Мак-Вильямс, Ф. Дж. Теория кодов, исправляющих ошибки / Ф. Дж. Мак-Вильямс, Н. Дж. А. Слоэн. – М.: Связь, 1979. – 354 с.
60. Математика. Большой энциклопедический словарь / Гл. ред. Прохоров Ю.В. 3-е изд.– М.: Большая Российская энциклопедия, 1998. – 848 с.
61. Морелос-Сарагоса, Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение / Р. Морелос-Сарагоса. – М.: Техносфера, 2005. – 320 с.
62. Овечкин, Г.В. Помехоустойчивое кодирование в цифровых системах передачи данных / Г.В. Овечкин, Ю.Б. Зубарев // ISSN 0013-2771, «Электросвязь», №12, 2008.
63. Питерсон, У. Коды, исправляющие ошибки / У. Питерсон, Э. Уэлдон; пер. с англ.; под редакцией Р.Л. Добрушина и С.Н. Самойленко. – М.: Мир, 1976. – 594 с.
64. Прокис, Джон. Цифровая связь / Джон Прокис; пер. с англ.; под редакцией Д.Д. Кловского. – М.: Радио и связь, 2000. – 800 с.
65. Семушин, И.В. Еще раз о больших обратных матрицах: от формализмов к реализации / И.В. Семушин // Автоматизация процессов управления. – № 4 (50). – 2017. – С. 36–41.

66. Скляр, Бернард. Цифровая связь. Теоретические основы и практическое применение / Бернард Скляр – Изд. 2-е, испр. пер. с англ. – М.: Издательский дом «Вильямс», 2003. – 1104 с.
67. Тихонов, В.И. Марковские процессы / В.И. Тихонов, М.А. Миронов. – М.: Радио и связь, 1977. – 448 с.
68. Толстяков, В.С. Обнаружение и исправление ошибок в дискретных устройствах / В.С. Толстяков, В.Н. Номоконов, М.Г. Карповский, И.Л. Ерош. – М.: Советское радио, 1972. – 288 с.
69. Финк, Л.М. Теория передачи дискретных сообщений / Л.М. Финк. – М.: Сов. радио, 1970. – 728 с.
70. Форни, Д. Каскадные коды / Д. Форни. – М.: Мир, 1970. – 207 с.
71. Чилихин, Н.Ю. Разработка и моделирование алгоритмов декодирования полярных кодов в системе информационно-управляющих комплексов / Н.Ю. Чилихин // Диссертация на соискание ученой степени к.т.н. – Самара.: ПГУТИ.– 2015. – 149 с.
72. Чуднов, А.М. Теоретико-игровые задачи синтеза алгоритмов формирования и приема сигналов / А.М. Чуднов // Проблемы передачи информации. – 1991.– том 27, вып. 3. – С. 57–65.
73. Харари, Ф. Перечисления графов / Ф. Харари, Э. Палмер. – М.: Мир, 1977.– 324 с.
74. Хошев, А.Ю. Алгоритм посимвольного декодирования параллельного каскадного кода во временной области / А.Ю.Хошев, А.М.Шлома // Цифровая обработка сигналов. – 2001. – №2. – С. 15–18.
75. Шеннон, К.Е. Математическая теория связи / К.Е. Шеннон // Работы по теории информации и кибернетики. – М.: Иностранная литература, 1963. – 476 с.
76. Шувалов, В.П. Прием сигналов с оценкой их качества/ В.П. Шувалов. – М.: Связь, 1979. – 240 с.
77. Ющенко, А.С. Интеллектуальное планирование в деятельности роботов / А.С. Ющенко // Мехатроника. – 2005. – № 3. – С. 15–18.

78. Ющенко, А.С. Управление роботами с использованием нечеткой логики: состояние и проблемы / А.С. Ющенко // Новости искусственного интеллекта. – 2006. – № 1. – С. 119–130.
79. Alon, N. Linear Time Erasure Codes with Nearly Optimal Recovery / N. Alon, J. Edmonds, and M. Luby // IEEE Symposium on Foundations of Computer Science, Proc. IEEE Vol. 3, 1995. – P. 512–519.
80. Berrou, C. A low complexity soft-output viterbi decoder architecture / C. Berrou, P. Adde, E. Angui, S. Faudeil // Proc. of the Intern. Conf. on Commun. – 1993. – May. – P. 737–740.
81. Berrou, C., Glavieux A. Near Optimum Error Correcting Coding and Decoding: Turbo-codes//// IEEE Trans. On Comm. – October 1996. – Vol.44. – № 10.
82. Carrasco, Rolando Antonio. Non-binary error control coding for wireless communication and data storage / Rolando Antonio Carrasco, Martin Johnston; John Wiley & Sons, Ltd – 2008. – P. 302.
83. Carrasco, R. Space-time ring-TCM codes for QAM over fading channels. / R. Carrasco, A. Pereira // IEE Proceedings Communications, – 2004, 151 (4). – P. 316–321.
84. Chen, L. Efficient list decoder for algebraic–geometric codes. / L. Chen, R.A. Carrasco // Presented at 9th International Symposium on Communication Theory and Application (ISCTA'07), – 2007. – Ambleside, Lake district, UK.
85. Chen, L. Performance of Reed–Solomon codes using the Guruswami–Sudan algorithm with improved interpolation efficiency./ L. Chen, R. A. Carrasco, E. G. Chester, // IET Commun, – 2007.– P. 241–250.
86. Chung, S., Forney D., Richardson T., Urbanke R. On the Design of Low-Density Parity-Check Codes within 0,0045dB of the Shanon Limit// IEEE Trans. Letters. – Feb. 2001. – V.5. – № 2. – P. 58–60.
87. Cideciyan, R., Eleftheriou E., Rupp M. Concatenated Reed-Solomon/Convolutional Coding for Data Transmission in CDMA-Based Cellular Systems// IEEE Trans. On Comm. – October 1997. – Vol.45. – № 10. – P. 1291–1303.

