В.В.Золотарёв

Теория и алгоритмы многопорогового декодирования

«РАДИО и СВЯЗЬ»

Горячая линия–Телеком

В.В. Золотарёв

Теория и алгоритмы многопорогового декодирования

Под редакцией члена-корреспондента РАН, профессора, доктора технических наук Ю. Б. Зубарева

Рецензент академик РАН, профессор, доктор технических наук В. К. Левин

М.: Радио и связь - Горячая линия – Телеком, 2006 г.

Изложено современное состояние теории и прикладных вопросов многопорогового декодирования. Описаны конкретные методы коррекции ошибок в каналах с большим уровнем шума на основе итеративных многопороговых процедур для блоковых и свёрточных кодов. Даны оценки сложности процедур коррекции ошибок при программной и аппаратной реализации. Рассмотрены алгоритмы декодирования каскадных кодов на базе внешних кодов с контролем по чётности и параллельного кодирования. Предложены мажоритарные декодеры для недвоичных кодов, более эффективные, чем коды Рида – Соломона.

Проанализированы специальные алгоритмы исправления стираний, сжатия данных и другие методы обеспечения высокой достоверности при передаче данных по каналам с шумами, основанные на идеях многопорогового декодирования.

Для специалистов в области теории и техники кодирования, разработчиков систем связи, студентов и аспирантов соответствующих специальностей.

ПРЕДИСЛОВИЕ НАУЧНОГО РЕДАКТОРА

Начавшийся в конце прошлого тысячелетия интенсивный переход к системам обработки и передачи информации цифрового формата на сегодня становится всё более масштабным и характеризуется весьма быстрым и значительным повышением требований к достоверности цифровых данных. Несомненно, ведущую роль в обеспечении высокого уровня надёжности и качества передачи дискретной информации играют современные методы помехоустойчивого кодирования.

За более чем полувековую историю развития теории и техники помехоустойчивого кодирования основные методы и подходы к решению главной проблемы этой научной дисциплины – максимально простого и одновременно очень эффективного декодирования – неоднократно и весьма существенно менялись. Если сначала ведущими направлениями теории кодирования были интересные разработки алгоритмов исправления ошибок на базе алгебры конечных полей, то затем, после некоторого периода увлечения специалистов очень простыми и понятными мажоритарными методами, наступила эра алгоритма Витерби. Этот алгоритм был с теоретической точки зрения максимально сложным, переборным, но настолько эффективным, что значительный период времени все развитие теории кодирования и создание конкретных устройств исправления ошибок для спутниковой связи были сконцентрированы именно на этом методе. Правда, использовать длинные коды для декодера Витерби было невозможно из-за проблемы сложности декодирования, экспоненциально растущей с увеличением длины кода.

Последовавший затем период эффективной реализации каскадных методов кодирования успешно завершился внедрением в технику связи каскадных кодов на базе свёрточных кодов и кодов Рида-Соломона. При этом, как и предсказывала теория, на практике действительно оказалось, что каскадные коды позволяли при меньшей сложности декодирования по сравнению с исходными некаскадными методами обеспечивать одновременно и гораздо более высокие характеристики помехоустойчивости. Однако, несмотря на большой прогресс в теории и в микроэлектронной технологии, характеристики систем кодирования и

последующего декодирования до конца 80-х г. оставались всё ещё весьма далёкими от теоретически возможных пределов.

Только появление в 1993 году турбо кодов показало специалистам, что практически полное использование ёмкости цифровых каналов связи оказывается уже вполне реальной технической задачей. Множества турбо подобных и некоторых других кодов доказали, что уже действительно появились способы гораздо более эффективного использования пропускной способности очень дорогих космических, спутниковых и многих других цифровых каналов связи, чем это было возможно до сих пор. Энергетика гауссовских каналов при использовании некоторых кодов этих классов может быть всего на несколько десятых долей децибела более высокой, чем это определяется основным теоретическим ограничением: равенством кодовой скорости и пропускной способности канала. Ни о чём подобном до этого специалисты не могли и помыслить. А ведь уже давно было известно, что снижение допустимой энергетики сигнала всего на несколько десятых долей децибела для каналов достаточно масштабных сетей приводит к огромному экономическому эффекту. Если в 1980 г. известный американский специалист, автор классических книг по теории кодирования Э. Берлекэмп в одном из своих обзоров утверждал, что каждый децибел снижения энергетики канала связи оценивается в миллион долларов, то при современном масштабе цифровых сетей экономическая ценность применения кодирования возросла во много десятков раз. Понятно, что это происходит в результате существенного повышения скорости передачи цифровых данных, значительного снижения размеров очень дорогих антенн, многократного увеличения дальности связи, а также многих других весьма важных достоинств систем связи, использующих кодирование. Этим и определяется важность для всей отрасли телекоммуникаций работ по созданию эффективных декодеров, в связи с чем на десятках ежегодных международных конференций вопросы помехоустойчивого кодирования практически всегда оказываются среди самых актуальных.

Однако истекшее десятилетие однозначно показало, что множества турбо подобных и некоторых других кодов всё же не

решили проблему сложности декодирования. Более того, сегодня даже продолжающееся весьма быстрое развитие микроэлектронных технологий не позволяет утверждать, что в достаточно высокоскоростных каналах можно рекомендовать применение турбо кодов. Во многих случаях декодеры для этих кодов будут гораздо более медленными, чем это требуется, или чрезмерно дорогими.

Новое очень эффективное решение проблемы сложности декодирования при одновременной реализации высоких энергетических характеристик систем кодирования на базе многопороговых декодеров (МПД) ясно и доступно изложено в предлагаемой читателю книге известного отечественного специалиста в области помехоустойчивого кодирования доктора технических наук В.В. Золотарёва. Первые авторские свидетельства на изобретения, закрепляющие приоритеты автора этого удивительно простого и очень эффективного метода, относятся к 1972 г. За истекший период им создана всеобъемлющая теория этого уникального метода, а в системы связи различного назначения внедрено множество конкретных разработок МПД декодеров с очень высокими характеристиками.

МПД алгоритмы, как и большинство декодеров для турбо кодов, являются итеративными процедурами. Однако турбо коды появились на 20 лет позже многопороговых алгоритмов, которые и в те годы, и в настоящее время продолжают весьма динамично развиваться и интенсивно патентуются. Но самое главное заключается в том, что мажоритарные процедуры позволяют реализовать фактически их полное распараллеливание и определяют, в конечном счёте, условия для создания высокоскоростных декодеров этого типа с очень высокими энергетическими характеристиками.

Другое важнейшее преимущество МПД алгоритмов перед многими другими процедурами коррекции ошибок состоит в том, что они обладают свойством строгого роста правдоподобия своих решений в течение всего процесса исправления ошибок в искажённом шумами сообщении. Никаких строгих доказательств подобных уникальных свойств для других методов декодирования до сих пор неизвестно. Разумеется, при достиже-

нии МПД декодером самого правдоподобного решения оно оказывается оптимальным, таким, которое обычно требует полного перебора всех возможных решений, как это очень элегантно выполняет, в частности, алгоритм Витерби. Но сложность МПД, конечно же, остается линейно растущей функцией от длины используемого кода. Поэтому МПД, в отличие от декодера Витерби, легко оперирует очень длинными кодами, что и позволяет ему обеспечивать высокие характеристики помехоустойчивости и энергетического выигрыша.

При прочтении книги читателям становится ясным ещё одно важное, можно даже сказать, драматическое обстоятельство: почему алгоритм МПД так и не был открыт зарубежными специалистами. В 70-е годы они публиковали большое число результатов по повторным попыткам декодирования сообщений, в которых некоторая доля искажённых символов уже была исправлена на первом шаге коррекции ошибок. Вполне очевидным это становится после прочтения предлагаемого читателю данного теоретического и прикладного исследования.

Причины абсолютного лидерства методов МПД декодирования состоят в следующем.

1. Никто до автора этой книги не пытался решать задачу такой модификации простейшего из известных методов декодирования, мажоритарного, в результате которой он обладал бы способностью строгого улучшения своих решений при всех изменениях декодируемых символов. В самом деле, стремление сделать из очень простого алгоритма метод, практически не отличающийся по своим характеристикам от оптимальных переборных процедур, может быть только похвальным, однако оно же является и чрезвычайно рискованным. Но такая задача была автором поставлена – и решена!

2. Ещё одна, идеологически намного более сложная проблема, одновременно решавшаяся – и решённая (!) автором, состояла в глубоком анализе причин группирования ошибок на выходе мажоритарного декодера. Именно это группирование делало бесполезным повторные попытки декодирования, что и подтверждалось многими экспериментальными работами по кодам 70-х годов. А на самом деле следовало бы на основе глубо-

кого и всестороннего анализа группирования ошибок декодера, известного как эффект размножения ошибок, максимально минимизировать его и найти такие коды, в которых эффект размножения ошибок почти не проявляется. И эта задача тоже была решена автором с использованием математических методов, ранее никогда не применявшихся в области помехоустойчивого кодирования.

Только одновременное решение этих двух взаимосвязанных проблем и позволило создать специальные коды и итеративные процедуры с простейшими мажоритарными функциями, которые даже при очень высоких уровнях шума могли постепенно в течение многих итераций улучшать достоверность принятых из канала сообщений и в абсолютном большинстве случаев находить оптимальные решения.

3. Но на самом деле успех разработок МПД алгоритмов связан с решением ещё одной классической задачи: оптимизации функционала от очень большого числа переменных. Как совершенно справедливо указывает автор, возможность вариации целого ряда параметров кодов и декодеров, в частности, весов проверок, значений пороговых элементов и разностных соотношений в полиномах используемых кодов создаёт дополнительные условия для улучшения характеристик МПД декодеров. Таких настраиваемых элементов в декодерах может быть много сотен и даже тысяч. Но после правильного выбора этих элементов оказывается, что автоматизированная компьютерная оптимизация параметров декодера ещё на этапе его проектирования заметно улучшает и так достаточно высокие характеристики многопорогового алгоритма вообще без какого-либо увеличения итоговой сложности и объёма вычислений реального разработанного декодера с такими улучшенными параметрами. Заметим, что постановку этой третьей проблемы для других систем декодирования даже невозможно вообразить, поскольку она может возникнуть только параллельно с решением первых двух описанных выше проблем эффективного и простого декодирования для МПД алгоритмов.

Таким образом, успех теории и прикладных достижений в области простого и эффективного декодирования средствами

МПД определяется одновременным успешным решением трёх вышеприведённых сложнейших проблем, каждая из которых так или иначе связана с решением задач оптимизации функционалов от большого числа переменных. Отсутствие удовлетворительных решений хотя бы одной из них, несомненно, многократно понизило бы ценность возможных достижений в области итеративных мажоритарных схем декодирования, поскольку все их характеристики в этом случае были бы весьма и весьма скромными.

В книге представлены и другие, очень необычные для традиционных способов декодирования методы. Фактически все они служат главной цели: максимальному увеличению эффективности декодера при минимальной сложности его схемы. К ним можно отнести каскадирование с простейшими кодами контроля по чётности, результаты по параллельному кодированию, а также коды с выделенными ветвями.

Совершенно особое место среди предложенных автором алгоритмов занимают также впервые описанные им МПД декодеры для недвоичных кодов. Они существенно перекрывают по своей эффективности коды Рида-Соломона, оставаясь столь же простыми в реализации, как и их двоичные аналоги. Удивительно, но за многие десятилетия развития теории кодирования такое очевидное обобщение мажоритарных методов на недвоичные цифровые потоки данных так и не было сделано ни одним исследователем, кроме автора этой монографии. Преимущество недвоичных МПД перед кодами Рида-Соломона оказывается сразу настолько значительным, что фактически можно говорить о том, что открытые более 20 лет назад эти новые коды и алгоритмы знаменуют собой совершенно новую эпоху в обработке символьной информации. Для этого типа МПД просто вообще нет никаких других методов любой сложности, которые могли бы сравниться с ним по эффективности. Как и при разработке других полезных подходов к коррекции ошибок, автор достиг очень значимых результатов для недвоичных кодов только за счёт перехода к гораздо более длинным кодам, чем единственные доступные в настоящее время коды Рида-Соломона. Разумеется, у недвоичного МПД сохранена предельно малая слож-

ность декодирования, присущая мажоритарным методам. Эти коды также найдут широкое применение в сфере обработки, хранения и передачи данных.

Интересно и то, что МПД алгоритмы, предназначенные для борьбы с ошибками тракта передачи данных, без каких-либо изменений можно успешно применять и для повышения помехоустойчивости, и для сжатия данных, т.е. для одновременного решения второй важнейшей задачи теории информации – кодирования некоторых видов источников.

Наконец, нельзя не подчеркнуть, что все описанные МПД алгоритмы настолько просты в реализации и одновременно высокоэффективны, что именно их программные версии успешно прошли строгие испытания и были приняты к использованию в системах специального цифрового телевидения, а для соответствующих им кодов начата процедура стандартизации.

Предполагалось, что появление данной книги должно было произойти лет на десять раньше. Тогда сейчас можно было бы говорить об её очередном переработанном издании. Однако её автор, тем не менее, на протяжении всего этого времени старался знакомить научно-техническую общественность с новыми разработками в области кодирования. Важным событием для отечественных специалистов стал выход в 2004 г. справочника В.В. Золотарёва и Г.В. Овечкина «Помехоустойчивое кодирование. Методы и алгоритмы» в издательстве «Горячая линия - Телеком». Он позволил значительно расширить сферу применения МПД алгоритмов и заметно ускорить их разработку для широкого круга прикладных задач.

Большой вклад в развитие теории и техники кодирования внесли также ставшие регулярными выступления автора книги и его многочисленных коллег на традиционных ежегодных Международных конференциях по цифровой обработке сигналов в Москве. Широко известен специалистам и ставший уже очень большим специализированный двуязычный сайт ИКИ РАН **www.mtdbest.iki.rssi.ru** по методам многопорогового декодирования. На нём представлено около двухсот единиц теоретических, методических, учебных и демонстрационных материалов по этому алгоритму, включающих даже серию специальных

компьютерных фильмов, ярко демонстрирующих в динамике особенности работы МПД декодеров.

Завершая представление этой, конечно же, весьма необычной по своим методам и результатам книги о лучших за последние годы достижениях отечественных исследователей в области помехоустойчивого кодирования, хочется пожелать автору и его ученикам дальнейшей успешной работы на необозримой ниве высококачественных цифровых сетей. Выход такой важной для теории и техники связи монографии в период интенсивного перехода мирового сообщества на полностью цифровые методы формирования, хранения, обработки и передачи данных, безусловно, ускорит все процессы совершенствования систем связи и дальнейшего роста качества информационного обслуживания нашего общества.

Быстрое современное развитие техники кодирования и непрерывный рост возможностей элементной базы ещё более расширят сферу применения как самого МПД алгоритма, так и множества его модификаций. Конечно, и для ряда других методов реализация декодирования окажется при этом вполне доступной задачей, даже если в настоящее время они ещё кажутся слишком сложными. Но совершенно очевидно, что только те методы кодирования, которые наиболее целенаправленно и экономно расходуют свои вычислительные ресурсы для решения задачи коррекции искажений в цифровых потоках данных, действительно окажутся предельно быстрыми, наиболее эффективными и самыми доступными для широкого применения в сетях связи.

Член-корреспондент РАН,
доктор технических наук, профессор,
Заслуженный деятель науки РФ
Лауреат Государственной премии РФ
и Премии Правительства РФ Ю.Б. Зубарев

ОТ АВТОРА

Выход в свет в 1963 г. книги Дж. Л. Месси «Пороговое декодирование» ознаменовал новый этап в развитии техники помехоустойчивого кодирования. Ясное описание очень простых методов со вполне удовлетворительными характеристиками определило в те годы их место в различных реальных системах связи.

Последующее появление в 1967 г. алгоритма Витерби вывело технику кодирования на принципиально новый уровень качества связи, поскольку предложенный алгоритм обеспечивал в гауссовском канале оптимальное декодирование кодов небольшой длины. В те годы большое число специалистов по теории и технике кодирования обратилось к проблеме повышения именно эффективности кодирования, поскольку всем тогда казалось, что быстрый рост возможностей цифровых технологий позволит очень просто строить каскадные и другие всё более сложные схемы кодирования. В связи с этим обстоятельством проблема сохранения простоты реализации декодеров на длительное время осталась как бы в тени, хотя формально требование простого декодирования никогда не снималось с повестки дня.

Несмотря на то, что публикации по вопросам эффективности пороговых алгоритмов в 70-х годах продолжали появляться, сформировавшееся мнение большинства специалистов о возможностях мажоритарных схем декодирования стало весьма консервативным. Для этого были все основания. Наиболее серьезным аргументом считалось наличие эффекта размножения ошибок. Он изначально серьезно снижал и без того невысокую эффективность пороговых процедур, поскольку приводил к сильному пакетированию ошибок на выходе декодера. К сожалению, сколько-нибудь результативных методов уменьшения этого эффекта так и не было найдено. Поиск специальных кодов для мажоритарных процедур также не принес более значимых результатов, чем те, которые были уже известны.

До некоторой степени полезные для практики порогового декодирования реальные результаты в те же 70-е годы были получены многими специалистами в экспериментах по повторному декодированию символов, в частности, в свёрточных кодах.

Они показали наличие небольшого дополнительного снижения итоговой вероятности ошибки декодирования в каналах с относительно малым уровнем шума. Но все эти сообщения никак не повлияли на справедливое в целом мнение о недостаточной эффективности пороговых декодеров, особенно при большом уровне шума.

В предлагаемой читателям книге изложены результаты тридцатипятилетних исследований процедур мажоритарного типа, из которых следует, что при выполнении некоторых достаточно простых условий и определенной модификации декодеров порогового типа возможно вполне успешное декодирование многих кодов в широком диапазоне параметров шума канала. Результаты применения таких усовершенствованных мажоритарных алгоритмов, названных многопороговыми декодерами (МПД), оказываются во многих случаях практически близкими к оптимальным, т.е. мало отличающимися по выходной вероятности ошибки от характеристик переборных алгоритмов. Это было показано автором в различных публикациях как теоретически, так и при моделировании работы соответствующих процедур для специальных кодов, удовлетворяющих ряду весьма строгих требований.

Декодеры, построенные в соответствии с изложенными ниже принципами, уже успешно внедрены в многочисленных системах связи. Во всех случаях программной и аппаратной реализации предлагаемых далее методов многопорогового декодирования были получены ожидаемые автором и разработчиками систем связи характеристики, которые были иногда совершенно недоступны для других известных алгоритмов коррекции ошибок с разумной сложностью реализации.

Основные положения, которые фактически и позволили поднять эффективность исключительно простых алгоритмов порогового типа до уровня оптимальных процедур, состоят всего из двух пунктов, обеспечивших решение задачи принципиального повышения качества декодеров мажоритарного типа.

1. Эффект размножения ошибок при пороговом декодировании действительно очень сильно ограничивает возможности пороговых декодеров. Но этот эффект вполне управляемый. Его

правильная интерпретация помогает сформировать требования и критерии, по которым можно строить коды с очень малым уровнем размножения ошибок на выходе соответствующего им декодера, что и позволяет, в конечном счете, существенно повысить эффективность итеративных процедур порогового типа.

2. Мажоритарные алгоритмы могут быть чрезвычайно эффективными. Существуют весьма простые МПД, которые обладают свойством стремления к оптимальному решению на всех шагах декодирования до тех пор, пока продолжается процесс изменения символов на пороговых элементах декодера.

Первое из приведенных выше утверждений заслуживает длительного обсуждения и серьёзного обоснования, что и сделано в гл.3. Успешное решение этой сложной проблемы позволило построить коды, которые особенно эффективны при их применении в МПД.

Более необычно второе свойство МПД, алгоритма, очень близкого внешне к классическому декодеру Месси, но обладающего воистину уникальным свойством стремления к оптимальному переборному решению, если выполнены весьма простые условия. Представляется правдоподобным, что никакие другие известные в настоящее время методы коррекции ошибок не обладают подобными свойствами.

Автор надеется, что читатели этой книги на многие естественные вопросы по проблеме сложности, эффективности и технологичности кодирования и многопорогового декодирования получат в той или иной степени содержательные ответы. В случае заинтересованности они, несомненно, смогут сами продолжить весьма перспективные для всех систем связи исследования МПД процедур, которые уже нашли свое место в целом ряде разработок.

Как будет показано далее, проблема сложности декодирования вовсе не девальвируется с появлением процедур класса МПД. На самом деле при разработке новых алгоритмов и соответствующих им кодов проблемой становится максимально аккуратное и оптимизированное по очень многим критериям одновременное проектирование декодера и применяемого в нем кода. Иначе говоря, простота реализации МПД достигается за

счёт более сложного и тщательно организованного этапа проектирования кода и алгоритма его декодирования. В этом случае проблема сложности реализации алгоритма целенаправленно трансформируется таким образом, чтобы технологические задачи построения более эффективного декодера решались именно за счет тех компонентов сложности, увеличение которых наиболее доступно. Например, в абсолютном большинстве случаев минимизации вычислительных затрат МПД объём его операций декодирования при сопоставимой эффективности оказывается почти на два десятичных порядка меньшим, чем для других алгоритмов за счёт значительного объёма памяти декодера, использующего весьма длинные коды, что вполне допустимо, а иногда даже необходимо в высокоскоростных системах связи. Множество других важных обменных соотношений между параметрами кодов и декодеров также будет обсуждаться ниже.

Завершая вводные комментарии, автор выражает свою глубокую уверенность, что первое достаточно полное изложение теории МПД, конечно, не лишенное в связи с этим определенных недостатков, позволит читателям найти собственные новые пути дальнейшего роста эффективности декодирования с использованием также и процедур класса МПД. Их универсальность, высокая однородность и крайняя простота обеспечивают существенный рост достоверности передачи данных в каналах с малым уровнем энергетики при минимальных затратах на реализацию кодирования.

Внимательный читатель, возможно, отметит, что многие свойства и возможности представленного в книге алгоритма неоднократно рассматриваются и комментируются в различных разделах книги с разных позиций. Автор должен признать, что это действительно так и сделано с единственной целью наиболее полного, всестороннего и в то же время максимально понятного доказательства или объяснения свойств и возможностей многопороговых декодеров. Такой способ изложения материала диктуется тем, что, хотя все ключевые результаты получены достаточно простыми методами, многие из них всё же не использовались ранее в публикациях по теории и технике кодирования и являются для этой отрасли науки новыми. Это требует

очень аккуратного и постепенного предъявления во многих случаях всё же весьма непростых и иногда даже неожиданных результатов, свойств и характеристик алгоритмов. Разнообразные комментарии и формы изложения материала как раз и облегчают читателю задачу понимания представленных в книге результатов, для усвоения которых иногда требуются немалые усилия и время.

В качестве последнего замечания автор считает полезным подчеркнуть, что все исходные предпосылки исследования, теоретические результаты, вытекающие из них практические следствия и выводы по результатам представленного исследования чрезвычайно просты. Они связаны только с самыми общепринятыми понятиями теории и техники кодирования и не требуют знаний специальных разделов других смежных дисциплин. Именно эта возможность взглянуть на потенциальные возможности кодов и многопороговых процедур, исходя только из самых простейших теоретических соображений и здравого смысла, создает условия для очень быстрого обучения студентов и специалистов новым возможностям техники кодирования на основе МПД алгоритмов. В свою очередь, правильное понимание возможностей алгоритмов этого типа позволит в дальнейшем в точных и ясных терминах ставить и успешно решать новые задачи по созданию все более быстродействующих, дешевых и максимально простых МПД декодеров для различных систем связи.

Автор считает своим приятнейшим долгом поблагодарить воистину огромное количество своих помощников, энтузиастов и просто высокопрофессиональных специалистов, которые в течение 35 лет помогали ему в проведении исследований и применении полученных результатов в конкретных системах и проектах.

Большую поддержку работам по МПД алгоритмам оказывали Научный совет по комплексной проблеме «Кибернетика» АН СССР, НИИ «КВАНТ», НИИРадио, Воронежский НИИСвязи, ЛЭИС им. М.А. Бонч-Бруевича, ИКИ РАН и Рязанский ГРТУ.

Наверное, исследования МПД не могли бы быть представлены в своём нынешнем виде, если бы не постоянное внимание

к ним академика РАН В.К. Левина, члена-корреспондента РАН Ю.Б. Зубарева, профессоров Э.М. Габидулина, С.И. Самойленко, Ю.Г. Дадаева и В.И. Коржика, которые в своё время высоко оценили представленные материалы исследований по этому алгоритму и способствовали их признанию научно-технической общественностью.

Особенную тёплую признательность автор выражает своему молодому коллеге кандидату технических наук, доценту Г.В. Овечкину, который взял на себя основные заботы по организации публикации этой книги и выполнил практически все редакторские и прочие непростые обязанности, которыми сопровождается выход в свет подобных монографий.

* * * * *

Для получения наглядного представления об эффективности работы МПД читателям предлагается небольшой демонстрационный мультфильм-программа, предназначенный для работы на IBM PC-совместимом компьютере под управлением операционных систем MS-DOS или Windows. В нём проиллюстрированы некоторые важнейшие особенности процедур декодирования многопорогового типа при исправлении ошибок в условиях большого уровня шума канала. Возможно, что именно небольшая предварительная подготовка психологического плана с помощью предлагаемой демопрограммы создаст необходимые эмоциональные и гносеологические предпосылки для последующей плодотворной работы с этой книгой. Инструкцию по работе с демонстрационной программой и сам мультфильм можно переписать со специализированного веб-сайта ИКИ РАН **www.mtdbest.iki.rssi.ru** на странице описания методов МПД. Там же можно найти самую разнообразную оперативную информацию по МПД алгоритмам.

Кроме того, на нашем сайте в разделах ответов на вопросы освещён целый ряд проблем, относящихся к общим постановкам задач кодирования и конкретным возможностям МПД алгоритмов.

Значительную поддержку в изучении методов декодирования на основе МПД алгоритмов могут оказать также три очень полезные лабораторные работы. Их можно переписать с образо-

вательной странички нашего веб-сайта и предложить студентам радиотехнических кафедр ВУЗов и слушателям системы профессиональной переподготовки специалистов в области телекоммуникаций.

Дополнительные сведения по многопороговым декодерам и другим полезным методам коррекции ошибок можно найти в нашем справочнике [1].

В. В. Золотарёв

ВВЕДЕНИЕ

Быстрый рост объемов обработки данных, развитие цифровых систем вещания и вычислительных сетей предъявляют весьма высокие требования к минимизации ошибок в используемой дискретной информации. Переход всех видов создания, хранения, использования и передачи данных, а также средств вещания на цифровые методы, происходящий сейчас во всём мире, ещё более повышает важность высококачественной передачи цифровых потоков. Успешная работа этих систем возможна только при наличии специальной эффективной аппаратуры, которая позволяет гарантировать достоверную передачу информации. Важнейший вклад в повышение достоверности обмена цифровыми данными вносит теория помехоустойчивого кодирования. На её основе разрабатываются всё новые методы защиты от ошибок, базирующиеся на использовании корректирующих кодов.

Повышение достоверности при обнаружении ошибок в системах с переспросом не представляет существенных трудностей. Если же приёмник не имеет возможности организовать переспрос ошибочно принятых сообщений, проблема высококачественного декодирования становится весьма актуальной и чрезвычайно сложной, особенно при значительном уровне шума в канале.

Возможность использования тех или иных алгоритмов коррекции ошибок в системах без обратной связи, где нельзя организовать переспрос, определяется весьма жесткими требованиями, предъявляемыми к этим алгоритмам, например, по числу операций в случае их программной реализации или по размерам, помехоустойчивости, быстродействию, энергопотреблению и технологичности при проектировании специализированных БИС. Большое число регулярно издающихся монографий, посвященных различным аспектам теории помехоустойчивого кодирования, и десятки международных конференций по этой тематике, организуемых каждый год во всём мире, свидетельствуют об огромной сложности и чрезвычайной актуальности проблемы эффективного декодирования.

Данная книга посвящена систематическому изложению методов коррекции ошибок в цифровых данных на базе итеративных мажоритарных методов декодирования, к которым последнее время вновь привлечено внимание специалистов в области систем связи после некоторого периода развития в основном оптимальных декодеров, реализующих алгоритм Витерби, турбо кодов и других схем коррекции ошибок.

Обращение автора к мажоритарным методам декодирования обусловлено в значительной мере тем, что, хотя вся теория кодирования развивается под лозунгами повышения эффективности декодеров при минимальной сложности, реальное положение дел в этой области улучшается в основном за счёт только усложнения алгоритмов декодирования и кодовых конструкций. Поэтому именно методы, изложенные в данной книге можно отнести к тем алгоритмам, которые действительно являются наименее затратными в вычислительном аспекте.

Невозможно переоценить особую важность для техники связи мажоритарных алгоритмов, которые позволяют исправлять большое число ошибок веса, существенно превышающего половину кодового расстояния используемых кодов. Мажоритарные декодеры рассматривались ранее как в классических монографиях Л.М. Финка [2], Л.Ф. Бородина [3], Дж. Месси [4] и В.Д. Колесника и Е.Т. Мирончикова [5], так и в книгах, изданных позднее [6, 7, 8]. Затем, как известно, последовал период, в течение которого мажоритарные методы были надолго забыты и мало анализировались. Еще более существенным достоинством порогового декодирования оказалась возможность эффективного многократного улучшения решений этого декодера, которая была доказана, в частности, в коллективной монографии [9] на примере систематических свёрточных кодов. Этот алгоритм, названный многопороговым декодированием (МПД) [10, 11], описан также в монографии [12] и использован в [13].

Данная книга посвящена изложению результатов обобщающих исследований многопороговых декодеров для двоичных и недвоичных кодов, используемых для передачи сообщений по каналам с ошибками и стираниями. Особое внимание уделяется решению проблемы минимизации объёма вычислений

при сохранении максимально высокой энергетической эффективности кодирования и небольшой сложности декодирования.

Теоретическое и экспериментальное исследование, изложенное в данной книге, преследовало две цели:

1) теоретическое обоснование метода многопорогового декодирования линейных кодов, сопоставимого по эффективности с лучшими известными алгоритмами;

2) анализ специальных методов кодирования с использованием МПД, не уступающих по эффективности лучшим каскадным схемам.

Структурно монография состоит из шести глав.

В первой главе введены основные понятия и определения, используемые в последующих разделах.

Во второй главе сформулированы основные принципы многопорогового декодирования для двоичных симметричных каналов, доказано стремление решений декодеров этого типа к решению оптимального переборного метода коррекции ошибок. Затем этот принцип роста правдоподобия решения МПД обобщается на двоичные гауссовские каналы при использовании «мягких» модемов, недвоичные и несистематические коды и на каналы со стираниями. Рассмотрена и возможность его использования для декодеров, работающих совместно с системами многопозиционных сигналов. Предложены также методы сжатия данных на базе МПД.

В третьей главе рассмотрены причины возникновения эффекта размножения ошибок при пороговом декодировании блоковых и свёрточных двоичных и недвоичных кодов. Результаты анализа размножения ошибок позволили построить множество кодов, которые наиболее эффективны при использовании в МПД для различных типов каналов связи.

В четвёртой главе выводятся нижние, верхние и приближенные аналитические оценки эффективности процедур многопорогового декодирования для различных кодов.

Пятая глава посвящена изучению экспериментальных результатов исследования МПД, полученных при компьютерном моделировании и при измерениях на специализированных стендах характеристик работы декодеров различного типа для кана-

лов с аддитивным белым гауссовским шумом и в других трактах передачи данных.

В шестой главе обсуждаются вопросы использования МПД в перспективных схемах каскадного, параллельного и других специальных методов кодирования.

В заключении сформулированы обобщающие выводы по проведенному исследованию и предложены направления дальнейшего развития тематики МПД.

Предполагается, что читатели знакомы с основами теории кодирования и методов вычислений в конечных полях. Никаких излишне сложных соотношений, свойств и результатов из теории конечных полей в предлагаемой читателям книге использоваться не будет. Это позволит сосредоточить основные усилия при чтении именно на понимании свойств и возможностей изучаемых многопороговых алгоритмов, что поможет заинтересованным читателям хорошо сориентироваться в современной проблематике построения систем помехоустойчивого кодирования и с максимальной степенью уверенности выбирать пути дальнейшего повышения эффективности таких систем.

Дополнительные информационные, научные и учебно-методические материалы по МПД алгоритмам можно найти на постоянно обновляемом специализированном двуязычном вебсайте ИКИ РАН по адресу: **www.mtdbest.iki.rssi.ru**.

Возможно, что первая обобщающая монография по многопороговым алгоритмам, в которой используются простые, но иногда весьма нетрадиционные для теории кодирования методы, вызовет у специалистов определённые вопросы и окажется не лишённой некоторых недостатков. Все предложения и замечания автор просит присылать по адресу: 117997, Москва, ул. Профсоюзная, д. 84/32, ИКИ РАН, В.В. Золотарёву, а также по электронной почте: **zolotasd@yandex.ru**.

ГЛАВА 1. ЗАДАЧА КОДИРОВАНИЯ В ТЕХНИКЕ СВЯЗИ

1.1. Линейные коды

Основным понятием, используемым для описания системы помехоустойчивого кодирования, является код – множество возможных сообщений. Пусть необходимо передать последовательность (вектор), состоящую из k информационных символов, $\bar{I} = (i_0, i_1, i_2, ..., i_{k-1})$, каждый из которых принадлежит алфавиту размера $q \geq 2$, причем эти символы принадлежат полю Галуа, состоящему из q элементов и обозначаемому как GF(q). Тогда линейный блоковый код задается порождающей матрицей G размера $k \times n$, $k < n$, так что для каждого информационного вектора $\bar{I}$ длины k кодовый вектор $\overline{A} = (a_0, a_1, a_2, ..., a_{n-1})$ определяется как

$$\overline{A} = \bar{I}G, \qquad (1.1)$$

где операции умножения и сложения выполняются в выбранном поле.

Важную роль в оценке возможностей кодов играют кодовая скорость $R = k/n$, $0 < R < 1$, и минимальное кодовое расстояние d. Расстоянием между двумя векторами одинаковой длины называется число символов, в которых они отличаются. Тогда значение параметра d – минимальное по всем парам ($\overline{A}_i$, $\overline{A}_j$), $i \neq j$, расстояние между кодовыми векторами данного кода. Минимальное кодовое расстояние d является существенной характеристикой кодов, в значительной мере определяющей их корректирующие возможности. Если первые k символов в кодовом слове $\overline{A}$ совпадают с вектором $\bar{I}$, то код называется систематическим, а последние $r = n - k$ кодовых символов являются проверочными.

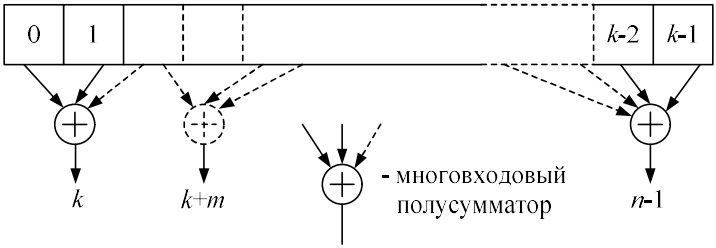
По заданной матрице G можно построить проверочную матрицу кода H размера $r \times n$ такую, что для кодового слова, порождаемого в соответствии с (1.1), справедливо равенство

$$H\overline{A} = 0.$$

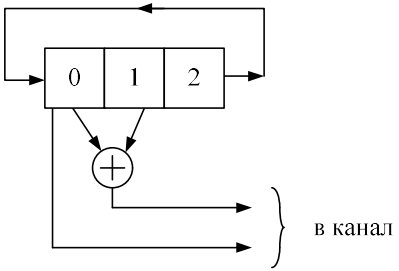
Заметим, что здесь и в большинстве случаев далее для того, чтобы не загромождать формулы, опускается знак транспонирования.

Для технической реализации систем кодирования весьма полезен тот факт, что сумма в поле GF(q) двух кодовых слов $\overline{A}_i$ и $\overline{A}_j$ линейного кода всегда также является кодовым словом. Это позволяет при кодировании не запоминать все возможные 2^k кодовых слов, а обходиться весьма простыми схемами. На рис. 1.1а представлен кодер линейного двоичного систематического кода, состоящий из k ячеек памяти для входной информации и ($n - k$) многовходовых сумматоров по mod 2 (полусумматоров). Однако и этот кодер может быть существенно упрощен за счет использования более регулярной структуры порождающей матрицы G.

На рис. 1.1б изображен кодер систематического квазициклического блокового кода, соответствующий порождающей матрице (1.2):



а) Общий вид кодера линейного систематического блокового кода



б) Кодер систематического квазициклического кода с $R = 1/2$, $n = 6$, $d = 3$

Рис. 1.1

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}. \qquad (1.2)$$

Кодер содержит регистр сдвига на 3 бита и один двухвходовый полусумматор. В трех информационных ячейках находятся данные, подлежащие кодированию. В этом положении на выходе полусумматора формируется первый из трех проверочных символов. После циклического сдвига вправо данных в регистре на выходе полусумматора формируется второй проверочный символ, а затем третий. Получившийся код, как легко проверить, имеет $R = 1/2$, $n = 6$, $d = 3$ и относится к классу квазициклических [14, 15].

Другой большой класс образуют свёрточные коды, определяемые полубесконечными матрицами G, состоящими из некоторых прямоугольных подматриц $G_{i,j}$ размера $k_0 \times n_0$, $k_0 < n_0$:

$$G = \begin{pmatrix} G_{1,1} & G_{1,2} & \ldots & G_{1,m} & 0 & 0 & 0 & \ldots \\ 0 & G_{2,1} & G_{2,2} & \ldots & G_{2,m} & 0 & 0 & \ldots \\ 0 & 0 & G_{3,1} & G_{3,2} & \ldots & G_{3,m} & 0 & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \end{pmatrix}.$$

которые, в частности, могут быть просто отдельными элементами поля GF(q). В свёрточных кодах эквивалентом длины блокового кода n является длина кодового ограничения n_{A}, определяемая как длина отрезка в полубесконечной кодовой последовательности $\overline{A} = (a_0, a_1, a_2, \ldots)$

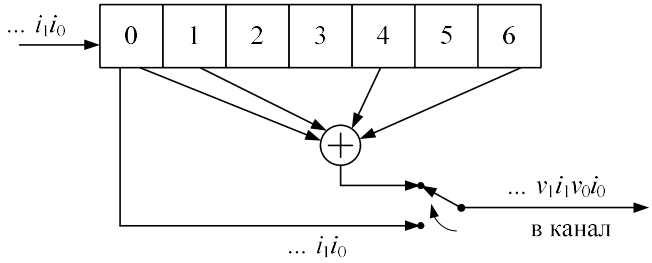
$$\overline{A} = \bar{I}G, \qquad (1.3)$$

в пределах которого значения кодовых символов a_j зависят от значения некоторого символа i_k из информационного полубесконечного вектора $\bar{I} = (i_0, i_1, i_2, \ldots)$.

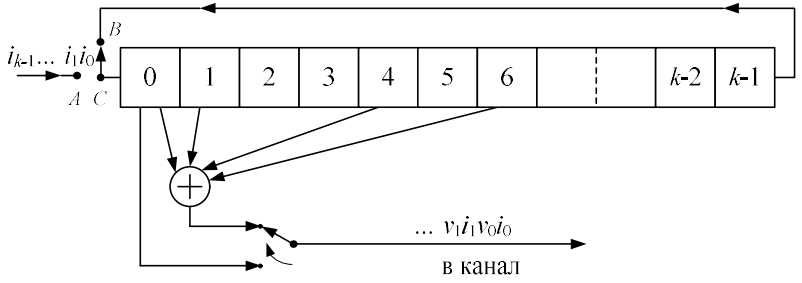
В линейном свёрточном коде с $R = k_0/n_0$ можно определить минимальное кодовое расстояние d как минимальный вес начальной части кодового слова длины n_{A} при условии, что хотя бы один символ i_j из первого информационного подблока, т.е. с

номером j, $0 \le j < k_0$, не равен нулю. Обеспечение максимальной помехоустойчивости возможно при полной реализации потенциальных возможностей используемых кодов. В этом случае корректирующие возможности кода в большей степени зависят не от d, а от свободного расстояния d_f, которое соответствует минимальному расстоянию между кодовыми словами произвольной длины. Для рассматриваемых линейных кодов это одновременно и минимальный вес ненулевого кодового слова. Как следует из определений, всегда справедливо неравенство $d \le d_f$.

В систематических блоковых кодах порождающая матрица имеет вид $G = (I_k{:}P)$, т.е. представима как совокупность единичной подматрицы I_k порядка k и прямоугольной подматрицы P размера $k \times (n–k)$. Тогда проверочная матрица двоичного кода приобретает вид $H = (P^{\mathrm{T}}{:}I_{n–k})$. В случае свёрточных кодов с фиксированными связями начальная часть подматрицы P^{T} превращается в совокупность треугольных матриц, полностью определяющих код. На рис. 1.2а представлен пример кодера для двоичного свёрточного кода с $R = 1/2$, $d = 5$ и $n_{\mathrm{A}} = 14$.



а) Кодер свёрточного самоортогонального кода с $R = 1/2$, $d = 5$, $n_{\mathrm{A}} = 14$



б) Преобразование свёрточного кодера в квазициклический блоковый кодер

Рис. 1.2

На каждом такте работы кодера в регистр сдвига поступает один информационный символ, который и передается через схему коммутатора в канал вместе с проверочным символом с выхода четырехвходового полусумматора. Этому коду соответствует проверочная матрица

$$H = \begin{pmatrix} 1 & & & & & & & & \\ 1 & 1 & & & & & & & \\ 0 & 1 & 1 & & & & & & \\ 0 & 0 & 1 & 1 & & & & : & I \\ 1 & 0 & 0 & 1 & 1 & & & & \\ 0 & 1 & 0 & 0 & 1 & 1 & & & \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 & & \\ . & . & . & & & & & & \end{pmatrix}. \qquad (1.4)$$

Отметим, что множество строк этой матрицы с номерами 0, 1, 4 и 6 имеют единицы в первом столбце, а во всех остальных столбцах есть не более одной единицы в строках из этого множества.