88. Djurdjevic, I., Xu J., Abdel-Ghaffar K., Lin S. A class of low-density parity-check codes constructed based on Reed-Solomon codes with two information symbols. *IEEE Commun. Lett*, 2003, vol. 7. – P. 317–319.
89. Elias, P. Error-correcting codes for list decoding / P. Elias // *Information Theory, IEEE Transactions*, – 1991, – № 37. – P. 5–12.
90. Fossorier, M. Soft-decision decoding of linear block codes based on ordered statistics / M. Fossorier, S. Lin // *IEEE Transactions on Information Theory*. – 1995.– № 5. – P. 1379–1396.
91. Fossorier, M.P.C. Reduced complexity iterative decoding of low-density parity check codes based on belief propagation / M.P.C. Fossorier, M. Mihaljevic, H. Imai // *IEEE Trans. on Comm.* – May 1999. – Vol. 47, № 5.
92. Forney, G.D. Codes and Graphs: Normal Realizations // *IEEE Transactions on Information Theory*. 2001. – Vol. 47. – N. 2. – P. 520–548.
93. Guruswami, V. Improved Decoding of Reed-Solomon and Algebraic-Geometry Codes / V. Guruswami, M. Sudan // *IEEE Transactions on Information Theory*,– Sept. 1999. – P. 1757–1767.
94. Hagenauer, J., Offer E., Papke L. Iterative decoding of binary block and convolutional codes//*IEEE Trans. Information Theory*. – Mart 1996. Vol. 42.
95. Hagenauer, J., Hoher P. A Viterbi Algorithm with Soft-Decision Outputs and Its Applications // *IEEE Global Telecommunications Conference (GLOBECOM'89)*. 1989. – P. 47.1.1–47.1.7.
96. Hirst, S., Honary B., Markarian G. Fast Chase Algorithm With an Application in Turbo Decoding// *IEEE Trans. On Comm.* – October 2001. – Vol.49. – № 10.
97. Justesen, J. On the Complexity of Decoding Reed-Solomon Codes /J. Justesen // *IEEE transactions on information theory*, – 1993. – Vol. 22, no. 2. – P. 237– 238.
98. Koetter, R. Algebraic Soft-Decision Decoding of Reed-Solomon Codes / R. Koetter, A. Vardy // *IEEE Int. Symp. Info. Theory (ISIT '00)* Sorrento, Italy: June 2000. – P. 61, 25–30.
99. Kschischang, F. R., Frey B. J., Loeliger H.A. Factor graphs and the sum-product algorithm. *IEEE Trans.Inform. Theory*, 2001, vol. 47, no. 2. – P. 498–519.

100. Koetter, R. and Vardy A., “Algebraic Soft-Decision Decoding of Reed-Solomon Codes”, Proc. 2000 IEEE Int. Symp. Info. Theory (ISIT ‘00), p. 61, Sorrento, Italy, June 25-30, 2000.
101. Mori, R. Non-binary polar codes using Reed-Solomon codes and algebraic geometry codes / R. Mori, T. Tanaka // IEEE Information Theory Workshop (ITW). – 2010. – P. 1–5.
102. Natalin, A. B. The Method of Theoretic Estimation of BER of ML Receiver for Binary Coded Systems with Square QAM. / A.B. Natalin, A. B. Sergienko // Proc. IEEE Int. Conf. on Communications (ICC2006), Istanbul, 11-15. – June 2006, – Vol. 3. P. 1206–1211.
103. Okamura, T. Designing LDPC codes using cyclic shifts. Proc. IEEE Int. Symp. Information Theory. Yokohama, 2003. – P. 151.
104. Peng, X. H. Erasure-control Coding for Distributed Networks / X. H. Peng // IEEE Proceedings on Communications, – 2005. – Vol. 152. P. 1075–1080.
105. Pyndiah, R. Near-Optimum Decoding of Codes: Block Turbo Codes// IEEE Trans. On Comm. – August 1998. – Vol.46. – № 8.
106. Roth, R. and Ruckenstein, G. (2000) Efficient decoding of Reed–Solomon codes beyond half the minimum distance / R. Roth, G. Ruckenstein // IEEE Trans. Inform. Theory, – 2000. – P. 246–257.
107. Sasoglu, E. Polarization for arbitrary discrete memoryless channels / E. Sasoglu, E. Telatar, E. Arıkan // Proc. IEEE Information Theory Workshop ITW, – 2009. P. 144–148.
108. Stefanov, A. and Duman T. M. Turbo-coded modulation for systems with transmit and receive antenna diversity over block fading channels: system model, decoding approaches, and practical considerations, IEEE J. on Sel. Areas in Comm, vol. 19, no. 5, May 2001.
109. Sudan, M. Decoding of Reed-Solomon Codes Beyond the Error-Correction Bound, J. Complexity, vol. 12. P. 180–193. Dec. 1997.

110. Takeshita, O. Y., Costello D.J., Jr. New classes of algebraic intervers for turbo-codes // in Proc. of IEEE Intern. Symp. on Inf. Theory, (MIT, Cambrige, MA USA). 1998. – Aug. – P. 419.
111. Taghavi, M.H. Adaptive methods for linear programming decoding / M.H. Taghavi, P.H. Siegel // IEEE Trans. Inform. Theory, – 2008. – Vol. 54, № 12. P. 5396–5410.
112. Tanner, M. A Recursive Approach to Low Complexity Codes // IEEE Trans. Inform. Theory. 1981. V. 27. № 5. – P. 533–547.
113. Wozencraft, J. Sequentail decoding for reliable communication // IRE Natl. Covn. Rec. – 1957. – V.5. – P. 11–25.
114. Valenti, V.C. Iterative detection and decoding for wireless communication. Dissertation submitted to the Faculty of the Virginia Polytechnic Institute. – Jule 8, 1999.
115. Viterbi, J. Error Bounds for Convolutional Codes and an Asymptotically Optimum Decoding Algorithm//IEEE Trans. Information Theory. – Apr. 1967. V. IT – 13, P. 260–269.
116. Zolotarev, V.V. The Multithreshold Decoder Performance in Gaussian Channels Proc. 7th Intern. Symp. on Commun. Theory and Applications 7ISCTA'03 (St. Martin's College, Ambleside, UK, 13-18 July). 2003. P. 18–22.
117. Zyablov, V., Potapov V., Groshev F. Low-complexity error correction in LDPC codes with constituent RS codes // Proc. 11th Int. Workshop on Algebraic and Combinatorial Coding Theory (ACCT'08). Pamporovo, Bulgaria. June 16-22, 2008, P. 348–353.

ПРИЛОЖЕНИЕ А

ЛЕКСИКОГРАФИЧЕСКИЙ ДЕКОДЕР КАСКАДНОГО КОДА

Изобретение относится к технике связи и может использоваться при проектировании новых и модернизации существующих систем передачи дискретной информации.

Известны устройства восстановления стираний и исправления ошибок, использующие индексы мягких решений (индекс достоверности символов, градации надежности символов) для повышения достоверности приема информации [30, 46, 60].

К недостаткам работы указанных аналогов следует отнести неполное использование введенной во внутренний и внешний коды избыточности из-за применения жестких алгоритмов обработки данных и использования одного из надежно принятых элементов кодовой комбинации в качестве стирания для оценки правильности декодирования принятого кодового вектора недвоичного кода на внешней ступени декодирования. Это повышает сложность декодера при вычислении недвоичных разрядов внешнего кода, поскольку в алгоритме используется операция умножения в недвоичном поле Галуа.

На рисунке 1 приведена структурная электрическая схема предложенного лексикографического декодера каскадного кода. Лексикографический декодер каскадного кода содержит блок 1 приема, выход которого через блок 2 индексов подключен к входу блока 3 статистических решений. Первый выход этого блока подключен к одному входу блока 4 итерации, а второй выход блока 3 статистических решений подключен к первому входу блока 6 приоритетов. Выход блока 4 итерации подключен к входу блока 5 внутреннего кода, первый выход которого соединен с другим входом блока 4 итерации, а второй выход блока 5 внутреннего кода подключен ко второму входу блока 6 приоритетов. Третий выход блока 5 внутреннего кода подключен к входу буфера внешнего кода 7.