После умножения на проверочную матрицу кода H принятого из канала вектора $\overline{Q} = \overline{A} + \overline{E}$, где $\overline{A}$ – передаваемое кодовое слово, $\overline{E} = (e_0, e_1, e_2, ...)$ - вектор аддитивного шума, получается вектор синдрома

$$\overline{S} = H\overline{Q} = H(\overline{A} + \overline{E}) = H\overline{A} + H\overline{E} = H\overline{E},$$

который в линейном коде не зависит от кодового вектора, а определяется только конфигурацией ошибок канала. Здесь и далее операции сложения выполняются в поле GF(q). В рассматриваемом примере проверочной матрицы свёрточного кода (1.4) множество компонент s_j синдрома $\overline{S}$, содержащих в качестве слагаемых ошибку e_0 в первом информационном символе i_0 будет иметь вид

$$
\begin{aligned}
S_0 &= e_0+e_{0v};\\
S_1 &= e_0+e_1+e_{1v};\\
S_4 &= e_0+e_3+e_4+e_{4v};\\
S_6 &= e_0+e_2+e_5+e_6+e_{6v}.
\end{aligned}
\qquad (1.5)
$$

Это множество проверок благодаря отмеченному выше свойству матрицы H содержит как в информационных, так и в проверочных символах (указанных в выражениях (1.5) с дополнительным индексом v), кроме ошибки e_0, не более одной ошибки с другими, отличными от 0 индексами. Такое свойство проверок, содержащих один декодируемый символ во всех проверках, а остальные – не более чем в одной из проверок рассматриваемого множества, называется ортогональностью, а коды, в которых таким свойством обладают компоненты вектора $\overline{S}$, называются самоортогональными (СОК). Эти коды, в основном, и обсуждаются далее.

1.2. Единство блочных и сверточных кодов

Единство свойств блочных и свёрточных кодов установлено уже достаточно давно [16, 17] и было дополнительно рассмотрено в [18]. Воспользовавшись результатами работы [19] покажем, как обширные множества самоортогональных кодов свёрточного типа использовать для построения блоковых кодов с теми же значениями параметров кодовой скорости R и кодового расстояния d.

Пусть некоторая входная информационная последовательность разбивается на блоки достаточно большой длины k и в положении А ключа С на рис. 1.2б вводится в кодер. После завершения ввода ключ переводится в положение В и при циклическом сдвиге информационного регистра на каждом такте сдвига формируется очередной символ блокового кода, который вместе с информационным символом из ячейки 0 поступает в канал.

Покажем, что для любых рациональных значений кодовой скорости $R = k_0/n_0 < 1$; k_0, $n_0 = 1, 2, \ldots$, из свёрточного СОК формируется блоковый квазициклический код, который также оказывается самоортогональным.

Поскольку квазицикличность рассматриваемого кода очевидна из построения, необходимо доказать только его самоортогональность. Напомним, что согласно [19] в СОК множество проверок, относящихся к некоторому декодируемому информационному символу i_m, будет в свёрточном коде ортогонально и с учетом информационных символов с меньшими, чем m, номерами, а не только в том случае, если учитывать символы лишь с более высокими индексами, как это видно из (1.5). Иначе говоря, если вместо треугольной проверочной матрицы H (1.4) рассмотреть полную матрицу свёрточного кода H_f

$$H_f = \begin{pmatrix}
1 & 0 & 1 & 0 & 0 & 1 & 1 & & & & & 0 & & \\
 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & & & & & & \\
 & & 1 & 0 & 1 & 0 & 0 & 1 & 1 & & & & & \\
 & & & 1 & 0 & 1 & 0 & 0 & 1 & 1 & & & : & I_{13} \\
 & & & & 1 & 0 & 1 & 0 & 0 & 1 & 1 & & & \\
 & & & & & 1 & 0 & 1 & 0 & 0 & 1 & 1 & & \\
 & & & & & & 1 & 0 & 1 & 0 & 0 & 1 & 1 & \\
0 & & & & & & & . & . & . & & & &
\end{pmatrix}. \qquad (1.6)$$

то при самоортогональности проверок, вычисляемых согласно (1.5), матрица H_f также определяет систематический самоортогональный свёрточный код.

Пусть длина кодового ограничения рассматриваемого исходного свёрточного кода равна n_A. Тогда любой информационный символ свёрточного кода i_m не входит в проверки относительно i_0, если значение номера m будет больше, чем $m_0 = n_A R$. В рассматриваемом примере свёрточного СОК с $R = k_0/n_0 = 1/2$ и $n_A = 14$ при $m_0 = 7$, как следует из (1.5), в проверках есть только ошибки с номерами не более 6, а с учетом вида H_f в (1.6) нет и индексов меньших, чем (–6).

Если теперь построить блоковый код так, чтобы регистр информационных символов был длины не менее $k = (2n_A – n_0)R$ (в кодере на рис. 1.2б $k = 13$), то это будет соответствовать переносу 6-ти первых столбцов левой части матрицы H_f, не менее чем на $(2n_A – n_0)R$ позиций вправо.

Результирующая проверочная матрица H_B для блокового кода принимает для рассматриваемого примера вид

$$H_B = \left(\begin{array}{ccccccccccccc:c}
1 & & & & & & & 1 & 0 & 1 & 0 & 0 & 1 & & \\
1 & 1 & & & & & & & 1 & 0 & 1 & 0 & 0 & & \\
0 & 1 & 1 & & & & & & & 1 & 0 & 1 & 0 & & \\
0 & 0 & 1 & 1 & & & & & & & 1 & 0 & 1 & & \\
1 & 0 & 0 & 1 & 1 & & & & & 0 & & 1 & 0 & & \\
0 & 1 & 0 & 0 & 1 & 1 & & & & & & & 1 & & \\
1 & 0 & 1 & 0 & 0 & 1 & 1 & & & & & & & : & I_{13} \\
 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & & & & & & & \\
 & & 1 & 0 & 1 & 0 & 0 & 1 & 1 & & & & & & \\
 & & & 1 & 0 & 1 & 0 & 0 & 1 & 1 & & & & & \\
 & & & & 1 & 0 & 1 & 0 & 0 & 1 & 1 & & & & \\
 & 0 & & & & 1 & 0 & 1 & 0 & 0 & 1 & 1 & & & \\
 & & & & & & 1 & 0 & 1 & 0 & 0 & 1 & 1 & &
\end{array}\right). \qquad (1.7)$$

где правая верхняя треугольная часть H_B – перемещенная левая часть матрицы (1.6). Но это значит, что при любых n_A и R все различные между собой индексы символов левой части (1.6) переносятся в матрицу H_B с увеличением номеров на одинаковую величину $(2n_\text{A}–n_0)R$ так, что даже наименьший индекс с номером информационного символа $(n_0–n_\text{A})R$ получает в блоковом коде значение

$$N = (n_0 - n_A)R + (2n_A - n_0)R = n_A R\ .$$

В рассматриваемом примере $N = 7$ и, значит, все новые номера ошибок в блоковом коде по сравнению со свёрточными имеющие значения не менее N, также различны между собой, что обеспечивает ортогональность проверок относительно символа i_0 и в коде, определяемом матрицей H_B. Если регистр на рис. 1.2б удлинить, то ясно, что код будет по-прежнему самоортогональным, но в проверочных уравнениях не будет ошибок с номерами $n_\text{A}R$ и, возможно, $n_\text{A}R$+1, … и т.д. Ясно, что аналогично случаю свёрточного кода, при этом сохраняется ортогональность проверок и относительно всех прочих информационных символов блока.

Таким образом, все множество свёрточных кодов класса СОК [19–24] при любых значениях R может использоваться для построения квазициклических блоковых кодов этого же класса.

Эта возможность была реализована в процессе разработки различных декодеров, обсуждаемых далее в главах о кодовых конструкциях и о характеристиках МПД алгоритмов.

Отметим также, что возможно и используемое далее более компактное описание блоковых и свёрточных СОК. Из вида матриц (1.4) и (1.6) следует, что первый столбец в H содержит единицы в строках с номерами, совпадающими с номерами тех ячеек кодера, которые соединены с полусумматором. Последующие столбцы этих матриц образуются сдвигом предыдущих k_0 столбцов на $(n_0–k_0)$ позиций вниз. Но тогда указание связей в кодере полностью определяет код. Таким образом, порождающий полином, задаваемый перечислением его степеней с ненулевыми коэффициентами: $P = (0, 1, 4, 6)$ – для рассматривавшегося примера определяет свёрточный и блоковый коды, причем длина блокового кода должна быть не менее 26 (в общем случае $2n_A–n_0$), что необходимо для сохранения самоортогональности блокового кода.

Разумеется, полиномы известных самоортогональных блоковых кодов [14] могут быть, наоборот, использованы в свёрточных кодах, причем длина кодового ограничения свёрточного кода n_A будет не больше, чем длина n исходного квазициклического СОК. Ясно, что в этом случае сохранение самоортогональности свёрточного кода следует из того, что его система проверок получается из системы проверок блокового кода просто вычеркиванием части ошибок из исходных проверочных уравнений.

1.3. Каналы связи

Существуют достаточно большие различия в закономерностях возникновения ошибок в тех или иных каналах связи. Поэтому в постановке задачи уменьшения числа ошибочно декодированных сообщений существенную роль играет модель канала, выбранная для описания процесса формирования потока ошибок. При анализе работы многих алгоритмов предполагается случайный характер появления ошибок канала, когда с вероятностью p_0 происходит искажение очередного передаваемого символа независимо от других символов сообщения. Графиче-

ское представление модели такого двоичного симметричного канала без памяти (ДСК) дано на рис. 1.3. Он достаточно хорошо соответствует многим высокоскоростным высокочастотным каналам спутниковой и космической связи [13, 25], что придает особенную ценность результатам, полученным в этой хорошо изученной теорией области.

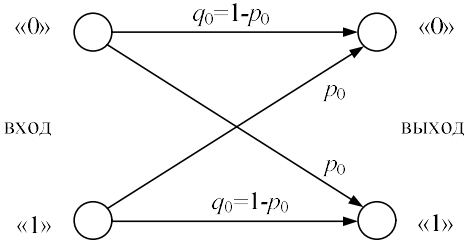


Рис. 1.3. Модель двоичного симметричного канала, $M = 2$, «жесткий» модем

Можно ожидать, что коды и алгоритмы их декодирования, обеспечивающие хорошие результаты в каналах с независимыми ошибками, позволяют достичь вполне приемлемых характеристик как составные части алгоритмов и для некоторых каналов с более сложным характером ошибок. Поэтому излагаемые ниже результаты относятся, в основном, к каналам, в которых действует аддитивный белый гауссовский шум (АБГШ), воздействующий на информацию, передаваемую, например, по спутниковым каналам связи. Это позволяет считать, что рассмотренные далее алгоритмы будут полезны и для исправления ошибок в некоторых других каналах связи.

В канале с АБГШ возможно не только использование «жестких» модемов, принимающих решение «0» или «1» о принятых символах, которые и образуют цифровой канал без памяти типа ДСК. Можно потребовать, чтобы модем был «мягким», т.е. принимал не только двоичные решения, но и оценивал их надежность. При этом выходной сигнал уже будет квантоваться на $M = 4$, $M = 8$ или $M = 16$ уровней, а решения модема становятся, например, последовательностями из двух, трех или четырех битов, как показано на рис. 1.4 для $M = 4$. Использование «мягких»

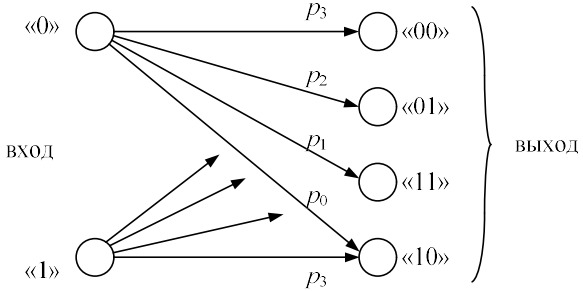


Рис. 1.4. Модель двоичного симметричного гауссовского канала с квантованием выходного сигнала на $M = 4$ уровня, «мягкий» модем

решений модема для декодеров оказывается чрезвычайно полезной возможностью, поскольку при этом повышается пропускная способность канала связи [1, 26]. Это, в свою очередь, создаёт возможность декодировать принятые цифровые потоки более эффективно по сравнению с обычным «жёстким» модемом, если алгоритмы коррекции ошибок предусматривают удобный способ учёта надёжности принимаемого двоичного потока. Напомним, что, например, переход к $M = 8$ в двоичном канале с АБГШ позволяет обеспечить с помощью декодирования по алгоритму Витерби (АВ) [1, 25, 31] высокую эффективность кодирования при уровне шума, примерно на 2 дБ более высоком по сравнению с «жёстким» модемом, когда $M = 2$. Именно эти цифры резкого увеличения энергетической эффективности фактически при сохранении той же сложности АВ и создают условия для широкого использования мягких модемов в системах высокоэффективной цифровой связи.

Третий тип каналов, которые будут рассматриваться, образуется, например, на базе q ортогональных сигналов в тракте с АБГШ. Модель данного канала для $q = 4$ представлена на рис. 1.5. В этом случае при передаче каждого q-ичного символа независимо от других с вероятностью $(1–p_0)$ происходит его правильное определение на приемной стороне и с вероятностью $p_0/(q–1)$ принимается то или иное ошибочное решение о его значении. Все ошибочные решения в этом случае оказываются ес-

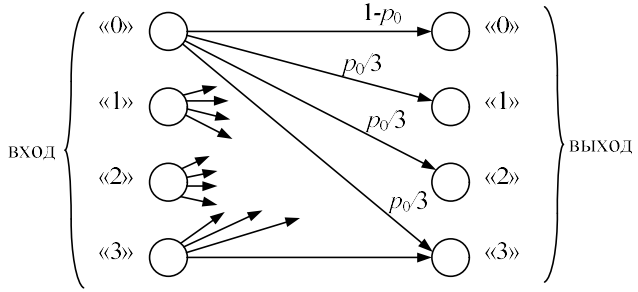


Рис. 1.5. Модель q-ичного симметричного канала, $q = 4$, QCK4

тественным образом равновероятны. Такие каналы мы будем в дальнейшем называть q-ичными симметричными и сокращенно обозначать QCKq, например, QCK4.

Симметричный канал с независимыми стираниями при любом основании q представлен на рис. 1.6. В этом случае оказывается, что символ может быть или принят правильно с вероятностью $q_s = 1–p_s$, или стёрт с вероятностью p_s. В целом ряде реальных систем возможность представить канал как стирающий позволяет существенно упростить процесс декодирования с очень высокой достоверностью.

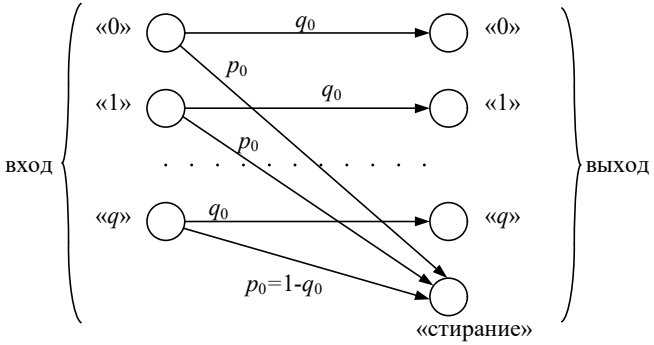


Рис. 1.6. Модель q-ичного симметричного стирающего канала, СтСКq

1.4. Многопозиционные системы сигналов

При использовании высокоэнергетичных сигналов и при наличии жестких требований к ширине полосы используемых частот достижение хороших значений энергетической эффективности кодирования возможно в случае совместного применения многопозиционных систем модуляции и кодирования [13, 26]. В этом случае возможно значительное уменьшение ширины полосы используемых частот сигнала по сравнению с обычной двоичной передачей, несмотря на увеличение объёма двоичного потока за счёт избыточных символов кода.

Рассмотрим некоторые принципы установления соответствия двоичных кодовых векторов и сложной системы сигналов на примере амплитудно-фазовой модуляции АФМ16, где расположение сигнальных точек в системе АМФ16 показано на рис. 1.7.

Двоичные пары битов на горизонталях и вертикалях дают представление об одном из вариантов соответствия между сигнальными точками и четверками битов, которые поступают в модем передатчика от кодера, а затем приходят из демодулятора в декодер приемника. Существенным для обеспечения достаточно хорошего согласования систем модуляции и кодирования является то, что для каждого данного сигнала соседние с ним по горизонтали и вертикали сигналы отличаются только в одном

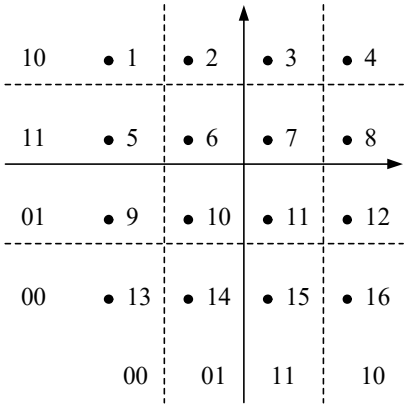


Рис. 1.7. Двумерная система сигналов для АФМ16

бите, а те, которые находятся на диагонали – в двух битах. Такое установление соответствия называется кодированием двумерным кодом Грея [13]. На самом деле можно проверить, что свойство увеличения веса Хемминга разности двоичных представлений сигнальных точек имеет место при удалении от любого исходного сигнала не только на 1, но и на 2 позиции. Это улучшает характеристики кодирования в модемах со сложными системами сигналов.

Аналогичные свойства могут быть справедливы и при росте числа сигнальных точек в рамках прямоугольной системы сигналов на плоскости или в пространствах большей размерности.

Таким же образом организуется соответствие между сигналами и двоичным их представлением в случае многопозиционной круговой системы сигналов, например, фазовой манипуляции вида ФМ2^m. Легко видеть, что в случае ФМ2^m также возможен рост веса Хемминга для разности двоичных представлений между всеми соседними или удаленными друг от друга на две позиции сигнальными точками (рис. 1.8). Эти свойства систем модуляции можно активно использовать при совместном применении эффективных кодов и любых сколько угодно сложных систем многопозиционных сигналов.

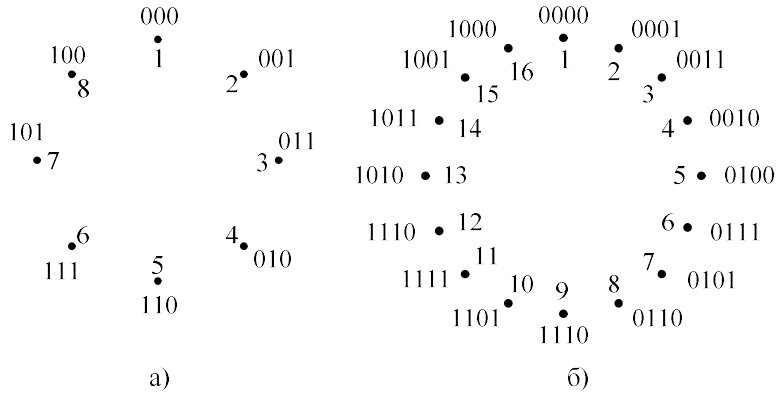


Рис. 1.8. Соответствие двоичных последовательностей сигнальным точкам систем ФМ8 и ФМ16 при использовании кода Грея

1.5. Алгоритмы декодирования корректирующих кодов

Среди взаимосвязанных задач поиска хороших корректирующих кодов и изучения их свойств, построения кодовых границ, анализа моделей каналов и других полезных для техники связи вопросов выделяется главная проблема разработки эффективных алгоритмов декодирования различных кодов. Ее решение непосредственно определяет как степень эффективности использования весьма дорогих каналов связи, так и затраты на создание кодеров и декодеров, реализующих эти алгоритмы. Ниже кратко охарактеризована сложившаяся к настоящему времени ситуация в технике декодирования. Ограничимся в анализе только системами передачи данных без обратной связи от приемника к передатчику, каналами с АБГШ и линейными кодами, которые существенно облегчают реализацию декодеров.

Развитие основополагающих идей В.В. Котельникова [27] и К. Шеннона [28], показавших специалистам в области связи, на каких путях можно обеспечить повышение качества передачи без увеличения энергетики сигнала, позволило довольно быстро пройти непростой путь от первых простейших кодов до важнейших алгебраических кодовых конструкций типа блоковых кодов Боуза-Чоудхури-Хоквингема (БЧХ) [29, 30]. С ними наступил период конструктивного развития теории помехоустойчивого кодирования, в которой сначала были доказаны интереснейшие теоремы существования, и лишь потом стали появляться результаты, которые можно было считать в той или иной мере практическими, прикладными.

Следующим важным этапом развития теории и техники кодирования стало появление пороговых декодеров (ПД) известнейшего американского специалиста Дж. Месси[4]. Пороговые (мажоритарные) методы были абсолютно справедливо оценены как важнейшие для своего времени практически применимые методы декодирования. Однако для излагаемых далее в этой книге подходов не менее важно отметить то обстоятельство, что появление ПД было связано с совершенно новыми конструктивными методами построения кодов и оценки их характеристик. К сожалению, корректирующие возможности ПД оказались не-

достаточно высокими. Поэтому специалисты продолжили поиск новых подходов к реализации эффективных декодеров.

Наибольшее влияние на развитие техники помехоустойчивого кодирования на начальном этапе оказало открытие алгоритма декодирования Витерби (АВ) для свёрточных кодов [25, 31]. Полученные даже для коротких свёрточных кодов с длинами кодирующего регистра $K = 5 \div 7$ при кодовых скоростях $R = 1/3 \div 3/4$ уровни помехоустойчивости при больших шумах в канале сразу оказались столь внушительными, что АВ на многие годы, вообще говоря, достаточно обосновано, был признан наиболее подходящей процедурой для коррекции ошибок в космических и спутниковых каналах связи [1, 13, 26].

Чрезвычайно значимым этапом в развитии теории и техники кодирования стали также каскадные коды [32]. Они существенно облегчили решение задачи обеспечения высокой достоверности передачи цифровых данных при средних уровнях шума. Дальнейшее развитие этой тематики показало большую эффективность каскадных конструкций при использовании на внутренних ступенях в каскадных кодах свёрточных кодов с декодированием по алгоритму Витерби [1, 26, 33], а на внешних – кодов Рида-Соломона (РС). Интенсивное развитие различных каскадных процедур является основой и текущего прогресса в технике декодирования [1, 35, 75, 89, 92, 97, 103].

1.6. Эффективность декодирования

Как известно, при передаче данных по двоичному симметричному каналу существует такое значение пропускной способности канала, равное, например, для ДСК [7, 34]

$$C = 1 + p_0 \log_2 p_0 + (1 - p_0) \log_2 (1 - p_0), \qquad (1.8)$$

где p_0 – вероятность ошибки в ДСК, что при выполнении условия $R < C$ существует такой двоичный линейный блоковый код длины n, что вероятность ошибки декодирования блока $P_B(e)$ может быть не хуже, чем

$$P_B(e) = ae^{-\alpha_B n}, \qquad (1.9)$$

где α_B – положительный параметр, зависящий от R и C, называемый функцией надежности, a – некоторая константа. Анало-

гичный результат имеет место и для свёрточных кодов, с несколько другой зависимостью α_C от R и C.

В случае «мягкого» приема двоичных символов по каналу с аддитивным белым гауссовским шумом пропускная способность канала оказывается несколько выше, чем при «жестком» приёме в канале типа ДСК [1, 26]. Это обстоятельство активнейшим образом используется во многих системах связи для более эффективной передачи цифровых потоков именно с помощью «мягких» модемов.

Таким образом, существуют коды такие, что при $R < C$ вероятность ошибки их декодирования при использовании достаточно эффективных методов будет с ростом длины кода n стремиться к нулю. К сожалению, абсолютное большинство доступных технике методов декодирования существенно менее эффективно, поскольку они не полностью реализуют потенциальные возможности применяемых кодов, которые к тому же имеют характеристики гораздо более скромные, чем лучшие из возможных кодов достаточно большой длины.

В связи с этим при сопоставлении различных методов коррекции ошибок важно иметь практически удобные критерии эффективности применения кодирования.

При проектировании конкретных систем связи всегда полезно оценивать условия, в которых будут работать те или иные системы и узлы коммуникационного комплекса. Например, при вариации такого важного параметра, как кодовая скорость R, можно выбрать такую степень расширения полосы частот $b = 1/R$ при кодировании, которая позволит реализовать систему помехоустойчивого кодирования с умеренной сложностью аппаратуры декодирования принятых сообщений на приёмной стороне.

Кроме того, всегда полезно знать величину конкретного отношения битовой энергетики сигнала к спектральной плотности мощности шума в канале связи E_b/N_0 для проектируемой системы связи. Это позволяет учитывать, как далеко отстоит создаваемая система связи по выбранным параметрам системы кодирования от потенциальных границ, определяемых основным теоретическим ограничением $R < C$. Поэтому при создании сис-

тем кодирования после выбора того конкретного уровня достоверности, который будет обеспечивать создаваемая система кодирования, полезно поместить точку, соответствующую выбранным параметрам R и E_b/N_0 на представленный на рис. 1.9 график для предельных соотношений R и E_b/N_0 [1]. В качестве примера на график помещена также точка А, соответствующая декодеру Витерби с $K = 7$, для которого $R = 1/2$ и $E_b/N_0 = 4{,}5$ дБ при выбранной типичной для него вероятности ошибки декодирования на бит $P_b(e) = 10^{-5}$.

Как видно из представленных на рис. 1.9 графиков предельно возможной энергетики гауссовского канала для «жёсткого» и «мягкого» модемов, разница по этому главному для теории кодирования параметру близка при $R = 1/2$ к 1,6 дБ. Особенно существенно для многих приложений, что с ростом кодовой скорости R теоретическая граница для предельной энергетики E_b/N_0 перемещается вверх, что является серьёзным ограничением в

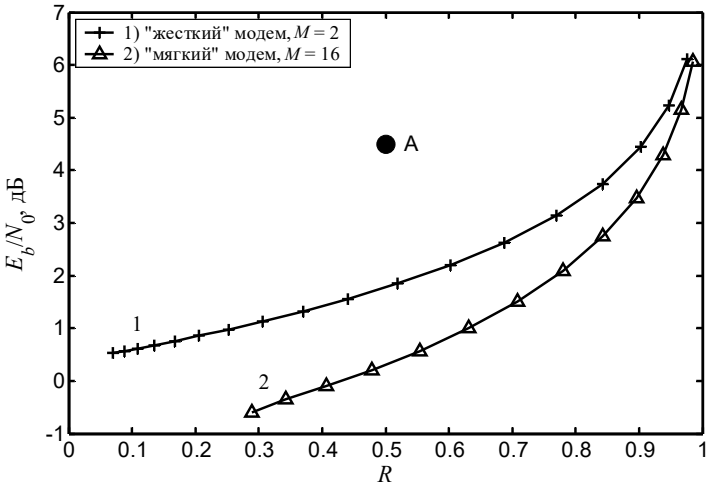


Рис. 1.9. Зависимость минимально возможного отношения битовой энергетики сигнала к спектральной плотности мощности шума в двоичном гауссовском канале E_b/N_0 от выбора кодовой скорости R для «мягкого» и «жёсткого» модемов

выборе уровня избыточности кодирования. Во многих системах связи нет чрезвычайно жёстких требований к минимизации расширения спектра сигнала из-за введения кодирования. Поэтому обычно можно ориентироваться на рекомендации, согласно которым желательно выбирать кодовую скорость R не большую, чем $R_L = 0{,}8$. Достаточно типичными значениями кодовой скорости R можно считать $R = 3/4$ и $R = 1/2$, а при необходимости получения рекордно малых значений E_b/N_0, в частности, в системах дальней космической связи часто рекомендуют $R = 1/4$ и даже более низкие её значения.

Как известно, в пределе при $R \to 0$ теоретически возможно достижение уровня энергетики порядка $E_b/N_0 = -1{,}6$ дБ [1]. Для конкретных конечных значений R можно указать, что при $R = 1/2$ минимальный возможный из условия $R = C$ уровень $E_b/N_0 = 0{,}2$ дБ для мягкого модема, а при $R = 4/5$ $E_b/N_0 = 2{,}1$ дБ.

Таким образом, допустимый уровень расширения спектра сигнала и требуемый уровень энергетики сигнала при использовании кодирования и определяют возможности и конкретный выбор кодовой скорости R, при которой будут работать проектируемые цифровые системы связи.

Другой широко используемый критерий эффективности применения кодирования в технике связи, называемый энергетическим выигрышем кодирования (ЭВК), определяет величину снижения энергетики сигнала, т.е. отношения энергии передачи, приходящейся на 1 бит передаваемых данных E_b, к спектральной плотности мощности шума N_0 ($a = E_b/N_0$) в случае использования кодирования по сравнению со случаем обычной передачи без использования кодов [26]. Из определения ЭВК следует, что это разностный критерий, определяемый из условий выбора заданной достоверности передачи без кодирования и требуемой для этого величины $a = E_b/N_0$, из которой затем вычитается или теоретически минимально достижимая величина a, определяемая, например, при условии $R = C$ из графика на рис. 1.9, или величина a, определяемая конкретным алгоритмом коррекции ошибок.

Оценить возможные значения ЭВК можно из графиков на рис. 1.10, где даны кривые зависимости максимально возмож-

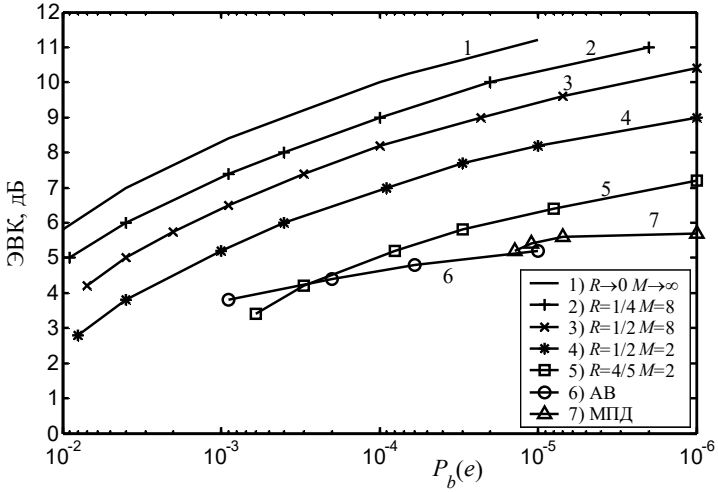


Рис. 1.10. Предельные значения ЭВК из условия $R < C$ в гауссовском канале для различных кодовых скоростей и уровней квантования сигналов в двоичном модеме

ного ЭВК от требуемой результирующей вероятности ошибки на бит $P_b(e)$ при двоичной фазовой модуляции ФМ2 без учета сложности реализации декодера и вносимой задержки, т.е. только при выполнении условия $R < C$. Для каждой кривой в названии указана кодовая скорость R и число уровней квантования M. При $M = 2$ предполагается использование «жесткого» модема, квантующего принятый сигнал на 2 уровня, а при $M = 8$ реализуется «мягкий» прием и обеспечивается более полное использование канала.

При переходе от $M = 2$ (случай «жесткого» модема, просто определяющего, какой символ пришел из канала) к «мягкому» модему с $M = 8$, который оценивает достоверность своих решений, для одного и того же кода нередко возможно получение дополнительного ЭВК порядка 2 дБ. При увеличении R, наоборот, предельные энергетические возможности кода даже при наилучшем декодировании заметно снижаются.

С ростом требований к достоверности необходимость использования кодирования также становится все более очевидной, так как достижимый с помощью кодов и хороших алгоритмов декодирования ЭВК, что хорошо видно из представленных на рис. 1.10 зависимостей, быстро растет. А это и значит, что ценность и обязательность применения кодирования действительно безусловны и в дальнейшем важность кодирования будет только расти.

Полезно также посмотреть, какие значения ЭВК обеспечивают конкретные коды и алгоритмы. Кривая «АВ» на рис. 1.10 показывает возможности алгоритма Витерби для стандартного свёрточного кода с длиной кодирующего информационного регистра $K = 7$ и $R = 1/2$, который широко используются и в настоящее время. Этот код при использовании АВ обеспечивает ЭВК порядка 5,1 дБ при $P_b(e) = 10^{-5}$, что можно признать значимым достижением для 70-х годов прошлого века, когда эти декодеры были разработаны. Но заметим, что около 2 дБ от этого уровня ЭВК, как отмечалось выше, получены при декодировании за счёт «мягкого» модема.

Кривая «МПД» на обсуждаемом рис. 1.10 представляет возможности декодирования на основе очень простой версии многопорогового алгоритма, который и будет основным предметом изучения в последующих главах этой книги. Весьма существенно, что этот график соответствует работе алгоритма МПД с «жёстким» модемом, т.е. при передаче по ДСК при $M = 2$, и обеспечивает для $R = 1/2$ ЭВК 5,6 дБ для $P_b(e) = 10^{-5}$. Этот пример показывает, насколько эффективно применение очень длинных кодов, используемых в МПД, поскольку с ними даже при «жёстком» модеме можно достаточно простыми методами получать более высокие характеристики, чем у «мягкого» АВ.

Как видно из сопоставления графиков для предельных возможностей и реальных характеристик некоторых кодов, до границы $R = C$, достижение которой допускает теория, еще очень далеко. Способы достижения больших уровней ЭВК по возможности более простыми методами и будут рассмотрены в последующих главах предлагаемой читателям книги.

Отметим также, что сопоставление эффективности кодирования возможно на основе ещё одного естественного критерия, который можно так и называть эффективностью или, если удобно, просто «к.п.д.», поскольку его смысл полностью соответствует обычному параметру к.п.д. для различных физических процессов.

Понятие «к.п.д. использования канала» непосредственно связано с предельными значениями $a = E_b/N_0$, которые соответствуют равенству $R = C$. При вычислении к.п.д. следует взять отношение a для этого равенства и определить конкретное рабочее значение a_d для обсуждаемого алгоритма декодирования. Их разность и есть мера эффективности использования канала в децибелах. А если преобразовать эту разность к процентам, то это и будет искомый к.п.д. – полный аналог для к.п.д. многих физических процессов.

Например, пусть равенству $R = C$ соответствует конкретное значение a_0, а анализируемый алгоритм коррекции ошибок при этой же кодовой скорости R и заданном уровне достоверности декодирования работает при уровне a_d, на 3 дБ более высоком, чем a_0. Вот эти 3 дБ и есть та величина, которая непосредственно указывает на отличие возможностей выбранного декодера от предельно допустимых теоретических значений a_0. Но 3 дБ – это 2 раза по энергетике. Именно во столько раз энергетика передачи для этого декодера больше, чем это возможно по теории. Но это и означает, что к.п.д. использования канала данным декодером по энергетике составляет 50%. А если найдётся декодер, который будет работать с превышением энергетики от предельно возможного её уровня только на 0,5 дБ, т.е. в 1,122 раз, то легко найти, что его к.п.д. равен 89%. Поэтому мы будем также пользоваться и этим весьма простым и удобным способом оценки возможностей кодирования.

При анализе характеристик алгоритмов декодирования различных кодов полезно знать также предельные для малого шума величины ЭВК для этих методов. Оказывается, что это соотношение для канала с АБГШ и двоичного сообщения просто равно произведению Rd при приеме в целом, т.е. для числа уровней квантования $M \to \infty$, что соответствует уровню ЭВК, равному

$$G_{\infty} = 10\lg[Rd] \text{ дБ} \qquad (1.10)$$

по традиционной логарифмической шкале [26].

Для $M = 2$, т.е. в двоичном симметричном канале

$$G_2 = 10\lg[R(t_0 + 1)] \text{ дБ}, \qquad (1.11)$$

где t_0 – максимальное целое, меньшее, чем $d/2$, d – минимальное кодовое расстояние применяемых кодов. Из сопоставления (1.10) и (1.11) видно, что в асимптотике при улучшении отношения сигнал/шум прием в целом обеспечивает на 3 дБ большее значение ЭВК, чем использование простого двоичного модема, если d также достаточно велико. Однако при реальных небольших отношениях сигнал/шум и умеренных значениях d разница обычно близка к 2 дБ [25, 26].

1.7. Длины используемых кодов

Как хорошо известно, получение больших уровней помехоустойчивости всегда связано с применением довольно длинных кодов. Это неудивительно, поскольку только при весьма больших значениях минимального кодового расстояния d для блоковых или свободного расстояния d_f для свёрточных кодов возможно достаточно далеко разнести друг от друга разрешённые кодовые комбинации, что и будет обеспечивать их правильное в конце концов определение хорошим декодером на приёмной стороне линии связи. На рис. 1.11 представлены нижние оценки средней вероятности ошибки декодирования блоковых кодов $P_B(e)$ в ДСК при $R = 1/2$ и разных длинах n этих кодов. Как видно из представленных кривых, для получения действительно небольших вероятностей ошибки декодирования в ДСК без памяти следует выбирать весьма высокие значения n. В противном случае достижение хорошей достоверности передачи при вероятности ошибки в ДСК $p_0 \lesssim 0{,}11$, т.е. когда $R \lesssim C$ в этом примере канала ДСК, окажется невозможным.

Как следует из представленных графиков, даже при $n \sim 10000$ битов вероятности ошибки канала p_0, при которых гипотетический наилучший переборный декодер мог бы обеспечить достаточно малые вероятности ошибки принятия решений относительно вида переданного блока, меньше, чем $p_0 = 0{,}1$.

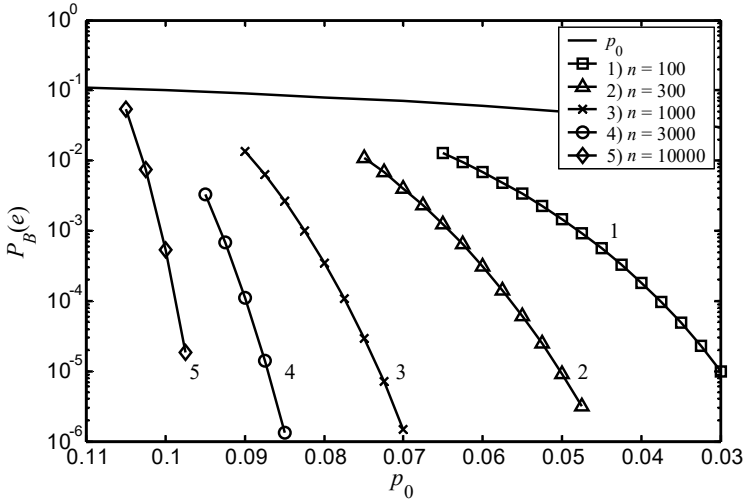


Рис. 1.11. Нижние оценки вероятности ошибки на блок $P_B(e)$ в ДСК без памяти для кодов с различной длиной n при $R = 1/2$

А это примерно ещё на 0,4 дБ меньше по уровню шума канала, чем разрешает граница $R = C$. Таким образом, даже представленные нижние оценки для вероятности ошибки декодера, полученные из известных границ сферической упаковки, показывают, что очень эффективные системы кодирования должны использовать и весьма длинные коды с $n \sim 10^5 \div 10^7$. Это обстоятельство дополнительно подчёркивает, что применяемые в технике связи алгоритмы коррекции ошибок должны быть максимально упрощены, поскольку только в этом случае окажется возможным действительно достаточно быстро и эффективно декодировать очень длинные коды.

1.8. Основные требования к новым алгоритмам

При наличии значительных достижений техники помехоустойчивого кодирования в этой важнейшей сфере исследований в области обработки цифровых потоков в условиях большого шума канала существует много проблем. Одной из наиболее

серьезных нерешенных задач по-прежнему является недостаточно высокая эффективность простых методов коррекции ошибок и неоправданно большая сложность тех методов, которые могут обеспечить высокие значения энергетического выигрыша кодирования.

Хорошей иллюстрацией того, сколь высоких характеристик кодирования и последующего декодирования можно добиться, если не обращать сколько-нибудь значительного внимания на сложность реализуемых алгоритмов, являются турбо коды [35] и многие другие методы подобного типа [71, 72, 73, 74, 75]. Они позволяют достичь достаточно высокой достоверности декодирования при отношениях E_b/N_0, в ряде случаев лишь на десятые доли децибела превышающих уровень $R = C$. Но эти итеративные методы, появившиеся на 20 с лишним лет позже многопороговых алгоритмов, которые далее рассматриваются в этой книге, нередко оказываются существенно более сложными или медленными, чем МПД декодеры.

Исходя из необходимости изучения применения высокоэффективных кодов при действительно минимальной сложности их декодирования, а также с учётом возможностей мажоритарных схем, рассмотренных в этой главе, укажем основные причины выбора для глубоких разносторонних исследований именно мажоритарных процедур:

– способность мажоритарных методов исправлять большое число ошибок за пределами гарантированной корректирующей способности;

– крайне незначительная сложность пороговых процедур декодирования;

– способность разработанных МПД алгоритмов достигать оптимальных решений при весьма высоких уровнях шума в канале связи;

– предельная легкость реализации МПД даже для очень длинных кодов, когда только и возможно достижение максимально допустимых значений эффективности кодирования.

Описанию возможностей и анализу характеристик этих перспективных алгоритмов и посвящена данная книга.

ГЛАВА 2. ПРИНЦИП РОСТА ПРАВДОПОДОБИЯ РЕШЕНИЯ МНОГОПОРОГОВОГО ДЕКОДЕРА

2.1. Эффективность и сложность: выбор направления исследований

Развитие высокоэффективных методов помехоустойчивого кодирования предполагает использование процедур декодирования, мало отличающихся от оптимальных или просто оптимальных по меньшей мере в некоторых наиболее ответственных системах. К ним относятся, например, декодеры, реализующие алгоритм Витерби [25, 31], а также внутренние декодеры тех каскадных схем кодирования [26, 33], которые обеспечивают большую эффективность.

Поскольку непосредственное использование метода оптимального (по максимуму правдоподобия) декодирования очень ограничено из-за сложности реализации, пропорциональной q^k или q^{n-k}, где q – основание кода, k – информационная часть кодового слова, n – его длина, необходимо строить процедуры декодирования, которые оптимальными не являются, но существенно проще оптимальных и мало отличаются от них по эффективности.

Среди самых простых способов исправления ошибок, которые пытались улучшить в 70-х годах прошлого века, можно указать рассматривавшиеся многими авторами методы повторного декодирования принятых сообщений. Но практически все они оказались малоэффективными вследствие сильного группирования ошибок на выходе соответствующих декодеров. Пример такой схемы с пороговым декодером (ПД) [76] для свёрточного кода с кодовой скоростью $R = 1/2$ и минимальным кодовым расстоянием $d = 5$ приведен на рис. 2.1.

Малая эффективность подобной схемы декодирования была следствием сильного группирования, т.е. размножения ошибок в пороговом декодере. В самом деле, если при некотором уровне шума в канале типа ДСК с независимыми ошибками в какой-то момент ПД принял неправильное решение об очередном информационном символе, то обычно на выходе этого ПД далее появлялся очень плотный пакет ошибок. Например, пусть с вы-

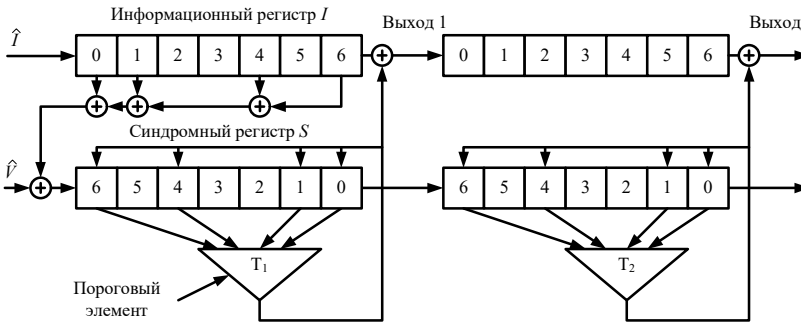


Рис. 2.1. Пример схемы повторного декодирования на основе порогового декодера свёрточного кода

хода первого ПД на рис. 2.1 на вход второго поступила немного улучшенная при первой попытке декодирования последовательность. Тогда, если ошибок в некоторой части информационной последовательности после первого ПД нет, то второй декодер не нужен. Но при появлении на выходе первого ПД ошибки, которая обычно является началом типичного пакета ошибок этого ПД, оказывается, что второй декодер, точно повторяющий схему первого и настроенный на исправление только случайных ошибок, скорее всего, не исправит этот пакет. Следовательно, он не нужен и в этом случае.

Подчеркнём, что коды с малым уровнем размножения ошибок в ПД в те годы были совершенно неизвестны. Поэтому попытки решить проблему роста эффективности мажоритарных методов повторным применением коррекции принятого потока были в 70-х годах прекращены. Однако позже эта проблема была полностью решена методами, описанными в [1, 9, 57, 98]. Они будут достаточно полно рассмотрены в главе 3. В связи с этим приобретает большое значение рассмотренный ниже новый подход к реализации простейших, но, однако, чрезвычайно эффективных итеративных процедур исправления ошибок, который развивается с 1972 г. [10] и назван многопороговым декодированием (МПД) [1, 9, 10, 86, 87, 88, 89, 90, 91].

Одной из наиболее существенных причин того, что именно мажоритарные декодеры стали объектом многолетних исследо-

ваний и разработок с целью создания высокоэффективных и простых методов коррекции ошибок, явилось, во-первых, крайне малое число операций на пороговом элементе такого декодера, что должно было стать основой для очень небольшого объёма вычислений в разрабатываемых алгоритмах. При этом дополнительно оказывается, что сама процедура этих вычислений позволяет применять множество технологически удобных способов для ускорения решений порогового элемента о декодируемых символах. В процессе разработки МПД эти предположения полностью подтвердились.

Второй же важнейшей причиной выбора мажоритарного алгоритма как главного объекта исследований явилась уникальная способность мажоритарных процедур исправлять во многих случаях гораздо большее число ошибок, чем это гарантируется минимальным кодовым расстоянием d используемого кода. И если многие технологические достоинства мажоритарного элемента для разных вариантов реализации очевидны, второе обстоятельство, повлиявшее на выбор именно мажоритарных методов, необходимо обсудить немного более подробно. На рис. 2.2 представлены экспериментальные результаты двукратного повторного декодирования в ДСК блокового самоортогонального кода с $R = 1/2$, $d = 11$ и $n = 1000$. По оси абсцисс отложено общее число ошибок канала в кодовом блоке перед его декодированием, а по оси ординат – доля правильно декодированных блоков. Нижняя кривая – для первой попытки коррекции принятого кодового блока. А верхняя – для второй коррекции этого же блока. Как следует из графиков, при 30 ошибках канала в блоке около 3/4 таких закодированных сообщений полностью очищаются пороговым декодером от ошибок. Заметим, что гарантированно ПД исправляет при $d = 11$ только 5 ошибок в блоке. Более того, даже при общем числе ошибок канала порядка 40 доля правильно декодированных блоков после первой попытки более четверти. Далее видно, что при числе ошибок в блоке порядка 50 и более пороговый алгоритм почти уже совсем не работает. Но ведь и при 40 ошибках ПД в заметной доле принятых блоков восстанавливает истинное сообщение, исправляя при этом в 8 раз большее число ошибок, чем это гарантировано

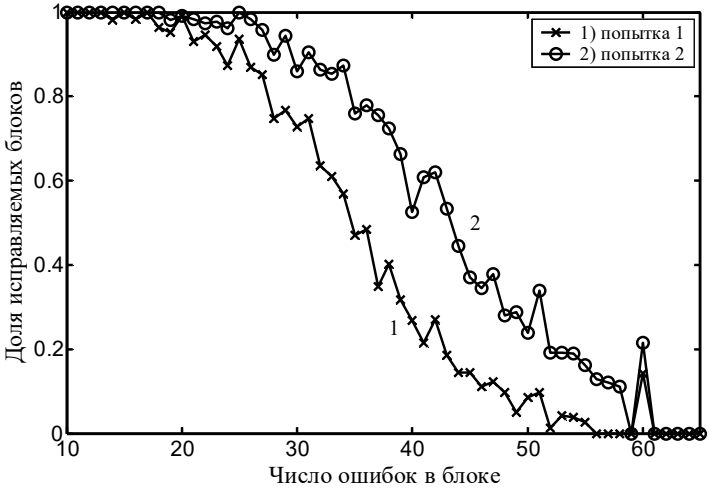


Рис. 2.2. Результаты моделирования повторного порогового декодирования СОК с $d = 11$, $n = 1000$ и $R = 1/2$

минимальным кодовым расстоянием $d = 11$! Более того, в рассматриваемом коде после второй попытки исправления ошибок число правильно декодированных блоков для исходных 40 ошибок увеличивается примерно вдвое и становится близким к половине. Отметим также, что и при второй попытке коррекции ошибок пороговый декодер снова пытается исправлять ошибки за пределами гарантированной корректирующей способности. Значит, и повторное декодирование тоже полезно.

И хотя третья попытка декодирования для рассматриваемого кода практически ничего уже не даёт, именно очень значительная «сверхнормативная» эффективность и первой, и второй попытки обычного порогового декодирования указывает на актуальность глубокой проработки потенциальных возможностей и исследования конкретных характеристик именно мажоритарных алгоритмов.

В этой главе будут рассмотрены основные принципы, положенные в основу высокоэффективных итеративных МПД алгоритмов. Сначала будут представлены на качественном уровне

простые по своему существу идеи, положенные в основу алгоритма МПД и его свойства строго приближаться к оптимальному переборному (!) решению. Затем будут уже более формально рассмотрены алгоритмы этого типа для классического двоичного симметричного канала, и для систематических кодов будет строго доказано действительно уникальнейшая способность стремления решений МПД алгоритмов к решению оптимального декодера. После этого будет рассмотрен способ реализации МПД процедур для несистематических кодов, а также для двоичного гауссовского канала, который образуется в результате использования «мягкого» модема. Далее принципы МПД изложены для недвоичного симметричного канала и для каналов со стираниями. Последними будут рассмотрены подходы к реализации идей сходимости МПД алгоритма для каналов с неравномерной энергетикой символов, коды с неравной защитой символов, а также применение МПД для систем сжатия данных. Различные оценки и границы эффективности, реальные возможности МПД декодеров и другие важные прикладные вопросы будут рассмотрены в последующих главах книги.

2.2. Принцип глобальной оптимизации функционала

Развитие методов декодирования помехоустойчивых кодов в течение длительного времени удивительным образом никак не было связано с методами решения задачи оптимизации функционала от многих дискретных переменных. Тем не менее, декодирование, т.е. поиск единственного кодового слова из экспоненциально большого числа возможных сообщений, совершенно естественно было бы рассматривать именно с таких позиций. Однако абсолютное большинство разрабатывавшихся ранее алгоритмов декодирования никак не использовало для поиска наилучших решений декодера хорошо известные разнообразные мощные итеративные оптимизационные процедуры, которые вполне можно было бы применить к поиску кодовых слов, находящихся на минимально возможном расстоянии от принятого сообщения. Заметим, что широко применяемый в технике связи алгоритм Витерби, используемый для декодирования по максимуму правдоподобия коротких свёрточных кодов, также не от-

носится к классу оптимизационных процедур, поскольку он непосредственно ищет оптимальное решение на основе очень удобного в реализации метода полного перебора.

Вместе с тем некоторые алгоритмы декодирования, в частности, пороговые декодеры, относящиеся к простейшим методам коррекции ошибок, почти уже обладают именно теми свойствами, которые необходимы для реализации полноценных эффективных и одновременно исключительно простых итеративных процедур декодирования, которые действительно могут быть методами поиска глобального экстремума функционала от очень большого числа переменных.

Для подтверждения этого рассмотрим пример простейшей системы кодирования/порогового декодирования с кодовой скоростью $R = 1/2$ и минимальным кодовым расстоянием $d = 3$, показанный на рис. 2.3.

Как следует из вида кодера и простейшего мажоритарного декодера, исправляющего в этом простом примере одну ошибку, в состав этого декодера входит точная копия кодера, которая формирует свои оценки проверочных символов кода по принятым из канала, возможно, с ошибками информационным символам кода. Эти символы появляются в точке К декодера и затем, после сложения на полусумматоре с принятыми из канала проверочными символами $\hat{V}$, образуют символы вектора синдрома $\overline{S}$, который зависит только от вектора ошибок канала. Эти сим-

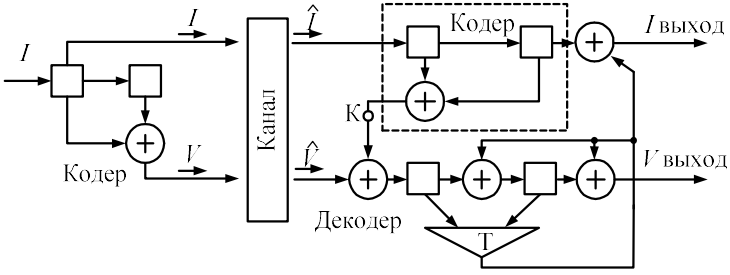


Рис. 2.3. Специальный вид системы кодирования, поясняющий новую интерпретацию вектора синдрома

волы и поступают потом на пороговый элемент декодера T из синдромного регистра, как это показано на рис. 2.3.

Уже сам вид ПД на представленной схеме кодирования/декодирования позволяет указать простой способ организации правильной процедуры оптимизации, т.е. поиска наилучшего возможного решения при декодировании. Укажем для этого на факт, который никогда не обсуждался для каких-либо линейных кодов ранее: в регистре синдрома декодера находится разность по проверочным символам между принятым с искажениями из канала вектором $\overline{Q} = (\hat{I}, \hat{V})$ и таким кодовым словом $\overline{A}_C$, информационные символы которого совпадают с принятой из канала информационной частью вектора $\overline{Q}$.

Значит, полная разница между кодовым словом – текущей гипотезой-решением декодера $\overline{A}_i$ о переданном кодовом слове и принятым зашумленным вектором $\overline{Q}$ будет в таком модифицированном декодере мажоритарного типа, где в ПД будет добавлен ещё всего лишь один новый вектор, который всегда должен соответствовать разности между принятым вектором $\overline{Q}$ и $\overline{A}_I$ – текущей гипотезой декодера по информационным символам. В таком декодере и будет содержаться текущее значение полной разности, и, следовательно, возможно измерение полного расстояния между текущим решением декодера, содержащимся в его информационном регистре, и принятым вектором. Это расстояние следует стараться уменьшить до минимально возможного, что и будет соответствовать решению оптимального декодера, которое, однако, обычно достигается переборными экспоненциально сложными методами.

Именно такой подход к проблеме высокоэффективного декодирования и является основой развиваемых с 1972 года специальных итеративных многопороговых декодеров (МПД) [9, 10], очень незначительно отличающихся от классических ПД, и таких же простых в реализации, как и их прототип.

Изменения, которые необходимо сделать в обычном ПД, чтобы преобразовать его в МПД, как следует из только что состоявшихся обсуждений принципа глобальной оптимизации,

состоят просто в том, что решения всех пороговых элементов об изменениях декодируемых символов сначала запоминаются в дополнительном разностном регистре D, первоначально, естественно, нулевом. Эти решения затем используются последующими пороговыми элементами декодера в качестве дополнительной проверки при дальнейшем уточнении значений декодируемых символов. Такой декодер измеряет полные расстояния между всё более новыми потенциальными решениями $\overline{A}_i$ и принятым вектором $\overline{Q}$. Он изменяет декодируемые символы так, что каждое новое решение такого МПД всегда ближе к принятому из канала вектору. Это позволяет во многих случаях практически полностью реализовать корректирующие возможности используемых кодов.

Декодер типа МПД для свёрточного СОК с $R = 1/2$, $d = 5$ и $n_A = 14$, рассматривавшегося ранее в качестве примера, представлен на рис. 2.4. Отметим ещё раз, что согласно правилу работы МПД первоначально в его разностном регистре D находятся только нули. Таким образом, на первой итерации коррекции ошибок МПД функционирует точно так же, как и обычный ПД.

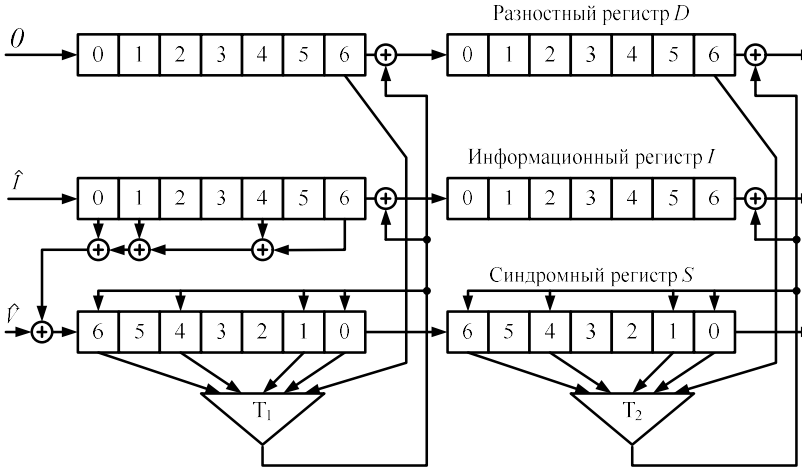


Рис. 2.4. Декодер типа МПД для свёрточного кода с $R = 1/2$, $n_A = 14$ и $d = 5$ при $I = 2$ итерациях

Только на последующих попытках декодирования МПД начинает реально учитывать содержимое соответствующих ячеек регистра *D*, в результате чего он и сохраняет свои свойства улучшения решений МПД при всех изменениях информационных символов сообщения.

Другие примеры конкретных схем МПД приведены в [1, 86, 100, 102].

Декодер после этого достаточно простого усовершенствования приобретает новые чрезвычайно полезные свойства [1, 9]. Решения МПД при каждом изменении декодируемых им информационных символов строго приближаются к решению оптимального декодера (ОД), обеспечивая во многих случаях реализацию этого процесса даже после нескольких десятков попыток коррекции кодового блока или потока символов свёрточного кода.

Подчеркнём, что используемые здесь и далее термины «стремление к решению ОД» или «приближение к решению ОД» означают всегда только то, что при изменении декодируемых символов МПД переходит к новому, возможно, промежуточному решению, которое всегда строго ближе к принятому из канала сообщению, чем предыдущее решение декодера. Это значит также, что новое решение декодера всегда строго более правдоподобно, чем предыдущее. А если будет достигнуто наиболее правдоподобное решение, то оно и будет оптимальным решением, т.е. решением ОД. Именно поэтому указанные термины удобны, отражают сущность процессов, происходящих в декодере, и будут использоваться в дальнейшем.

Заканчивая качественные наглядные описания свойств МПД, напомним, что для обеспечения высокой эффективности МПД при больших шумах канала необходимо выбирать только специальные коды с малым уровнем размножения ошибок. Этот принципиально важный для эффективного декодирования на базе алгоритмов МПД вопрос рассматривается в третьей главе.

2.3. Алгоритм многопорогового декодирования

Рассмотрев достаточно полно на качественном уровне основные идеи, положенные в основу многопороговых алгоритмов, обратимся к строгому формальному обоснованию их возможностей.

Пусть задан двоичный линейный систематический блоковый или свёрточный код со скоростью передачи $R = k/n$, где k – число информационных символов, n – длина кодовой комбинации.

При передаче по ДСК без памяти оптимальный декодер, минимизирующий среднюю вероятность ошибки декодирования, из множества возможных 2^k равновероятных кодовых слов $\{\overline{A}\}$ выбирает такой вектор $\widetilde{A}$, для которого расстояние Хэмминга $r = |\overline{Q} \oplus \widetilde{A}|$, где $\overline{Q}$ – принятое сообщение, $\overline{Q} = \overline{A} \oplus \overline{E}$, $\overline{A}$ – переданное кодовое слово, $\overline{E}$ – вектор шума канала, $\oplus$ – сложение по mod 2, было бы минимальным по всему множеству кодовых слов $\{\overline{A}\}$.

Будем для удобства доказательства последующих утверждений любой двоичный вектор $\overline{X}$ длины n представлять парой векторов $\overline{X}_I$ и $\overline{X}_V$ длины k и $(n–k)$ соответственно, относящихся к информационной и проверочным частям вектора:

$\overline{X} = (\overline{X}_I, \overline{X}_V)$.

Тогда, полагая, что проверочная матрица кода представлена в систематическом виде $H = (P^T : I)$, имеет место следующая лемма.

Лемма 2.1. Для любого кодового вектора $\overline{A}$ и принятого сообщения $\overline{Q}$ справедливо соотношение

$$\overline{A} \oplus \overline{Q} = (\overline{D}, H(\overline{Q}_I \oplus \overline{D}, \overline{Q}_V)), \tag{2.1}$$

где вектор $\overline{D}$ длины k определяется соотношением

$$\overline{A}_I = \overline{Q}_I \oplus \overline{D}. \tag{2.2}$$

Доказательство. В силу линейности кода

$$\overline{S} = H(\overline{Q}_I \oplus \overline{D}, \overline{Q}_V) = H(\overline{A}_I, \overline{A}_V \oplus \overline{A}_V \oplus \overline{Q}_V) =$$

$$= H\overline{A} \oplus H(\overline{0}_I, \overline{A}_V \oplus \overline{Q}_V),$$

где $\overline{0}_I$ – нулевое информационное слово.

Так как $H\overline{A} = 0$, поскольку $\overline{A}$ – кодовое слово, а $H(\overline{0}_I, \overline{A}_V \oplus \overline{Q}_V) = \overline{A}_V \oplus \overline{Q}_V$, так как $\overline{A}_V \oplus \overline{Q}_V$ умножается только на единичную подматрицу *I* матрицы *H,* то получаем, что вектор $\overline{S}$ равен

$$\overline{S} = \overline{A}_V \oplus \overline{Q}_V. \qquad (2.3)$$

Проводя в правой части (2.1) замены с учетом (2.2), находим, что

$$(\overline{D}, \overline{S}) = (\overline{D}, \overline{A}_V \oplus \overline{Q}_V) = (\overline{D} \oplus \overline{Q}_I \oplus \overline{Q}_I, \overline{A}_V \oplus \overline{Q}_V) = \overline{A} \oplus \overline{Q}.$$

Таким образом, вектор синдрома $\overline{S}$ действительно, как это и было представлено на рис. 2.2, есть разница по проверочным символам между пришедшим из канала частично искажённым сообщением и определённым выше кодовым словом.

Лемма доказана.

Ее содержание заключается в том, что разность $\overline{B} = \overline{Q} \oplus \overline{A}$ для любого принятого вектора $\overline{Q}$ и кодового слова $\overline{A}$ определяется парой векторов $(\overline{D}, \overline{S})$. Перебором всех возможных векторов $\overline{A}$ можно найти вектор $\widetilde{A}$, минимизирующий $|\overline{B}|$ и являющийся решением ОД. В силу определения при $\overline{D} = 0$ вектор $\overline{S}$ является обычным синдромом принятого сообщения $\overline{Q}$: $\overline{S} = H\overline{Q}$. Для простоты изложения будем в дальнейшем и при $\overline{D} \neq 0$ называть $\overline{S}$ синдромом, поскольку это обобщение естественно и не приводит в дальнейшем к каким-либо противоречиям. Отметим также, что при каждом изменении $\overline{A}$ нет необходимости заново вычислять все компоненты синдрома. Достаточно на каждом шаге изменения инвертировать только те компоненты $\overline{S}$, которые содержат нечетное число ошибок в изменяемых информационных символах. Однако переборные алгоритмы слишком сложны.

Поэтому рассмотрим алгоритм декодирования, который очень близок к пороговому методу исправления ошибок и в связи с этим весьма просто реализуем.

1. Пусть на первом подготовительном этапе декодер выполняет вычисление и запоминание вектора синдрома принятого сообщения $\overline{S}$. Затем начинается выполнение собственно процедуры декодирования.

2. Выбирается некоторый информационный символ i_j и для него вычисляется обычная сумма компонент синдрома s_{j_k}, содержащих в качестве слагаемых ошибку e_j в декодируемом символе i_j (т.е. находится сумма проверок $s_{j_k} \in \{S_j\}$, где $\{S_j\}$ – множество проверок относительно компоненты e_j, соответствующей символу i_j) и символа d_j (компонент вектора $\overline{D}$), также относящегося к декодируемому символу i_j:

$$L_j = \sum_{s_{j_k} \in \{S_j\}} s_{j_k} + d_j. \qquad (2.4)$$

Будем при этом полагать, что первоначально $\overline{D} = 0$, потому что перед началом операций декодирования в памяти декодера есть только принятый вектор $\overline{Q}$, так как декодер не имеет никаких других более предпочтительных гипотез о переданном сообщении.

Выберем порог T равным половине всех слагаемых в (2.4). Для СОК это число равно $T = d/2 = (J+1)/2$.

3. Пусть, наконец, все $J = d$–1 проверок, i_j и d_j инвертируются при $L_j > T$ и остаются неизменными при $L_j \le T$.

4. Выбирается очередной декодируемый информационный символ и декодер возвращается в п.2, если не принято решение о прекращении процедуры декодирования.

Предлагаемая процедура при первой попытке декодирования, пока все $d_j = 0$, совпадает с обычным алгоритмом для ПД. Будем в дальнейшем называть декодер, реализующий предлагаемый алгоритм, многопороговым декодером (МПД). При выполнении основных шагов декодирования 2÷4 все k информационных символов сообщения могут перебираться в любом порядке и, что составляет суть многопорогового метода, многократно,

до 5-ти, 20-ти и более раз. Разумеется, при этом часть решений декодера может быть на каких-то символах ошибочной, и некоторые из этих ошибок могут быть исправлены при следующих итерациях-попытках декодирования тех же символов.

При этом справедлива следующая теорема.

Теорема 2.2. Основная теорема многопорогового декодирования.

Если на произвольном *j*-м шаге декодирования МПД изменяет информационный символ i_j, то:

а) при этом МПД находит новое кодовое слово $\overline{A}_2$, более близкое к принятому сообщению $\overline{Q}$, чем то кодовое слово $\overline{A}_1$, которому соответствовало значение i_j перед *j*-м шагом декодирования:

$$|\overline{B}_1| = |\overline{A}_1 \oplus \overline{Q}| > |\overline{A}_2 \oplus \overline{Q}| = |\overline{B}_2|;$$

б) после окончания *j*-го шага возможно декодирование любого очередного символа i_k, $k \neq j$, так что при его изменении будет осуществлено дальнейшее приближение к принятому сообщению.

Доказательство. Перед началом декодирования символа i_j согласно лемме 2.1 справедливо

$$(\overline{D}_1, \overline{S}_1) = (\overline{A}_{1I} \oplus \overline{Q}_I, H(\overline{Q}_I \oplus \overline{D}_1, \overline{Q}_V)) = \overline{A}_1 \oplus \overline{Q},$$

где

$$\overline{A}_1 = (\overline{A}_{1I}, \overline{A}_{1V}),\ \overline{A}_{1I} = \overline{Q}_I \oplus \overline{D}_1.$$

Вес вектора $\overline{B}_1$ перед этим шагом, равный $|\overline{B}_1| = |\overline{D}_1| + |\overline{S}_1|$, можно представить в виде обычной суммы весов $W_1 = L_{1j} + X$, где L_{1j} определено выражением (2.4) и равно сумме проверок и символа d_j, на пороговом элементе, а X – вес остальных компонент $\overline{S}_1$ и $\overline{D}_1$, не входящих в L_{1j}.

Рассмотрим кодовый вектор $\overline{A}_2$, отличающийся от $\overline{A}_1$ только в одном информационный символе i_j, и соответствующую ему разность $\overline{B}_2 = \overline{A}_2 \oplus \overline{Q}$. Поскольку $\overline{B}_1$ и $\overline{B}_2$ отличаются между собой только в тех компонентах, которые поступают на пороговый элемент, то $|\overline{B}_2| = L_{2j} + X$, где $L_{1j} + L_{2j} = J + 1$, потому что

в силу линейности кода каждая проверка и символ d_j точно в одном из двух векторов $\overline{B}_i$ равны 1.

Так как МПД изменяет i_j, если $L_{1j} > T$, то для этого необходимо, чтобы было $L_2 < L_1$ и, следовательно, $|\overline{B}_1| > |\overline{B}_2|$, чем доказан пункт а) теоремы.

Далее, очевидно, если символ i_j не изменялся, то можно декодировать любой другой символ i_k, $k \neq j$, поскольку при этом сохраняются условия леммы. В случае же изменения i_j в соответствии с правилами работы МПД после декодирования i_j имеют место равенства $\overline{A}_{2I} = \overline{Q}_I \oplus \overline{D}_2$ и $\overline{S}_2 = H(\overline{Q}_I \oplus \overline{D}_2, \overline{Q}_V)$, где $\overline{D}_2$ отличается от $\overline{D}_1$ в символе d_j, поскольку при изменении через обратную связь с порогового элемента проверок, относящихся к i_j, инвертируются именно те компоненты $\overline{S}_1$, в которых $\overline{S}_2$ отличается от $\overline{S}_1$. Отсюда получаем, что после изменения i_j для определенных выше векторов $\overline{D}_2$, $\overline{A}_2$ и $\overline{S}_2$ также имеет место равенство

$$(\overline{D}_2, \overline{S}_2) = (\overline{A}_2 \oplus \overline{Q}),$$

аналогичное тому, которое по лемме 2.1 имело место перед изменением i_j. Тем самым при последующих шагах декодирования и изменениях символов i_k, $k \neq j$, также будет осуществляться дальнейшее строго монотонное приближение к принятому из канала сообщению $\overline{Q}$.

Основная теорема МПД доказана.

Из этой теоремы следует, что МПД при каждом изменении декодируемых символов приближается к принятому вектору $\overline{Q}$, отыскивая тем самым новые текущие все более правдоподобные вектора-гипотезы $\overline{A}_i$. МПД просматривает и сравнивает не экспоненциально большое количество кодовых слов, а только пары, отличающиеся между собой лишь в одном информационном символе, причем, одно из сравниваемых слов находится в самом декодере. В случае если второе кодовое слово окажется ближе к принятому вектору $\overline{Q}$, чем то, информационные символы которого находятся в соответствующих регистрах памяти МПД, де-

кодер переходит к нему и дальнейшие сравнения производятся уже с новым промежуточным вектором $\overline{A}_i$. Ясно, что в принципе можно проводить достаточно большое число попыток декодирования всех символов кода. Тем самым будет осуществляться движение, стремление решения МПД к решению ОД – вектору $\widetilde{A}$. Принципиально важно, что при этом сложность МПД остаётся такой же, как и у обычного ПД – линейной.

Подчеркнем, что только что доказанная основная теорема многопорогового декодирования устанавливает, что посредством простейшей из известных процедурой порогового типа при каждом изменении декодируемых символов обеспечивается строгое приближение к оптимальному решению, т.е. строгий рост правдоподобия каждого нового решения МПД. При этом сложность процедуры для сообщения длины k становится пропорциональной не 2^k, а просто k. Ни для каких других алгоритмов декодирования неэкспоненциальной сложности не известно аналогичное строго доказанное свойство монотонной сходимости к решению ОД.

Хотя для МПД алгоритма только что доказана уникальная теорема о стремлении его решений к решению ОД, не следует забывать, что речь идёт об итеративном применении к декодируемым символам простейшей пороговой функции. При большом уровне шума в канале со случайными ошибками и на первой, и на последующих итерациях декодирования возможно неправильное решение порогового элемента декодера о тех или иных отдельных декодируемых символах. С другой стороны, при всех изменениях декодируемых символов, согласно доказанным результатам, этот декодер только строго улучшает свои решения по критерию правдоподобия. Но это значит, что после ошибочных решений относительно декодируемых символов на следующих шагах МПД может исправить собственные ошибки, внесенные на предыдущих итерациях. При большом уровне шума доля первоначально неправильных решений МПД на первых итерациях коррекции ошибок может быть довольно значительной. Но при этом относительно всего сообщения, принятого из канала, каждое новое решение МПД, как следует из основной теоремы, будет всегда строго более правдоподобным.

Именно такое поведение МПД хорошо наблюдается при анализе процесса декодирования в компьютерном демомультфильме, который можно переписать со специализированного веб-сайта ИКИ РАН **www.mtdbest.iki.rssi.ru** (гиперссылка «демонстрационная программа» на странице «О методе»). Там же приведена инструкция по использованию этой программы.

Наконец, заметим, что из доказанной теоремы совершенно не следует, что переход от одного кодового слова $\overline{A}$ к другому будет продолжаться до тех пор, пока $|\overline{B}| = |\overline{Q} \oplus \overline{A}|$ не станет минимальным, т.е. $\overline{A}$ будет решением ОД $\widetilde{A}$. Таким образом, МПД не является оптимальным декодером. Значительная часть следующих глав этой книги будет посвящена поискам таких кодов и декодеров, для которых процесс декодирования действительно будет почти всегда продолжаться до тех пор, пока не будет достигнут вектор $\widetilde{A}$, решение оптимального переборного декодера.

Допустим далее, что МПД достиг решения ОД, т.е. в информационном регистре МПД находятся символы вектора $\widetilde{A}$. Тогда справедливо следующее следствие.

Следствие 1. МПД не изменит решения ОД.

Доказательство. Если бы МПД изменил на некотором шаге хотя бы один информационный символ в векторе $\widetilde{A}$, то это означало бы, что нашелся другой кодовый вектор $\widetilde{A}^*$, который ближе к $\overline{Q}$, чем $\widetilde{A}$, что невозможно, потому что, по определению, ближайшим к $\overline{Q}$ словом является вектор $\widetilde{A}$.

Следствие доказано.

Таким образом, в следствии доказан один из аспектов устойчивости решения МПД относительно оптимального решения: достигнув его, МПД останется в нём. Это очень важно, поскольку алгоритм допускает возможность многократного изменения одних и тех же декодируемых символов.

Можно также заметить, что при доказательстве основной теоремы МПД единственность декодируемого на каждом шаге символа i_j не использовалась сколько-нибудь существенным образом. Отсюда следует, что данная процедура декодирования

может применяться и к любой группе информационных символов. Опишем этот результат формально.

Для осуществления на каждом шаге декодирования перехода к кодовым векторам $\overline{A}$, все более близким к $\widetilde{A}$, совсем не обязательно изменять только по одному информационному символу на каждом шаге.

Рассмотрим пороговый декодер, отличающийся от определенного выше МПД тем, что:

а) на каждом *j*-ом шаге декодирования выбирается множество $\{J_j\}$ из k_j информационных символов, $k_j > 1$;

б) для выбранного множества $\{J_j\}$ информационных символов на пороговый элемент подаются все k_j компонент вектора $\overline{D}$, относящиеся к ним, и все те m_j компонент вектора $\overline{S}$, которые содержат в качестве слагаемых нечетное число ошибок в информационных символах из $\{J_j\}$;

в) значение порога T порогового элемента декодера не менее $(k_j+m_j)/2$;

г) если значение суммы на пороговом элементе больше T, то инвертируются все (k_j+m_j) компонент векторов $\overline{D}$ и $\overline{S}$, поданных на порог, и все k_j рассматриваемых информационных символов.

Для такого декодера справедлива следующая теорема.

Теорема 2.3. Пусть на вход декодера, работающего согласно пунктам а) – г), поступают векторы $\overline{D}_1, \overline{A}_{1l}$ и $\overline{Q}_v$ определенные в лемме 2.1.

Тогда, если на *j*-ом шаге декодирования декодер изменит множество $\{J_j\}$, то:

1) для кодовых векторов $\overline{A}_1$ и $\overline{A}_2$, где $\overline{A}_2$ отличается от $\overline{A}_1$ в k_j информационных символах, справедливо следующее неравенство: $|\overline{B}_1| = |\overline{Q} \oplus \overline{A}_1| > |\overline{B}_2| = |\overline{Q} \oplus \overline{A}_2|$;

2) после завершения *j*-го шага декодирования в декодере находятся векторы $\overline{A}_{2l}$, $\overline{D}_2 = \overline{Q}_l \oplus \overline{A}_{2l}$, $\overline{S}_2 = H(\overline{A}_{2l}, \overline{Q}_v)$, такие, что $\overline{A}_2 \oplus \overline{Q}_2 = (\overline{D}_2, \overline{S}_2)$.

Доказательство теоремы совпадает с тем, которое было приведено для теоремы об МПД, поскольку там нигде сущест-

венным образом не использовалась единственность декодируемого на каждом шаге информационного символа принятого сообщения, т.е. то, что $k_j = 1$.

При разработке МПД действительно оказалось полезным использовать пороговые элементы, настроенные сразу на определённые группы информационных символов. Смысл последнего результата состоит просто в том, что можно сравнивать правдоподобие любых пар кодовых слов, а не только отличающихся в единственном информационном символе, как это имеет место в основной теореме МПД (теорема 2.2). Необходимо только сделать так, чтобы пороговый элемент был настроен именно на эту пару, т.е. на пороговый элемент должны поступать все символы векторов $\overline{D}$ и $\overline{S}$, которые соответствуют несовпадающим символам сравниваемых кодовых слов.

Пусть далее на вход МПД поступают векторы $\overline{A}_I$, $\overline{Q}_V$ и $\overline{D}$, соответствующие решению $\overline{A}^*$, которое отличается от решения ОД $\widetilde{A}$ только в одном информационном символе блокового кода длины n с k информационными битами. Ниже формулируются условия, которым должен удовлетворять МПД, гарантированно исправляющий это одиночное отклонение от $\widetilde{A}$.

Теорема 2.4. Пусть МПД устроен так, что изменение символа и соответствующих компонент $\overline{S}$ и $\overline{D}$ происходит только в том случае, если соответствующая ему сумма проверок a_j максимальна среди всех a_i, $0 \le i < k$, и $a_j > T$.

Пусть, кроме того, код таков, что вес всех кодовых слов с одной информационной единицей нечетен и равен J+1, а $T = (J+1)/2$.

Тогда, если решение $\widetilde{A}$ для данного $\overline{Q}$ единственно, то после завершения процедуры декодирования решение МПД будет совпадать с оптимальным.

Доказательство. Пусть векторы на входе МПД соответствуют решению, отличающемуся от оптимального в символе i_j, а соответствующая ему сумма на пороговом элементе равна a_j, $a_j > T$. Покажем, что она строго больше суммы a_k, относящейся к любому символу i_k, $k \ne j$.

Докажем это от противного.

Пусть найдется i_k, $k \neq j$ такое, что $a_k \geq a_j$. Тогда, поскольку $\widetilde{A}^*$ отлично от $\widetilde{A}$ в символе i_j, то $a_j = T + b_j > T$; $b_j = 0{,}5; 1{,}5; \ldots$; $a_k = T + b_k > T$; $b_k \geq b_j$.

Обозначим $W_j = a_j + x = |\overline{B}_j| = |\overline{Q} \oplus \widetilde{A}^*|$, где x – вес всех оставшихся компонент $\overline{S}$ и $\overline{D}$ не поступивших на вход порогового элемента.

Если $b_k \geq b_j$, то после инверсии i_k и соответствующих ему компонент векторов $\overline{S}$ и $\overline{D}$ вес суммы на пороге уменьшится на величину $\Delta = a_k - (J + 1 - a_k) = 2a_k - J - 1 = 2T + 2b_k - J - 1 = 2b_k > 0$.

После инверсии i_j вес суммы на пороге уменьшился бы на $2b_j$. Поскольку входным вектором, который изменялся бы в обоих этих случаях был $\widetilde{A}^*$, то это соответствует случаю, когда кодовый вектор $\widetilde{A}_k^*$, отличающийся от $\widetilde{A}^*$ в символе i_k, ближе к $\overline{Q}$, чем $\widetilde{A}$, что невозможно. В силу единственности $\widetilde{A}$ невозможен также и случай $a_k = a_j$. Но это значит, что сумма a_j максимальная среди всех a_i и МПД действительно изменит i_j.

Теорема доказана.

Отметим, что введенным в теореме ограничениям удовлетворяют многие самоортогональные блоковые коды, и что данный результат справедлив независимо от того, верное или ошибочное решение об i_j принял ОД. Таким образом, рассматриваемый пороговый декодер не ухудшает оптимальное решение и может исправлять одиночные отклонения от оптимального решения.

Для систематических свёрточных кодов теорема 2.4 может быть переформулирована так, что сумма a_j должна быть максимальной среди всех a_j только в пределах длины кодового ограничения n_A от i_j. Это связано с тем, что суммы, относящиеся к информационным символам, которые находятся на более далеких расстояниях, оказываются обязательно состоящими из различных компонент векторов $\overline{S}$ и $\overline{D}$ и, следовательно, независящими друг от друга. При этом МПД свёрточного кода будет

исправлять все одиночные отклонения от оптимального решения, разделенные интервалом не менее n_A. Заметим, что последние результаты показывают, что МПД не только не уходит из оптимального решения, если достиг его, но и переходит в него из некоторой окрестности оптимального решения. Совокупность рассмотренных и доказанных выше свойств МПД можно назвать его устойчивостью относительно решения ОД [57].

Наконец, сформулируем критерий качества декодирования МПД, который может быть использован при анализе результатов моделирования работы декодеров.

Теорема 2.5. Пусть МПД неоднократно декодирует в некотором порядке каждый информационный символ сообщения. Тогда, если он совершил единственную ошибку в символе i_j и не может ее исправить при вторичной попытке декодирования, то ОД декодирует данное сообщение также ошибочно.

Доказательство. Пусть ошибка МПД сделана в символе i_j. Так как при последующих попытках декодирования никакие символы уже не были изменены, то все суммы a_j на пороговых элементах менее T. Это значит, что правильное кодовое слово с инвертированным i_j не может быть решением, потому что сумма a_j будет в этом случае больше T и, значит, оно будет дальше от $\overline{Q}$, чем то кодовое слово, которому соответствует состояние МПД. Может найтись другое кодовое слово, отличающееся от переданного кодового вектора в большем числе информационных символов и находящееся ближе к $\overline{Q}$, чем решение МПД. Но это значит, что ОД все равно совершит ошибку.

Теорема доказана.

Для свёрточного кода может быть также сформулирована следующая теорема.

Теорема 2.6. Пусть МПД свёрточного кода не изменяет решение после некоторого числа попыток улучшить принятое сообщение. Тогда число ошибок ОД при декодировании этого сообщения не меньше числа одиночных ошибок в решении МПД, находящихся на расстоянии более $2n_A$ от других ошибок.

Доказательство теоремы использует ту особенность структуры ошибок ОД и МПД, что вблизи одиночной ошибки МПД всегда будет одна ошибка или пакет ошибок ОД.

Результаты, сформулированные в двух последних теоремах, позволяют легко идентифицировать ошибки ОД, возникающие при использовании МПД, при анализе работы МПД на испытательных стендах и при моделировании его работы: все одиночные ошибки МПД, не исправляемые при повторном декодировании, приводят к ошибкам и при использовании ОД.

2.4. Гауссовский канал

Рассмотрим случай использования в гауссовском канале «мягких» модемов, которые характеризуются тем, что для $M = 2^m$, $m = 2, 3, 4, \ldots$ и двоичной фазовой манипуляции при передаче «0» есть вероятности p_i, $i = 0, 1, \ldots, M–1$, появления выходного напряжения демодулятора приемника в одной из m областей разбиения этого напряжения, пронумерованные последовательно [46, 47]. При передаче «1» попадание в i-ю область имеет вероятность $p_{M–i–1}$. Фактически тем самым вводится m-битовое квантование выходного сигнала «мягкого» модема приёмника для двоичной модуляции ФМ2. Ясно, что при передаче «0» попадание в области, более близкие к «1», т.е. если $i > (M–2)/2$, соответствует ошибочному решению модема, а ошибка при передаче «1» происходит, если $i < M/2$.

Рассмотрим, что следует делать соответствующему мажоритарному декодеру для таких мягко принятых символов с оценками достоверности решений двоичного модема. Для этого сравним правдоподобие двух кодовых слов, отличающихся в некотором произвольно выбранном информационном символе i_j. Для определения того, какое из этих двух слов более правдоподобно, нужно рассмотреть вероятности приёма символов канала только в тех d позициях, в которых i_j и его инверсия $\bar{i}_j$ различны. Вероятность того значения символа i_j, которое и было принято, пропорциональна

$$P(i_j) = p_{j\inf} \prod_{jv=1}^{d-1} p_{jv} ,$$

а для его инверсии $\bar{i}_j$

$$P(\bar{i}_j) = p_{M-j-1\,\mathrm{inf}} \prod_{jv=1}^{d-1} p_{M-jv-1},$$

откуда отношение вероятностей приёма $\bar{i}_j$ и i_j может быть представлено в виде

$$L = P(\bar{i}_j)/P(i_j) = (p_{M-1-j\,\mathrm{inf}} / p_{j\,\mathrm{inf}}) \prod_{jv=1}^{d-1} (p_{M-jv-1} / p_{jv})$$

Здесь используется обозначение номера используемой вероятности символа проверки *jv* для того, чтобы указать на то, что все *d*–1 символов, стоящих за знаком умножения, являются проверочными символами принятого сообщения. Индекс inf используется для обозначения вероятности приёма декодируемого информационного символа.

Для упрощения вычислений удобно рассматривать не функцию правдоподобия *L*, а её логарифм

$$L' = \log(L) = \log(p_{M-1-j\,\mathrm{inf}} / p_{j\,\mathrm{inf}}) + \sum_{jv=1}^{d-1} \log(p_{M-jv-1} / p_{jv}). \qquad (2.5)$$

Функция L' является суммой из *d* слагаемых и, следовательно, может быть реализована с помощью порогового элемента, на входе которого есть уже не просто «0» и «1», как в «жёстком» модеме, а *d* логарифмов отношений вероятностей со знаками «+» или «–». Ясно, что если $L' > 0$, то инвертированный $\bar{i}_j$ более правдоподобен, чем исходное принятое его значение. Если $L' \le 0$, то исходный символ более вероятен и его менять не нужно.

Так должен работать пороговый элемент в случае «мягкого» приёма символов из канала связи. В этом случае получается обычный «мягкий» ПД.

Далее, выделим в принятом потоке оценок символов бит, отвечающий за значение принятого символа, а также те *m*–1 битов, которые в этом случае будут просто указывать на надёжность приёма принятых символов сообщения, что фактически однозначно определяется амплитудой сигнала демодулятора, выносящего решения о принятом символе. Таким образом, не-

обходимо только решить вопрос о простой двоичной перекодировке принятых из канала связи символов, удобной для реализации в мягком МПД.