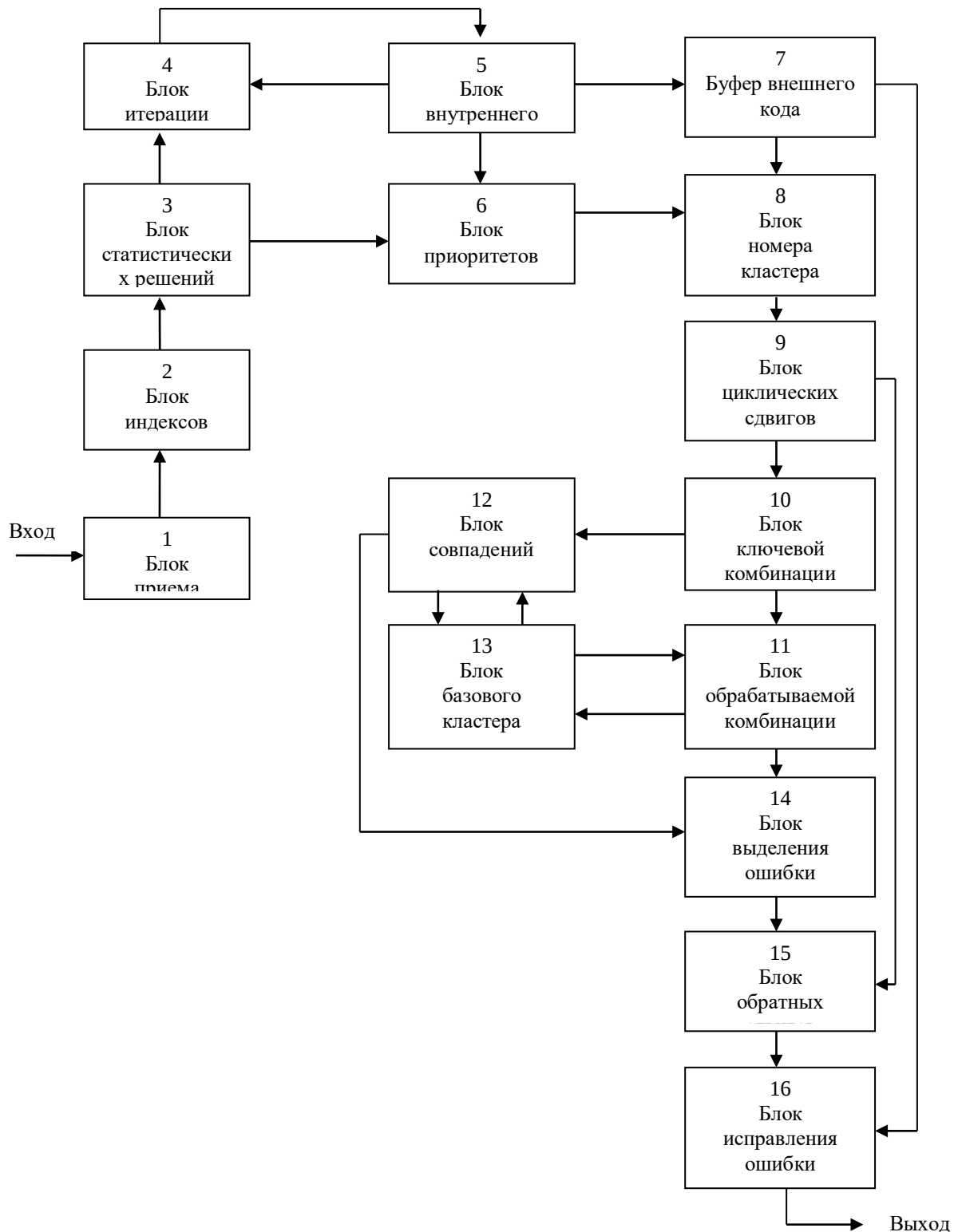


Рисунок 1 – Лексикографический декодер каскадного кода

Отличительная особенность устройства заключается в том, что дополнительно введены блок 8 номера кластера, блок 9 циклических сдвигов, блок 10 ключевой комбинации, блок 11 обрабатываемой комбинации, блок 12 совпадений, блок 13 базового кластера, блок 14 выделения ошибок, блок 15

обратных сдвигов, блок 16 исправления ошибки. При этом первый выход буфера внешнего кода 7 подключен к первому входу блока 8 номера кластера, выход которого подключен к входу блока 9 циклических сдвигов. Первый выход этого блока через один выход блока 10 ключевой комбинации подключен к первому входу блока 11 обрабатываемой комбинации, один выход которого подключен к первому входу блока 12 базового кластера, второй выход которого подключен ко второму входу блока 11 обрабатываемой комбинации. Другой выход этого блока через первый вход блока 14 выделения ошибки подключен к одному входу блока 15 обратных сдвигов, выход которого подключен к первому входу блока 16 исправления ошибок, второй вход которого подключен ко второму выходу буфера внешнего кода 7. Другой выход блока 10 ключевой комбинации подключен к первому входу блока 12 совпадений, один выход которого подключен ко второму входу блока 13 базового кластера, первый выход которого подключен ко второму входу блока 12 совпадений, другой выход которого подключен ко второму входу блока 14 выделения ошибки. Второй выход блока 9 циклических сдвигов подключен к другому входу блока 15 обратных сдвигов при этом выход блока 6 приоритетов подключен ко второму входу блока 8 номера кластера.