Теперь, имея значения принятых битов, вычислим обычным образом синдром принятого сообщения. Ясно, что при этом остаётся справедливой лемма о свойствах синдрома $\overline{S}$ и разностного вектора $\overline{D}$, поскольку она вообще никак не связана с достоверностью принятых символов. Отметим далее, что если для некоторого символа синдрома результат его вычисления дал «0», то соответствующее ему логарифмическое слагаемое в (2.5), очевидно, отрицательно, а если «1», то это слагаемое положительно и имеет то же абсолютное значение, что и при нулевом результате вычисления.

Полагая, что разностный регистр D также предусмотрен и в мягком декодере, получаем, что этот МПД просто оценивает знак той же функции правдоподобия L', но представленной в более удобной для вычислений форме:

$$L' = W_{\text{inf}}(2d_{\text{inf}} - 1) + \sum_{jv=1}^{d-1} W_{jv}(2s_{jv} - 1), \qquad (2.6)$$

где W_{inf} и W_{jv} – веса проверок, определяемые логарифмическими слагаемыми в (2.5), d_{inf} – значение 0 или 1 соответствующей ячейки в разностном регистре D, как это было и в случае жёсткого МПД для ДСК, и s_{jv} – символы регистра синдрома S, являющиеся проверками декодируемого символа i_j. Изменение декодируемых символов, если L' в (2.6) положительно и определяет все выполняемые операции в мягком МПД, каждое новое решение которого оказывается строго более правдоподобным, чем его предыдущее промежуточное решение.

При $M = 2$ уровнях квантования (2.6) превращается в мажоритарную функцию для проверок обычного порогового декодера в канале типа ДСК, все веса которых $W_{\text{inf}} = W_{jv} = 1$. Заметим, что применение мягких решений модема столь же эффективно в МПД, как и для алгоритма Витерби, позволяя при типичных значениях уровня шума в канале повысить ЭВК декодера примерно на 2 дБ.

2.5. Недвоичные коды

Рассмотрим канал с передачей q, $q > 2$, равновероятных недвоичных символов, которые под воздействием шума могут независимо с вероятностью p_0 приобретать равновероятно одно из $q–1$ оставшихся ошибочных значений. Назовем по аналогии с ДСК такой канал QСК и построим декодер, реализующий для данного алфавита процедуру, аналогичную двоичному МПД, называемую далее QМПД [1, 11, 64, 78, 86, 101]. Используемая модель QСК описана в первой главе.

Ценность QМПД алгоритма заключается в том, что мажоритарные алгоритмы имеют всего лишь линейный рост сложности (числа операций декодирования) от длины кода n. Поскольку обычно оптимальные методы характеризуются экспоненциально нарастающей с длиной кода сложностью, применение недвоичных МПД представляется особенно желательным, потому что решения недвоичных декодеров этого типа также стремятся к решению ОД, но при линейной от длины кода сложности своей реализации.

Заметим, что за более чем полувековой период развития теории и техники кодирования фактически единственными используемыми в реальных системах связи недвоичными кодами оказались прекрасно изученные и реализованные во множестве своих модификаций коды Рида-Соломона (РС). Только для перечисления всевозможных успешных приложений кодов РС потребуется не одна страница текста. Фактически никаких других кодов, которые могли бы применяться для кодирования недвоичных потоков данных и, главное, последующего их успешного и достаточно простого декодирования, до появления QМПД просто не существовало. И это при том, что характеристики кодов РС гораздо дальше от потенциальной шенноновской границы хороших корректирующих возможностей $R = C$, чем даже у просто эффективных алгоритмов для двоичных кодов [1]. Главная проблема здесь связана с тем, что длина кодов РС для технически реализуемых параметров кодирования очень ограничена. Поэтому задача реализации недвоичных лёгких простых алгоритмов для кодов, гораздо более длинных, чем коды РС, остаётся чрезвычайно актуальной, поскольку для выбранного осно-

вания кода q максимальная длина недвоичного кода РС не может быть более q символов. В настоящее время коды РС длины более 256 не применяются. Для QМПД такого ограничения нет в принципе.

Ещё более существенно то, что в случае больших значений основания кода q, $q > 10$, практически вообще невозможно создать эффективные истинно оптимальные декодеры, в том числе и алгоритм Витерби, поскольку при этом их сложность в большинстве случаев, аналогично двоичной передаче, видимо, будет иметь вид q^k, где k – длина кодирующего регистра, выраженная числом q-ичных символов. Но даже для $q = 16 \div 32$ реализация ОД для кодов длиннее, чем $k \sim 3$, очень проблематична, а их эффективность будет для таких небольших длин совершенно незначительной. С другой стороны, например, код РС для $q = 256$ при любой избыточности и всех допустимых длинах кода n всё же малоэффективен, если сравнивать его возможности с границей $R = C$. Это и определяет особую ценность применения QМПД алгоритмов, которые могут использоваться с кодами сколь угодно большой длины [11, 101]. При этом сложность реализации QМПД всегда оказывается весьма незначительной и будет иметь тот же порядок, что и в двоичном случае.

Таким образом, фактическое отсутствие действительно эффективных недвоичных алгоритмов и огромная потребность в их использовании, как это следует из факта массового применения кодов РС, приводит к необходимости разработки существенно более простых и более эффективных декодеров, которые могли бы декодировать длинные недвоичные коды достаточно простыми средствами.

Рассмотрим далее формальное описание алгоритма QМПД.

Пусть задан линейный недвоичный систематический свёрточный или блоковый код, проверочная матрица H которого имеет такой же вид, как и в двоичном случае, т.е. состоит только из нулей и единиц, за исключением того, что вместо 1 в единичной подматрице будут –1. Предположим также, что все операции сложения и вычитания будут производиться в некоторой группе целых чисел, например, по mod q. После передачи кодового вектора $\overline{A}_0$ длины n с k информационными символами по

QCK в декодер поступает вектор $\overline{Q}$, отличающийся, вообще говоря, от исходного кодового вектора из-за искажений в канале: $\overline{Q} = \overline{A}_0 + \overline{E}$, где $\overline{E}$ – вектор шума канала типа QCK.

Будем, как и в двоичном случае представлять каждый вектор $\overline{X}$ длины n в виде пары векторов $\overline{X}_I$, $\overline{X}_V$ длины k и $(n–k)$ соответственно.

Пусть $\overline{Q} = \overline{A} + \overline{E}$, где $\overline{E}$ – вектор ошибки, «+» и «–» – операции сложения и вычитания в определённой некоторым образом группе, $\overline{A}$ – некоторое произвольное кодовое слово.

Определим $\overline{D}$ – q-ичный вектор длины k, равный $\overline{D} = \overline{A}_I - \overline{Q}_I$, где $\overline{Q}_I$ – информационная часть принятого сообщения $\overline{Q} = (\overline{Q}_I, \overline{Q}_V)$.

Тогда справедлива следующая лемма.

Лемма 2.7.

$$(\overline{D}, H(\overline{Q}_I + \overline{D}, \overline{Q}_V)\ ) = \overline{A} - \overline{Q}\ . \qquad (2.7)$$

Доказательство. В силу линейности кода справедлива цепочка равенств

$$\overline{S} = H(\overline{Q}_I + \overline{D}, \overline{Q}_V) = H(\overline{Q}_I + \overline{D}, \overline{Q}_V + \overline{A}_V - \overline{A}_V) =$$

$$= H\overline{A} + H(\overline{0}_I, \overline{Q}_V - \overline{A}_V),$$

где $\overline{0}_I$ – нулевой вектор длины k.

Учитывая, что для систематического кода для $q > 2$ $H(\overline{0}_I, \overline{X}_V) = -\overline{X}_V$, получаем, что $\overline{S} = \overline{A}_V - \overline{Q}_V$. А так как $\overline{D} = \overline{A}_I - \overline{Q}_I$, то $(\overline{D}, \overline{S}) = \overline{A} - \overline{Q}$.

Лемма доказана.

Она устанавливает простое полезное соответствие между произвольным кодовым словом и принятым сообщением, аналогичное двоичному случаю [1, 9, 86], представленному в лемме 2.1. Лемма 2.7 позволяет доказать главное свойство QMПД, алгоритм функционирования которого описан ниже.

Отметим в силу большой важности ещё раз, что поскольку проверочные (а значит, и порождающие) матрицы систематического кода содержат только 0, 1 и –1, то операции кодера и декодера по формированию проверочных символов кода и вычис-

лению синдрома $\overline{S}$ принятого сообщения являются только сложениями или вычитаниями. Таким образом, для кодирования и декодирования не требуется не только наличие недвоичного поля, но даже кольца целых чисел. Для организации операций сложения достаточно создать только группу по сложению. Это дополнительно и очень существенно упрощает все процедуры кодирования и реализации последующего декодирования.

Пусть при передаче по QCK кодового слова $\overline{A}_0$ в декодер поступил искажённый в канале связи вектор $\overline{Q} = \overline{A}_0 + \overline{E}$. Аналогично двоичному случаю, разностный вектор $\overline{D}$, теперь уже q-ичный, перед началом процедуры декодирования примем равным 0.

Пусть декодер QMПД устроен так, что после вычисления обычным образом вектора синдрома $\overline{S} = H\overline{Q}$ принятого сообщения процедура декодирования состоит в следующем.

1. Для произвольно взятого символа q-ичного декодируемого информационного символа i_j принятого сообщения подсчитывается число двух наиболее часто встречающихся значений проверок из общего числа J всех проверок относящихся к символу i_j, а также символа d_j вектора $\overline{D}$, соответствующего символу i_j. Пусть значения этих двух проверок равны h_0 и h_1, а их количество равно m_0 и m_1, соответственно, причем $m_0 \geq m_1$.

Эта процедура аналогична подсчёту суммы проверок на пороговом элементе двоичного МПД.

2. Если $m_0 – m_1 \leq T$, где $T = 0, 1, 2, \ldots$ – целое неотрицательное число, то осуществляется переход к новому произвольному i_m, $m \neq j$, и далее к п.1.

Это – тоже аналог процедуры сравнения с порогом в двоичном декодере.

3. Если $m_0 – m_1 > T$, то из i_j, d_j и всех J проверок относительно i_j вычитается оценка ошибки, равная h_0, затем происходит выбор нового i_m, $m \neq j$, и переход к п.1.

Этот последний шаг цикла декодирования очередного символа есть просто процесс изменения декодируемого символа и коррекции через обратную связь всех символов синдрома, яв-

ляющихся проверками декодируемого символа. Нужно только учитывать, что процедуры сложения и вычитания в QМПД не тождественны, как это имеет место в двоичном МПД. Пример схемной реализации QМПД представлен в [1].

Такие попытки декодирования по пп.1÷3 могут быть повторены для каждого символа принятого сообщения, например, 3, 10 и более раз.

При реализации алгоритма QМПД, как и в двоичном случае, удобно все информационные символы перебирать последовательно, а останавливать процедуру декодирования после фиксированного числа попыток коррекции ошибки или если при очередной такой попытке ни один из символов не изменил своего значения.

Для описанного алгоритма QМПД справедлива следующая теорема.

Теорема 2.8. Основная теорема многопорогового декодирования недвоичных кодов.

Пусть декодер реализует алгоритм QМПД для описанного выше СОК. Тогда при каждом изменении декодируемых символов происходит переход к более правдоподобному решению по сравнению с предыдущими состояниями декодера.

Предварительное обсуждение.

Напомним, что для классического канала типа QСК из двух кодовых векторов более близким к принятому из канала сообщению и, следовательно, более правдоподобным будет тот из них, который отличается от принятого вектора в меньшем числе символов. Поэтому доказательство роста правдоподобия решений QМПД при каждом изменении декодируемых символов состоит просто в том, чтобы показать, что число символов нового кодового слова, совпадающих с символами принятого сообщения, увеличилось, т.е. расстояние Хемминга между ними уменьшилось. Для недвоичных символов это расстояние как раз соответствует количеству несовпадающих символов в двух векторах равной длины.

Итак, согласно свойствам вектора синдрома и разностного регистра по лемме 2.7 для QМПД расстояние между принятым вектором и текущим решением QМПД равно числу ненулевых

символов синдрома. Значит, для уменьшения этого расстояния, что будет соответствовать росту правдоподобия решений этого декодера, нужно найти другое кодовое слово, для которого общее число нулевых символов синдрома $\overline{S}$ и разностного вектора $\overline{D}$ увеличится. Напомним, что, как и в двоичном случае, здесь имеется в виду то кодовое слово, информационные символы которого находятся в соответствующих регистрах декодера.

Доказательство.

Пусть декодер содержит векторы

$$\overline{A}_{0I},\ \overline{D} = \overline{A}_{0I} - \overline{Q}_I \text{ и } \overline{S} = H(\overline{Q}_I + \overline{D}, \overline{Q}_V), \tag{2.8}$$

где $\overline{A}_0 = (\overline{A}_{0I}, \overline{A}_{0V})$ – произвольное кодовое слово, $\overline{Q}$ – принятое сообщение.

Покажем, что в случае использования алгоритма QМПД при изменении очередного декодируемого символа i_j в текущем информационном векторе-решении декодера $\overline{A}_{0I}$ получается такой новый вектор $\overline{A}_{1I}$, что расстояние Хемминга до принятого вектора $\overline{Q}$ у кодового слова $\overline{A}_1$ меньше, чем у предыдущего решения декодера $\overline{A}_0$, т.е. $|\overline{A}_0 - \overline{Q}| > |\overline{A}_1 - \overline{Q}|$.

В самом деле, если некоторый символ i_j изменен, значит нашлось единственное значение h_0, $h_0 \neq 0$, на множестве проверок символа i_j, которое встречается строго чаще всех других, m_0 раз, а все другие – не более m_1 раз, $m_0 > m_1$. Отметим, что если $h_0 = 0$, декодируемый символ не изменяется.

В этом случае при изменении i_j, d_j и всех имеющихся J проверок в регистре синдрома, т.е. после вычитания из них величины h_0, все m_0 проверок (и, может быть, символ d_j), которые были равны h_0, станут равными 0. Количество нулевых проверок в векторе синдрома (конечно, с учётом и значения символа d_j), которые до изменения символа i_j были равны нулю, не может быть больше m_1. Но это значит, что при изменении i_j за счет этих символов вес вектора синдрома не может возрасти на этих позициях более, чем на m_1. Тогда общее изменение веса равно $m_1 – m_0 < 0$, т.е. суммарный вес векторов $\overline{D}$ и $\overline{S}$ после изменения декодируемого символа i_j уменьшится.

Также заметим, что вектор $\overline{S}_1$ отличается от $\overline{S}_0$ только в тех символах, которые являются для i_j проверками, а разностные векторы $\overline{D}_1$ и $\overline{D}_0$ не совпадают только в позиции d_j на величину h_0, как и соответствующие символу i_j проверки. Но это значит, что после изменения i_j в декодере типа QMПД содержатся векторы $\overline{S}_1$ и $\overline{D}_1$, соответствующие разности принятого вектора и нового решения декодера, т.е. выполняются условия, соответствующие (2.8). Но тогда получаем, что и в новом состоянии декодера снова справедливы условия леммы 2.7, что позволяет перейти к очередной попытке коррекции символа i_m, $m \neq j$, после которой изменение следующего декодируемого символа снова гарантирует переход к новому ещё более правдоподобному решению и т.д.

Теорема доказана.

Как видим, при переходе от двоичного к недвоичному МПД стиль доказательства основной теоремы изменился довольно незначительно.

Отметим два наиболее существенных момента, характеризующих предложенный новый алгоритм. Во-первых, как и в случае двоичных кодов, нельзя утверждать, что улучшение решения при многократных попытках декодирования будет иметь место до тех пор, пока не будет достигнуто решение ОД. На самом деле и в блоковых, и в свёрточных кодах возможны конфигурации ошибок, не исправляемые в QMПД, но которые могут быть исправлены в ОД. Поэтому основной способ повышения эффективности QMПД состоит в поиске кодов, в которых такие неисправляемые конфигурации ошибок довольно редки даже при большом уровне шума.

Другим важнейшим моментом является то, что по сравнению с традиционным подходом к мажоритарным схемам [4], в QMПД для изменения декодируемого символа достаточно наличие не абсолютного, а только относительно строгого большинства проверок, как это следует из условия $m_0 - m_1 > T$. Например, в самоортогональном коде с $d = 9$ ошибка в декодируемом символе будет исправлена даже в том случае, если из 9 его проверок (включая и символ d_j разностного регистра) правильными будет

только 2, а остальные 7 – ошибочными. Такого невозможно вообразить для двоичных кодов, а для QМПД данная ситуация типична. Единственным условием для этого частного примера являются разные значения ошибок в проверках относительно декодируемого символа i_j. А для больших значений q именно это условие практически всегда и реализуется. Эти свойства QМПД существенно расширяют возможности недвоичного многопорогового алгоритма при работе в больших шумах, сохраняя при этом весьма малую сложность процедур мажоритарного типа и в q-ичных каналах.

2.6. Декодирование в каналах со стираниями

Развитие техники связи ведет к значительному росту разнообразия каналов передачи, среди которых следует указать каналы со стираниями. Согласно модели канала с независимыми стираниями при передаче каждого символа независимо с вероятностью p_s происходит его стирание (о чем декодер извещается, например, дополнительным битом признака стирания) или с вероятностью $q_s = 1 - p_s$ осуществляется правильная передача. Пропускная способность такого канала равна в двоичном случае $C = q_s$.

ОД в этом канале должен найти такое кодовое слово, которое содержало бы минимальное число стираний (или в лучшем случае совсем их не имело бы на позициях информационных символов) и совпадало бы абсолютно со всеми правильными, т.е. известными символами поступившего сообщения. Иначе говоря, решение ОД, как и пришедшее из канала сообщение, является кодовым словом, содержащим, может быть, стирания на некоторых своих позициях.

В [4] описан алгоритм декодирования в стирающих каналах, который может быть существенно улучшен.

Метод многопорогового, точнее, многошагового декодирования в стирающих каналах (СтМПД) не требует такого же обоснования, как, скажем, в ДСК или в QСК. Если есть стёртый информационный символ i_j, то он, очевидно, может быть точно восстановлен, если хотя бы один правильно принятый символ из множества относящихся к нему проверок содержит именно этот

единственный стертый символ, а все остальные символы, которые входят в эту проверку, приняты правильно. Тогда, очевидно, выбранный символ i_j будет верно восстановлен. В рассматриваемом случае достаточно отметить только, что после первой попытки коррекции возможно лишь, что часть информационных символов, которые были стерты, не удалось восстановить. При этом по смыслу самого алгоритма он вообще не вносит никаких ошибок в сообщение. Но тогда попытка повторного декодирования сообщения, в котором количество стираний стало меньше, безусловно, оправдана, поскольку в рассматриваемом канале мерой эффективности декодирования является именно число восстановленных стираний в кодовом слове. Готовность декодера к повторению исправления стираний определяется просто тем, что после первой успешной попытки исправления одного из стираний для некоторого другого стёртого символа i_m в одной из проверок уменьшится число оставшихся стираний. Если в этом проверочном символе единственным оставшимся стиранием будет именно стирание символа i_m, то в этом случае появится гарантированная возможность исправления и этого стирания, даже если во всех других проверках, содержащих i_m, количество стёртых символов не менее двух.

Поскольку для исправления конкретного стёртого информационного символа достаточно всего одного соответствующего правильно принятого проверочного символа без прочих стёртых информационных символов, входящих в него, то и СтМПД будет работать в канале со стираниями при гораздо более высоких вероятностях стирания передаваемых битов по сравнению с каналами, в которых происходят только ошибки.

Таким образом, конечно, новый алгоритм сохраняет полное тождество между всеми правильно принятыми из канала кодовыми символами и восстановленным (может быть, не полностью) сообщением.

2.7. Несистематические коды

Рассмотренные выше алгоритмы МПД позволяют находить последовательность все более правдоподобных решений на основе простых вычислений, проводимых над непрерывно изме-

няемыми вектором синдрома $\overline{S}$ и разностным вектором $\overline{D}$. Выше было показано, что пара векторов ($\overline{D}$, $\overline{S}$) является разностью между текущим решением декодера и принятым сообщением. При этом следует отметить, что между векторами $\overline{S}$ и $\overline{D}$ нет принципиального различия.

Введенные для них обозначения и выполняемые над ними действия всего лишь отражали тот факт, что, например, если рассматривался код с $R = 1/2$, то из двух порождающих полиномов кода один был $G_1(x) = 1 + x^{P_1} + ... + x^{P_{J-1}}$, а другой – $G_2(x) = 1$, т.е. код был систематическим. Принципиальным обстоятельством оказывается то, что процедура вычисления синдрома соответствует вычислению разности между некоторой первоначальной гипотезой о переданном кодовом слове и принятым сообщением. Этой гипотезой в систематическом коде всегда оказывается то кодовое слово, информационные символы которого приняты из канала. Разумеется, никаких более предпочтительных «догадок» у декодера, принявшего из шумящего канала очередное сообщение, быть не может.

Задача построения МПД для всех описанных выше, а также других каналов в случае декодирования несистематических кодов сильно осложняется двумя обстоятельствами. Первое состоит в выборе кодов, которые даже при использовании оптимальных процедур должны тщательно проверяться на некатастрофичность [26, 37, 38, 39, 40]. Второе состоит как раз в том, чтобы уметь найти для МПД некоторую достаточно хорошую первоначальную гипотезу о переданном кодовом слове $\overline{A}_0$, которое будет затем улучшаться в смысле перехода от него ко все более правдоподобным решениям. Кроме того, как уже неоднократно подчёркивалось, к используемым в МПД кодам предъявляются весьма строгие требования по уровню размножения ошибок при пороговом декодировании.

Таким образом, не требуется формулировка и доказательство каких-либо дополнительных утверждений о существовании МПД для несистематических кодов. Для них после генерации любого кодового слова используемого кода и вычитания из него принятой из канала последовательности тоже формируется век-

тор, который удобно называть синдромом и для которого с учетом сделанного замечания об интерпретации вектора $\overline{D}$ становится очевидной основная теорема о многопороговом декодировании несистематических линейных двоичных и недвоичных кодов. Однако серьезные проблемы реализации в МПД потенциальной эффективности, т.е. хорошей сходимости к наиболее правдоподобному решению в этом случае также останутся.

Успешный вариант решения проблемы МПД декодирования несистематического кода описан в [65].

2.8. Многопозиционные системы сигналов

При использовании высокоэнергетичных сигналов и жестких требованиях к ширине полосы частот хорошие значения эффективности возможны в случае совместного применения многопозиционных систем модуляции и кодирования [13, 26]. Принципы использования МПД для систем сигналов на плоскости типа АФМ*N* и ФМ*N* также разработаны уже достаточно давно [62, 63, 103]. Это позволяет считать, что возможность применения МПД с этими обширными типами сигналов в настоящее время уже также вполне очевидна. При переходе к многомерным сигналам все подходы к применению МПД совместно с такими сигнальными конструкциями остаются аналогичными двумерному случаю, что позволяет одновременно получить значительный энергетический выигрыш кодирования и ещё более существенно сэкономить полосу частот передаваемого сигнала.

Рассмотрим принцип многопорогового декодирования для такой системы сигналов на примере АФМ16, для которой расположение сигнальных точек было показано на рис. 1.7.

Двоичные пары битов на горизонталях и вертикалях дают представление об одном из вариантов соответствия между сигнальными точками и четверками битов, которые поступают в модем передатчика от кодера, а затем приходят из демодулятора в декодер приемника. Существенным для обеспечения достаточно хорошего согласования систем модуляции и кодирования является то, что для каждого данного сигнала соседние с ним по горизонтали и вертикали сигналы отличаются только в одном бите, а те, которые находятся на диагонали – в двух битах. Такое

установление соответствия между сигнальными точками и четверками битов называется кодированием двумерным кодом Грея [13]. На самом деле можно проверить, что свойство увеличения веса Хемминга разности двоичных представлений сигнальных точек имеет место при удалении от любого исходного сигнала не только на 1, но и на 2 позиции, причём соответствующие логарифмы отношений вероятностей для случая удвоения веса Хемминга также примерно удваиваются. Это позволяет двоичные вектора $\overline{D}$ и $\overline{S}$, как и в случае обычной ФМ2, считать хорошей мерой разности расстояний между передаваемыми символами такой недвоичной системы передачи.

Аналогичные свойства справедливы и при росте числа сигнальных точек в рамках прямоугольной системы сигналов на плоскости или в пространствах большей размерности.

Таким же образом организуется соответствие между сигналами и двоичным их представлением в случае многопозиционной круговой системы сигналов, например, фазовой манипуляции вида ФМ*N*. Легко видеть, что в случае ФМ*N* имеет место рост веса Хемминга для разности двоичных представлений между всеми соседними или удаленными друг от друга на две позиции сигнальными точками (см. рис. 1.8).

Но из такого монотонного увеличения веса разности двоичного представления сигналов по мере их удаления от любого передаваемого символа в системе АФМ*N* или ФМ*N* получаем, что и в случае «жёсткого» модема, и при использовании «мягкого» модема рост весов и сумм проверок на пороговых элементах с хорошей точностью пропорционален логарифму отношения вероятностей текущего решения МПД и того удалённого потенциального нового решения, для которого и вычисляется сумма проверок двоичного кода со специально подобранными кодовыми полиномами для системы многопозиционной модуляции. Именно в этом случае суммы проверок соответствуют сравнению кодовых слов, у которых нет различий в том, рассматриваются ли разности в битах внутри передаваемых символов или все различия наблюдаются только между некоторыми битами в различных символах. Такое устранение различий между двоичными представлениями соотношения расстояний в разностных

векторах $\overline{S}$ и $\overline{D}$ при использовании кода Грея и позволяет успешно применять двоичные МПД и со сложными системами сигналов. При этом МПД обеспечит во многих случаях такое же практически оптимальное декодирование, как и переборные алгоритмы.

2.9. Сжатие данных

Принцип МПД без изменения алгоритма или устройств, его реализующих, может быть положен в основу одного из методов кодирования источников, известного как сжатие данных или кодирование с заданным критерием качества [12, 41, 42]. При такой постановке задачи последовательности информационных символов длиной, например, n двоичных символов кодируются в некоторые другие последовательности длины n/k_c, где k_c – коэффициент сжатия, и с достаточной достоверностью передаются по каналу, где восстанавливаются до исходной длины n, но с некоторой погрешностью. Например, вполне возможно, что после восстановления доля ошибочных символов не должна быть в среднем больше, чем 10^{-3} или 10^{-5}.

Рассмотрим вопрос о применении для этих целей методов мажоритарного декодирования на примере кода с $R = 2/3$.

На рис. 2.5 представлена обычная схема кодирования и передачи по ДСК двоичным линейным свёрточным кодом сообщения, которое потом декодируется пороговым декодером. На вход двух информационных регистров 1 и 2 кодера поступают два потока данных, из которых с помощью полусумматоров формируется поток проверочных символов, которые затем вместе с информационными символами направляются в канал. ДСК представлен для удобства описания как три отдельных полусумматора на каждый поток. Поскольку аддитивный шум в ДСК представляет собой наложение на кодовый вектор некоторой последовательности с биномиальным распределением, то декодирование в такой схеме всегда может рассматриваться как разделение кодовых слов и случайного биномиального потока по известной их сумме.

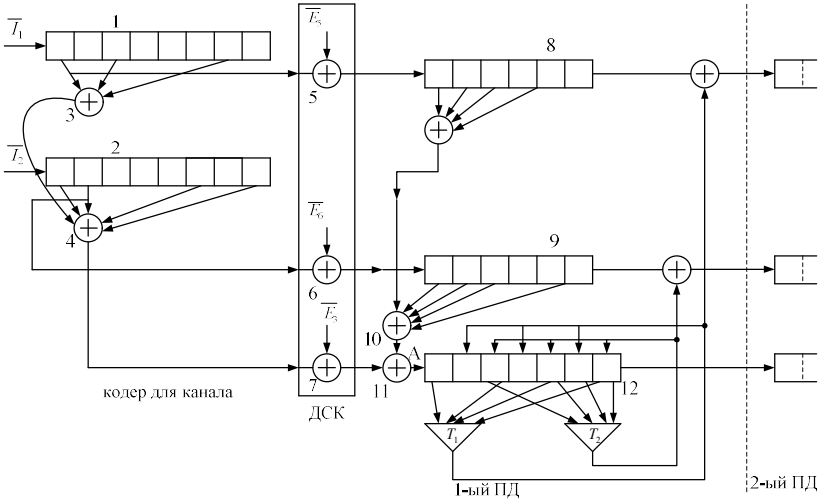


Рис. 2.5. Традиционная схема свёрточного кодирования и мажоритарного декодирования

Перейдем к другому описанию работы схемы без изменения функций ее основных частей. Пусть для некоторых параметров кода и канала мажоритарный декодер позволяет достичь малой вероятности ошибки декодирования на бит $P_b(\text{e}) << 1$. Тогда в силу линейности кода при замене информационных потоков $\bar{I}_1$ и $\bar{I}_2$ на нулевые схема сохранит эти же достоверности решений на приеме. Но в этом случае оказывается, что регистры 1 и 2, а также полусумматоры 3 и 4 не нужны.

Будем теперь ошибки ДСК, через полусумматоры 5 и 6 накладывающиеся на нулевые информационные последовательности, рассматривать как новые информационные потоки, которые должны быть переданы получателю. При этом информационные регистры декодера 8 и 9 принадлежат уже передающей стороне и образуют сжимающий кодер. Таким образом, в точке А кодера передатчика в новой интерпретации на рис. 2.6 находятся символы сжатой бернуллиевской последовательности от источников 5 и 6.

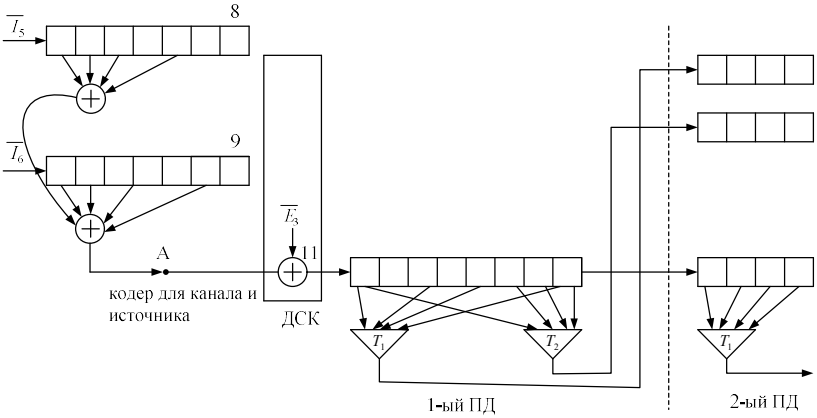


Рис. 2.6. Трансформация схемы кодирования для сжатия информации источника в 2 раза

Поскольку полусумматор 7 для шума ДСК по проверочным символам, как и полусумматоры 5 и 6, выродился в такой схеме в проходное соединение, т.к. на вторых их входах всегда нули, то собственно введение шума ДСК при передаче теперь осуществляется только через полусумматор 11. Результирующая схема совместного кодирования источника и канала с сохранением тех же обозначений для оставшихся элементов устройств кодирования и декодирования показана на рис. 2.6.

Как следует из модифицированной схемы, в канал поступает сумма по mod 2 двух бернуллиевских потоков (источников данных), которые восстанавливаются пороговыми элементами, например, с использованием МПД. Разумеется, вероятности p_1 появления единиц в кодируемой последовательности и p_0 ДСК могут быть неравными, что, конечно, повлечет за собой изменение характеристик алгоритма. В общем случае при использовании кодов с $R = k_c/(k_c+1)$ обеспечивается сжатие в k_c раз. При введении весов проверок схема, как и «мягкий» МПД, работает в гауссовских каналах. Без каких-либо изменений структуры схемы на рис. 2.6 можно сжимать и недвоичные потоки. Поскольку, как было показано, сжатие осуществляется той же кодирующей схемой, а восстановление, например, с помощью

МПД, то дополнительного доказательства роста правдоподобия решения не требуется, т.к. изменение функции алгоритма связано лишь с другой интерпретацией его работы.

2.10. Расширение области приложения принципов МПД

Хотя в этой главе были рассмотрены многие классические каналы связи, в которых возможно успешное применение МПД, потребности техники связи становятся всё более разнообразными и сфера приложения кодирования стремительно расширяется, а условия их применения всё более изменяются. Отметим некоторые такие области применения кодирования.

Одним из практически важных приложений теории кодирования для передачи цифровых данных стали коды с неравной защитой символов (НЗ-коды) [43, 44]. Они обеспечивают более эффективную, чем традиционные методы, защиту передаваемых данных в среднеквадратичном смысле путем достижения меньшей вероятности ошибки декодирования, например, старших разрядов передаваемых целых чисел, чем младших. Это достигается в общем случае тем, что часть информационных символов кода входит в большее число проверочных соотношений, что позволяет обеспечить для них и большее минимальное кодовое расстояние d, чем для символов, соответствующих младшим разрядам передаваемых чисел.

Поскольку в МПД происходит последовательное посимвольное принятие решений, то при переходе от символа с одним уровнем защиты к другому символу с меньшей или большей защищенностью будут изменяться не только множества соответствующих им проверок $\{S_{j_k}\}$, но и размеры этих множеств. Очевидно, что это никак не меняет принципов работы МПД и его главного свойства перехода к более правдоподобным словам при изменении декодируемых символов.

Другой обширной областью, в которой может эффективно работать МПД, являются различные каналы с неравномерной энергетикой (НЭК) [45]. К таким каналам можно перейти от обычных систем модуляции, если изменить соотношение энергий и, следовательно, расстояний между различными сигнальными точками многих традиционных систем модуляции, на-

пример, ФМN или АФМN, что приводит к росту достоверности передачи одних групп символов и уменьшению достоверности других. Это означает, что, например, при вычислении функции правдоподобия L' в (2.5) веса проверок будут во многих случаях вычисляться иначе. Остальные принципы МПД остаются вполне работоспособными и в этом случае.

Реализация принципов НЭК возможна и в более простых системах обычных параллельных каналов путём прямого перераспределения мощности передатчика между одинаковыми по своим прочим параметрам каналами передачи информационных и проверочных символов.

Наконец, вполне эффективным оказывается и комбинирование рассмотренных в этой главе методов и подходов к применению кодирования и декодирования с использованием МПД. Разумеется, при этом эффективность применения кодирования будет только возрастать, причём принципы сходимости решений МПД к решениям ОД во всех подобных случаях вполне успешно реализуются при минимальных затратах.

2.11. Выводы

В этой главе рассмотрен фундаментальный принцип роста правдоподобия решений МПД, который приложим ко многим основным симметричным аддитивным каналам без памяти: двоичным, q-ичным, гауссовским, стирающим, многопозиционным и другим моделям, охватывающим значительную часть реальных или близких к реальным теоретических моделей каналов. Кроме того, описан вариант использования МПД для новой сферы применения – сжатия данных.

Высокая степень общности этого принципа формирования итеративных методов коррекции ошибок открывает возможности для единого подхода к декодированию в каналах разного типа и качества, причем сам подход базируется на самом простейшем из известных методов коррекции – мажоритарном. Это позволяет ожидать высокой степени эффективности многопорогового метода при условии, что рост правдоподобия решения будет достаточно устойчивым и быстрым вплоть до полного или почти полного исправления ошибок в принятом сообщении.

Однако это условие на самом деле ставит перед разработчиками систем кодирования и алгоритмов декодирования новую весьма сложную проблему поиска таких кодов, которые при реализации МПД, максимально им соответствующего, обеспечили бы и наибольшую эффективность декодирования.

Методы ее решения рассмотрены в следующей главе.

ГЛАВА 3. РАЗМНОЖЕНИЕ ОШИБОК В МАЖОРИТАРНЫХ ДЕКОДЕРАХ

3.1. Понятие размножения ошибок

Результаты предыдущей главы показывают принципиальную возможность существенного повышения эффективности итеративной модификации мажоритарного метода декодирования линейных кодов во всем основном многообразии каналов без памяти с аддитивным шумом. Вместе с тем было указано, что для многих каналов и конкретных кодов можно легко найти такие конфигурации ошибок канала, которые не будут исправлены при любом числе итераций в блоковом МПД или сколь угодно длинными цепочками пороговых элементов в его свёрточном варианте, но которые исправляются оптимальным декодером (ОД) по максимуму правдоподобия. Таким образом, МПД не является ОД ни в каких из рассматривавшихся выше каналов.

Наиболее плодотворным подходом к решению проблемы максимально эффективного применения МПД оказывается оптимизация параметров МПД по порогам и весам проверок, а также выбор кодов с минимальным уровнем размножения ошибок (РО) при пороговом декодировании (ПД). В этом случае существенно снижается число и вероятность появления комбинаций ошибок, которые исправляются в ОД, но не корректируются в МПД.

Понятие РО и методы его анализа неодинаково трактуются разными авторами [4, 19, 20, 37, 48]. Анализ общих свойств кодов, влияющих на РО, проводился в [37, 48, 49, 50, 51]. Однако перенесение полученных там результатов на пороговое декодирование затруднительно в связи с тем, что использовавшиеся в этих работах методы декодирования предполагали наличие декодеров, осуществляющих полный или почти полный перебор. Отметим только, что, как указывают некоторые авторы, при использовании несистематических кодов бороться с размножением ошибок оказывается на практике значительно сложнее, чем в случае применения систематических, даже если проводится тщательный отбор кодов.

Все основные исследования по размножению ошибок при пороговом декодировании состояли до недавнего времени в выборе достаточно реального способа определения длины зоны размножения и поиске этого параметра для различных кодов. Его значение определяло максимальную длину пакета ошибок на выходе ПД при некоторых ограничениях, налагаемых на канал или декодер, после того, как произошла первая ошибка.

В работах [19, 20, 52, 53, 54, 55] вводились различные определения длины зоны РО и была доказана её конечность для различных классов кодов при использовании ПД. Во всех случаях предполагалось, что после первой ошибки декодера канал или сам ПД переходили в другое состояние и оставались в нем до прекращения генерации ошибочных решений декодера. Это были очень полезные результаты для начального этапа анализа свойств ПД 70-х годов прошлого века.

Но, с другой стороны, такой искусственный подход не может обеспечить качественный анализ поведения декодера в реальном канале при достаточно большом уровне шума. В связи с этим ниже предлагается достаточно общий метод оценки размножения ошибок декодирования, основанный на использовании производящих функций вероятности (ПФВ) [4, 9, 56, 57, 76], которая применяется к двум классам свёрточных кодов, допускающих мажоритарное декодирование, а также к блоковым кодам. Эти оценки непосредственно зависят от уровня шума канала. Такой подход позволяет сделать реальные оценки характеристик и выработать действенные рекомендации по минимизации исследуемого эффекта РО. Именно в такой постановке решается задача приближения эффективности МПД к возможностям ОД.

При этом нужно, вообще говоря, различать две совершенно различные причины группирования ошибок декодера. Первая в каналах без памяти обусловлена выбранным алгоритмом декодирования и его особенностями: наличием обратной связи на регистр синдрома декодера, правилом принятия последовательных решений о необходимости коррекции, способом ортогонализации проверок или выбором величины порогов.

Второй причиной оказываются свойства самого используемого кода. Например, в коротких свёрточных кодах несистематического типа есть обычно много кодовых слов веса порядка d, что и приводит к группированию ошибок на выходе декодера, реализующего алгоритм Витерби, который является оптимальным для этих кодов.

Большая трудность в улучшении характеристик МПД состоит именно в том, чтобы учесть свойства и кода, и самой мажоритарной процедуры принятия решений для максимального уменьшения числа и вероятности появления тех ошибок, которые МПД и ОД декодируют с различными результатами. При этом нужно сохранить предельную простоту и однородность мажоритарного алгоритма, обеспечивая рост эффективности фактически лишь посредством увеличения числа совершенно одинаковых операций или элементов декодера и выбором хороших кодов.

Указанный подход к явлению РО оказался достаточно продуктивным для самоортогональных и равномерных свёрточных кодов [9, 57]. На основе многомерных производящих функций вероятности (ПФВ) удалось вычислить условные вероятности ошибки декодирования или их оценки $P(e_j{=}1/e_0{=}1)$ в j-ом символе, $j > 0$, если имеет место неправильное решение декодера относительно символа i_0. Полученные результаты в свою очередь оказались полезными при поиске кодов с малым РО и созданием МПД с низким уровнем группирования ошибок на первых пороговых элементах декодера. Ниже будут рассмотрены основные результаты, относящиеся к анализу РО в свёрточных и блоковых кодах для двоичных, недвоичных и других каналов, что позволит сформулировать критерии поиска кодов с наиболее подходящими для МПД свойствами и сравнить уровни РО в блоковых и свёрточных кодах.

3.2. Размножение ошибок в свёрточных самоортогональных кодах

Свёрточные коды, в которых множества $\{S_k\}$ всех символов синдрома $\overline{S}$, содержащих в качестве слагаемого ошибку e_k в некотором информационном символе i_k, образуют ортогональ-

ные относительно e_k проверки, называются самоортогональными [4].

Обширные множества самоортогональных кодов (СОК) для большого диапазона скоростей передачи с различными минимальными расстояниями предложены в [4, 20, 21, 22, 23, 58], а результаты моделирования этих кодов и их параметры в реальных каналах представлены в [20, 23]. Основной особенностью СОК является отсутствие этапа формирования сложных проверок относительно декодируемых символов, что несколько упрощает реализацию соответствующего им декодера.

В [9, 57] были введены ПФВ, которые позволили находить оценки вероятностей совместных ошибок в информационных символах i_0 и i_j, $j > 0$, при мажоритарном декодировании свёрточных кодов.

Ниже будет предложена нижняя оценка вероятности появления одиночной ошибки свёрточного ПД, использующая основное свойство СОК, согласно которому каждая ошибка канала может входить не более чем в одну проверку относительно любого из декодируемых символов.

Рассмотрим СОК с некоторыми значениями кодовой скорости R, длины кодового ограничения n_A и минимального кодового расстояния d. Введем производящую функцию вероятности вида $A_{m,k}(x,y) = (p_0 x_m y_k + q_0)$ для символа i_j, ошибка e_j которого входит в m-ю проверку относительно символа i_0 и в k-ю проверку относительно i_l, $l = 1, 2,....$ Если некоторая ошибка e_x канала отсутствует в проверках относительно i_0 или i_l, то её ПФВ имеет соответственно вид $A_k(y) = p_0 y_k + q_0$ или $A_m(x) = p_0 x_m + q_0$.

Индекс 0 в x_0 и y_0 будет использован для декодируемого в данный момент символа i_0 и символа i_l, $l > 0$, соответственно.

Отметим, что метод ПФВ был успешно адаптирован для вычисления вероятности ошибки в первом символе свёрточного кода Дж. Месси в классической книге [4]. Но там был использован одномерный вариант этого мощного средства вероятностных вычислений. Применяемые в данной главе ПФВ будут многомерными, что и позволит получать новые результаты в области размножения ошибок.

Введем далее правило вычисления ПФВ для двух ошибок канала e_1 и e_2. Если в двух ПФВ, относящихся к e_1 и e_2, есть переменные x и y с одинаковыми индексами, то ПФВ для этой пары находится перемножением ПФВ для символов e_1 и e_2, причем, показатели степеней переменных с одинаковыми индексами суммируются по mod 2. Для большего числа ошибок это правило также сохраняется. Такой вид операций с индексами обусловлен тем, что наличие одинаковых индексов соответствует случаю, когда ошибки входят в одну и ту же проверку относительно некоторой информационной ошибки. При этом значение проверки не может быть более чем 1, а добавление новой ошибки увеличивает вероятность того, что проверка будет искажена.

Сделаем два существенных замечания. Для оценки размножения ошибок нужно учесть, что при $e_0 = 1$, т.е. при ошибке ПД в первом символе кода через обратную связь в декодер попадает пакет ошибок. Поскольку в СОК проверки ортогональны и с учётом наличия ошибок декодирования (см. [19] и раздел 1.2), то для последующих вычислений удобно считать, что через обратную связь изменяются проверочные символы, которые входят в соответствующие проверки относительно e_0. ПФВ для такого символа есть

$A_{m,k}(x, y) = p_0 x_m + q_0 y_k$.

Далее, для ошибки e_0 символа i_0 ПФВ должна иметь вид

$A_0(x) = p_0 x_0 + q_0$,

поскольку эта ошибка отсутствует в проверках относительно последующих символов $i_j, j > 0$.

Предложенные ПФВ позволяют вычислить совместную вероятность $P(e_0=1,\ e_1=1)$. Если записать произведение всех ПВФ, которые относятся к символам, входящим во все проверки относительно e_0 и e_1, то получим

$$A_{0,1}(x, y) = \prod_{m,k=0}^{J} A_{m,k}(x, y) = \sum_{k=0}^{2^{2d}} a_k \prod_{i=0}^{J} x_i^{m_i} \prod_{j=0}^{J} y_j^{n_j} , \qquad (3.1)$$

где показатели степени m_i и n_j равны 0 или 1.

Общее число ненулевых слагаемых в (3.1) не превышает 2^{2d}. Показатели степени при x_i и y_j относятся к сочетаниям ошибок

канала, которые с вероятностью a_k искажают $\sum_{i=0}^{J} m_i$ и $\sum_{j=0}^{J} m_j$ проверок относительно i_0 и i_1 соответственно.

Поскольку в (3.1) важно общее число сомножителей, то, избавляясь от индексов при x и y, получаем

$$A_{0,1}(x, y) = \sum_{i,j=0}^{d} a_{i,j} x^i y^j,$$

где $a_{i,j}$ – вероятность того, что в проверках относительно i_0 будет i ошибок, а относительно i_1 – j ошибок. Тогда получаем, что

$$P(e_0 = 1, e_1 = 1) = \sum_{i,j>T} a_{i,j} \ . \qquad (3.2)$$

Опишем теперь метод вычислений нижней оценки вероятности $P(e_0=1, 0)$, т.е. вероятности появления одиночной ошибки декодирования, которая окажется наиболее существенной для дальнейшего анализа.

Рассмотрим ПД с «джином» [57, 60], который работает таким образом, что через цепь обратной связи в регистр синдрома S после неправильного декодирования первого символа i_0 посылается неправильное значение e_0, а после декодирования всех прочих символов i_j, $j > 0$, посылаемое значение e_j истинно.

Ясно, что при ошибке $e_0 = 1$ обычный ПД и ПД с «джином» (ПДД) имеют совпадающие вероятности $P(e_0=1, e_j=1)$, поскольку перед декодированием i_j, $j > 0$, состояния обоих декодеров также одинаковы.

Единственной особенностью вычисления вероятностей $P(e_0=1, e_1=1)$ для ПДД состоит в том, что согласно свойству этого декодера ошибки в информационных символах i_{j-k}, $0 < k < j$ отсутствуют в проверках относительно e_j и поэтому для всех этих ошибок e_{j-k} ПФВ имеют вид

$A_m(x) = (p_0 x_m + q_0)$,

независимо от того, входят ли ошибки в этих символах в проверки относительно e_j или нет.

Такого изменения ПФВ достаточно для вычисления всех вероятностей ошибок ПДД вида $P(e_0=1, e_j=1)$, $j > 0$ по методике, рассмотренной выше для обычного ПД. Суммируя все эти вероятности появления пакета ошибок ПДД веса 2 и более

$$P(e_0 = 1,1) = \sum_{j=1}^{Rn_A} P(e_0 = 1, e_j = 1)$$

получаем, что $P(e_0=1,\ 0) = P_1(e)$ – $P(e_0=1,\ 1)$ – нижняя оценка вероятности появления одиночной ошибки ПДД. Здесь $P_1(e)$ – вероятность первой ошибки декодирования, определяемая с помощью одномерной ПФВ [4].

Отметим теперь, что на всех тех потоках ошибок канала, которые включены в оценку $P(e_0=1,0)$, обычный ПД и ПДД ведут себя одинаково. Но это значит, что эта оценка справедлива и для обычного ПД.

Полученные оценки можно непосредственно применить, например, к СОК с $R = 1/2$, $n_A = 14$ и $d = 5$ с порождающим полиномом $P = (0, 1, 4, 6)$ [9].

В частности, вычисление $P(e_0=1, e_1=1)$ для этого кода следует проводить, используя ПФВ вида

$$A_{0,1}(x,y) = (p_0x_0 + q_0)(p_0x_1 + q_0)(p_0x_2 + q_0y_1)(p_0x_2y_0 + q_0)\cdot$$
$$\cdot(p_0x_3y_4 + q_0)(p_0x_3y_3 + q_0)(p_0x_3 + q_0)(p_0x_4y_2 + q_0)\cdot$$
$$\cdot(p_0x_4y_3 + q_0)(p_0x_4y_4 + q_0)(p_0x_4 + q_0)(p_0y_2 + q_0)(p_0y_3 + q_0)\cdot$$
$$\cdot(p_0y_4 + q_0)(p_0y_4 + q_0) = \sum_{m,n=0}^{15} p_0^m q_0^n \prod_{i=0}^{d} x_i^{m_i} \cdot \prod_{j=0}^{d} y_j^{n_j}.$$

Тогда в соответствии с (3.2) при не очень большом шуме канала задача вычисления $P(e_0=1,\ e_1=1)$ сводится к суммированию слагаемых вида

$$p_0^3 \prod_i x_i^{m_i} \prod_j y_j^{n_j}, \qquad (3.3)$$

где количество различных сомножителей вида и x_i, и y_j не менее трех. С учетом только существенных членов получаем, что искомый результат равен $27p_0^3$.

Проводя аналогичные расчеты для $P(e_0=1,\ e_j=1)$, $2 \le j \le 4$ можно вычислить и все эти вероятности. Для случая малого шума они равны $8p_0^3$. При $j > 4$ оказалось, что рассматриваемые совместные вероятности имеют порядок p_0^4 и, следовательно, при малом шуме их вклад в оценку размножения ошибок несущественен.

Тогда верхняя оценка вероятности появления пакетов ошибок веса 2 и более равна

$$P(e_0 = 1,1) = \sum_{j=1}^{4} P(e_0 = 1, e_j = 1) = (27 + 8 + 8 + 8)\, p_0^3 = 51 p^3.$$

Так как вероятность ошибки в первом символе рассматриваемого свёрточного кода равна $P_1(e) = P(e_0{=}1) = 85 p_0^3$, то нижняя оценка вероятности одиночной ошибки в первом символе $P_{1i}\ (e_0 = 1,0) = P_1(e) - P(e_0 = 1,1) = 34 p_0^3$.

Поскольку вероятность $P(e_0{=}1,\ e_1{=}1)$ была вычислена выше точно, то вероятность появления одиночной ошибки оценивается сверху соотношением $P_B(e_0{=}1,0) = P_1(e) - P(e_0{=}1,\ e_1{=}1) = {=}58 p_0^3$. Следовательно, вероятность появления одиночной ошибки ПД лежит между $34 p_0^3$ и $58 p_0^3$. Поскольку лучшие СОК с $d = 5$ имеют вероятность ошибки оптимального декодирования, которая, как можно проверить, при малых значениях p_0 равна $10 p_0^3$, получаем, что одиночные ошибки в рассматриваемом ПД можно исправлять, т.к. такие ошибки в ОД возникают в 4÷5 раз реже, чем у ПД.

Представляется интересным сравнить результаты проведенного выше расчета размножения ошибок с поведением ПД при моделировании работы декодера в ДСК без памяти. Результаты моделирования показали, что при весьма высоком шуме канала, когда $p_0 = 0{,}05$, доли одиночных ошибок и пакетов ошибок веса 2÷5 примерно равны, а средняя вероятность одиночных ошибок близка к $40 p_0^3$. При уменьшении шума до $p_0 = 0{,}02$ вероятность одиночных ошибок оценивается как $45 p_0^3$. Как видно, оценки размножения ошибок выполнены с точностью, достаточной для практических целей: вероятности одиночных ошибок лежат примерно посередине между верхней и нижней оценками.

Следует указать на то, что рассмотренный код является наихудшим с точки зрения размножения ошибок, так как в каждой из проверок относительно декодируемых символов обязательно присутствуют все ошибки в информационных символах в пределах длины кодового ограничения. Можно построить

много других кодов, в несколько меньшей степени подверженных размножению ошибок, поскольку проверки в этих кодах будут менее зависимы друг от друга. Однако даже для сколь угодно длинных кодов с $R = 1/2$ и $d = 5$ нельзя уменьшить совместную вероятность ошибки в двух первых символах для малого шума ниже уровня $23p_0^3$.

Дальнейшее уменьшение размножения ошибок возможно при переходе к переменным во времени кодам. Например, среди кодов длины $n \sim 1000$ при $R = 1/2$ и $d = 5$ можно найти коды с 5÷8 вариантами столбцов проверочной матрицы такие, что для них вероятность появления двух ошибок в пределах длины кодового ограничения свёрточного кода будет порядка p_0^4. Это значит, что условная вероятность появления второй ошибки после первой в пределах длины кодового ограничения имеет вероятность порядка p_0, т.е. падает с уменьшением уровня шума, а соответственно вероятность одиночных ошибок стремится к 1. Иначе говоря, при использовании в ПД этого кода при достаточно малом шуме все его ошибки окажутся одиночными. Это обстоятельство очень необычно для простого порогового декодирования, когда обычно ошибки ПД заметно группируются.

Аналогичные характеристики уровня размножения ошибок в кодах могут быть получены и для более высоких значений d при любых значениях R.

3.3. Блоковые самоортогональные коды

Ниже рассмотрены аналогичные оценки размножения ошибок для блоковых СОК.

Пусть задан самоортогональный квазициклический блоковый код с кодовой скоростью $R = 1/2$, расстоянием $d = 5$, длиной $n = 26$ и порождающим полиномом $P = (0, 1, 4, 6)$, который уже использовался в качестве примера в предыдущем параграфе.

Для вычисления совместной вероятности $P(e_0=1, e_1=1)$ ошибок ПД с обратной связью в двух первых символах i_0 и i_1 требуется выписать произведение ПФВ для всех ошибок, которые входят в проверки хотя бы относительно одного из i_0 или i_1:

$$A_{0,1}(x,y) = (p_0x_0 + q_0)(p_0x_2y_0 + q_0)(p_0x_4y_2 + q_0y_1)(p_0x_3y_4 + q_0)\cdot$$
$$\cdot(p_0x_3y_3 + q_0)(p_0x_4y_3 + q_0)(p_0x_4y_4 + q_0)(p_0x_1y_4 + q_0)(p_0x_2y_1 + q_0)\cdot$$
$$\cdot(p_0x_1y_2 + q_0)(p_0x_2y_1 + q_0)(p_0x_3y_2 + q_0)(p_0x_1y_3 + q_0)(p_0x_1 + q_0)\cdot \quad (3.4)$$
$$\cdot(p_0x_3 + q_0)(p_0x_4 + q_0)(p_0y_2 + q_0)(p_0y_3 + q_0)(p_0y_4 + q_0)(p_0x_2 + q_0y_1)$$

Используемые здесь индексы при x и y также, как и в случае свёрточных кодов, соответствуют номерам проверок, в которые входит тот или иной символ при декодировании i_0 или i_1 согласно матрице (1.7). Нулевые индексы соответствуют тривиальным проверкам кода.

После упрощений, аналогичных оценкам версии для соответствующего свёрточного кода с тем же порождающим полиномом, получим, что для блокового кода

$P_{1,1}(e) = P(e_0{=}1,\, e_1{=}1) = 87p_0^3$.

Напомним, что для свёрточного кода с тем же порождающим полиномом вероятность $P_{1,1}(e)$ равна $27p_0^3$.

Графики зависимости вероятности ошибки в первом символе $P_1(e)$ и в двух первых символах $P_{1,1}(e)$ блокового кода от вероятности p_0 в ДСК представлены кривыми 1 и 2 на рис. 3.1. Оба графика достаточно близки, что соответствует одинаковому степенному уменьшению этих вероятностей с улучшением качества канала по закону, близкому к p_0^3.

Если же в (3.4) первый сомножитель заменить на $(p_0x_0y_1{+}q_0)$, а последний – на $(p_0x_2y_1{+}q_0)$, то будет получена ПФВ дефинитного, без обратной связи ПД [19]. Кривая 3 соответствует вероятности $P_{1,1}(e)$ для такого декодера.

Графики условной вероятности ошибки ПД во втором символе кода при наличии ошибки декодера в первом

$$P_{1/1}(e) = P(e_0 = 1/e_1 = 1) = P(e_0 = 1, e_1 = 1)/P_1(e) \qquad (3.5)$$

для ПД с обратной связью и дефинитного декодера (кривые 4 и 5 соответственно) на рис. 3.1 показывают, что вероятности $P_{1,1}(e)$ в хорошем канале фактически не зависят от p_0.

Отметим также для сравнения, что средняя вероятность ошибки и вероятность $P_1(e)$ дефинитного ПД свёрточного кода совпадает с вероятностью $P_1(e)$ и для блокового. Но в свёрточ-

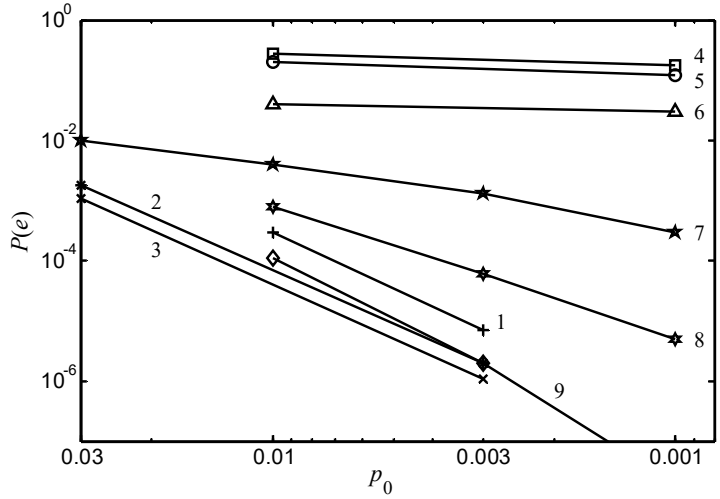


Рис. 3.1. Размножение ошибок в ПД при различных уровнях шума в ДСК для самоортогональных кодов

ном коде с обратной связью вероятность $P_1(e)$ близка к $85p_0^3$ и лежит между кривыми 2 и 3 на рис. 3.1.

Уменьшение РО возможно при росте n и фиксированном значении d. Кривая 6 показывает предельную зависимость вероятности $P_{1/1}(e)$ для ПД с обратной связью от p_0 при использовании кода сколь угодно большой длины с $d = 5$ и $R = 1/2$. Как следует из её вида вероятность $P_{1/1}(e)$ для любого квазициклического кода с $R = 1/2$ при $p_0 \to 0$ оказывается постоянной величиной, т.к. $P_{1,1}(e)$ и $P_1(e)$ имеют при этом одинаковый порядок малости, как и в случае коротких кодов. Это свойство сохраняется для всех самоортогональных кодов с $R = k/(k+1)$, $k = 1, 2, \ldots$

Дальнейшее уменьшение РО возможно при переходе к кодовым скоростям вида $R = mk_0/mn_0$, где m – некоторое небольшое целое число. Кривая 7 соответствует вероятности $P_{1/1}(e)$ для ПД с обратной связью квазиклического достаточно длинного самоортогонального блокового кода с $R = 4/8$ и $d = 5$, найденного на компьютере программным путём.

Ещё один пример кода с малым уровнем РО был также найден с помощью другой специально написанной программы. Коды такого типа могут быть названы также кодами с переменными связями [57]. Построенный свёрточный код представлен кривой 8 для $P_{1/1}(e)$ при $R = 6/12$, $d = 7$ и $n \approx 40000$. Как следует из вида последней кривой, вероятность $P_{1/1}(e)$ для этого кода с переменными связями убывает по закону $\sim p_0^2$ для малых p_0. Для сравнения приведен также график 9 вероятности $P_1(e)$ ошибки в первом символе этого кода.

Как следует из анализа графиков на рис. 3.1, размножение ошибок как степень группирования пар ошибок на выходе мажоритарной схемы декодирования вполне однозначно зависит от степени пересечения множеств ошибок, входящих в проверки относительно разных информационных символов, а также от уровня шума канала. В некоторых пределах группирование можно снижать выбором более длинных кодов при фиксированных значениях минимального кодового расстояния d. Однако эти возможности для снижения уровня РО довольно ограничены. Качественно новый уровень снижения этого эффекта может быть достигнут при переходе к кодам с переменными связями, хотя для этого коды должны быть на два и более порядков длиннее, чем необходимо для построения обычных достаточно коротких СОК с теми же значениями d. Нужно отметить, что простое применение кодов с переменными связями также оказывается лишь частичным решением проблемы снижения уровня РО.

Таким образом, качественное проявление эффекта РО в блоковых СОК оказывается таким же, как и в свёрточных кодах подобного типа.

Все основные сведения по размножению ошибок в блоковых и свёрточных кодах с $R = 1/2$ и $d = 5$ при наличии обратной связи и для дефинитных вариантов декодирования, т.е. без обратной связи сведены в таблицу 3.1. В неё внесены параметры кодов, которые обсуждались в данном разделе, а также данные о свёрточных кодах. Разделение дефинитных декодеров на две группы по признаку начала или середины кода связано с тем, что в начале процедуры декодирования свёрточных кодов в про-

верках дефинитного декодера отсутствуют ошибки в тех символах, которые уже были декодированы, что приводит к более высокой достоверности декодирования свёрточного кода в начале сообщения, а, начиная с информационного символа i_6 для короткого кода (полагая, что первым был i_0), размерности всех проверок и вероятности ошибок ПД становятся максимальными. Как уже было показано, для рассматриваемых кодов вероятность ошибки в первом символе $P_1(e)$ и в двух первых символах для малого шума имеют оценки вида ap_0^3, где p_0 – вероятность ошибки в ДСК. В таблице указаны величины коэффициентов a: в числителе – для $P_{1,1}(e)$, а в знаменателе – для $P_1(e)$. Тогда значение дроби в каждой клетке соответствует вероятности $P_{1/1}(e)$ для малых значений p_0.

Т а б л и ц а 3.1. Сравнение блоковых и сверточных кодов с $R = 1/2$, $d = 5$ по критерию размножения ошибок

Тип кода / Наличие ОС	Свёрточный, $n_A = 14$	Блоковый, $n = 26$	Свёрточный длинный	Блоковый длинный
Обратная связь	$\frac{27}{85} = 0{,}32$	$\frac{87}{352} = 0{,}25$	$\frac{10}{85} = 0{,}118$	$\frac{16}{352} = 0{,}045$
Дефинитное начало	$\frac{17}{85} = 0{,}20$	$\frac{58}{352} = 0{,}16$	–	–
Дефинитная середина	–	–	$\frac{7}{352} = 0{,}020$	–

Наиболее существенным результатом сопоставления кодов по таблице является уменьшение эффекта РО с увеличением длины. Кроме того, при сопоставлении свёрточных кодов оказывается, что декодер с обратной связью по вероятности появления пар ошибок менее чем в полтора раза уступают дефинитному ПД. Учитывая, что для ПД с обратной связью средняя вероятность ошибки $P_{ср}$ не намного выше, чем $P_1(e)$ и меньше, чем у дефинитного ПД, можно утверждать, что использование дефинитных декодеров нецелесообразно, т.к. они имеют более слабые характеристики по достоверности, а размножение оши-

бок снижают лишь незначительно. Правда, из-за существенно худшей средней вероятности ошибки декодирования $P_{ср}$ вероятность $P_{1/1}(e)$ у дефинитного ПД всегда меньше. Но это не столь существенно для решения вопроса об использовании тех или иных алгоритмов. Полученные основные соотношения между вероятностями группирования ошибок справедливы и для кодов с более высокими значениями d при $R = k/(k+1)$, $k = 1, 2, \ldots$

Проведенный анализ является свидетельством действительной сложности эффекта РО и демонстрирует необходимость аккуратного анализа и правильной интерпретации изучаемых явлений.

Рассмотренный здесь подход к РО через двумерные ПФВ оказывается довольно общим и позволяет при переходе к ПФВ более высоких размерностей оценивать и вероятности появления групп из трех, четырех и большего числа ошибок декодера на любых конкретных позициях блока. В принципе, перебирая все возможные сочетания ошибок ПД можно вычислить и точное значение вероятностей ошибки на символ, на блок или их среднего значения на некотором расстоянии от начала свёрточного кода. В отдельных случаях можно уменьшить объем вычислений, если определять, наоборот, вероятности одного, двух и более подряд правильных решений ПД также методами многомерных ПФВ.

Вместе с тем, целесообразно ограничиться анализом появления наиболее частых сочетаний ошибок, которые и определяют основные конфигурации ошибок в ошибочно декодированных блоках.

Достаточным для большинства случаев поиска хороших кодов оказывается рассмотрение вероятностей появления пакетов ошибок декодера веса не более чем 3. Соответствующие программные средства, учитывающие эти критерии, были разработаны и применялись для построения кодов с требуемым малым уровнем РО.

3.4. Интегральные оценки размножения ошибок

Выше были предложены методы оценки РО свёрточного кода, состоящие в построении верхних оценок условной вероятности появления второй ошибки в пределах длины кодового ограничения, если произошла ошибка в первом символе.

Рассмотрим на основе такого подхода метод оценки РО в блоковом коде как верхнюю оценку вероятности появления не менее двух ошибок декодера в принятом блоке. Он также основывается на идее анализа гипотетического порогового декодера с «джином» (ПДД), который «подсказывает» пороговому декодеру, какие истинные символы следует направлять через обратную связь в регистр синдрома, независимо от решения порогового элемента о текущем декодируемом символе [9, 57]. Для такого ПДД легко оцениваются вероятности появления небольшого числа ошибок декодера, через которые оцениваются и свойства реального ПД.

Пусть необходимо оценить вероятность ошибок ПД в m-м и j-м символах, $m < j$, полагая, что в других информационных символах i_l, $l \neq \mathrm{m}$, $l \neq j$ решения декодера несущественны.

Построим ПФВ $A_{mj}(x,y)$ для ПДД, содержащую элементарные ПФВ тех ошибок, которые входят хотя бы в одну из систем проверок относительно i_m или i_j. Они должны удовлетворять свойствам, следующим из определения ПДД: ошибки в информационных символах i_l, $l < m$, участвующих в проверках относительно i_m и i_j отсутствуют, а ошибки e_n, $m < n < j$, есть только в проверках относительно i_m и, значит, имеют ПФВ вида $(p_0x_s+q_0)$, где s – номер проверки относительно символа i_m. Отметим, что поскольку при $m > 0$ в проверках отсутствуют ошибки во всех информационных символах i_l, $l < m$, то при прочих равных условиях вероятности ошибки $P_{m,j}(e)$ для ПДД в символах i_m и i_j всегда будут не больше, а обычно меньше, чем для пар символов i_0 и i_{j-m}.

Заметим, что можно анализировать и такой ПДД, который обладает свойством обеспечивать при декодировании символов i_m и i_j поступление через обратную связь в регистр синдрома реального решения порогового элемента, тогда как во все осталь-

ные моменты через обратную связь поступают истинные значения ошибок в декодируемых символах. Именно он и будет рассматриваться далее.

Сравним теперь различные реализации векторов шума $\overline{E}$ при использовании введенного выше ПДД. Часть этих векторов будет такова, что для конкретных выбранных значений m и j, $0 \le m < j$, ошибки ПДД произойдут только в информационных символах именно с этими номерами. Сопоставим поведение ПД и ПДД на тех векторах шума $\overline{E}_{m,j}$, которые приводят к ошибкам ПДД именно в i_m и i_j, а поведение ПДД после декодирования i_j будем считать несущественным. Из правила работы ПДД следует, что на векторе $\overline{E}_{m,j}$ решения ПДД совпадают с решениями его пороговых элементов для всех i_l, $0 \le l \le j$. Но тогда на векторе $\overline{E}_{m,j}$ для всех символов с номерами $0 \le l \le j$ обычный ПД ведет себя аналогично ПДД.

Вычислим теперь для некоторого блокового СОК с k информационными символами все возможные вероятности $P_{m,j}(e)$ соответствующего ему ПДД. Определим

$$P_2(e) = \sum_{\substack{m,j \\ m<j}} P_{m,j}(e) . \qquad (3.6)$$

Покажем, что $P_2(e)$ – верхняя оценка вероятности появления двух и более ошибок в блоке рассматриваемого кода при использовании обычного ПД. В самом деле, пусть при некотором произвольном векторе $\overline{E}$ ПД сделал более одной ошибки в символах i_m, i_j, i_p, …, $m < j < p <$ …, причем третья, четвертая и прочие ошибки ПД, если они есть, сделаны в символах с номерами большими, чем j. Разумеется, наличие третьей и последующих ошибок допустимо, но не обязательно. Но тогда вектор $\overline{E}$ относится к векторам класса $\overline{E}_{m,j}$ и вероятность этого события из не менее двух ошибок ПД входит в оценку сверху (3.6), которая содержит все вероятности вида $P_{m,j}(e)$.

Наконец, можно рассматривать и нижнюю оценку $P_{1НБ}$ вероятности наличия не более одной ошибки в блоке, равную

$$P_{1НБ} = 1 – P_2(e). \qquad (3.7)$$

Полученные соотношения представляют достаточно полную интегральную характеристику РО конкретного блокового СОК при мажоритарном декодировании и позволяют отбирать коды, обладающие малой степенью группирования ошибок, т.е. низким уровнем РО. Аналогичные вероятности можно использовать для свёрточных кодов при нижних оценках одиночных $P_{1НС}$ и двойных ошибок $P_{2С}(e)$ на длине $n_А$.

На рис. 3.2 представлены верхние оценки вероятностей двух ошибок в блоке $P_2(e)$ и появления ошибочного блока $P_В(e)$ для кода с $R = 4/8$, $d = 5$ и $n = 1480$.

3.5. Группирование ошибок в равномерных кодах

В [60] была предложена оценка вероятностей появления ошибок на любом месте пакета в равномерном свёрточном коде. Ниже будет изложена улучшенная методика получения более точных оценок вероятностей ошибок на разных позициях пакета и показано, что с уменьшением шума канала доля одиночных ошибок может быстро возрастать по сравнению с долей пакетов веса 2 и более.

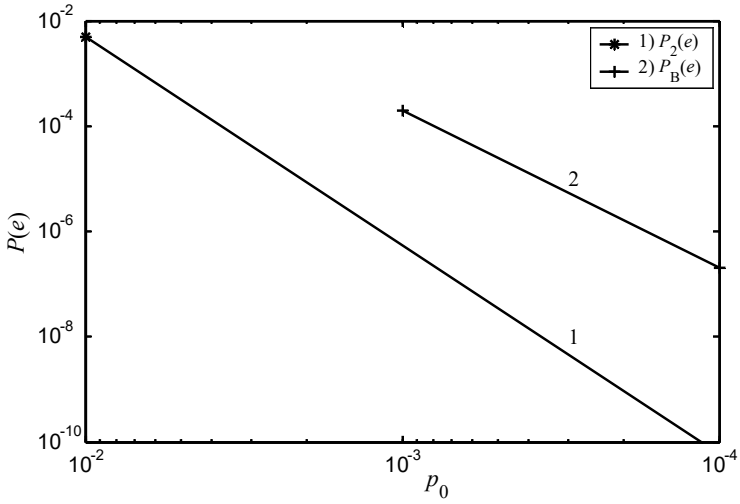


Рис. 3.2. Верхние оценки вероятностей появления двух ошибок ПД и ошибочного блока длины $n = 1480$

Рассмотрим двоичный систематический равномерный свёрточный код [4, 39]. Для любого $m = 1, 2, 3,...$ существует такой код с параметрами

$R = 2^{-m} = 1/n_0$, $n_A = (m+1)n_0$, $d = (n_A+n_0)/2$.

Значение d является максимально возможным среди всех кодов с заданными R и n_A. Эти коды допускают полную ортогонализацию, причем многими способами, если m велико [39].

Лучшая схема ортогонализации проверок для этих кодов была предложена в [39] как для случая ПД с обратными связями на синдром, так и без обратных связей в случае прямого (дефинитного) декодирования, рассмотренного ранее для самоортогональных кодов [19].

Для кодов с заданным m можно рассматривать только часть проверочной матрицы H, соответствующую начальному кодовому слову, так как более удаленные от первого символа части кодового слова не оказывают влияния на решение ПД.

Тогда подматрица P^T матрицы H состоит из $(n_0–1)$ треугольников, расположенных один под другим. Каждый треугольник состоит из $(m+1)$ столбцов, получаемых сдвигом вниз на одну позицию последнего из добавленных столбцов и отбрасыванием нижнего символа в новом столбце. Первые столбцы в каждом треугольнике – все возможные столбцы с единицей в верхней позиции и хотя бы одной единицей в прочих. Ниже приводится проверочная матрица H кода с $m = 2$ и $R = 1/4$, $n_A = 12$, $d = 8$:

$$H = \left(\begin{array}{cccc} 1 & & & \\ 1 & 1 & & \\ 0 & 1 & 1 & \\ & & & \\ 1 & & & \\ 0 & 1 & & : \quad I \\ 1 & 0 & 1 & \\ & & & \\ 1 & & & \\ 1 & 1 & & \\ 1 & 1 & 1 & \end{array}\right).$$

Пусть $e_{i,k}$ – i-я ошибка k-го кодового подблока свёрточного кода, $k = 0, 1, 2,...$, причем $e_{1,k}$ ошибка в информационном символе. Правило формирования оптимальных в смысле размножения ошибок сложных проверок [39] может быть сформулировано так:

а) в каждую сложную проверку размерности 2 входят 2 ошибки с одинаковыми номерами $k > 0$;

б) разность номеров i_1 и i_2 двух ошибок, входящих в проверку, равна 2^{k-1}.

Для получения таких проверок необходимо произвести сложение по mod 2 тех компонент синдрома $\overline{S}$, которые содержат ошибки с номерами, удовлетворяющими пунктам а) и б). В связи с тем, что число проверочных символов в блоке нечетно, в каждом k-ом блоке, $k > 0$, остается по одной простой проверке из компонентов синдрома с номерами $(2^{k-1}+1, k)$ для всех $0 < k \le m$. Они тоже образуют проверки размерности 2.

Такая ортогонализация соответствует наличию $(n_0–1)$ проверок размерности 1 и $mn_0/2$ проверок размерности 2.

Следуя [56, 60] можно с помощью двумерных производящих функций вероятности построить верхние оценки вероятности появления пакета ошибок.

Уточним вид одной из таких функций, используемых для вычисления совместной вероятности ошибки декодирования $P(e_0=1, e_1=1)$ в двух первых информационных символах кода. При этом окажется возможным получить точное выражение для этой вероятности по сравнению с оценкой, предложенной в [60].

Улучшаемая ПФВ имеет вид

$$A_7(x, y) = p_0^2 y + p_0 q_0 x + p_0 q_0 x y^2 + q_0^2 y, \qquad (3.8)$$

где p_0 – вероятность ошибки в ДСК, $q_0 = 1–p_0$. Этот сомножитель относится к информационной ошибке $e_{1,1}$, а также к ошибке в проверочном символе $e_{2,1}$.

Для вычисления точного значения вероятности $P(e_0=1, e_1=1)$ следует учесть, что в [60] при вычислении верхней оценки $P(e_0=1, e_1=1)$ занижалось значение порога T, что обуславливало включение в оценку некоторых сочетаний ошибок канала, которые не приводят к ошибке $e_1=1$ в информационном символе i_1 после ошибки $e_0=1$ в i_0.

Перебором четырех возможных комбинаций из двух ошибок, для которых строилась рассматриваемая ПФВ, может быть введена новая точная функция

$$A_7'(x,y) = p_0^2 y^2 + p_0 q_0 x + p_0 q_0 x y^3 + q_0^2 y\ .$$

Тогда, если ввести обозначения

$$\begin{aligned}
&A_1(x,y) = (2p_0^2 q_0^2 x^2 y^2 + 2p_0^2 q_0^2 x^2 + 2p_0^2 q_0^2 y^2 + \\
&+ 4p_0 q_0 (p_0^2 + q_0^2) xy + p_0^4 + q_0^4),\\
&A_2(y) = 2p_0 q_0 y + p_0^2 + q_0^2,\\
&A_3(x) = p_0 x + q_0,\\
&A_4(x,y) = p_0^2 y + p_0 q_0 x + p_0 q_0 x y^2 + q_0^2 y,\\
&A_5(x) = p_0 x^2 + q_0,\\
&A_6(x) = 2p_0 q_0 x + p_0^2 + q_0^2,
\end{aligned} \tag{3.9}$$

то для кода с параметром m

$$P(e_0 = 1, e_1 = 1) = \sum_{i>T} \sum_{j>T} a_{i,j}\ ,\ T = d/2, \tag{3.10}$$

где $a_{i,j}$ определяются из выражения

$$\begin{aligned}
&A_{0,1}(x,y) = [A_1(x,y)]^{(m-1)2^{m-2}} \cdot [A_2(y)]^{2^{m-1}} \cdot [A_3(x)]^{2^m - 1} \cdot \\
&\cdot [A_4(x,y)]^{2^{m-1}-1} \cdot A_5(x) \cdot A_7'(x,y) = \sum_{i=0}^{d+1} \sum_{j=0}^{d+1} a_{i,j} x^i y^j .
\end{aligned} \tag{3.11}$$

Для того, чтобы вычислить верхнюю оценку вероятности ошибки в i_0 и i_2, а затем i_0 и i_m переход от $A_{0,(i-1)}(x,y)$ к $A_{0,i}(x,y)$ осуществляется заменой в $A_{0,(i-1)}(x,y)$ сомножителя $[A_1(x,y)]^{2^{m-2}}$ на $[B(x,y)]^{2^{m-2}}$, где

$$\begin{aligned}
&B(x,y) = (2p_0 q_0 x + p_0^2 + q_0^2)^2 (2p_0 q_0 y + p_0^2 + q_0)^2 = \\
&= [A_2(y)]^2 \cdot [A_6(x)]^2 .
\end{aligned}$$

После этого суммирование коэффициентов a_{ij} проводится в соответствии с (3.10).

Уровень размножения ошибок декодирования может быть охарактеризован условной вероятностью ошибки во втором символе пакета $P_{1/1} = P(e_1 = 1/e_0 = 1)$ при наличии ошибки в первом. Вероятности ошибок в последующих символах довольно

быстро убывают [60] и их влияние на число ошибок в пакете весьма невелико.

На рис. 3.3 приводится график полученных для $m = 3$ вероятностей $P_{1/1}$ при различных уровнях шума в канале (кривая 1), из которого видно, что относительная доля ошибок ПД типа (e_0=1, e_1=1) падает с уменьшением вероятности ошибки p_0.

Размножение ошибок, обусловленное ошибками, поступившими через обратную связь, следует отличать от размножения ошибок в схеме декодера с «джином» [39]. В последнем случае на каждом шаге декодирования вместо решения декодера через обратную связь в ячейки регистра синдрома S поступают истинные значения ошибок в соответствующих информационных символах. Пакетирование ошибок при использовании этого метода связано с тем, что в таком декодере первая ошибка декодирования $e_0 = 1$ происходит только в том случае, если их число больше T, т.е. превышает на длине кодового ограничения их среднее значение. Но тогда эти же совокупности ошибок при-

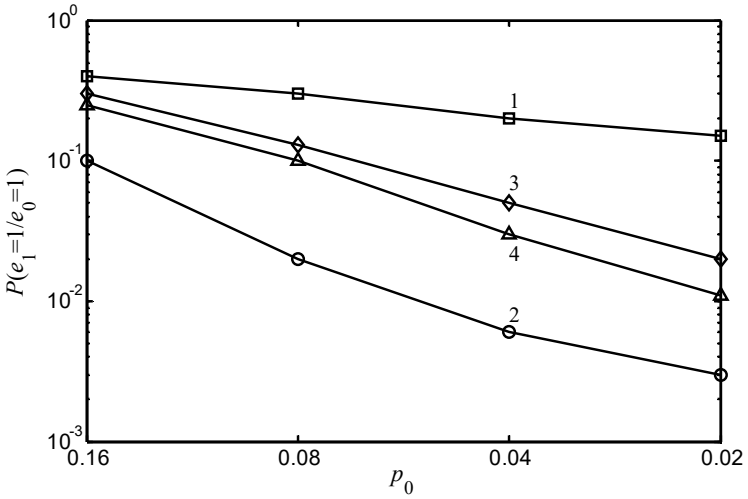


Рис. 3.3. Размножение ошибок декодирования в равномерном коде с $R = 1/8$

сутствуют, в основном, и на следующем шаге декодирования, увеличивая условную вероятность ошибки $e_1 = 1$.

Анализ производящих функций при декодировании с «джином» показал, что $P(e_0=1,\ e_1=1)$ для этого случая может быть вычислена заменой $A_4(x,y)$ из (3.9) на

$$A_4'(x,y) = p_0^2 y^2 + 2p_0 q_0 xy + q_0^2$$

и использованием тех же формул (3.11) для $a_{i,j}$.

Аналогичная оценка относительной доли пакетов ошибок вида ($e_0=1$, $e_1=1$) при декодировании с «джином» представлена для $m = 3$ на рис. 3.3 кривой 2.

Как следует из графика, влияние ошибок канала на вероятность появления пакета ошибок длины более 1 значительно меньше влияния ошибок, поступивших через цепь обратной связи в регистр синдрома. Поэтому для уменьшения размножения ошибок в обычном ПД была использована схема ортогонализации, также предложенная в [60], в которой, однако, отсутствовала обратная связь и декодирование было дефинитным. Эта связь была восстановлена, следствием чего было уменьшение вероятности $P_1(e)$. Кроме того, с целью уменьшения влияния ошибки декодирования соседнего символа в декодере была изменена одна проверка. В результате проверки относительно i_k не содержат ошибку в i_{k-1}, что должно значительно уменьшить размножение ошибок.

Пусть номера простых проверок $S_{i,0}$ совпадают с номерами входящих в них ошибок в проверочных символах. Тогда правило формирования из проверок $S_{i,0}$ размерности 1 сложных проверок $\gamma_{i,0}$, ортогональных относительно $e_{1,0}$ имеет для $m = 3$ следующий вид:

$$\gamma_{2,0} = S_{2,0} \oplus S_{5,-1};\ \gamma_{4,0} = S_{4,0} \oplus S_{2,-1};\gamma_{6,0} = S_{6,0} \oplus S_{3,-1};$$
$$\gamma_{7,0} = S_{7,0} \oplus S_{2,-1};\gamma_{8,0} = S_{8,0} \oplus S_{4,-1}.$$

Остальные проверки имеют тот же вид, что и в [60],

Перебирая все возможные сочетания ошибок канала, входящие в проверки относительно i_0 и i_1, построим производящие функции для вычисления $P(e_0=1,\ e_1=1)$ при $m = 3$. Введём обозначения

$$A_8(x,y) = p_0^2 q_0 x^2 y^2 + p_0^2 q_0 y^2 + p_0^2 q_0 x^2 + p_0(3q_0^2 + p_0^2)xy + q_0^3,$$

$$A_9(x,y) = p_0^2 q_0 x^2 y^3 + p_0(p_0^2 + q_0^2)xy^2 + p_0^2 q_0 y^3 +$$

$$+ p_0^2 q_0 x^2 + 2p_0 q_0^2 xy + q_0^3,$$

$$A_{10}(x,y) = (p_0^4 + p_0^2 q_0^2)y + p_0 q_0(p_0^2 + q_0^2)x + 2p_0^3 q_0 xy^2 +$$

$$+ p_0 q_0(p_0^2 + 3q_0^2)xy + p_0^2 q_0^2 x + p_0^2 q_0^2 x^2 y^2 + p_0^2 q_0^2 y^2 + q^4 +$$

$$+ 2p_0^2 q_0^2 x^2 y.$$

Тогда $P(e_0=1,\ e_1=1)$ при использовании ПД вычисляемся с помощью производящей функции

$$A'_{0,1}(x,y) = [A_1(x,y)]^5 [A_2(x,y)]^4 A_5(x,y)[A_6(x,y)]^3 A_8(x,y) \cdot$$

$$\cdot A_9(x,y) A_{10}(x,y).$$

с последующим суммированием коэффициентов $a_{i,j}$ согласно (3.10).

Результаты расчета условной вероятности ошибки $P_{1/1} = P(e_0=1,\ e_1=1)$ при $m = 3$ приведены на графике рис. 3.3 в виде кривой 3, которая свидетельствует о резком уменьшении размножения ошибок в этом случае по сравнению с обычной ортогонализацией (кривая 1) предложенной в [39].

Влияние ошибок декодирования, поступающих через обратную связь, на размножение ошибок можно проиллюстрировать с помощью следующего преобразования кода и декодера.

Пусть $(a_0, a_1, \ldots, a_m)^{\mathrm{T}}$ – первый столбец одного из проверочных треугольников кода. Тогда, если этот столбец преобразовать так, что между некоторыми элементами будут вставлены несколько нулей, то применение такой процедуры по всем столбцам приводит к некоторому коду с теми же значениями R и d, но большим n_{A}. Неизменность R и увеличение n_{A} следует из построения, а неизменность d определяется тем, что согласно правилу ортогонализации проверок в ПД в каждую проверку входят только ошибки, относящиеся к одному блоку n_0.

Рассмотрим в качестве примера $m = 3$ и преобразование

$(a_0, a_1, a_2, a_3)^{\mathrm{T}} \rightarrow (a_0, 0, a_1, 0, 0, a_2, a_3)^{\mathrm{T}}$

Для такого кода вероятность $P(e_0=1,\ e_1=1)$ совпадает с $P(e_0=1,\ e_3=1)$ для короткого кода, которая оказывается существенно меньшей. Соответствующая ей кривая 4 на рис. 3.3 пока-

зывает ещё меньшую степень размножения ошибок, чем в модифицированном декодере (кривая 3).