Работу декодера рассмотрим на примере использования в качестве внутреннего кода – код с проверкой четности, а в качестве внешнего кода – код РС (7, 3, 5), построенного над полем $GF(2^3)$.

Порождающий полином такого кода РС $g(x)$ определяется как

$$g(x) = (x - \alpha)(x - \alpha^2)(x - \alpha^3)(x - \alpha^4) = x^4 + x^3\alpha^3 + x^2 + x\alpha + \alpha^3.$$

Используя значение $g(x)$, представим некоторые кластеры кода РС в виде таблиц 1-4. Номера кластеров формируются по любым двум элементам кодовой комбинации кода РС одинаковыми для всего множества разрешенных кодовых векторов (см. Гладких, А.А. Обобщенный метод декодирования по списку на базе кластеризации пространства кодовых векторов. Радиотехника. – 2015. – №6. – С. 37–41) и упорядочиваются лексикографически. Пусть в качестве таких элементов

для всех кодовых комбинаций выбраны первые два символа. Общее число комбинаций любого кода РС, рассматриваемого над двоичным полем Галуа степени расширения k_1 , оценивается как $N = 2^{k_1 \times k_2}$, где k_1 – степень расширения двоичного поля, а k_2 – число информационных разрядов кода РС. В примере $k_1 = k_2 = 3$, тогда для рассматриваемого кода может быть сформировано 64 кластера, каждый из которых содержит по 8 комбинаций. Базовым кластером считается кластер с номером 00.

В общем случае признаком ключевой комбинации для любого кластера является размещение на очередных позициях вслед за нумератором кластера единичного элемента поля по операции сложения. В примере нумератор кластера занимает две первые позиции, значит, следующая (третья) позиция в ключевой комбинации должна быть равна нулю. Любая ключевая комбинация декодером может быть сформирована по известному номеру кластера и размещением на третьей позиции символа 0 или при небольших длинах кодовых комбинаций хранится в памяти декодера. В последнем случае в декодере полностью исключается арифметическая операция умножения, что существенно снижает сложность реализации декодера.

Таблица 1 – Структура комбинаций базового (нулевого) кластера

1	0	0	0	0	0	0	0
2	0	0	α^0	α^3	α^0	α^1	α^3
3	0	0	α^1	α^4	α^1	α^2	α^4
4	0	0	α^2	α^5	α^2	α^3	α^5
5	0	0	α^3	α^6	α^3	α^4	α^6
6	0	0	α^4	α^0	α^4	α^5	α^0
7	0	0	α^5	α^1	α^5	α^6	α^1
8	0	0	α^6	α^2	α^6	α^0	α^2

Таблица 2 – Структура комбинаций кластера $\alpha^1 0 = 010000$

Ключевая комбинация	α^1	0	0	α^5	α^1	α^5	α^6
2	α^1	0	α^0	α^2	α^3	α^6	α^4
3	α^1	0	α^1	α^0	0	α^3	α^3
4	α^1	0	α^2	0	α^4	α^2	α^1
5	α^1	0	α^3	α^1	α^0	α^0	0
6	α^1	0	α^4	α^4	α^2	0	α^2
7	α^1	0	α^5	α^6	α^6	α^1	α^5
8	α^1	0	α^6	α^3	α^5	α^4	α^0

Таблица 3 – Структура комбинаций кластера $\alpha^1 \alpha^1 = 010010$

Ключевая комбинация	α^1	α^1	0	α^2	0	α^4	α^2
2	α^1	α^1	α^0	α^5	α^0	α^2	α^5
3	α^1	α^1	α^1	α^1	α^1	α^1	α^1
4	α^1	α^1	α^2	α^3	α^2	α^6	α^3
5	α^1	α^1	α^3	α^0	α^3	0	α^0
6	α^1	α^1	α^4	α^6	α^4	α^0	α^6
7	α^1	α^1	α^5	α^4	α^5	α^3	α^4
8	α^1	α^1	α^6	0	α^6	α^5	0

Таблица 4 – Структура комбинаций кластера $\alpha^6 \alpha^6 = 101101$

Ключевая комбинация	α^6	α^6	0	α^0	0	α^2	α^0
2	α^6	α^6	α^0	α^1	α^0	α^4	α^1
3	α^6	α^6	α^1	α^5	α^1	0	α^5
4	α^6	α^6	α^2	α^4	α^2	α^5	α^4
5	α^6	α^6	α^3	α^2	α^3	α^1	α^2
6	α^6	α^6	α^4	0	α^4	α^3	0
7	α^6	α^6	α^5	α^3	α^5	α^0	α^3
8	α^6	α^6	α^6	α^6	α^6	α^6	α^6

Работа блока приема 1 организуется по принципу стирающего канала связи с симметричным интервалом стирания ρ , где $0 \leq \rho < 1$, и представляет долю расстояния в системе условных плотностей вероятностей в гауссовском канале связи между математическими ожиданиями $-\sqrt{E_b}$ и $\sqrt{E_b}$, соответствующих приему информационных нулей и единиц, где E_b – энергия сигнала, приходящаяся на бит. В целях повышения достоверности индексов мягких

решений параметр ρ выбирают достаточно большим, например, $\rho = 0,9$. Зафиксированный в блоке приема 1 сигнал $|z|$ и соответствующее ему жесткое решение 0 или 1 передаются в блок индексов 2.