Таким образом, для класса равномерных свёрточных кодов полученные верхние оценки показывают, что размножение ошибок в случае умеренного шума весьма невелико, уменьшается по мере улучшения качества канала и может быть сведено к минимуму при выборе соответствующего правила ортогонализации.

3.6. Недвоичные коды

Рассмотрим методы оценки эффекта РО в обсуждавшихся в главе 2 недвоичных линейных кодах. Пусть задан q-ичный СОК с некоторой скоростью R и произвольным d для QCK с вероятностью ошибки p_0. Тогда для любого символа i_j такого, что его ошибка e_j входит в m-ю проверку относительно одного символа i_k и в n-ю проверку относительно другого символа i_p, производящая функция вероятности ПФВ имеет вид

$$A_{m,n}(x,y)=\sum_{i=1}^{q-1}\left(\frac{p_0 x_m^i y_n^{i+j}}{q-1}+(1-p_0)\right).$$

Для учета эффекта РО из-за ошибочного решения порогового элемента о символе i_k при декодировании некоторого другого символа i_p производящая функция проверочного символа кода, входящего в обе системы проверок, имеет вид

$$A_{m,n}(x,y)=\sum_{i=1}^{q-1}\left(\frac{p_0 x_m^i y_n^{i+j}}{q-1}+\frac{(1-p_0) y_n^j}{q-1}\right), \qquad (3.12)$$

где j – разность между значением ошибки в символе i_k и решением порогового элемента относительно него.

Введем правило перемножения ПФВ для q-ичного случая, обобщающее двоичный случай. Допустим, что сложение символов в кодере производится по mod q. Тогда после умножения двух ПФВ показатели степеней i в x_m^i и j в y_n^j для переменных x и y с одинаковыми индексами складываются по mod q, а остальные преобразования выполняются обычным образом.

Пусть вычислено произведение всех ПФВ, входящих в проверки относительно информационных символов i_0 и i_1 с учетом, если необходимо, особой ПФВ (3.12):

$$A_{0,1}(x,y) = \prod_{0\le m,n\le d} A_{m,n}(x,y) = \sum_{\substack{k_t,m_s \\ 0\le t,s\le d}} a_{k_1,k_2,\ldots,k_d,m_1,m_2,\ldots,m_d} \prod_{i=1}^{d} x_i^{k_i} \prod_{j=1}^{d} y_j^{m_j}, \quad (3.13)$$

где k_j, $m_s = 0 \div (q-1)$, а суммирование ведется по всем возможным индексам при k и m.

Тогда в недвоичном многопороговом декодере (QMПД) для первого порогового элемента вероятность ошибки $P_{1,1}(e)$ в двух первых символах i_0 и i_1 кода в соответствии с правилами работы QMПД будет определяться коэффициентами $a_{k_1k_2\ldots k_d m_1 m_2\ldots m_d}$, удовлетворяющими одновременно следующим требованиям:

1) значения h_0 максимально часто встречающихся n_0 раз одинаковых индексов, отличны от нуля, а все остальные значения встречаются реже, n_1 раз, $n_0 > n_1$;

2) в случае нескольких одинаково часто встречающихся значений индексов, иначе говоря, при $n_0 = n_1$ индексы, относящиеся к декодируемым символам i_0 и i_1, т.е. к тривиальным проверкам, не равны нулю.

Предложенная методика вычисления вероятности $P_{1,1}(e)$ обеспечивает точное значение искомой вероятности. Однако преобразования (3.13) весьма сложны и труднообозримы. Поэтому целесообразно их упростить, если результирующие оценки изменятся достаточно мало, чтобы отражать реальный уровень РО. Пусть для примера рассматривается блоковый СОК с $d = 5$ и $R = 4/8$. Тогда вероятность ошибки в символе i_1 при условии ошибочного декодирования i_0 будет больше, чем вероятность ошибки декодирования i_0, т.е. вероятность $P_1(e)$, если у символов i_0 и i_1, есть общая проверка, которая в части ситуаций оказывается при наличии ошибки декодера в i_0 правильной, а в другой части – неправильной.

Будем для получения верхней оценки $P_{1/1}(e)$ считать, что общая проверка при декодировании i_1 всегда неправильна. Это позволит найти искомую оценку только путем вычисления вероятностей ошибки, аналогично методу вычисления вероятности $P_1(e)$, т.е. перебором всех возможных значений проверок

кода и декодируемого символа. При этом будем считать, что для определенности четвертая проверка всегда ошибочна. Эта проверка определяет единственный способ влияния решения о i_0 на решение про i_1.

В таблице 3.2 перечислены все возможные ситуации для значений ошибки в i_0 или i_1 и четырех проверок, которые приводят к неправильному решению порога. Нулем обозначены правильные проверки, значком «X» – ошибочные проверки, имеющие все различные между собой значения, а единицы означают совпадающие значения ошибочных проверок. Правые столбцы таблицы содержат значения вероятностей соответствующих событий $P_1(e)$ и $P_{1/1}(e)$.

При оценках $P_{1/1}(e)$ учитывалось, что, например, последняя проверка для i_1 должна быть всегда ошибочна, а при вычислении $P_1(e)$ эта проверка, как и другие, может быть и истинной. Более компактные формы представления вероятности $P_1(e)$ для q-ичного кода, чем табличный, будут представлены в 4-й главе. Здесь отметим, что для q-ичной проверки вероятность быть правильной определяется выражением

$$q_v = 1-(1-q_0^m)\left(1-\frac{1}{q-1}\right),\ q_0 = 1-p_0,$$

где размерность проверки для рассматриваемого случая равна $m = 4$ [11, 64]. Тогда $P_1(e)$ определяется суммой вероятностей событий, перечисленных в 5-ом столбце таблицы, а верхняя оценка $P_{1/1}(e)$ – событиями, вероятности которых указаны в столбце 6.

Заметим, что для более компактной записи в выражениях для вероятностей событий $P_1(e)$ и $P_{1/1}(e)$ использовались следующие обозначения:

$$\alpha = \frac{1}{q-1},\ p_v = \left(1-q_0^4\right)(1-\alpha),\ q_v = 1-p_v.$$

В графах 3 и 4 таблицы указаны по одному из возможных сочетаний проверок в группах, например, в строке 4 подразумевается перечисление четырех сочетаний:

```
1   1   1   X
1   1   X   1
1   X   1   1
X   1   1   1.
```

Вероятности $P_1(e)$ и $P_{1/1}(e)$ в графах 5 и 6 указаны для всей группы таких событий.

Т а б л и ц а 3.2. Сочетание ошибочных проверок, приводящих к ошибке QMПД в первом символе и втором символе, если произошла ошибка в первом

№	e_j	Сочетания проверок	Общая проверка	$P_1(e)$	$P_{1/1}(e)$
1	2	3	4	5	6
1	0	111	0	$4p_v^3 q_v q_0 \alpha^2$	$3qp_v^2 q_v \alpha^2$
2	0	111	1	$p_v^4 q_0 \alpha^3$	$q_0 p_v^3 \alpha^3$
3	0	11X	X	$6p_v^4 q_0 \alpha(1-2\alpha)$	$6p_v^3 q_0 \alpha(1-\alpha)(1-2\alpha)$
4	0	111	X	$4p_v^4(1-\alpha)\alpha^2 q_0$	$4p_v^3 \alpha^2(1-\alpha)q_0$
5	1	110	0	$6p_0 p_v^2 q_v^2 \alpha^2$	$3p_0 p_v q^2 \alpha^2$
6	1	11X	0	$12p_0 p_v^3 q_v(1-\alpha)\alpha^2$	$9p_0 p_v^2 q_v(1-\alpha)\alpha^2$
7	1	11X	X	$6p_0 p_v^4 \prod_{i=1}^{4}(1-2\alpha)\alpha^2$	$6p_0 p_v^3(1-\alpha)(1-2\alpha)\alpha^2$
8	1	1XX	X	$4p_0 p_v^4 \prod_{i=1}^{3}(1-i\alpha)\alpha$	$4p_0 p_v^3 \alpha \prod_{i=1}^{3}(1-i\alpha)$
9	X	XXX	X	$p_0 p_v^4 \prod_{i=1}^{4}(1-i\alpha)$	$p_0 p_v^3 \prod_{i=1}^{4}(1-i\alpha)$
10	X	11X	0	$12p_0 q_v p_v^3(1-\alpha)(1-2\alpha)\alpha$	$9p_0 p_v^2 q_v(1-\alpha)(1-2\alpha)\alpha$
11	X	11X	X	$6p_0 p_v^4 \prod_{i=1}^{3}(1-i\alpha)\alpha$	$6p_0 p_v^3 \alpha \prod_{i=1}^{3}(1-i\alpha)$
12	X	111	X	$4p_0 p_v^4(1-\alpha)(1-2\alpha)\alpha^2$	$4p_0 p_v^3 \alpha^2(1-\alpha)(1-2\alpha)$
13	X	110	0	$6p_0 p_v^2 q_v^2(1-\alpha)\alpha$	$3p_0 p_v q_v^2(1-\alpha)\alpha$
14	X	111	0	$4p_0 p_v^3 q_v(1-\alpha)\alpha^2$	$3p_0 p_v^2(1-\alpha)\alpha$
15	X	111	1	$p_0 p_v^4(1-\alpha)\alpha^3$	$p_0 p_v^3(1-\alpha)\alpha^3$

На рис. 3.4 приведены результаты вычислений вероятности $P_1(e)$ и оценки для $P_{1/1}(e)$ для рассматриваемого кода с $q = 16$ согласно таблице 3.2: кривая 1 – вероятность $P_1(e)$, 2 – верхняя оценка для $P_{1/1}(e)$, а кривая 3 – условная вероятность ошибки $P_{1/1}(e)$ для аналогичного двоичного блокового кода с теми же параметрами $R = 4/8$ и $d = 5$. Из сопоставления кривых 2 и 3 видно, что уровень РО в q-ичных кодах меньше, чем в двоичных при одинаковых значениях вероятности p_0 канала, что позволяет считать возможной работу алгоритмов QМПД при более высоких вероятностях ошибки p_0 в QСК, чем в двоичном симметричном канале. Из поведения вероятностей $P_1(e)$ в более общем случае, чем только что рассмотренный пример, как будет видно в главах 4 и 5, граница области эффективности работы QМПД действительно сдвигается в сторону более высоких значений вероятностей p_0 ошибки в канале. Таким образом, уровень РО, наряду с вероятностью $P_1(e)$ для блокового кода, достаточно точно определяют границы области применения QМПД по входному уровню шума.

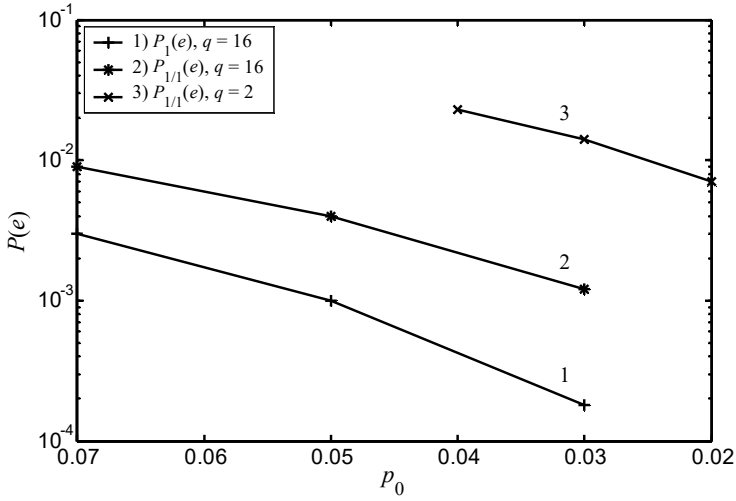


Рис. 3.4. Графики размножения ошибок в недвоичных кодах

3.7. Группирование ошибок в кодах максимальной длины

Рассмотрим вопросы РО в блоковых кодах с плотной упаковкой кодовых слов, имеющих при этом максимально возможное для заданной длины n расстояние. К ним относятся, например, коды максимальной длины с $n = 2^k–1$, $d = (n+1)/2$ [4, 34].

Одной из основных задач, решение которой определяет уровень РО, является выбор способа ортогонализации проверок в коде. Воспользуемся идеями, положенными в основу правил формирования проверок в равномерных свёрточных кодах [39, 60] для построения проверок в кодах максимальной длины, декодируемых мажоритарным методом.

Выпишем порождающую матрицу G кода как все возможные двоичные строки, упорядоченные в лексико-графическом порядке. При $k = 3$ порождающая матрица кода G^{T} имеет вид

$$G^T = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \begin{matrix} 1) \\ 2) \\ 3) \\ 4) \\ 5) \\ 6) \\ 7) \\ 8) \end{matrix}$$

Хотя в этом случае первая строка матрицы бесполезна, оставим ее для более регулярного описания правил ортогонализации. Цифры справа от матрицы – номера строк в G^{T}. Скобки правее номеров строк указывают пары кодовых символов, которые при суммировании образуют правый (первый) информационный символ кода. Крайняя группа скобок указывает пары тех же кодовых символов, образующих при сложении средний (второй) информационный символ кода.

Исключая теперь из рассмотрения первую (полностью нулевую) строку и учитывая, что $T = d/2$, получаем для первой тройки кодовых символов ПФВ при пороговом декодировании

$$A_1(x,y) = p_0^3 x^2 y^2 + p_0^2 q_0 (x^3 y^3 + y^2 + x^3) +$$
$$+ p_0 q_0^2 (x^2 y + x y^3 + x) + q_0^3 y.$$

Для второй группы (четверки) кодовых символов ПФВ имеет вид

$$A_2(x,y) = 2p_0^2 q_0 x^2 y^2 + 2p_0^2 q_0^2 x^2 + 2p_0^2 q_0^2 y^2 +$$
$$+ 4p_0 q_0 (p_0^2 + q_0^2) xy + p_0^4 + q_0^4.$$

Тогда полная ПФВ для некоторого $k \geq 3$ имеет вид

$$A_{0,1}(x,y) = A_1(x,y) A_2^{2^{(k-2)}-1}(x,y) = \sum_{i=0}^{d+1} \sum_{j=0}^{d+1} a_{i,j} x^i y^j ,$$

а вероятность ошибки в двух рассматриваемых символах

$$P_{1,1}(e) = \sum_{i,j>d/2} a_{i,j} .$$

На рис. 3.5 представлены графики вероятностей ошибок в первом символе $P_1(e)$ для кодов максимальной длины с $k = 5$ и $k = 7$, а также вероятностей двух соседних ошибок $P_{1,1}(e)$ в этих же кодах. Сравнение вероятностей $P_1(e)$ и $P_{1,1}(e)$ показывает, что имеет место довольно сильная зависимость между решениями

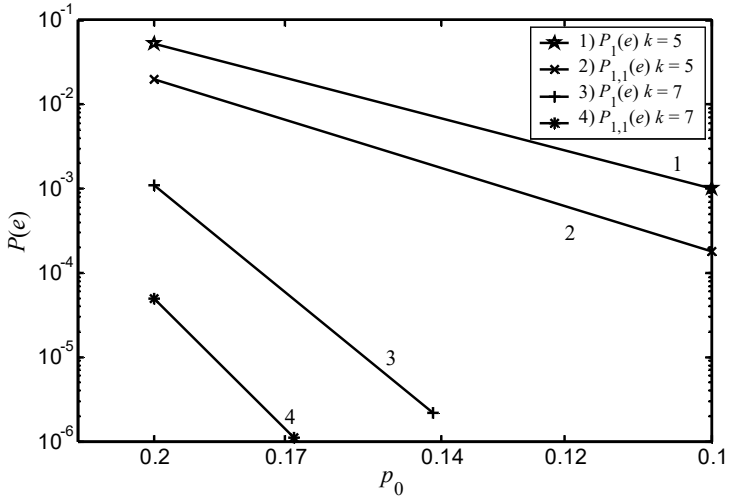


Рис. 3.5. Размножение ошибок в кодах максимальной длины при $k = 5$ и $k = 7$

порогового декодера, что и следовало ожидать в кодах с плотной упаковкой, какими являются рассматриваемые коды максимальной длины.

Аналогичные результаты были получены выше для равномерных свёрточных кодов, также имеющих максимально возможные значения отношения d/n_A [4].

3.8. Зависимость решений декодеров в каналах со стираниями

Рассмотренная во второй главе многопороговая процедура исправления стираний характеризуется тем, что она не вносит ни своих ошибок, ни новых стираний и поэтому для них нецелесообразно использовать термин РО. В этом случае предлагается использовать термин «зависимость решений». Введем ПФВ для канала с независимыми стираниями. Пусть есть символ i_j, входящий в две системы проверок относительно символов i_k и i_m. Если p_s – вероятность стирания, $q_s = 1–p_s$ – вероятность правильного приема символа, то ПФВ для рассматриваемого символа принимает $A_{l,n}(x,y) = (p_s x_l y_n + q_s)$. Произведение двух ПФВ для стирающего канала выполняется по обычным алгебраическим правилам без преобразований показателей степеней:

$$A_{0,1}(x,y) = \prod_{\{B\}} (p_s x_m y_n + q_s),$$

где $\{B\}$ – множество символов канала, ошибки в которых входят в проверки относительно хотя бы одного из двух информационных символов пары, совместная вероятность невосстановления которой должна быть вычислена, а m и n – номера проверок относительно 1-го и 2-го символов соответственно.

Тогда с учетом правила работы МПД вероятность невосстановления двух первых символов из конечного представления ПФВ

$$A_{0,1}(x,y) = \sum_{k_1,\ldots,k_d,l_1,\ldots,l_d} a_{k_1,k_2,\ldots,k_d,l_1,l_2,\ldots,l_d} \prod_{i=1}^{d} x_i^{k_i} \prod_{j=1}^{d} y_j^{l_j},$$

для самоортогонального кода с минимальным расстоянием d будет иметь вид

$$P_{1,1}(s) = \sum_{\{P\}} a_{\{k,l\}},$$

где $\{P\}$ – совокупность таких наборов индексов типа k и l, в которых все k_i, l_j для $i, j = 1, \ldots, d$, одновременно положительны. Это соответствует случаю, когда сами декодируемые символы и все относящиеся к ним ортогональные проверки стёрты.

На рис. 3.6 представлены следующие графики: 1 – вероятности невосстановления двух первых символов $P_{1,1}(s)$ при декодировании с обратной связью блокового СОК с $d = 5$, $R = 1/2$, $n = 26$ и аналогичная кривая 2 для длинного кода с переменными связями при $R = 4/8$ и тем же $d = 5$. Кроме того, для сравнения приведен график 3 вероятности невосстановления первого символа блока $P_1(s)$.

Как следует из сопоставления кривых, группирование моментов невосстановления стираний невелико, в коде с переменными связями оно может быть меньшим, чем у обычного кода с фиксированными связями, причем при улучшении качества канала доля одиночных остаточных стираний после декодирования растет.

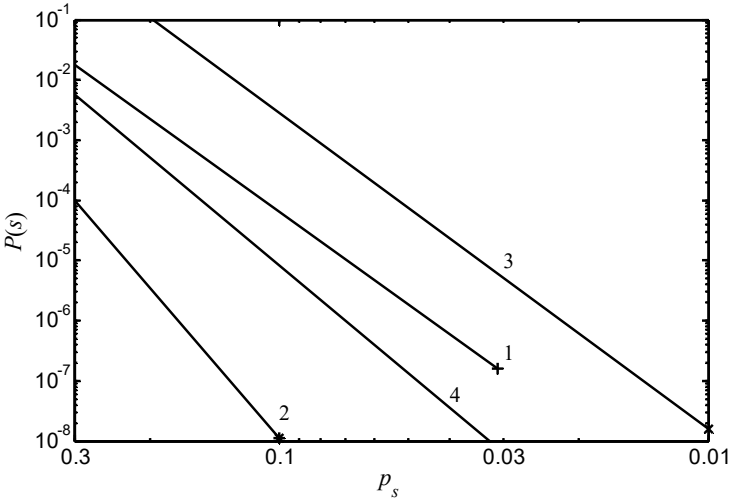


Рис. 3.6. Зависимость решений МПД от вероятностей p_s стирания символов в канале

Аналогичная кривая 4 для вероятности $P_1(s)$ свёрточного кода с $R = 1/2$ и $n_A = 14$ демонстрирует естественное для рассматриваемого случая преимущество свёрточных кодов.

3.9. Построение кодов с малым уровнем размножения ошибок

Как следует из оценок размножения ошибок проанализированных выше кодов, более высокие уровни вероятностей ошибок одновременно в двух символах кода будут у пар информационных символов i_j и i_k, имеющих большее число таких ошибок в системах проверочных уравнений, которые входят в обе системы проверок. Все эти ошибки имеют соответствующую им ПФВ вида $(p_0 x_m y_n + q_0)$, чем и определяется больший уровень РО для таких кодов.

Оценим сложность построения кода с заданными весами полиномов $G_{i,j}$ такого, чтобы он имел минимальный уровень РО. Более формально, нужно оценить вычислительные затраты на построение такого кода с $R = k_0/n_0$ класса СОК, чтобы для всех пар символов i_m и i_j, $m = 0, 1, \ldots, k_0–1$, $j \neq m$ число двух и более ошибок, входящих одновременно в проверки относительно обоих символов пары, было бы минимально. Заметим, что при переходе от одного кода к другому с меньшим уровнем РО снижение числа пар символов с двумя, тремя и более общими ошибками происходит за счет увеличения числа пар i_m и i_j, имеющих единственную общую ошибку.

Поэтому число одиночных общих ошибок в более устойчивых к РО кодах растет, а число двойных, тройных и прочих ошибок уменьшается. При этом можно считать, что если в одном коде число пар, имеющих, например, 6 общих ошибок равно 26, а в другом число таких пар превышает 100, то первый код лучше второго по критерию РО, даже если во втором коде меньше пар символов с тремя общими ошибками по сравнению с первым.

Таким образом, множество чисел m_j, $j = 1, 2, \ldots$, определяющих количество пар символов i_m, i_k, которые имеют j общих ошибок, характеризует степень подверженности кода эффекту РО, причем предпочтительнее уменьшать числа m_j с более вы-

сокими индексами j, $j > 1$. Множество $\{m_j\}$ естественно назвать спектром РО.

Сформулировав критерии качества, рассмотрим оценки сложности построения кодов. Пусть по заданный весам порождающих полиномов $G_{i,j}$ СОК нужно построить для $R = k_0/n_0$ спектр РО, используя множество проверок относительно символов i_0, i_1, …, i_{k-1} первого кодового подблока. Общее число информационных ошибок, входящих в полные проверочные уравнения кода с некоторым значением d оценивается сверху как

$$N_1 = \frac{k_0(d-1)^2}{n_0 - k_0}.$$

Пусть величина кодового ограничения строящегося свёрточного кода равна n_A. Тогда число проверяемых пар равно

$$N_2 = k_0(k_0 - 1)/2 + k_0(4n_A R - 2k_0),$$

а сама проверка каждой пары состоит в том, что в них проверяются k_0 потоков информационных символов, каждый из которых содержит по $l \approx (d–1)^2/(n_0–k_0)$ символов. Полагая, что первое слагаемое в N_2 много меньше второго, получаем, что нужно произвести порядка $b = 4k_0^2 l^2 n_A R$ сравнений, что составляет величину

$$b \sim \frac{4d^4 k_0^3 n_A R}{n_0(n_0 - k_0)^2}.$$

Полагая k_0 и n_0 близкими к 1, получаем искомую сложность сравнения порядка

$$b \sim 4d^4 n_A R. \qquad (3.14)$$

Вычисление наилучших значений спектра размножения ошибок, т.е. множества $\{m_j\}$ весьма трудная задача, особенно, если в общем случае веса полиномов $G_{i,j}$, определяющих СОК, различны. Поэтому гораздо удобнее после достройки очередного слагаемого кодового полинома попытаться найти еще более хороший по спектру код, чем последний из построенных кодов, и, в случае наличия улучшения спектра, вести отсчет от нового кода и т.д. Если прежде, чем выносить окончательное решение о коде, будет построено несколько, например, m кодов с наилучшим p-м слагаемым строящегося на данном шаге полинома $G_{i,j}$, то тогда, если самый первый вариант p-го слагаемого взять за

окончательно принятый, можно ожидать, что построенный код будет лучшим или одним из лучших по критерию спектра РО. Опыт прохождения тестов для искомых кодов показал, что при $m = 4 \div 8$ действительно можно построить вполне эффективные коды с хорошим спектром РО.

Однако большой требуемый объем вычислений можно существенно сократить. Рассмотрим номера множества ошибок, входящих в проверки, например, относительно i_0. Возьмём также некоторый другой произвольный информационный символ i_t. Пусть в результате сравнения выясняется, что эта пара имеет g общих ошибок. Если i_t принадлежал одному из k_0 информационных потоков кода с $R = k_0/n_0$, тому, в котором находится и i_0, то это означает, что множество ошибок в проверках относительно i_t имеют такие же номера, как и ошибки в проверках относительно i_0, но увеличенные все на одинаковую величину t. Поскольку общих ошибок в проверках было g, то в совокупности k_0 множеств тех проверок, в которых ищутся общие ошибки, есть в общей сложности g совпадающих ошибок. Но тогда, если найти все возможные разности между номерами элементов проверок, т.е. всех ошибок каждой информационной ветви для символа i_0, то число разностей, равных t, должно быть точно g. Далее, если предположить, что i_0 и i_t принадлежат разным информационным потокам, то, заменив i_t, например, на i_3 для $k_0 = 5$ и вычислив раздельно все разности между ошибками k_0 информационных потоков, получаем, что количество разностей, равных t, также совпадает с g.

Это позволяет следующим образом упростить процедуру оценки спектра РО. Возьмем $k_0(k_0+1)/2$ всех пар, составленных из символов начального кодового блока: i_0, i_1, …, i_{k_0-1}, включая собственные пары i_0 и i_0, i_1 и i_1, …, i_{k_0-1} и i_{k_0-1}. Для получившихся пар символов найдем k_0 всех возможных групп разностей между номерами ошибок внутри одного информационного потока, и все разности во всех k_0 потоках посчитаем вместе. Тогда для каждой из $k_0(k_0+1)/2$ пар символов i_j, i_k результирующее число разностей m_j есть просто количество пар m_j, содержащих j общих ошибок. А отсюда в свою очередь следует, что объём вы-

числений снижен согласно (3.14) с величины порядка $d^4 n_{\text{A}}$ до d^4, что для длинных кодов может составить ускорение счета при построении кодов на два-три порядка.

Для поиска таких кодов был разработан пакет программ, обеспечивающий в широком диапазоне кодовых скоростей $R = 0{,}1 \div 0{,}9$ построение кодов с фиксированными и переменными связями, имеющих $3 \le d \le 41$ и относящихся к классу самоортогональных.

В программах можно задавать степень уменьшения доли общих ошибок во всех парах проверок строящихся кодов, включая и абсолютную их минимизацию, что позволяет строить коды с предельно малым уровнем РО для заданных параметров кода d и R с учётом ряда дополнительных критериев отбора кодов.

Новые множества кодов типа СОК позволяют более свободно выбирать кодовые скорости при реализации мажоритарных методов. Это существенно расширяет возможности алгоритмов класса МПД, практически снижая уровень группирования ошибок в декодерах этого типа до весьма несущественных уровней.

3.10. Выводы

В этой главе на примерах разных каналов и кодов были показаны проявления эффекта размножения ошибок, методы его оценки и способы его уменьшения. Здесь были опущены оценки РО для кодов в системах сложных сигналов, а также в случае применения мягких модемов и некоторых других приложениях алгоритмов МПД. Можно отметить, что известны также оценки РО для быстропросматриваемых несистематических кодов [40, 103], указывающие на значительный уровень РО при их использовании, как и должно быть в этом случае. Применение МПД для декодирования хороших кодов, стандартизованных для АВ, описано в [65]. Вопросы применения МПД с многопозиционными сигналами рассматривались в [62, 63], в [103] был проведен анализ размножения ошибок в таких условиях.

Как следует из сопоставления графиков вероятностей одиночных и двойных ошибок, при правильном выборе кодов вероятность следующей ошибки декодера после того, как произошла

ошибка в одном из первых символов кода, оказывается все-таки небольшой, мало возросшей по сравнению с вероятностью ошибки в первом символе. С другой стороны, некоторые из методов уменьшения эффекта РО, в частности, дефинитные декодеры увеличивают не только среднюю вероятность ошибки на бит и блок обычного мажоритарного декодера, но и приводят к близким значениям совместной вероятности появления пар ошибок, как и ПД, имеющего обратную связь, т.е. почти не снижают РО некоторых длинных кодов. Это свидетельствует о значительной сложности проблемы группирования ошибок на выходе ПД, требующей аккуратного анализа и правильной интерпретации изучаемых явлений.

Полученные выше оценки РО выполнены не для многопорогового декодера, изучению которого была посвящена вторая глава, а для обычного порогового алгоритма. Для проведения достаточно полного и точного анализа РО на выходе последующих, например, 2-го, 4-го или 10-го порогового элемента в свёрточном МПД или соответственно после i-й, $i = 2, 3,...$ итерации декодирования блокового МПД есть такие объективные трудности, как быстрое увеличение размерности решаемой задачи, что не позволяет получать простые, но достаточно точные оценки.

Однако, чрезвычайно важно, что весь проведенный анализ выполнен для порогового элемента, который стоит на первой позиции в блоковом и в сверточном МПД. Этот пороговый элемент исправляет самый плотный поток ошибок, поступающий прямо из канала и, значит, работает в самых тяжелых условиях. Следовательно, остальные пороговые элементы МПД работают в более легком режиме, исправляя ошибки, пропущенные на предыдущих итерациях, а выполненные оценки относятся к самому критичному узлу МПД, эффективная работа которого определяет возможности всего алгоритма в целом.

Как следует из проведенного в этой главе анализа, наиболее важным полученным результатом является выяснение внутренних причин РО, свойственных самим кодам. Для уменьшения РО нужно сокращать в максимальной степени число пересекающихся множеств ошибок, которые есть в проверках относительно любых пар символов кода. Достижение достаточно не-

большого числа таких ошибок возможно лишь для чрезвычайно длинных кодов с переменными связями. При этом нужно помнить, что даже полный учёт всех пересекающихся групп символов в проверках относительно различных символов даёт, тем не менее, незначительный эффект, если алгоритм работает в области больших шумов канала. В таких случаях нужно проверять достаточно много условий на проверки, выполнение которых обязательно. Но использование и других кодов с большой длиной, но существенно более коротких, чем наилучшие коды по критерию РО, также может быть в ряде случаев вполне эффективно. Другие способы уменьшения РО также достаточно просты: некоторое увеличение порога принятия решения об ошибке и формирование для разных ступеней декодирования разных наборов ортогональных проверок, где это возможно [57]. Вместе с тем поиск хороших кодов для МПД требует достаточно аккуратного анализа и довольно большого объёма вычислений. Ещё бóльших затрат требует моделирование работы найденных кодов и оптимизация параметров МПД декодера. Число таких параметров может достигать многих сотен и тысяч позиций. Но столь долгий процесс проектирования кодека (системы кодер/декодер) нисколько не увеличивает число операций, выполняемых уже построенным декодером, что и оправдывает сложность процедуры создания такого, вроде бы, предельно простого кодека.

Именно простые критерии РО как числа общих ошибок в парах проверок и решают проблему выбора лучших кодов для рассматриваемого алгоритма коррекции ошибок. Для этого достаточно уметь находить коды с минимальной вероятностью появления пакетов ошибок декодера веса не более трёх. Отмеченные же трудности получения оценок РО для нескольких итераций декодирования фактически не являются сколько-нибудь существенным препятствием для понимания принципов и важных условий работы МПД.

Основным итогом данной главы является разработка методов оценки РО в линейных кодах, которые позволяют сравнивать между собой различные коды и отбирать те из них, которые наилучшим образом удовлетворяют требованию минимизации

этого эффекта. Полученные результаты и выработанные критерии сравнения позволили разработать методы построения достаточно длинных кодов с минимальным уровнем эффекта размножения ошибок при их декодировании мажоритарными алгоритмами.

ГЛАВА 4. АНАЛИТИЧЕСКИЕ ОЦЕНКИ ЭФФЕКТИВНОСТИ МНОГОПОРОГОВОГО ДЕКОДИРОВАНИЯ

4.1. Методы оценок характеристик

Развитие теории помехоустойчивого кодирования в течение длительного времени в одном из своих важнейших аспектов состояло в поиске более эффективных для своего этапа развития алгебраических кодов и методов их декодирования. Оценка корректирующей способности таких методов не представляла трудностей, поскольку для этого использовались, например, биномиальные распределения. Полностью аналогичной была ситуация и с оценкой возможностей каскадных процедур, базировавшихся на алгебраических методах. Но уже давно было установлено, что по многим причинам декодеры для таких кодов малоэффективны.

Дальнейший прогресс в технике кодирования, связанный с появлением более сложных методов, например, последовательных процедур, также в течение длительного времени был связан с отработкой самих алгоритмов и поиском соответствующих им кодов. Оценки характеристик этих методов носили обобщенный характер, т.е. были справедливы «для класса кодов», или выполнялись при некоторых существенных ограничениях, например, на уровень шума канала [66]. Реальные характеристики этих алгоритмов при большом уровне шума получались обычно уже на основе компьютерного моделирования при использовании конкретных кодов.

Наконец, текущий период, связанный с исследованием очень мощных методов кодирования, значительная часть которых содержит в качестве одного из шагов алгоритм Витерби, декодеры для турбо кодов или другие оптимальные и субоптимальные процедуры, характеризуются тем, что для получения результатов приемлемой степени точности моделирование оказывается обязательным элементом оценок эффективности, по крайней мере, некоторых этапов процедур декодирования.

Сложившаяся ситуация является весьма показательной. Она соответствует столь высоким требованиям, предъявляемым в

каналах с независимыми ошибками к корректирующим кодам, что для обеспечения необходимой эффективности эти коды должны исправлять большое число ошибок далеко за границами, гарантируемыми минимальным кодовым расстоянием d используемых блоковых или свободным расстоянием d_f свёрточных кодов. Более того, в этом случае декодером должно правильно корректироваться абсолютное большинство ошибок канала, существенно превышающее половину минимального кодового расстояния используемого кода. Во всех других случаях декодер не сможет эффективно работать при всех уровнях шума, существенно превышающих кодовую скорость R по параметру вычислительной скорости канала R_C, т.е. когда $R > R_C$. Таким образом, тонкая структура кода, его спектр в больших шумах канала оказывают решающее влияние на эффективность наиболее мощных алгоритмов декодирования. При этом надо отметить, что даже для таких хорошо изученных алгоритмов, как алгоритм Витерби, являющихся оптимальными, хорошие оценки их эффективности в большом шуме получить существенно проще в результате моделирования, хотя в силу оптимальности аналитические оценки должны были бы учитывать лишь спектр весов и другие свойства самого кода.

Все вышеупомянутые соотношения в целом справедливы и для многопороговых алгоритмов декодирования, обеспечивающих в широком диапазоне параметров шума канала хорошее приближение к декодированию по максимуму правдоподобия, т.е. к оптимальным решениям.

Рассмотрим особенности оценки характеристик мажоритарных алгоритмов декодирования. В свете отмеченных общих методических трудностей становятся более четко очерченными и проблемы изучения процедур такого типа. В настоящее время после более двух десятилетий развития мажоритарных методов по-прежнему известна только методика вычисления точного значения вероятности ошибки декодирования первого символа сообщения $P_1(e)$ пригодная как для блоковых, так и для свёрточных кодов [4]. Эта вероятность может интерпретироваться и как средняя вероятность ошибки на бит $P_b(e)$ для дефинитных пороговых декодеров. Однако, как отмечалось в предыдущей

главе, дефинитные декодеры на самом деле незначительно уменьшают эффект размножения ошибок в его наиболее точном и естественном смысле, для компенсации которого они первоначально рассматривались. Кроме того, средняя вероятность ошибки $P_b(e)$ у этих декодеров, особенно в свёрточном их варианте, существенно выше, чем у ПД с обратной связью, и, тем более, чем у МПД. Поэтому точное определение характеристик дефинитных декодеров не представляет реальной практической ценности.

Еще более трудные задачи возникают при оценке корректирующих возможностей МПД, реализующего от трех до десяти и более попыток декодирования символов принятого сообщения, поскольку при этом необходимо учитывать и возможности самого кода, и такое чрезвычайно сложное явление, как размножение ошибок, описанию и изучению которого была посвящена третья глава.

Далее обсуждается связь между параметрами кодов и предельными возможностями МПД алгоритмов и приводятся верхние оценки вероятности ошибки в первом символе $P_{1-2}(e)$ для свёрточного МПД, реализующего две попытки декодирования. Несмотря на совсем небольшое по сравнению с традиционными ПД усложнение, такой декодер обеспечивает при малом уровне шума характеристики, мало отличающиеся от оптимальных. Разумеется, для этого следует выбирать достаточно хорошие коды по критерию размножения ошибок, что позволяет существенно упростить предлагаемые оценки.

Рассмотрены также различные оценки вероятности ошибки недвоичных кодов, «мягких» МПД и описаны методы улучшения характеристик для большого уровня шума. Изложена методика усреднённых оценок вероятностей ошибки МПД, позволяющая определять границы эффективного использования этого алгоритма.

Обсуждаются возможности методики, позволяющей с помощью ПФВ большей размерности повысить точность оценок для вероятности $P_b(e)$ декодера типа МПД.

4.2. Самоортогональные коды

Пусть рассматривается линейный двоичный блоковый мажоритарно декодируемый самоортогональный код (СОК) с кодовой скоростью $R = k_0/n_0 = 1/2$ и $d = 2t_0+1$, т.е. исправляющий t_0 ошибок.

Напомним методику вычисления вероятности ошибки обычного порогового декодирования в первом символе декодируемого блокового кода $P_1(e)$, повторяющую в основном материал, изложенный в [4]. Поскольку в рассматриваемом случае число проверок кода равно $J = d–1$, то можно считать, что для $R = 1/2$ все они имеют размерность J. Под размерностью проверок будем понимать, как и в [4], общее число ошибок в проверочных уравнениях, без учёта самой ошибки в декодируемом символе i_0. С учётом этого замечания вероятность того, что некоторая k-я проверка окажется неправильной, равна

$p_J = 0{,}5[1–(1–2p_0)^J]$,

где p_0 – вероятность ошибки в ДСК.

Тогда, вычисляя

$$A(x) = (p_0x + q_0)(p_Jx + q_J)^J = \sum_{m=0}^{d} a_m x^m ,$$

где $q_0 = 1–p_0$, $q_J = 1–p_J$, получаем, что вероятность ошибки в первом символе кода при пороговом декодировании равна

$$P_1(e) = \sum_{m=(d+1)/2}^{d} a_m .$$

В общем случае при $R = k_0/n_0 = k_0/(k_0+r_0)$ размерности проверок могут довольно сильно отличаться от рассмотренного примера с $R = 1/2$, что может быть связано также с различными весами порождающих полиномов того или иного кода, использованием методов параллельного кодирования, кодов с переменными связями, с выделенными ветвями (которые будут рассмотрены несколько позже) или с другими причинами. Поэтому правильное определение размерности проверок может помочь в поиске методов повышения эффективности применения и собственно алгоритма МПД. Первоначальное уменьшение средней вероятности ошибки декодирования всегда непосредственно связано с возможностями обычного ПД, т.е. с тем, получается

ли у него хотя бы небольшое снижение средней вероятности ошибки декодирования по сравнению с вероятностью ошибки канала, в котором он работает. На последующих итерациях декодирования происходит лишь дальнейшее понижение вероятности ошибки относительно достигнутой на первом шаге (итерации) коррекции ошибок.

Как следует из приведённых на рис. 4.1 графиков зависимостей $P_1(e)$, при мажоритарном декодировании в ДСК коды с большим d более эффективны при малом уровне шума. При большой вероятности ошибки в канале более эффективны, наоборот, коды с меньшими значениями d. Кроме того, поскольку в блоковых кодах размерность всех проверок максимальна, а в свёрточных увеличивается от минимальной до максимальной, вероятность ошибки в первом символе кода $P_1(e)$ для свёрточных кодов с равными d и R всегда меньше, чем для блоковых.

Рассмотрим вероятность наличия единичной ошибки ОД в сообщении, закодированном самоортогональным свёрточным или блоковым кодом. Для этих кодов все кодовые слова веса d имеют только одну информационную единицу. Тогда нижняя

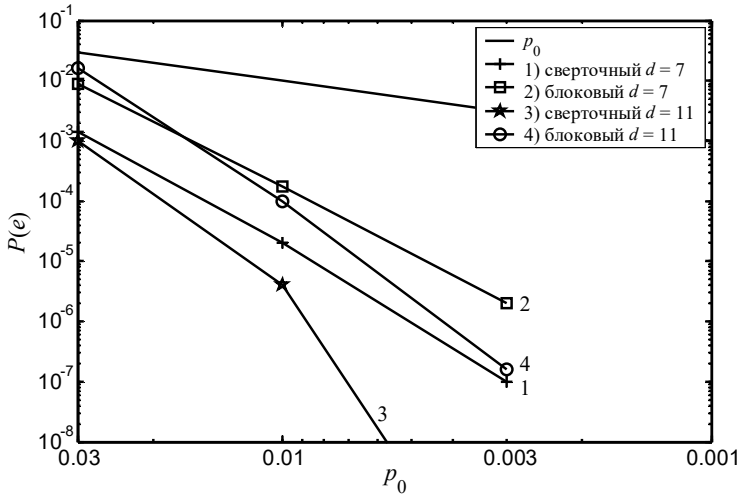


Рис. 4.1. Вероятности ошибки обычных ПД в первых символах $P_1(e)$ кодов с $R = 1/2$

оценка вероятности перехода решения ОД в ближайшее конкретное кодовое слово с одной информационной единицей $P_{b\text{ОД}}(e)$ на заданной позиции имеет для ДСК без памяти вид, соответствующий наличию ошибок канала более, чем в половине из d ненулевых позиций этого кодового слова:

$$P_b(e) = P_{b\text{ОД}}(e) = \sum_{i=(d+1)/2}^{d} C_d^i p_0^i (1-p_0)^{d-i} . \qquad (4.1)$$

Графики зависимости вероятностей ошибки на бит $P_b(e)$ для СОК, имеющих большое значение для МПД алгоритмов, приведены на рис. 4.2 для нечётных значений d. Эти оценки оказываются существенно нижними, поскольку никак не связаны с кодовой скоростью этих кодов, учёт которой существенно повышает вероятности ошибки на бит на блок при большом уровне шума. Однако при соотношениях шума канала и кодовых скоростей $R \sim R_C$, где R_C – вычислительная скорость канала, и даже при немного более высоком уровне шума выражение (4.1) даёт достаточно правильные значения для предварительных оценок вероятности ошибки на бит $P_b(e)$ МПД с этими кодами при числе итераций декодирования $I \sim 3 \div 10$.

Поставим задачу оценки сверху вероятности ошибки в первом символе свёрточного кода $P_{1,2\text{МПД}}(e)$ после второй попытки декодирования всего кода и этого символа алгоритмом МПД. Для упрощения этой проблемы воспользуемся реальными свойствами лучших конкретных построенных кодов типа СОК с переменными связями $R = 1/2$. Эти коды таковы, что для любой пары декодируемых символов i_m и i_j есть не более двух общих проверок, включая тривиальную, а количество символов в этих проверках не превышает d – минимального кодового расстояния. Для этого случая можно вычислить стандартным способом вероятность ошибки в первом символе $P_1(e)$ обычного ПД, а затем упрощённым методом найти оценку сверху для условной вероятности ошибки ПД в некотором другом символе i_j кода, который также входит в проверки относительно первого символа кода i_0, если в i_0 ПД уже сделал ошибку. Ясно, что в худшем случае при двух неправильных проверках относительно i_j ПД совершит ошибку при декодировании i_j, если в оставшихся d–2

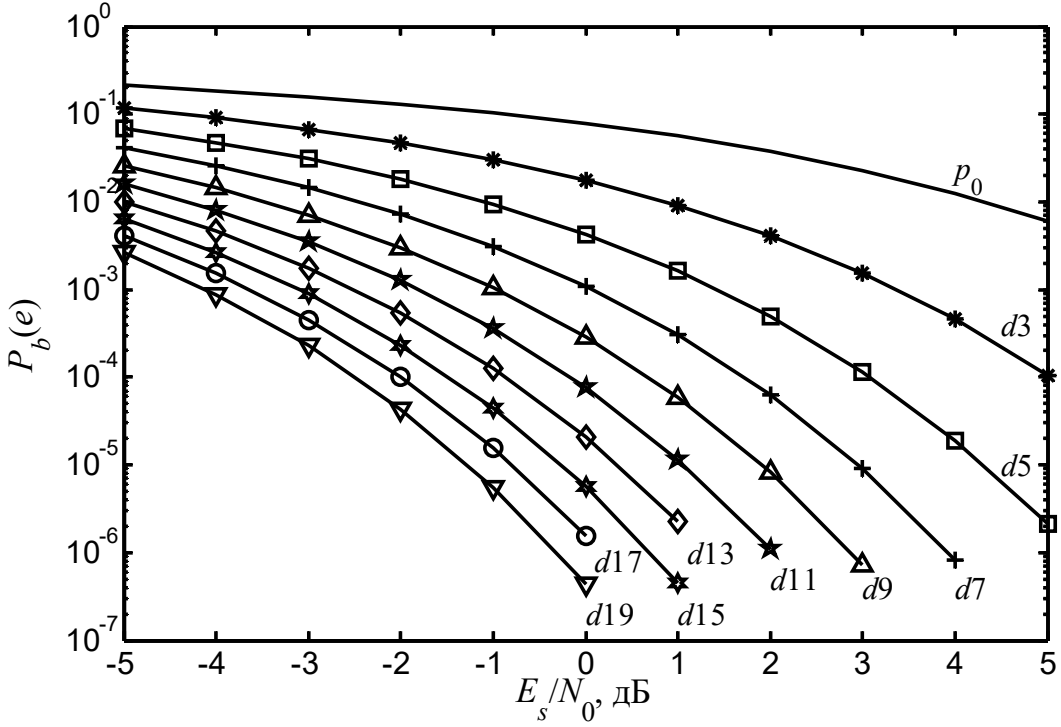


Рис. 4.2. Нижние оценки вероятности ошибки на бит $P_b(e)$ для ОД при использовании самоортогональных кодов в ДСК

проверках будет более (d–1)/2–2 неправильных проверок. Для верхней оценки надо предположить, что это все проверки максимально возможной размерности d–1. Тогда верхняя оценка рассматриваемой условной вероятности ошибки в конкретном символе i_j $P_{1/1}(e)$ равна

$$P_{1/1}(e) = \sum_{m=(d-1)/2-1}^{d-2} C_{d-2}^{m} p_0'^{m} (1-p_0')^{d-2-m}, \qquad (4.2)$$

где $p_0' = 0{,}5[1-(1-2p_0)^{d-1}]$.

Общее число ошибок в информационных символах, входящих в проверки относительно i_0, равно (d–1)(d–2). Именно для такого числа двойных ошибок в пределах длины кодового ограничения вероятность их появления будет определяться выражением (4.2). Верхняя оценка появления других пар ошибок, первая из которых – e_0, как следует из [57, 103], может быть представлена как $[P_1(e)]^2$ для этого кода. Эти же несколько завышенные оценки могут быть использованы и для оценок появления двух ошибок на любых двух позициях в пределах длины кодового ограничения свёрточного СОК. Отсюда верхняя оценка вероятности появления более одной, т.е. двух и более ошибок в пределах длины кодового ограничения $P_2(e)$ равна

$$P_2(e) = (d-1)(d-2)kP_1(e)P_{1/1}(e) + k^2[P_1(e)]^2/2, \qquad (4.3)$$

где k – количество информационных символов в пределах длины кодового ограничения n_A.

Поскольку целью выводимых оценок является доказать аналитически возможность успешной работы МПД всего с двумя итерациями при малом уровне шума, то не будем стремиться очень сильно минимизировать константы в (4.3), которые не оказывают существенного влияния на основные тенденции в поведении декодера. Возьмём в качестве примера, на котором будет демонстрироваться работа рассматриваемого МПД с двумя итерациями, свёрточный СОК с R = 1/2, d = 9 и n_A = 200000. Ясно, что для него k = 100000.

Тогда будем считать, что МПД на второй итерации обязательно ошибётся в первом символе i_0, если в пределах длины кодового ограничения после первой попытки коррекции ошибок будет более одной ошибки. Вероятность этого события уже най-

дена, это $P_2(e)$. Вместе с тем, очевидно, что при наличии единственной ошибки первого декодера, возможность ошибки на второй итерации ничтожна. Как уже было показано ранее, мажоритарные схемы обычно исправляют и ошибки, вес которых превышает величину $d/2$ даже в несколько раз. Но с помощью оценок появления ошибок ПД веса 2 сложно получить более мощные оценки, чем приведённые в этом разделе.

В случае же, если после первой итерации на длине кодового ограничения осталось не более одной ошибки, согласно результатам, вытекающим из следствия 1 теоремы 2.2 и теорем 2.4 – 2.6 МПД на второй итерации примет оптимальное решение об i_0.

Таким образом, согласно весьма завышенной оценке для $P_2(e)$ вероятность ошибки в первом символе после второй итерации будет определяться выражением

$$P_{1,2\,\text{МПД}}(e) = P_2(e) + [1 - P_2(e)]P_{b\text{ОД}}(e), \qquad (4.4)$$

где $P_{b\text{ОД}}(e)$ вычисляется в соответствии с (4.1) для СОК с $d = 9$.

Поскольку при $p_0 \to 0$ $P_2(e) \sim p_0^8$, а $P_{b\text{ОД}}(e) \sim p_0^5$, то для достаточно малых p_0 практически все ошибочные решения МПД после первой итерации будут одиночными. В этом случае после второй итерации они или будут исправлены, или согласно указанным выше теоремам в некоторых позициях декодируемого потока будут находиться ошибки ОД. Иначе говоря, при достаточно больших значениях p_0 основной вклад в сумму (4.4) вносит первое слагаемое, а при малых – второе.

Ещё раз подчеркнём, что вероятность $P_2(e)$ в целях получения упрощённых оценок на много порядков завышена, поскольку, конечно, МПД и на первой, и на второй итерации исправляет много конфигураций ошибок канала большого веса, тогда как для упрощённого вывода оценки понадобилось считать, что на второй итерации МПД ошибётся всегда при двух и более ошибках в пределах длины кодового ограничения. Тем не менее, даже при этом условии оказалось возможным показать, что при малых p_0 при выполнении алгоритмом МПД всего двух итераций коррекции ошибок оказывается, что $P_{1,2\text{МПД}}(e) = P_{b\text{ОД}}(e)$, так как в этом случае $P_2(e) << P_{b\text{ОД}}(e)$.

Результаты расчёта $P_{1,2\text{МПД}}(e)$ для рассматриваемого кода представлены на рис. 4.3, на котором приведены вероятности: 1 – обычная $P_1(e)$ для классического ПД, 2 – $P_{b\text{ОД}}(e)$ и 3 – $P_{1,2\text{МПД}}(e)$, а также вероятность ошибки p_0 в канале ДСК.

Представляет несомненный интерес оценить реальные возможности обсуждаемого длинного кода с низким уровнем размножения ошибок, поскольку полученные оценки полезны из принципиальных соображений оценки поведения МПД в асимптотике, но не отражают его реальные возможности. Пунктир М представляет экспериментальную оценку $P_{1,2\text{МПД}}(e)$, которая, как и следовало ожидать, соответствует гораздо более эффективной реальной работе декодера и достижению оптимальных характеристик, соответствующих переборным алгоритмам, при весьма высоком уровне шума в ДСК.

Дальнейшее улучшение оценок $P_b(e)$ для двух, трех и т.д. итераций МПД возможно при увеличении размерности используемых ПФВ и детальном анализе вероятности появления трех ошибок декодирования и более. Например, в [77] показано, что трехмерные ПФВ позволяют для заданных вероятностей ошиб-

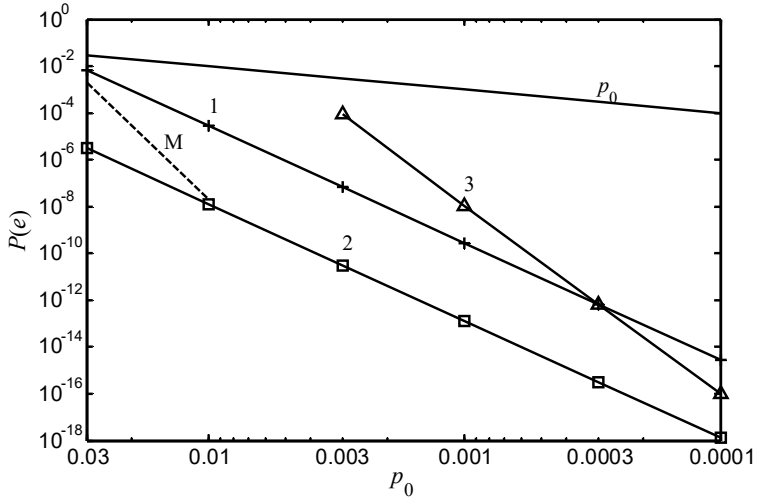


Рис. 4.3. Характеристики МПД в ДСК для двух итераций декодирования СОК с $d = 9$

ки p_0 на два и более порядков улучить оценки $P_b(e)$ для кодов с малым уровнем размножения ошибок, как в свёрточном, так и в блоковом варианте МПД.

Дальнейшее улучшение оценок требует перехода ко все более сложным ПФВ и точного просчета всех вероятностей на ЭВМ. Однако и уже выполненный анализ дает вполне достаточное представление о природе и степени улучшения решения таких итеративных схем коррекции ошибок, что позволяет пока ограничиться сделанными оценками.

4.3. Многопороговые процедуры для недвоичных кодов

Ниже на основе методов, применявшихся для анализа размножения ошибок в недвоичных кодах в разделе 3.6, получены вероятности ошибки ПД в первом символе линейного систематического блокового или свёрточного q-ичного кода при $q > 2$. Будем считать, что ПД работает в соответствии с процедурой декодирования, описанной для QМПД во второй главе. В этом случае считаем, что ошибки в декодируемых информационных символах имеют вероятность p_0 и независимы, а соответствующие ячейки разностного регистра D перед началом процедуры декодирования равны 0.

Эти правила учитывались при выборе тех конфигураций ошибок, которые приводили к неправильному решению ПД при анализе явления размножения ошибок.

Ниже будут приведены более общие соотношения, определяющие вероятность ошибки в первом символе ПД $P_1(e)$. Как и ранее, будем считать, что декодер работает в канале с независимыми равновероятными ошибками QСК.

Если в двоичном случае для определения вероятности ошибки в первом символе кода типа СОК нужно было просто определить вероятность того, что сумма искаженных проверок и, возможно, ошибок в декодируемом символе, более $d/2$, то в q-ичном коде ошибка происходит, если число ошибочных проверок с одинаковым значением превышает число правильных или (при неправильном декодируемом символе) не меньше этого числа. Тем самым определяется возможность исправления большого числа ошибок веса, гораздо большего, чем $d/2$. Это

происходит всегда, когда число правильных проверок относительно декодируемого символа больше числа одинаковых ошибочных значений проверок.

Определим вероятности наиболее частых сочетаний ошибок канала, приводящих к ошибкам ПД. Если задан код $R = k_0/n_0$, то в блоковом СОК с $J = d–1$ размерность проверки равна $m = Jk_0/(n_0–k_0)$. Полагая оценку вероятности того, что проверка ошибочна, равной

$$p_v = [1-(1-p_0)^m](1-a),$$

где $a = 1–1/(q–1)$, поскольку сумма нескольких ошибок может в $1/(q–1)$-ой доле случаев дать правильную проверку, можно указать следующие искомые непересекающиеся события, приводящие к ошибкам ПД [11, 78].

1. Все проверки и первый декодируемый символ i_0 ошибочны:

$$P_1 = p_0 p_v^J.$$

2. Все проверки ошибочны, среди них есть две одинаковые по значению проверки, а i_0 правилен

$$P_2 = \frac{(1-p_0)\,p_v^J J(J-1)}{2(q-1)} \prod_{i=1}^{J-2}\left(1-\frac{i}{q-1}\right). \qquad (4.5)$$

3. Есть одна правильная проверка, а остальные ошибочны; i_0 также принят неправильно:

$$P_3 = J\,p_0(1-p_v)\,p_v^{J-1}.$$

4. Есть одна правильная проверка, i_0 принят правильно, но среди неправильных проверок есть точно три, совпадающие по значению:

$$P_4 = \frac{(1-p_0)(1-p_v)\,p_v^{J-1}J!}{6\,(q-1)^2(J-4)!} \prod_{i=1}^{J-4}\left(1-\frac{i}{q-1}\right).$$

5. Есть две правильные проверки, i_0 принят неправильно, а среди ошибочных проверок точно две совпадают:

$$P_5 = \frac{(1-p_v)^2\,p_0 p_v^{J-2}J!}{4(q-1)(J-4)!} \prod_{i=1}^{J-4}\left(1-\frac{i}{q-1}\right).$$

6. Из $(J–3)$ неправильных проверок 3 совпадают, а i_0 принят неправильно:

$$P_6 = \frac{p_0(1-p_v)^3 p_v^{J-3} J!}{36(q-1)^2 (J-6)!} \prod_{i=1}^{J-6} \left(1 - \frac{i}{q-1}\right).$$

7. Из (J–2) неправильных проверок есть две пары совпадающих проверок, а i_0 принят неправильно:

$$P_7 = \frac{p_0(1-p_v)^2 p_v^{J-2}(q-2)J!}{8(q-1)^2 (J-6)!} \prod_{i=1}^{J-6} \left(1 - \frac{i}{q-1}\right).$$

8. При двух правильных проверках и правильном символе есть четыре совпадающих проверки, а остальные все различны:

$$P_8 = \frac{(1-p_0)(1-p_v)^2 p_v^{J-2} J!}{48(q-1)^3 (J-6)!} \prod_{i=1}^{J-6} \left(1 - \frac{i}{q-1}\right).$$

Ясно, что при малых J не все из перечисленных выше событий могут быть реализованы. Например, при $J = 4$ события 6, 7 и 8 не происходят и не учитываются. Вероятности других типов событий несущественно влияют на результирующую вероятность ошибок в первом символе $P_1(e)$. График вероятности $P_1(e)$ представлен для блокового кода с $d = 9$, $R = 1/2$ и $q = 256$ на рис. 4.4 кривой 1. Кривой 2 на этом же рисунке показана вероятность $P_1(e)$ для блокового кода с $d = 5$, $R = 1/2$ и $q = 256$. Очень важно, что мажоритарные декодеры в недвоичных каналах оказываются более эффективными в том смысле, что они существенно снижают вероятности ошибки декодера при гораздо более высоком уровне шума p_0 в QCK, чем в ДСК, результаты декодирования ПД в котором были показаны на рис. 4.1.

Вычисление характеристик первого шага (итерации) QМПД указывает на область, в которой уже после первой попытки декодирования происходит заметное снижение доли оставшихся ошибок. Ясно, что в этом случае последующие итерации ещё более понизят плотность оставшихся ошибок. Возможность достижения уровня помехоустойчивости оптимальных методов определяется при этом и кодом, и уровнем шума канала, т.е. так же, как в двоичных кодах.

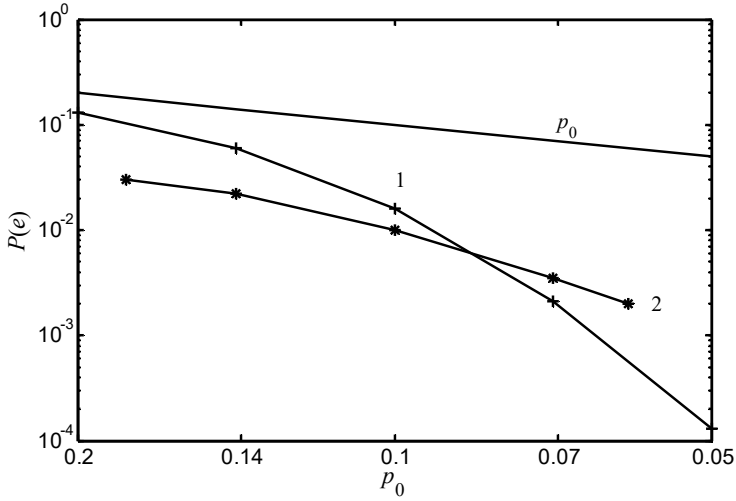


Рис. 4.4. Характеристики недвоичных блоковых ПД в QCK

4.4. Нижние оценки вероятности ошибки недвоичного оптимального декодера

Оценим теперь вероятности ошибки ОД для QCK также в случае использования СОК. Эти оценки могут быть получены двумя способами. С первой точки зрения можно представить недвоичный МПД, который при хорошем выборе параметров кода с небольшим уровнем размножения ошибок будет последовательно улучшать свои оценки в канале QCK. Ясно, что размерности проверок на 2-й, 5-й и прочих итерациях как бы уменьшаются, потому что вероятности всех информационных ошибок на итерациях с большими номерами в проверках оказываются много меньшими, чем неизменяемые вероятности в проверочных символах. Иначе говоря, можно считать, что на достаточно больших итерациях все проверки как бы имеют размерность, равную 1 и меньше этого быть не могут. В этом смысле ситуация, которая имела место при рассуждениях о нижних оценках для вероятности ошибки ОД для двоичных кодов, полностью повторяется и для недвоичных аналогов ОД. А тогда

получается, что это и определяет нижнюю оценку вероятности ошибки МПД, про который из второй главы известно, что его решения сходятся к оптимальному решению.

С другой стороны, можно найти нижние оценки для вероятности ошибки оптимального декодера, рассматривая переходы нулевого кодового слова в ближайшие кодовые слова под воздействием шума ОСК. Очевидно, что в случае СОК это фактически один и тот же подход, при котором все мажоритарные элементы работают так, чтобы сравнить два кодовых слова, отличающихся всего в одном информационном символе. Значит, нижняя оценка для вероятности ошибки ОД будет получена из приведённых выше вероятностей $P_1(e)$ для недвоичных ПД, где вероятности p_ν заменяются вероятностями ошибки канала p_0, как если бы размерности всех проверок становятся равными 1.

Итак, обсудим методику получения нижних оценок вероятностей ОД. Во всех анализируемых далее случаях это будет выявление наиболее часто встречающихся условий того, что вектор ошибки будет иметь расстояние Хемминга до ближайшего кодового слова меньшее, чем его собственный вес. В силу линейности кода этого достаточно для вынесения неправильного решения даже оптимальным переборным (!) алгоритмом. Рассматривая вектор ошибки с такими свойствами, будем учитывать, что нужно анализировать только те символы этого вектора, которые соответствуют позициям проверок относительно очередного декодируемого символа i_0. Выпишем вероятности таких наиболее частых событий, которые всегда приводят к ошибкам оптимального декодера.

К искомым векторам ошибки относятся следующие [1, 64].

1. Все проверочные символы и декодируемый символ i_0 ошибочны:

$$P_1 = p_0^{J+1}, \tag{4.6}$$

где $J = d–1$, d – минимальное кодовое расстояние самоортогонального кода.

2. Все проверочные символы ошибочны, но два из них одинаковы, а i_0 принят верно:

$$P_2 = \frac{(1-p_0)\,p_0^J J(J-1)}{2(q-1)} \prod_{i=1}^{J-2} \left(1 - \frac{i}{q-1}\right). \quad (4.7)$$

3. Есть один правильно принятый проверочный символ, а остальные ошибочны, как и i_0**:**

$$P_3 = J(1-p_0)\,p_0^J. \quad (4.8)$$

4. Есть один правильно принятый проверочный символ, а также i_0, но из всех остальных неправильно принятых символов есть 3 с одинаковыми значениями ошибок:

$$P_4 = \frac{(1-p_0)^2\,p_0^{J-1} J!}{6\,(q-1)^2 (J-4)!} \prod_{i=1}^{J-4} \left(1 - \frac{i}{q-1}\right). \quad (4.9)$$

5. Есть 2 правильных проверочных символа, а все остальные, включая i_0, неправильны, причем есть 2 ошибочно принятых проверочных символа с одинаковыми значениями ошибок:

$$P_5 = \frac{(1-p_0)^2\,p_0^{J-1} J!}{4(q-1)(J-4)!} \prod_{i=1}^{J-4} \left(1 - \frac{i}{q-1}\right). \quad (4.10)$$

6. Есть 3 правильных проверочных символа, а все остальные, включая i_0, неправильны, причем есть 3 ошибочно принятых проверочных символа с одинаковыми значениями ошибок:

$$P_6 = \frac{(1-p_0)^3\,p_0^{J-2} J!}{36(q-1)^2 (J-6)!} \prod_{i=1}^{J-6} \left(1 - \frac{i}{q-1}\right). \quad (4.11)$$

Заметим, что если кодовое расстояние $d < 7$, то уже последний случай рассматривать не следует, так как он предполагает наличие $J = 6$ проверок в коде, тогда как для самоортогональных кодов $d = J+1$. Таким образом, нижняя оценка вероятности ошибки оптимального декодирования определяется суммой найденных выше вероятностей P_i, i =1..6.

Более полное перечисление событий, приводящих к ошибкам недвоичного ОД, и оценки их вероятностей, а также вероятностей ошибки в первом символе недвоичного ПД приведены в [11]. Простая схема QMПД дана в [1]. Разумеется, перечисленных здесь событий, приводящих к ошибке ОД, также вполне достаточно для того, чтобы определяемые ими вероятности ошибки ОД были достаточно точны для всех предварительных оценок.

Далее, поскольку QMПД на каждом шаге стремится к решению ОД, можно ожидать, что при некотором достаточно высоком уровне шума он в большинстве случаев также будет достигать искомого оптимального решения.

4.5. Характеристики мягких МПД алгоритмов

Во второй главе были рассмотрены методы реализации МПД алгоритмов при использовании мягких модемов.

Оценим предельные возможности мягких МПД методами, которые использовались для оценки снизу характеристик ОД в канале типа ДСК. Напомним, что для этого предлагалось вычислять вероятности ошибки при определении значения декодируемого символа в самоортогональном коде только по тем d символам, в которых отличаются два соседних кодовых слова. Для этого удобно использовать производящие функции вероятности, аналогичные ПФВ для двоичных кодов и порогового декодера, работающего в ДСК.

Пусть есть $M = 2^m$ уровней квантования сигнала при передаче двоичного потока и вероятности p_i, $i = 0..M–1$, попадания решения мягкого модема в i-й фрагмент области решения, в соответствии с разделом 2.4. В достаточно общем случае выполнения оценок можно определить ПФВ для мягкого модема:

$$A_M(x) = \sum_{j=0}^{M-1} p_j x^{(2j-M)b} ,$$

где b – это небольшое число, не превышающее обычно 5.

Тогда для рассматриваемого кода с $d = J–1$ вероятность ошибки при правильном выборе областей решений мягкого модема и достаточно удобных для вычислений значений параметра b будет определяться выражением

$$P_{b\text{ОД}}(e) = \sum_{i>0} c_i , \qquad (4.12)$$

где c_i определяются из выражения

$$A_d(x) = A_M(x)^{J+1} = \sum_{\{I\}} c_i x^i , \qquad (4.13)$$

где $\{I\}$ – множество всех возможных значений показателей степени, которые получаются при обычном возведении в степень ПФВ (4.13).

На рис. 4.5 представлены нижние оценки вероятности ошибки ОД при мягком приёме двоичных потоков для $M = 16$ и различных значений d, вычисленные согласно (4.12). Сопоставление этих графиков показывает, что мягкие ОД на самом деле на 1,5–2 дБ более эффективны, чем жёсткие. Это весьма большое преимущество мягкого приёма имело решающее значение при почти полном переходе к мягким декодерам в большинстве реальных систем и сетей связи.

4.6. Характеристики МПД для каналов со стираниями

Рассмотрим характеристики самоортогонального кода при декодировании в каналах со стираниями с использованием МПД. Допустим, что на различных итерациях декодирования происходит постепенное восстановление стираний в информационных символах. Полагая, что есть стирающий канал с вероятностью случайно появляющихся стёртых символов p_s мы получим вероятность невосстановления первого декодируемого символа блокового кода, если сам символ стёрт и все проверки стёрты из-за того, что, по меньшей мере, один символ в каждой из проверок, относящихся к стёртому символу, также стёрт. Эти же условия подразумевались при анализе зависимости группирования символов в главе 3.

Итак, пусть анализируется в качестве примера самоортогональный код с $R = 1/2$ и некоторым d. В этом случае размерность всех проверок равна $J = d–1$. Тогда вероятность того, что данная проверка стёрта, равна

$$p_v = 1 - (1 - p_s)^J .$$

И, наконец, вероятность невосстановления первого символа равна в рассматриваемом декодере

$$P_s(s) = p_s p_v^J .$$

Ясно, что на различных итерациях при таком алгоритме будут последовательно исправляться, точнее, восстанавливаться информационные символы. Но на следующих итерациях будут новые успешные попытки восстановления. Если часть информационных символов будет восстановлена, что создаст новые проверки, способствующие восстановлению других символов,

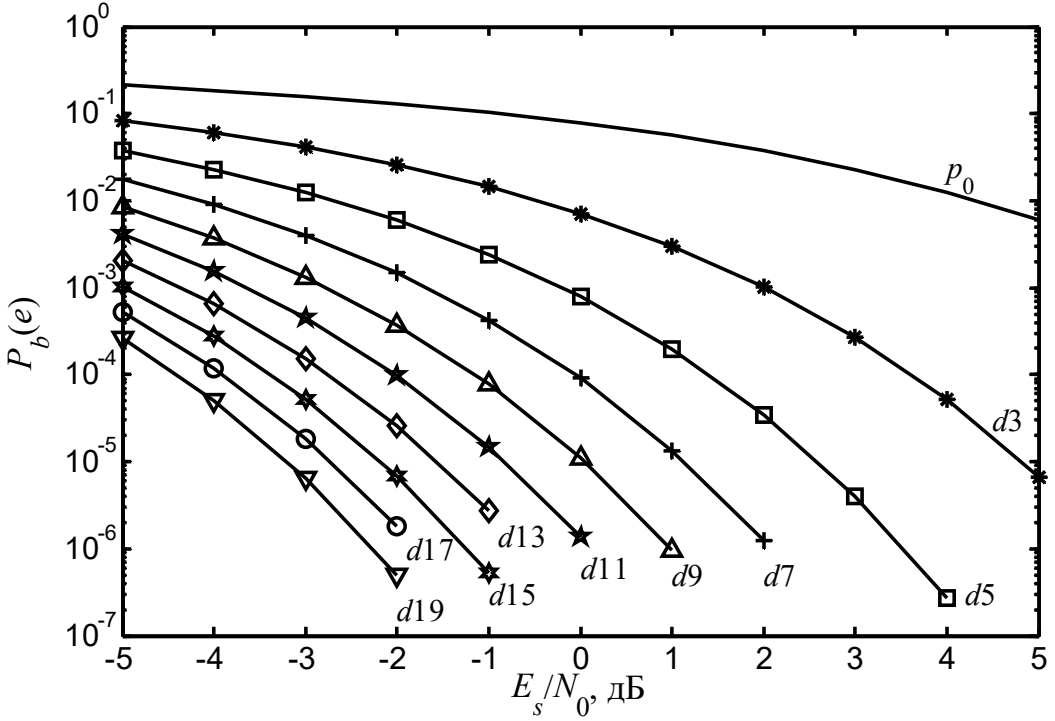


Рис. 4.5. Нижние оценки вероятностей ошибки на бит оптимального декодера для СОК в гауссовском канале

то итеративный процесс будет успешным. Но если в проверке стёрт проверочный символ, такая проверка никогда не будет полезной для восстановления каких-либо символов.Этим и определяется нижняя оценка для вероятности невосстановления информационных символов. Символ точно не будет восстановлен, если он стёрт, как и все J проверочных символов, относящихся к нему, что и определяет нижнюю оценку для невосстановления символов даже в оптимальном переборном декодере:

$$P_{s\text{ОД}}(s) = p_s^d .$$

На рис. 4.6 представлены графики вероятности невосстановления стёртых символов $P(s)$ кода с $R = 1/2$ и $d = 7$ для одношагового декодера (кривая «МПД, $I = 1$») и в оптимальном декодере – $P_{s\text{ОД}}(s)$ (кривая «ОД») для стирающего канала с вероятностями стираний p_s (кривая «p_s»). Кроме того, представлены экспериментальные результаты для многошагового МПД декодера при числе итераций $I = 8$ (кривая «МПД, $I = 8$»). Как видно из графиков, многошаговая процедура восстановления стираний хорошо работает даже непосредственно вблизи пропускной способности канала при p_s~0,5.

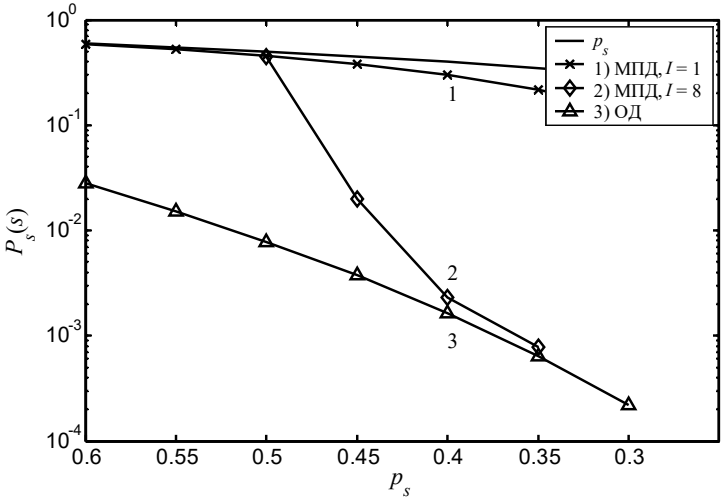


Рис. 4.6. Характеристики блоковых МПД декодеров на потоках стираний в каналах с замираниями при $d = 7$ и $R = 1/2$

4.7. Методы улучшения верхних оценок характеристик алгоритма

Рассмотренные выше аналитические оценки характеристик относительно простых вариантов МПД предусматривали для упрощения оценок использования кодов с переменными связями, что позволяло упростить учет влияния эффекта размножения ошибок. Кроме того, при вычислениях вероятностей ошибки на тех или иных шагах декодера неоднократно вместо истинных значений этих величин приходилось пользоваться их верхними оценками. Наконец, при итоговых преобразованиях выражений для вычислений средних вероятностей ошибки на бит и на символ приходилось существенно завышать получаемые вероятности, поскольку иначе нужно было вносить в анализ характеристик правильные, но не доказанные строго предположения о свойствах алгоритма.

Перечисленные причины привели к тому, что несущественное отличие характеристик МПД от оптимальных для данных кодов имеет место для МПД с двумя итерациями декодирования только при малых уровнях шумов. Вместе с тем, как было показано в предыдущей главе, чрезвычайно важным является то обстоятельство, что можно найти именно такие длинные коды, что эффект размножения ошибок будет проявляться в них в весьма малой степени. Иначе говоря, вероятность наличия не только второй, но и третьей ошибки ПД стремится для таких кодов в ДСК к нулю при $p_0 \to 0$. Но это одновременно означает, что при наличии двух ошибок декодирования в блоке кода рассматриваемого типа для условной вероятности ошибки в третьем символе $P_{3/1,1}(s)$ справедливо неравенство $P_{3/1,1}(s) << 1$ [77].

При переходе к производящим функциям вероятностей более высокой размерности с учетом трех, четырех и большего числа ошибок удалось бы еще точнее определить реальные возможности МПД аналитическими методами. Однако это сопряжено со значительными вычислительными трудностями. Кроме того, потенциальная эффективность МПД оказывается реализованной в достаточной степени, если осуществляется от 3 до 10 и более итераций декодирования. Поэтому необходимо кроме получения принципиальных аналитических результатов, изложен-

ных в этой главе, иметь и методы приближенной оценки реальной эффективности МПД при большом числе итераций декодирования.

4.8. Границы эффективного использования мажоритарных методов

Результаты 3 главы свидетельствуют о возможности реального снижения уровня размножения ошибок при выборе достаточно длинных кодов с переменными связями. Это значит, что в таких случаях для любых символов i_m и i_j кода имеет место если не точное, то хотя бы приблизительное равенство

$$P(e_j=1) \sim P(e_j=1/e_m=1),$$

где e_j и e_m – ошибки декодирования обычного, т.е. одношагового мажоритарного алгоритма.

Но если эти ошибки декодера оказываются почти независимыми, то, очевидно, оценить те граничные значения вероятности ошибки, например, p_0 в ДСК, ниже которых применение МПД эффективно, можно путем вычисления средней вероятности ошибки на бит после первой, второй и последующих итераций так, как если бы и ошибки декодера на всех итерациях, входящие в проверки, были независимы.

Этот очень простой и удобный подход состоит, например, для свёрточных кодов в том, что все ошибки, вероятности появления которых участвуют в вычислениях вероятностей ошибки декодирования, делятся на ошибки предыдущей итерации (или канала ДСК или гауссовского с мягким модемом для первого порогового элемента) с вероятностью p_{i-1} и ошибки текущей i-ой попытки коррекции с вероятностью p_i. Тогда для нахождения вероятности p_i нужно при заданной вероятности p_{i-1} решить уравнение

$$p_i = f(p_i, p_{i-1}, p_0), \qquad (4.14)$$

где $f(\cdot)$ – функция, определяющая обычный способ вычисления вероятности ошибки декодера, описанный в [4] и в данной главе, однако, реализованный для различных вероятностей входящих в проверки ошибок.

Например, для свёрточного кода с $R = 1/2$, $d = 7$ при шести проверках в j-ой проверке оказывается j–1 символов с вероятно-

стью ошибки p_i, 6–j символов с вероятностью p_{i-1} и один (проверочный) с вероятностью канала p_0. Вероятность того, что j-ая проверка, содержащая перечисленные ошибки будет также ошибочна, равна

$$P_j = p_a(1-p_b)(1-p_0)+(1-p_a)p_b,$$

где

$p_a = 0{,}5[1-(1-2p_i)^j]$,

$p_b = 0{,}5[1-(1-2p_{i-1})^{d-1-j}]$,

p_0 – вероятность ошибки в ДСК.

Тогда, используя ПФВ, включающую и тривиальную проверку системы проверочных уравнений для вычисления вероятности ошибки порогового декодера вида

$$A(x) = (p_{i-1}x + 1 - p_{i-1})\prod_{j=1}^{6}(P_j x + 1 - P_j) = \sum_{j=0}^{7} a_j x^j ,$$

получаем, что

$$p_i' = \sum_{j=4}^{7} a_j . \qquad (4.15)$$

Численное решение уравнения (4.14) состоит в выборе такого p_i, чтобы в (4.15) для найденных из предыдущей итерации значений p_{i-1} имело место равенство $p_i' = p_i$.

Результаты применения предложенных оценок к свёрточному СОК для определения вероятностей ошибок декодера после первой, второй и третьей итерации представлены на рис. 4.7 для кодов с $d = 7$ (группа кривых 3–5) и $d = 11$ (группа кривых 6–8). Отмечая, что кривая с «I=1» в каждой группе является оценкой для обычного ПД, можно сделать вывод о существенном улучшении результатов декодирования свёрточных кодов МПД по сравнению с традиционными ПД по меньшей мере в случае использования длинных кодов класса СОК с малым уровнем.

Наконец, подчеркнем, что предложенная методика является всего лишь оценочной, зависимость решений декодера по мере увеличения номера итерации и уменьшения числа оставшихся ошибок декодера возрастает, а реальные характеристики декодирования будут, конечно, для большого числа итераций хуже, чем получается в результате использования изложенного здесь

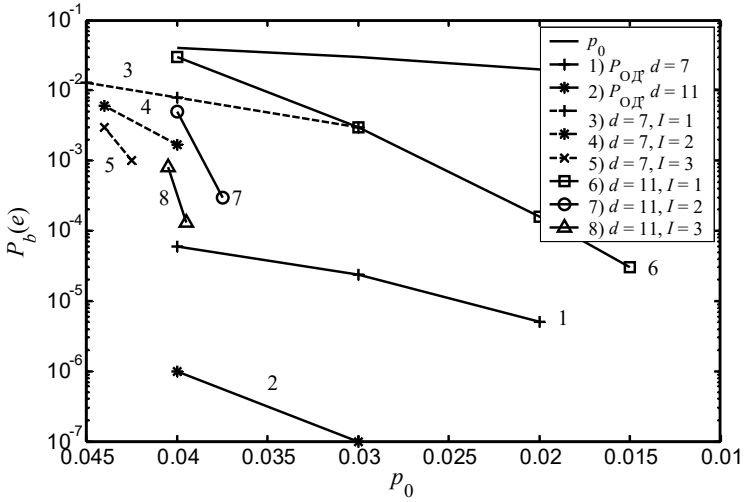


Рис. 4.7. Вероятности ошибки МПД после первой, второй и третьей итерации декодирования свёрточного СОК

подхода. Но основную свою задачу – оценку границы области эффективной работы – данный подход вполне решает. На рис. 4.7 указаны также зависимости вероятности ошибки ОД для СОК с $d = 7$ (кривая 1) и $d = 11$ (кривая 2).

Анализ кривых для СОК с $d = 7$, который анализировался выше, показывает, что предложенные в этом параграфе методы действительно существенно улучшают оценки характеристики МПД по сравнению с нижними оценками эффективности, изложенными в разделе 4.3.

Ясно, что в случае использования блоковых кодов также применим рассматриваемый подход. Однако построение оценок для блоковых кодов несколько осложняется по сравнению со свёрточными в связи с тем, что даже в пределах выполнения одной итерации фактическая размерность проверок оказывается переменным числом. Это происходит из-за того, что, например, после декодирования самого первого символа блока может оказаться, что ошибка в этом символе есть в проверках относительно второго символа, но, возможно, что ее и не будет, что опре-

деляется порождающими полиномами кода. Отсюда следует, что вероятности появления ошибочных проверок также зависят от номера символа, к которому эти проверки относятся. Таким образом, вероятности ошибки декодирования всех символов, входящих в проверки относительно некоторого символа, оказываются все различными между собой и поэтому должны при оценке вероятности декодирования очередного символа учитываться, т.е. перерассчитываться отдельно.

Чтобы не выполнять эту трудоемкую вычислительную цепочку, можно воспользоваться оценками вероятности ошибки дефинитного декодера, которые фактически будут верхними оценками для более эффективного декодера с обратной связью. Исходя из того, что сначала вероятности ошибки в символах, поступивших в декодер, равны p_0, а затем p_1, p_2 и т.д., получаем, что для вычисления оценки p_i необходимо просто вычислить с помощью ПФВ вероятность ошибки на символ после первой итерации

$$p_1 = \varphi(p_0, p_0),$$

где первая переменная в функции $\varphi(.)$ соответствует вероятности ошибки в информационных символах, а вторая – в проверочных. Затем, поскольку информационные ошибки на второй итерации декодирования в МПД имеют вероятность p_i, а проверочные – p_0:

$$p_2 = \varphi(p_1, p_0),$$

и т.д.:

$$p_i = \varphi(p_{i-1}, p_0).$$

Ясно, что исходя из такого подхода к получению верхних оценок, изменяется лишь способ вычисления вероятности ошибки p_{i-1} в $J = d-1$ одинаковых проверках. Для $i = 1$ имеем для j-ой проверки

$$P_{j,1} = [1-(1-2p_0)^J].$$

Тогда результирующая ПФВ имеет вид

$$A(x) = (p_0 x + 1 - p_0)(P_{j,i} x + 1 - P_{j,i})^J, \qquad (4.16)$$

где $i = 1$.

Для всех же $i \geq 2$ вероятность наличия ошибочной проверки оказывается равной

$$P_{j,i} = 0{,}5[1-(1-2P_{j,i-1})^{J-1}](1-p_0) + 0{,}5[1-(1-2P_{j,i-1})^{J-1}](1-p_0),$$

для $i \geq 2$, а вероятность ошибки на символ вычисляется вновь на основе ПФВ (4.16), но уже и для $i \geq 2$.

Предложенный подход реализован при оценках граничных входных вероятностей эффективности блокового двоичного СОК с $d = 11$. Результаты вычисления верхних оценок вероятности при одной, двух и трех итерациях декодирования представлены на рис. 4.8, которые показывают, что более реальные, чем верхние строгие оценки раздела 4.2, и простые методы вычисления вероятностей ошибки МПД оказываются существенно лучшими. Как оказалось, в частности, МПД с $R = 1/2$ для СОК $d = 11$ действительно позволяет осуществлять эффективное декодирование при $p_0 = 0{,}035 \div 0{,}07$.