В блоке индексов 2 оценивается влияние мешающих факторов на двоичные символы переданного вектора внутреннего кода в виде целочисленных мягких решений символов (МРС). Для вычисления МРС применяется линейная зависимость (см. Гладких, А.А. Основы теории мягкого декодирования избыточных кодов в стирающем канале связи. Ульяновск : УлГТУ, – 2010. – 379 с. на С. 211). Пусть выбрано максимальное значение МРС $\lambda_{\max} = 7$. Тогда минимальное значение МРС будет равно $\lambda_{\min} = 0$. Промежуточные оценки для i -го символа в блоке индексов 2 получают по правилу

$$\lambda_i = \left\lfloor \frac{\lambda_{\max}}{\rho\sqrt{E}} \times z \right\rfloor, \quad (\text{A1})$$

где z – уровень сигнала после воздействия на него аддитивной помехи, символ $\lfloor \bullet \rfloor$ означает округление полученного значения λ_i до целочисленной величины в сторону уменьшения (расчет на наихудший случай), $\rho = 0,9$. Таким образом, выражение (A1) при заданных условиях упрощается и принимает вид $\lambda_i \cong 5,5 \times z$. Следовательно, если $z \geq 1,27$, то $\lambda_i = \lambda_{\max}$.

На основе полученных данных для двоичных символов в блоке статистических решений 3 осуществляется интегрированная оценка надежности q -ичных символов кода РС. Для выполнения такой оценки в блоке статистических решений 3 решается задача поиска целевой функции для каждого q -ичного символа кода РС. Обозначим через $(+pc)$ выполнение условия четности на приемной стороне для принятого кодового вектора внутреннего кода. В противном случае приемник фиксирует значение $(-pc)$. Работу декодера с проверками на четность целесообразно описывать целевой функцией вида

$$Q\{S; M(\lambda); \sigma(\lambda)\} \Rightarrow \underset{S \rightarrow (-pc)}{\text{sign}(S)}; \underset{\max}{M(\lambda)}; \underset{\min}{\sigma(\lambda)}, \quad (\text{A2})$$

где S – значение четности по всем информационным разрядам принятого вектора; параметр $|M(\lambda)|$ – среднее значение кортежа модулей мягких решений символов; параметр $\sigma(\lambda)$ является показателем разброса мягких решений, вычисляемого по правилу

$$\sigma(\lambda) = (1/n - 1) \sum_{i=1}^n (|M(\lambda)| - |\lambda_i|)^2. \quad (A3)$$

По отдельности представленные параметры не являются информативными и не позволяют взвешенно оценить приоритеты очередности обработки нескольких кодовых символов комбинации кода РС. В соответствии с $Q\{\bullet\}$ блок 3 выполняет проверку четности, на втором шаге обработки данных оценивает среднее значение принятых индексов МРС и в последнюю очередь определяет дисперсию для МРС кодовой комбинации внутреннего кода. Максимальное значение параметра $|M(\lambda)|$ соответствует высокой достоверности принятых символов, но на длине кодовой комбинации кода РС может быть получено несколько одинаковых значений $|M(\lambda)|$. В подобной ситуации блок 3 дополнительно оценивает параметр $\sigma(\lambda)$. Если возникает ситуация неопределенности, когда $|M_i(\lambda)| = |M_j(\lambda)|$ при $i \neq j$, то приоритетной для последующей обработки данных является комбинация, у которой разброс оценок оказывается меньше, т.е. при $\sigma_i(\lambda) < \sigma_j(\lambda)$ приоритет отдается комбинации с номером i . Для символов кода РС назначается всего три приоритета двоичных символов (ПНС): низкий – 0; средний – 1 и высокий – 2.

В случаях невыполнения условий четности в блоке итерации 4 осуществляется повышение значений МРС при условии, что проверочные символы комбинаций приняты надежно.

Обработанная подобным образом комбинация внутреннего кода хранится в блоке внутреннего кода 5, а ее значение $Q\{\bullet\}$ хранится в блоке приоритетов 6. Комбинация кода РС накапливается в буфере внешнего кода 7, а оценки ПНС комбинации кода РС накапливаются в блоке номера кластера 8, который оценивает надежность номинальных символов кластера, и в случае выполнения

условий по надежности для этих символов (нумераторы кластера имеют высокие приоритеты) объединенные данные блока 7 и блока 8 передаются в блок циклических сдвигов 9 с указанием « $\Delta=0$ », при этом значения кодовой комбинации кода РС передаются в блок обрабатываемой комбинации 11, а команда « $\Delta=0$ » транслируется в блок обратных сдвигов 15. Параметр Δ указывает число циклических сдвигов элементов кодовой комбинации влево.

Пусть кодер канала связи сформировал вектор

$$V_{nep} = \alpha^0 \quad \alpha^3 \quad \alpha^6 \quad \alpha^6 \quad \alpha^5 \quad \alpha^3 \quad \alpha^5,$$

в котором для защиты номера кластера, содержащего первые два элемента α^0 и α^3 , выполняется их поразрядное сложение по модулю два, и результат сложения записывается на заранее обусловленное место в векторе V_{nep} (см. патент РФ № 24444127). $\alpha^0 \oplus \alpha^3 = 001 \oplus 011 = 010 = \tilde{\alpha}$. Если результат фиксируется на последней позиции передаваемой комбинации, то вектор V_{nep} принимает вид

$$V'_{nep} = \alpha^0 \quad \alpha^3 \quad \alpha^6 \quad \alpha^6 \quad \alpha^5 \quad \alpha^3 \quad \tilde{\alpha}.$$

Пусть при передаче вектора V'_{nep} по каналу связи вектор помех имел вид

$$V_{ном} = 0 \quad 0 \quad 0 \quad \alpha^3 \quad \alpha^4 \quad \alpha^5 \quad 0.$$

В этом случае приемник получает вектор

$$V_{np} = \alpha_2^0 \quad \alpha_2^3 \quad \alpha_2^6 \quad \alpha_0^4 \quad \alpha_1^0 \quad \alpha_1^2 \quad \tilde{\alpha}_2^1,$$

где нижние индексы степеней примитивного элемента поля показывают значения ПНС, по результатам анализа которых в соответствии с $Q\{\bullet\}$ первые три символа кода РС $\alpha^0 \alpha^3 \alpha^6$ оказываются с наибольшим приоритетом. В блоке номера кластера 8 проверяется четность элементов $(\alpha^0 \quad \alpha^3)$. Используя эту информацию блок ключевой комбинации 10 путем кодирования первых трех надежных символов $\alpha^0 \alpha^3 0$ формирует ключевую комбинацию по номеру кластера $(\alpha^0 \quad \alpha^3)$

$$c_{\alpha^0 \alpha^3 0} = \alpha^0 \quad \alpha^3 \quad 0 \quad \alpha^0 \quad \alpha^1 \quad \alpha^1 \quad \alpha^3.$$

В блоке обрабатываемой комбинации 11 выполняется сложение (по правилу недвоичного поля) найденной ключевой комбинации из блока 10 с вектором, полученным из буфера внешнего кода 7, что соответствует одной из комбинаций базового кластера

$$V_{np} \oplus c_{\alpha^0 \alpha^3 0} = 0 \ 0 \ \alpha^6 \ \alpha^5 \ \alpha^3 \ \alpha^4 \ \alpha^3.$$

Результат сложения по надежно принятому элементу α^6 сравнивается с подходящей комбинацией из блока базового кластера 13, в результате чего выделяется комбинация вида

$$c_{0,0,\alpha^6} = 0 \ 0 \ \alpha^6 \ \alpha^2 \ \alpha^6 \ \alpha^0 \ \alpha^2,$$

которая априори известна приемнику и является безошибочной. Сложение этой комбинации с принятым вектором в блоке обрабатываемой комбинации 11 формирует истинный вектор ошибок, который передается в блок выделения ошибок 14

$$\begin{aligned} V_{np} &= \alpha^0 \ \alpha^3 \ \alpha^6 \ \alpha^4 \ \alpha^0 \ \alpha^2 \ \tilde{\alpha}^1 \\ c_{\alpha^0 \alpha^3 0} &= \alpha^0 \ \alpha^3 \ 0 \ \alpha^0 \ \alpha^1 \ \alpha^1 \ \alpha^3 \\ c_{0,0,\alpha^6} &= 0 \ 0 \ \alpha^6 \ \alpha^2 \ \alpha^6 \ \alpha^0 \ \alpha^2 \\ V_{ном} &= 0 \ 0 \ 0 \ \alpha^3 \ \alpha^4 \ \alpha^5 \ 0 \end{aligned}$$

Значение этого вектора через блок обратных сдвигов 15, который получил команду « $\Delta=0$ », без изменений поступает в блок исправления ошибок 16, в котором устраняется действие мешающих факторов.

В случае поражения помехой элементов кодовой комбинации, относящихся к номеру кластера, в блоке номера кластера 8 определяются наиболее надежные символы, которые не совпадают с номинальными символами кластера. Блок циклических сдвигов 9 определяет количество шагов, которые необходимо выполнить для установки на позиции символов кластера символы с наиболее высокими МРС.

Пусть кодер канала связи сформировал вектор

$$V_{пер} = \alpha^3 \ \alpha^3 \ \alpha^0 \ \alpha^6 \ \alpha^0 \ \alpha^5 \ \alpha^6,$$

который по условию проверки номера кластера приводится к виду

$$V'_{nep} = \alpha^3 \quad \alpha^3 \quad \alpha^0 \quad \alpha^6 \quad \alpha^0 \quad \alpha^5 \quad \tilde{0}$$

Пусть при передаче вектора V_{nep} по каналу связи вектор помех имел вид

$$V_{ном} = \alpha^1 \quad \alpha^2 \quad 0 \quad \alpha^4 \quad 0 \quad 0 \quad 0.$$

В результате принятый вектор $V_{np} = V'_{nep} \oplus V_{ном}$ становится равным

$$V_{np} = \alpha_1^0 \quad \alpha_1^5 \quad \alpha_2^0 \quad \alpha_1^3 \quad \alpha_2^0 \quad \alpha_2^5 \quad \tilde{0}_2.$$

Проверка четности элементов кластера в блоке номера кластера 8 дает отрицательный результат: $\alpha_1^0 \oplus \alpha_1^5 \neq \tilde{0}_2$, но имеются надежные элементы α_2^0 и α_2^5 . На основе анализа ПНС блок циклических сдвигов 9 выполняет сдвиг элементов комбинации из буфера внешнего кода 7 влево на $\Delta = 4$ шага, при этом ПНС примитивных элементов поля синхронно сопровождают элементы кодовой комбинации из блока номера кластера 8. При условии $\Delta = 4$ на третьей позиции оказывается проверочный символ, который не может быть использован для идентификации комбинации базового кластера, поэтому блок циклических сдвигов 9 передает эту информацию блоку ключевой комбинации 10

$$V'_{np} = \alpha_2^0 \quad \alpha_2^5 \quad \tilde{0}_2 \quad \alpha_2^0 \quad \alpha_1^5 \quad \alpha_2^0 \quad \alpha_1^3.$$

Блок 10 путем кодирования комбинации вида $(\alpha^0 \alpha^5 0)$ формирует ключевую комбинацию по надежным символам номера кластера $(\alpha^0 \quad \alpha^5)$

$$c_{\alpha^0 \alpha^5 0} = \alpha^0 \quad \alpha^5 \quad 0 \quad \alpha^5 \quad \alpha^4 \quad 0 \quad \alpha^0.$$

Команда из блока циклических сдвигов 9 в блок 10 говорит о том, что стандартная схема декодирования путем выбора кодовой комбинации из списка комбинаций базового кластера неприемлема. Поэтому полученная ключевая комбинация из блока 10 направляется в блок совпадений 12, который выбирает наиболее надежный символ из разряда, не относящегося к первым трем позициям, и сопоставляет эту позицию с соответствующими позициями комбинаций базового кластера. Получив ключевую комбинацию в блоке 10 и, выполняя операцию сложения векторов,

$$V'_{np} \oplus c_{\alpha^0 \alpha^5 0} = \begin{pmatrix} 0 & 0 & \alpha^6 & \alpha^4 & \alpha^0 & \alpha_2^0 & \alpha^1 \end{pmatrix},$$

по надежно принятому элементу α_2^0 в базовом кластере отыскивается комбинация

$$V_{\bar{b}k} = \begin{pmatrix} 0 & 0 & \alpha^6 & \alpha^2 & \alpha^6 & \alpha_2^0 & \alpha^2 \end{pmatrix},$$

которая не содержит влияния мешающих факторов. Следовательно, выполняя в блоке выделения ошибок суммирование

$$V'_{np} \oplus c_{\alpha^0 \alpha^5 0} \oplus V_{\bar{b}k} = V'_{ном},$$

получают циклически сдвинутый вектор ошибок

$$V'_{ном} = \begin{pmatrix} 0 & 0 & 0 & \alpha^1 & \alpha^2 & 0 & \alpha^4 \end{pmatrix}.$$

Вектор $V'_{ном}$ нуждается только в обратных циклических перестановках, которые выполняются в блоке 16.

В большинстве случаев конфигурация ошибок носит случайный характер, и вероятность того, что число непораженных помехой подряд идущих символов кодовой комбинации кода РС оказывается достаточно низкой. Если блок номера кластера 8 выявляет отсутствие достаточного количества надежных и подряд идущих символов для реализации первого или второго варианта декодирования, то за счет проверочного символа восстанавливается номер кластера. Далее процесс декодирования осуществляется в соответствии со вторым вариантом с использованием блока совпадений 12.

Таким образом, предложенный декодер обеспечивает исправление всех конфигураций ошибок, кратность которых не превосходит значения $(n_2 - k_2 - 1)$. Кроме того, в декодере выполняется минимальное число операций умножения и полностью исключается процедура подбора порождающего полинома для выявления локаторов ошибок.