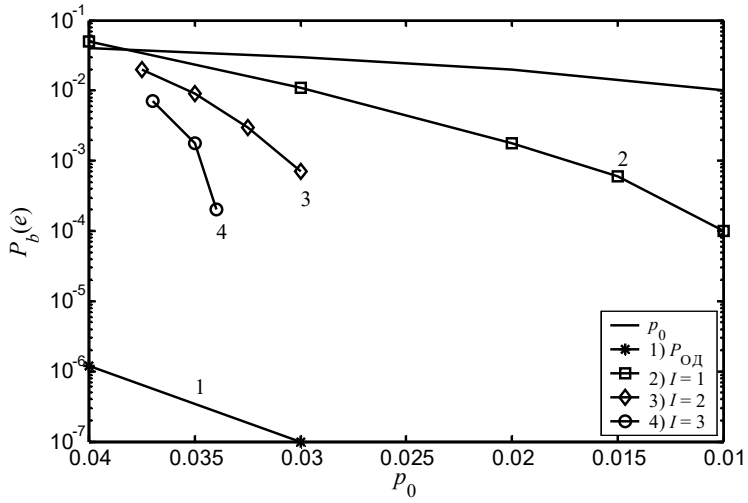


Рис. 4.8. Верхние оценки вероятности ошибки при одной, двух и трех итерациях МПД декодирования

4.9. Методы улучшения характеристик МПД

Изложенные в предыдущем разделе методы оценки тех уровней шума канала типа ДСК, ниже которых декодер МПД может работать существенно эффективнее, чем традиционные мажоритарные ПД, оказываются весьма близкими к реальным, особенно для кодов с малым проявлением эффекта размножения ошибок, то есть достаточно длинных. Почти все методы, улучшающие реальные характеристики МПД алгоритмов, оказываются уже не столь простыми, как сама идея многократного использования мажоритарного декодера. Ниже описан, пожалуй, единственный способ простого улучшения возможностей мажоритарного алгоритма, не требующий усложнения декодера, но позволяющий расширить границы эффективной работы МПД.

Рассмотрим поведение обычного ПД, если увеличить значение порога в пороговом элементе на 1 и 2 по сравнению со стандартным уровнем $T_0 = J/2$, где J – число ортогональных проверок кода типа СОК. Пусть выбран код с $d = 11$. Тогда, следуя [4] и методам, изложенным в разделах 4.2, с помощью ПФВ вычисляется вероятность ошибки декодирования, например, первого символа кода, складывающаяся из двух групп событий. К первой относятся все сочетания проверок, когда декодируемый символ i_0 с вероятностью $1–p_0$ принят верно, а ко второй, когда он принят ошибочно.

Если для вероятности наличия m или более ошибочных проверок ввести обозначение P_m, то вероятность ошибки в первом символе [4] $P_1(e)$ приобретает простой вид

$$P_1(e) = P_{T_0} p_0 + P_{T_0+1}(1 - p_0) .$$

Если увеличить значение порога T на небольшую величину $\Delta = 1, 2,...$, т.е. $T = T_0+\Delta$, то декодер не будет вносить ошибок в сообщение, если искаженных проверок не более T, $T > T_0$, хотя и будет отказываться от коррекции некоторых ошибок веса $T_0 – \Delta$, т.е. менее T_0:

$$P_{1\Delta}(e) = P_{T_0-\Delta} p_0 + P_{T_0+\Delta}(1 - p_0) . \qquad (4.17)$$

Это значит, что ПД с завышенным порогом вносит меньшее число собственных ошибок, но не исправляет некоторых ошибок в информационных символах, принятых из канала. В част-

ности, для компонент выражения (4.17) для малой вероятности ошибки в канале справедливо соотношение

$$P_{T_0+\Delta+1} / P_{T_0-\Delta} \sim p_0^{2\Delta+1}.$$

Именно уменьшение вклада самого декодера в формирование ошибок, которые потом придется передавать другому ПД, является самым существенным свойством такой схемы. Неисправленные же при первой попытке декодирования ошибки будут в своём большинстве обнаружены и откорректированы на следующих каскадах МПД.

На рис. 4.9 представлены результаты расчета вероятности ошибки в первом символе $P_1(e)$ блокового кода с $R = 1/2$, $d = 11$ и $\Delta = 0, 1, 2$ (кривые 2–4).

Как следует из вида графиков, лучшие результаты при малом уровне шума дают ПД с $\Delta = 0$, что и должно иметь место для рассматриваемых типов каналов и кодов. Однако, при большой вероятности ошибки в канале более хорошие, хотя и не намного, результаты получаются при $\Delta > 0$, что позволяет рекомендовать этот метод при реализации предельно возможных характеристик МПД.

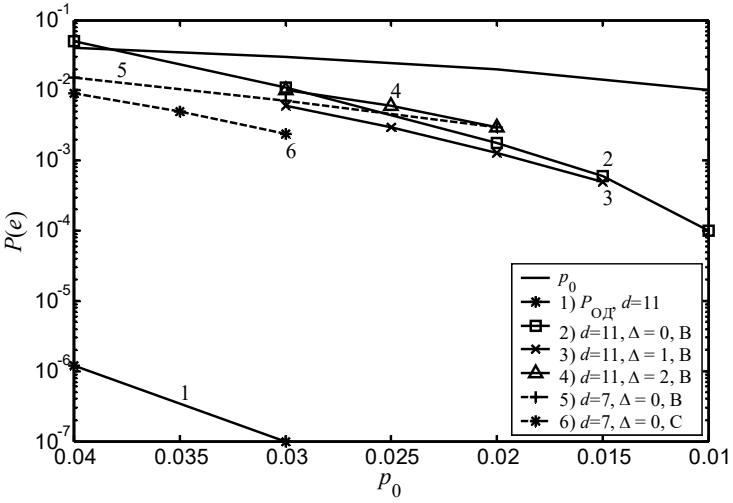


Рис. 4.9. Вероятность ошибки в первом символе $P_1(e)$ блокового кода

Сделаем еще одно замечание, связанное со всегда сложной проблемой выбора кодов. На этом же рис. 4.9 приведены пунктиры 5 и 6 соответственно для блокового и свёрточного кодов, которые для СОК с $d = 7$ являются, как и кривая 2 для $d = 11$ на этом рисунке, результатом вычисления вероятности $P_1(e)$ при $\Delta = 0$. Аналогично алгебраическим методам декодирования, для ПД с $\Delta = 0$ можно также отметить более высокие характеристики кодов с меньшими значениями d по сравнению с более мощными, если уровень шума достаточно высок. Это обстоятельство окажется полезным при формировании эффективных процедур кодирования на основе МПД.

4.10. Улучшение оценок характеристик «мягких» МПД

В [46] обсуждались вопросы реализации эффективных мажоритарных функций в «мягких» МПД и было показано, что при малом уровне шума мажоритарные схемы с модемами, квантующими свои решения о двоичных принятых символах на $M = 4$ уровня, могут обеспечить в гауссовском канале предельные характеристики, на 1,2÷1,4 дБ лучше, чем «жесткие» модемы. При этом оказывается, что требуется вычислить достаточно простую функцию правдоподобия L' из (2.6)

$$L' = W_{\text{inf}}(2d_{\text{inf}} - 1) + \sum_{jv=1}^{d-1} W_{jv}(2s_{jv} - 1), \qquad (4.18)$$

где s_{jv} – значения 0 или 1 проверок относительно декодирующего символа i_j, W_{jv} – коэффициенты, равные небольшому целому числу, если проверочный символ, соответствующий рассматриваемой проверке, оценен как надежный, и равный 1, если достоверность принятого решения по оценке модема мала, d_{inf} – значение символа разностного регистра D, относящегося к символу i_j, W_{inf} – аналогичный коэффициент, определяемый надежностью принятого символа i_j.

Однако, для определения границы области эффективной работы «мягкого» МПД использование соотношения (4.18) показывает, что улучшение характеристик первого декодера в «мягком» МПД по сравнению с «жёстким» мало, что не позволяет применять его эффективно, т.е. при существенно более высоком

уровне шума. Правда, более простая задача повышения достоверности в малых шумах при этом решается.

Анализ причин малой эффективности такого МПД показал, что недостатки принятой схемы декодирования связаны с тем, что веса проверок определяются в (4.18) только надежностью приема проверочного символа кода. В то же время большинство ошибочных проверок, т.е. проверок, значения которых отличаются от истинной ошибки в декодируемом информационном символе i_j, связаны с ненадежным решением о каком-либо другом символе i_n, входящем в проверки, что приводит к резкому снижению эффективности использования весовых коэффициентов, поскольку их значения обычно не соответствуют реальной достоверности проверок.

Рассмотрим достаточно простое изменение в принципе выбора весов W_{jv}, которое позволит более эффективно использовать весовые коэффициенты проверок именно при начальных итерациях МПД при большом шуме, поскольку функция (4.18) уже является оптимальной для малого шума и небольшой доли остаточных ошибок на последних ступенях МПД. Пусть веса всех проверок определяются наименее надежным символом i_m, входящим в проверки относительно символа $m \neq j$. Иначе говоря, если все символы, кроме i_j, приняты надежно, то и $W_{jv} = 3$ для данной проверки независимо от надежности приема декодируемого символа. В противном случае $W_{jv} = 1$.

Проводя с использованием функции L' вычисление вероятности $P_1(e)$ с оценками надёжности по этому принципу, получаем существенно улучшенную для больших шумов оценку вероятности ошибки в первом символе блокового кода $P_1(e)$ для $R = 1/2$ и $d = 5$ при $M = 4$ уровнях квантования, как показано кривой «М=4, 2В» на рис. 4.10. Этот график зависимости вероятности ошибки $P_1(e)$ дополнен кривой «М=4, 1В» для такого же блокового кода, соответствующей первому этапу вычисления весов проверок, определяемых надежностью приема только проверочных символов кода, а также кривыми «М=2, Т=2.5» и «М=2, Т=3.5» для вероятности $P_1(e)$ МПД для $M = 2$ при $T_0 = 2{,}5$ и $T_1 = 3{,}5$.

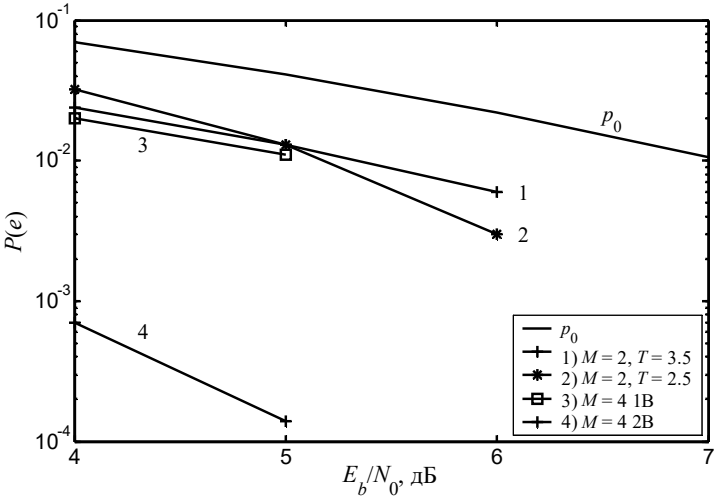


Рис. 4.10. Сравнение влияния методов вычисления весов проверок и назначения порогов на вероятности ошибки ПД

Таким образом, небольшое изменение способа вычисления весовых коэффициентов проверок позволяет существенно улучшить характеристики используемых кодов при их декодировании методами МПД при большом уровне шума в случае использования мягких модемов. Обобщение полученных результатов на 8 и 16 уровней квантования очевидно и также может быть в некоторых случаях полезным.

Из рассмотренного материала следует также важный результат, который активно используется при проектировании МПД: даже когда пороги для мажоритарных элементов не равны величине $J/2$, а превышают её, условия теоремы многопорогового декодирования выполняются, и алгоритм на каждом шаге при изменении декодируемых символов приближается к оптимальному решению. На самом деле верно и ещё более общее утверждение: для некоторых наборов весов проверок в МПД декодере для ДСК также будут выполняться условия теоремы 2.2, и при этих весах превышение порога также будет строго приближать решение МПД к оптимальному решению. Очевид-

но, что таких наборов весов проверок может достаточно много. Эти вопросы будут обсуждаться в главе 5.

4.11. Выводы

В данной главе получены приближенные оценки средней вероятности ошибки на бит $P_b(e)$, вероятности ошибки и невосстановления стираний в первом символе блоковых, свёрточных, двоичных и недвоичных кодов, исправляющих ошибки и стирания для различных вариантов многопорогового декодирования.

Сопоставление полученных оценок с известными данными по мажоритарным методам декодирования различных кодов позволяет уже на основе только аналитических оценок сделать следующие выводы.

Использование МПД значительно улучшает достоверность передачи данных, как в блоковом, так и в свёрточном варианте применения алгоритма.

Эффект размножения ошибок декодирования значительно усложняет оценку характеристик декодирования, особенно при большом уровне шума. Однако этот эффект оказывается существенно меньшим в более длинных кодах, чем в коротких, что позволяет для длинных кодов строить оценки характеристик, достаточно хорошо совпадающих с теми или иными реальными возможностями рассматриваемого алгоритма: вероятностями невосстановления символов и приближенными оценками средних вероятностей ошибки.

Рассмотренные оценки являются полезными ориентирами при изучении экспериментальных характеристик МПД, полученных при моделировании каналов и декодеров на ЭВМ, которые изложены ниже.

ГЛАВА 5. ХАРАКТЕРИСТИКИ МНОГОПОРОГОВОГО АЛГОРИТМА

5.1. Экспериментальные методы исследования

Изложенные в предыдущей главе результаты свидетельствуют о возможности достижения весьма высоких характеристик декодирования на основе алгоритма МПД без существенного усложнения исходного мажоритарного декодера [4]. Вместе с тем, получение аналитических характеристик с приемлемой точностью для МПД, как и для других алгоритмов, возможно для используемых кодов только при относительно небольшом уровне шума. Перечисленные причины приводят к необходимости изучения экспериментальных характеристик декодирования кодов с числом итераций декодирования $I = 3 \div 50$ в каналах с большим шумом с помощью имитационных методов. Важным полезным обстоятельством, облегчающим проведение таких исследований средствами моделирования каналов и алгоритмов на ЭВМ, оказывается то, что вероятности ошибки декодирования для кодов с невысокими значениями кодового расстояния при малом отношении сигнал/шум оказываются достаточно большими, лежащими в диапазоне от 10^{-3} до 10^{-7}. Это позволяет обеспечивать достаточный объем моделирования при умеренных вычислительных затратах и рациональных потребностях в машинном времени.

Достижение точности и полноты изучения работы декодера при передаче сообщений по каналам с шумами возможно только при использовании хороших и достаточно быстродействующих датчиков случайных чисел. Вопросы их реализации и качества рассматривались в [56, 79, 80, 81, 82, 83, 84, 85].

Таким образом, моделирование оказывается единственным возможным методом исследования работы МПД с большим числом итераций, особенно при большом уровне шума канала, что, в конце концов, и представляет наибольший интерес при решении вопросов реализации тех или иных декодеров. При этом за относительно небольшое время, обычно от нескольких секунд до 1÷3 часов могут быть получены при моделировании, например, на ПЭВМ с тактовой частотой около 3 ГГц результа-

ты, достаточно точные для правильной предварительной оценки характеристик любой модификации МПД.

5.2. Системы имитационного моделирования

Для реализации простого и быстрого моделирования работы различных алгоритмов декодирования в каналах с большим уровнем шума были разработаны программный и программно-аппаратный имитационные комплексы оценки эффективности цифровой передачи данных по спутниковым и иным каналам связи, в которые включено достаточно большое число различных современных эффективных систем повышения достоверности передачи данных, используемых в реальных сетях связи [86]. Эти имитаторы позволяют оценивать возможность применения в разрабатываемых системах различных декодеров корректирующих кодов, что создает возможность быстро и правильно спроектировать все узлы создаваемых новых коммуникационных систем с учётом требуемых уровней энергетической эффективности, сложности реализации, задержки принятия решения и других критериев выбора систем повышения достоверности. Аналоги таких имитаторов, хотя бы приблизительно сопоставимые с ними по качеству представления результатов, удобству работы и разнообразию используемых методов кодирования в настоящее время неизвестны.

Подчеркнём, что многие возможности исследования и анализа методов кодирования, которые обеспечивает применение имитатора, являются действительно уникальными. Это относится как к возможности моделирования алгоритма Витерби с длиной кодирующего регистра до $K \sim 20$, так и к способности анализировать турбо коды, многопороговые и некоторые другие алгоритмы при задержках решений о коррекции ошибок до миллиона и более битов. Применение имитаторов обеспечивает возможность заглянуть в будущее техники кодирования, анализировать потенциальные возможности ещё только проектируемых систем связи. Заметим, что программное обеспечение имитаторов постоянно обновляется и соответствует уровню лучших мировых достижений в технике и технологии кодирования. Использование программно-аппаратных версий имитатора позво-

ляет на 2–3 порядка повысить скорость имитационного моделирования работы декодеров в каналах с большим уровнем шума по сравнению с чисто программной версией имитатора. Разумеется, программный имитатор оказывается более гибким в выборе моделируемых кодов. При этом обеспечивается примерно в 20–50 раз более быстрое выполнения работ по моделированию работы декодеров по сравнению с традиционными подходами к проблеме определения эффективности алгоритмов декодирования, основанными на разработке отдельных программ имитации их работы.

Развитие обеих систем имитации каналов и алгоритмов декодирования продолжается путём расширения типов анализируемых каналов и алгоритмов декодирования.

Вместе с программами построения кодов с низким уровнем размножения ошибок и средствами оптимизации тысяч значений весов, порогов и разностных соотношений кодов описанные программные и аппаратно-программные средства образуют важную часть автоматизированной системы проектирования МПД декодеров, успешно используемую при создании этих алгоритмов для конкретных систем заказчика.

Далее в этой главе рассмотрены основные характеристики МПД для блоковых и свёрточных двоичных и недвоичных кодов в каналах с независимыми ошибками и стираниями, полученные на основе моделирования алгоритма. Кроме того, приводятся результаты по использованию МПД в режиме сжатия данных. В выводах по данной главе анализируются основные соотношения и свойства метода, выявленные в процессе изучения полученного экспериментального материала.

5.3. Характеристики МПД в двоичном симметричном канале

На рис. 5.1 представлены возможности МПД и АВ в канале типа ДСК. На нём даны графики зависимости эффективности декодирования на основе МПД для разных длин кодов с кодовой скоростью $R = 1/2$, поскольку длина кода полностью определяет размеры кодера и может быть достаточно критическим параметром системы кодирования. Кривая «МПД, n_A=100» от-

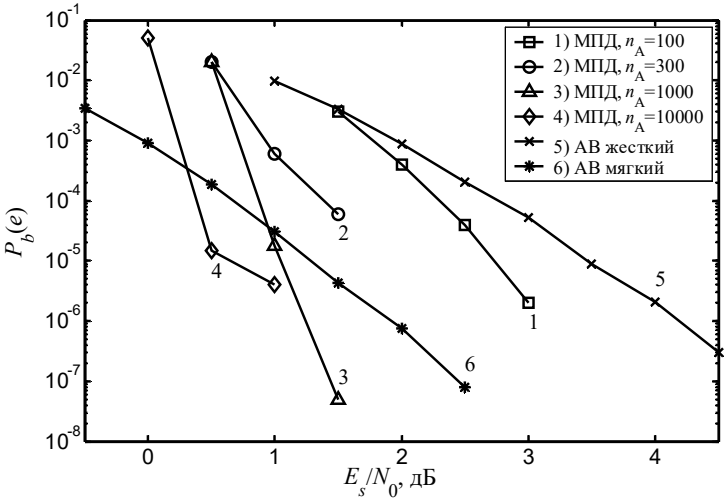


Рис. 5.1. Характеристики некоторых эффективных алгоритмов декодирования в каналах типа ДСК

носятся к коду длины $n_A = 100$, декодируемому с помощью МПД с не более чем $I = 10$ итерациями, а кривые «МПД, n_A=300» и «МПД, n_A=1000» соответствуют кодам с длинами 300 и 1000. Наконец, график, обозначенный как «МПД, n_A=10000» относится к особенно мощной системе кодирования/декодирования в ДСК для кода длины 10000 и $I \sim 20$ итерациями декодирования.

Для удобства сопоставления возможностей МПД и АВ на этом же графике показаны характеристики АВ для стандартного кода с $K = 7$ и $R = 1/2$ как в ДСК (кривая «АВ жесткий»), так и в гауссовском канале с мягким модемом (кривая «АВ мягкий»).

Как следует из вида графиков, в канале типа ДСК достаточно эффективными при вероятностях ошибки декодирования $P_b(e) \sim 10^{-6}$ и менее будут МПД для кода длины порядка 1000. При этом аппаратная версия МПД на приёмной стороне будет также очень простой, быстродействующей и гораздо более эффективной, чем даже декодер Витерби с мягким модемом. Это

оказывается возможным из-за фактически оптимального декодирования достаточно длинного кода на основе алгоритма МПД.

В качестве ещё одной возможной схемы кодирования, представленного на рис. 5.1, можно рассматривать и очень длинный код «МПД, n_A=10000». Целесообразность его применения очевидна, если нет ограничений по задержке принятия решения.

5.4. Характеристики МПД в гауссовских каналах

На рис. 5.2 показаны характеристики МПД алгоритмов для гауссовского канала и «мягких» модемов с параметрами, аналогичными рассмотренным на графиках рис. 5.1 для канала ДСК.

Как и для случая канала ДСК характеристики всех МПД построены с числом итераций во всех случаях равным $I = 10$. Исключением является самый левый на рис. 5.2 график «МПД, n_A=5000» очень эффективного и длинного кода (его длина кодового ограничения $n_A = 5000$ битов) с $I = 25$. Кроме того, представлены пунктирные графики для жёсткого и мягкого стандартного АВ для кода с $K = 7$, возможности МПД для свёрточных кодов с длинами n_A, равными 100, 300, 1000**.** Дополни-

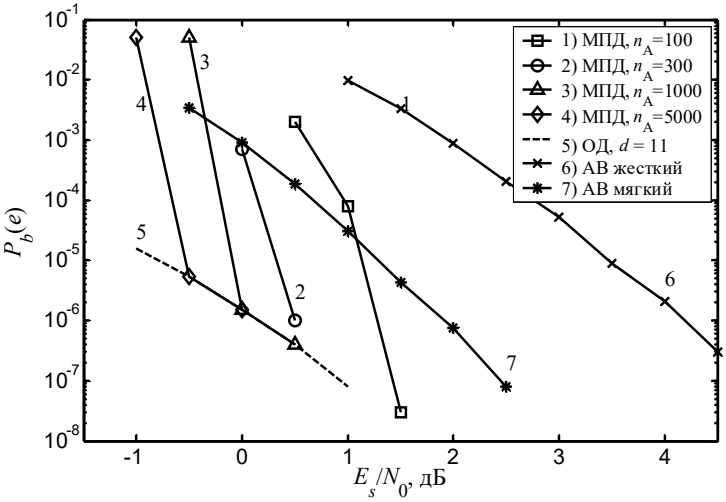


Рис. 5.2. Характеристики мягких МПД и АВ в гауссовском двоичном канале связи

тельно приведен также график «ОД, d=11» для случая оптимального декодирования при использовании кодов с $d = 11$.

Поскольку на рис. 5.2 для МПД использовались коды именно с $d = 11$, эта нижняя оценка хорошо отображает вместе с графиками для МПД его возможности как алгоритма, который при очень малых вычислительных затратах обеспечивает практически оптимальные характеристики, обычно достижимые только для переборных экспоненциально сложных методов. Анализ последних публикаций о возможностях МПД показывает также, что при других значениях R и d характеристики МПД оказываются столь же высокими, как и при параметрах, представленных на рис. 5.2.

Сравнение возможностей МПД и АВ показывает, что во всех рассмотренных случаях применения МПД обеспечиваемая им энергетика оказывается на 1÷2 дБ лучшей, чем при использовании АВ. Заметим, что при аппаратной реализации МПД будет весьма быстродействующим, с производительностью порядка 100 Мбит/с и более.

Переход к блоковым кодам требует применения более длинных блоков по сравнению с длиной кодового ограничения свёрточного кода. В этом случае при небольшом, порядка 0,2÷0,4 дБ снижении характеристик будет в несколько раз уменьшена задержка принятия решений по сравнению со свёрточными кодами.

5.5. Малоизбыточные коды

Если использование кодов со скоростью $R = 1/2$ невозможно из-за необходимости двукратного расширения полосы частот канала связи, можно применить малоизбыточный код с $R = 4/5$. В этом случае расширение полосы частот составляет около 25%. На рис. 5.3 приведены характеристики самоортогональных кодов с $d = 7$ и $d = 9$ совместно с «жесткими» и «мягкими» модемами. Во всех случаях предполагается использование в МПД $I = 10$ итераций. Как следует из приведённых результатов моделирования двух кодов в ДСК и кода с $d = 7$ в гауссовском канале улучшение характеристик декодирования при работе в гауссов-

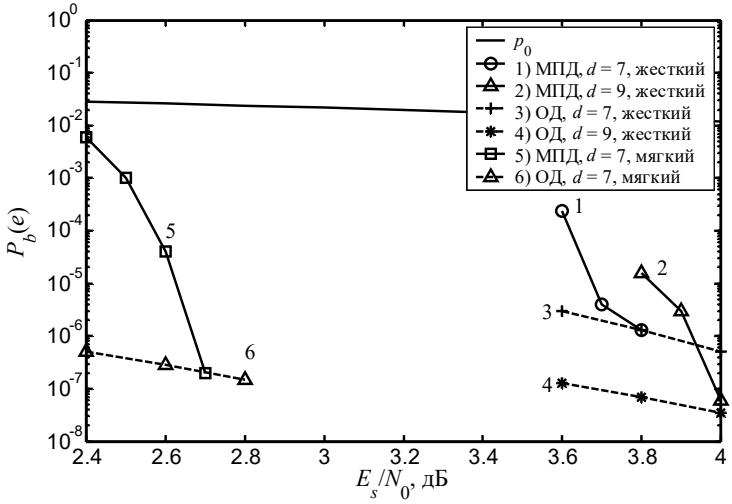


Рис. 5.3. Характеристики самоортогональных кодов с $d = 7$ и $d = 9$ при их использовании с «жесткими» и «мягкими» модемами

ском канале может составить около 1,3 дБ, что и демонстрирует полезность применения «мягких» модемов.

5.6. Недвоичные декодеры многопорогового типа

Во многих системах особенно удобно работать с данными, имеющими байтовую структуру. Это соответствует кодам с $q = 256$. Отметим, что, кроме кодов Рида-Соломона (РС), в настоящее время вообще нет других сколько-нибудь эффективных и просто реализуемых методов декодирования недвоичных символьных данных. Сравним вероятностные характеристики кодов РС с возможностями QМПД. Будем считать, что выбран код РС длины 255 символов (символ – 8 битов). Подчеркнём, что для QМПД никаких ограничений по длине кода вообще нет, поскольку он выполняет только операции сложения и вычитания по mod 256 и сравнения.

Очевидно, что недвоичный пороговый элемент, рассмотренный в главе 2 при описании операций в QМПД, является простейшим устройством или подпрограммой с числом опера-

ций N сложения и сравнения небольших целых чисел $N \sim 20 \div 50$ для всех тех небольших значений минимального кодового расстояния d, $d < 15$, которое следует применять в таком декодере.

На рис. 5.4 представлены характеристики декодеров для кодов РС с различной кодовой скоростью R и длиной $n = 255$ и QМПД в QСК. По горизонтальной оси отложены вероятности ошибки p_0 в указанном канале, а по оси ординат – средние вероятности ошибки на символ в результате декодирования.

Для достижения решения, совпадающего с оптимальным или близкого к решению ОД, QМПД для $q = 256$ необходимо от 5 до 20 итераций (повторных попыток) декодирования принятого сообщения. Это полностью соответствует возможностям метода МПД для двоичных кодов. Укажем также ещё раз, что реальная граница эффективности недвоичных МПД соответствует гораздо более высокому уровню шума, чем в двоичном случае.

Как следует из вида графиков зависимостей средней вероятности ошибки декодирования на символ $P_S(e)$ от вероятности p_0 канала QСК на входе декодеров для кодовых скоростей $R = 1/2$, $R = 4/5$ и $R = 7/8$ (кривые 4–6), простейший по своему

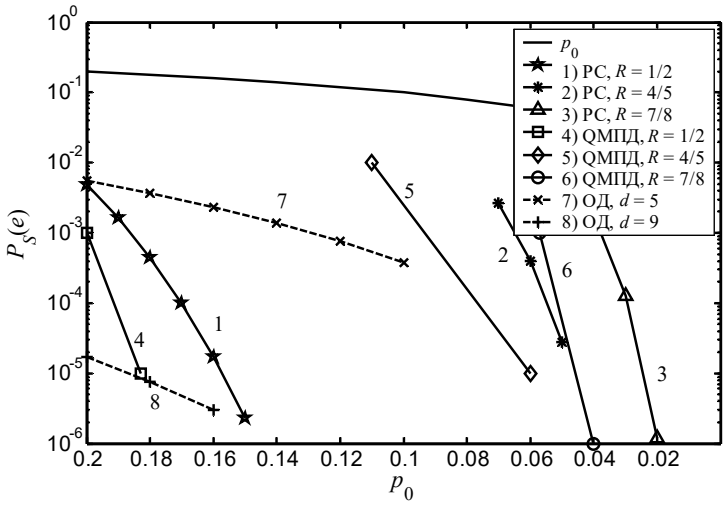


Рис. 5.4. Эффективность QМПД и кодов Рида-Соломона

устройству QMПД обеспечивает гораздо более высокие характеристики, чем декодеры для кода РС (кривые 1–3), благодаря несколько большей длине $n = 1000$ используемых кодов и вследствие этого хорошей сходимости решений QMПД к решению ОД. Разница по вероятности ошибки декодирования QMПД и кодов РС составляет для рассмотренных случаев несколько десятичных порядков.

Для сопоставления на рис. 5.4 приведены также нижние оценки для применявшихся при моделировании недвоичных СОК в случае оптимального декодирования для $d = 5$ и 9 (кривые 7 и 8), полученные с использованием методов главы 4.

Заметим, что в настоящее время неизвестны другие алгоритмы декодирования с приемлемой сложностью реализации, которые могут обеспечить такие же характеристики. При увеличении длин кодов характеристики QMПД могут быть ещё существенно улучшены без каких-либо дополнительных вычислительных затрат.

Очевидно, что каскадирование нескольких недвоичных МПД также значительно улучшит вероятностные характеристики декодирования без значительного увеличения сложности, т.е. числа операций, осуществляемых декодером, работающим только с целыми числами и не выполняющего никаких операций умножения или деления. Это является его решающим преимуществом перед алгоритмами для кодов РС при сопоставлении их по сложности реализации.

Представленные результаты позволяют утверждать, что описанные более 20 лет назад недвоичные МПД обладают действительно высокой эффективностью, недоступной для декодеров кодов РС. При этом сложность реализации QMПД весьма невелика и, как показывает детальный анализ, может быть дополнительно значительно снижена [1, 64, 78, 101].

5.7. Декодирование в стирающих каналах

На рис. 5.5 представлены результаты моделирования работы МПД в каналах с независимо возникающими стираниями.

Для канала с большой вероятностью стираний $p_s \sim 0{,}5$ показаны возможности МПД декодера с $I = 10$ итерациями для трёх вариантов выбора кодовых скоростей $R = 1/3$, $R = 1/2$ и $R = 2/5$ (кривые 1–3). Как следует из приведённых данных, итеративный подход на много порядков улучшает характеристики восстановления ошибок по сравнению с [4]. Заметим, что успешная коррекция с помощью МПД возможна в непосредственной близости от теоретической границы – пропускной способности канала C, поскольку она равна $C = 1–p_s \sim 1/2$.

Во второй версии кода с $R = 2/5$ (кривая 4) число итераций восстановления символов было увеличено при моделировании процесса декодирования до $I = 15$. Кроме того, для этого второго эксперимента потребовалось найти специального вида код, более адаптированный к работе вблизи пропускной способности канала. Как следует из сопоставления результатов двух экспе-

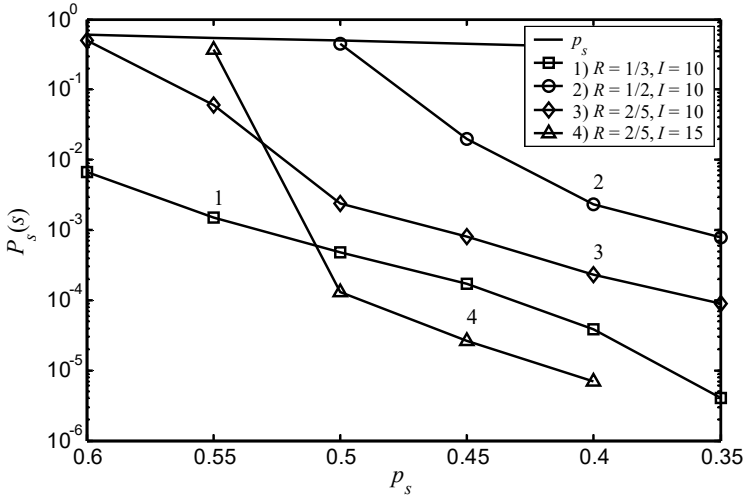


Рис. 5.5. Характеристики многошаговых МПД в каналах со стираниями

риментов при $R = 2/5$, даже весьма высокие характеристики восстановления стираний в первом варианте могут быть дополнительно улучшены при небольших дополнительных усилиях, как это сделано во втором случае.

5.8. Сжатие данных на базе МПД

Как уже было показано в главе 4, МПД без всяких изменений может быть использован для сжатия, например, двоичных последовательностей с сильно неравновероятным распределением нулей и единиц. Фактически поведение МПД в шумящем канале в режиме сжатия ничем не отличается от работы при наличии неравномерной энергетики канала [45], когда вероятности появления ошибок в подканалах передачи информационных и проверочных символов кода различны из-за неодинакового отношения сигнал/шум в этих подканалах.

На рис. 5.6 представлены графики экспериментально полученной зависимости вероятности неправильного восстановления символов кода $P_r(e)$ при сжатии в $A = 4$ раза бернуллиевских последовательностей с различными вероятностями появления еди-

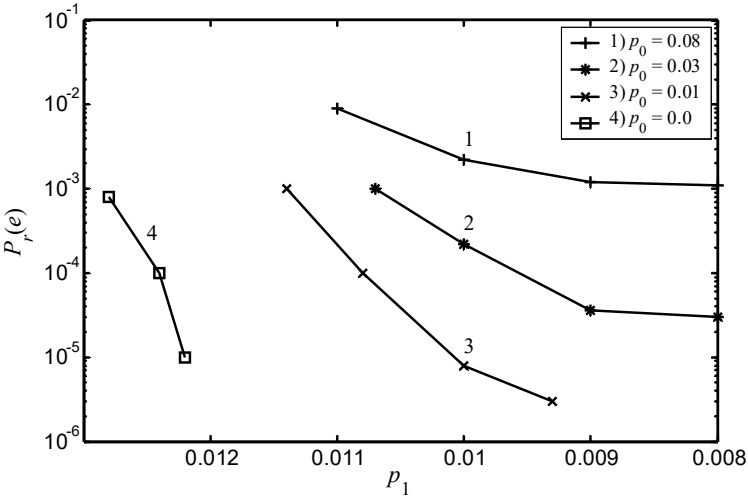


Рис. 5.6. Характеристики сжатия бернуллиевских источников с $A = 4$ в ДСК на базе МПД

ниц p_1. Цифры около каждой кривой соответствуют вероятности ошибки p_0 в ДСК, по которому ведется передача сжатой последовательности перед ее восстановлением с использованием кода с $R = 4/5$. Отметим, что полученные для МПД результаты соответствуют его работе при столь высоких уровнях шума и значений вероятностей ошибки p_0, что, например, вероятности $P_r(e) = 10^{-4} \div 10^{-5}$ на выходе МПД, недостижимы для всех последовательных алгоритмов декодирования, поскольку коэффициент сжатия $A = 4$ оказывается больше, чем вычислительный коэффициент сжатия A_b для рассматриваемого потока в канале.

Например, $A_b = 4$ при $p_0 = p_1 = 0{,}0055$, тогда как МПД успешно восстанавливает данные даже при $p_0 = 0{,}03$.

5.9. Сложность программной реализации

Рассмотрев характеристики эффективности МПД, обратимся к сложностным параметрам этого алгоритма. При рассмотрении сложности программной реализации декодера фактически применяется классический для теории алгоритмов подход к проблеме сложности как к оценке числа операций, необходимых для того, чтобы декодировать один информационной символ.

Начнём с простейшего порогового алгоритма для двоичных потоков данных. При кодировании необходимо выполнить только вычисление проверочных символов. Если применяется код типа СОК с минимальным кодовым расстоянием d, то каждый информационный символ следует добавить по mod 2 к проверочным символам кода в качестве слагаемого d–1 раз. Это и есть сложность кодирования, которое всегда оказывается очень простой процедурой.

В декодере, который содержит в линейном коде всегда и кодер для обеспечения вычисления синдрома кода, сначала нужно снова вычислить проверочные символы кода по принятым информационным, а затем сложить вычисленные и принятые из канала символы по mod 2 для вычисления вектора синдрома, что приводит к сложности этого шага, равной d. Далее идёт собственно шаг декодирования, на котором просто складываются обычным образом $J = d$–1 проверок относительно декодируемого символа i_j. И в том случае, если алгоритм выбран так,

что почти все символы канала в нём исправляются, т.е. вероятность ошибки p_0 в ДСК достаточно мала, то с вероятностью порядка p_0 все проверки и декодируемый символ должны быть инвертированы, для чего требуется d операций. Таким образом, среднее число операций декодера оценивается как

$N_{\text{ПД}} = (2+p_0)d$.

Рассмотрим оценки сложности МПД. Он отличается от ПД тем, что многократно, а именно I раз суммирует проверки и элемент разностного регистра для каждого информационного символа. Число исправлений декодируемых символов в ряде случаев определяется тем, что часть декодируемых символов на первых этапах (итераций) декодирования корректируется ошибочно. Эти дополнительные ошибочные символы будут исправлены на последних итерациях декодирования. Поэтому ориентировочно можно считать, что доля изменений от общего числа информационных символов близка к $2p_0$. Этого достаточно, чтобы оценить среднюю сложность МПД для СОК при I итерациях с учётом наличия разностного регистра как

$$N_{\text{МПД}} = (I+1+2p_0)(d+1). \qquad (5.1)$$

Как следует из последнего выражения, фактическая сложность МПД равна просто произведению числа итераций I на кодовое расстояние d. Переходя к оценкам сложности программной реализации на основе формальной алгоритмической оценки (5.1), можно считать, что программные затраты, связанные с архитектурой процессора, с вычислением индексов массивов и организацией циклов вычислений могут в 3–8 раз увеличивать число необходимых для реализации МПД алгоритма операций. Опыт проектирования программных кодовых систем показывает, что эти оценки вполне приемлемы. В частности, подписанный в процессе разработки МПД протокол сопоставления сложности программной реализации алгоритма Витерби и МПД, подтверждает, что предложенные оценки уровней «накладных расходов» для IBM-совместимых персональных компьютерах с операционной системой семейства Windows вполне реалистичны и могут использоваться в предварительных оценках производительности программных МПД. Как следует из протокола, МПД на компьютере с тактовой частотой 2,8 МГц обеспечивает

на 3,0 дБ более высокие уровни ЭВК при одновременно в 4 раза большей производительности по сравнению с АВ при кодовой скорости $R = 3/4$.

Измерение производительности МПД на микропроцессорной технике также соответствует сделанным оценкам.

Углублённый анализ программных версий МПД показал также, что основное время работы декодера тратится на то, чтобы подсчитывать суммы проверок на различных итерациях декодирования. При этом в большинстве случаев результат подсчёта суммы проверок не приводит к инвертированию декодируемых символов. Это связано как с тем, что эти суммы оказываются просто такими же, что и на прошлой итерации, так и с тем, что сумма проверок для типичного информационного символа в абсолютном большинстве случаев существенно меньше значения порога почти на всех итерациях с достаточно большими номерами, даже если некоторые из символов, входящие в проверки сами тоже были перед вычислением проверок изменены. Эта ситуация стала отправной при исследовании возможности дополнительного снижения объёма вычислений в программных версиях МПД, которые и так весьма малы.

Оказалось, что при достаточно незначительном снижении реализуемого в МПД ЭВК, можно дополнительно во много раз снизить число операций МПД алгоритма. Если у конкретного МПД алгоритма ЭВК близок, например, к 8 дБ, то 0,1 дБ потерь вполне приемлемая величина. Итоговая средняя сложность МПД алгоритма при столь незначительных потерях ЭВК оказалась равной

$$N_{\text{МПД2}} = c_1 d + c_2 I, \qquad (5.2)$$

где c_1 и c_2 – небольшие целочисленные коэффициенты.

Подчеркнём, что сложность такого модифицированного МПД алгоритма оказывается по числу операций примерно на 2 десятичных порядка меньшей, чем для других методов коррекции ошибок с сопоставимой эффективностью [1, 76, 86, 87, 88, 89, 100].

Хороший пример программной версии МПД декодера в модификации, соответствующей чрезвычайно малой сложности реализации (5.2), может быть переписан со специализированно-

го информационно-методического и научно-образовательного двуязычного сайта ИКИ РАН **www.mtdbest.iki.rssi.ru**. На образовательной странице «Обучение» нужно найти гиперссылку «demo_quick» и переписать exe-модуль этой сверхбыстрой демопрограммы вместе с массивами входных данных и простой инструкцией по её использованию. Эта программа одновременно демонстрирует высокую эффективность работы МПД и в канале с заметной пакетной компонентой шума. На массиве размером 3 млн. битов программный МПД демонстрирует производительность порядка 1 млн. битов информации на каждые 1 ГГц тактовой частоты работы компьютера при достаточно высоком уровне шума канала. Эта программа может быть использована для декодирования реальных цифровых потоков в специальной цифровой телевизионной системе с кодированием в канале связи специальными кодами, которые заявлены стандартизованными для телевизионных систем такого типа. Одновременно эта программа успешно декодирует наряду с гауссовской компонентой шума одновременно возникающие пакеты ошибок размером в несколько десятков битов, полностью исправляя такие «всплески» шума без снижения производительности. Длительность пакета ошибок в демопрограмме регулируется, как и уровень шума гауссовской компоненты потока ошибок, что хорошо иллюстрирует высокие характеристики МПД в трудной шумовой обстановке.

Другие алгоритмы декодирования с сопоставимой эффективностью и столь экстремально высокой производительностью в программной версии неизвестны.

5.10. Требования к аппаратуре кодирования

К аппаратным версиям декодеров предъявляются совершенно другие требования, чем к их программным вариантам. Хотя многие микропроцессоры позволяют коллективное использование памяти и имеют многоядерные процессорные узлы, тем не менее, эти обстоятельства весьма просто учитываются при оценке таких усовершенствованных модификаций компьютеров и степени ускорения вычислений в программных реализациях алгоритмов.

В случае создания аппаратных декодеров наличие десятков и сотен параллельно работающих небольших вычислителей принципиально меняет подход к проблеме выбора алгоритма декодирования цифровых потоков в больших шумах. Это в полной мере относится также и к аппаратуре, построенной на элементной базе ПЛИС, в том числе Xilinx, Altera и других типов. В этом случае решающим фактором является способность алгоритма к достаточно полному распараллеливанию, что только и обеспечивает действительно огромное преимущество аппаратных версий декодеров перед программными. Неплохим примером метода, хорошо поддающегося распараллеливанию, является алгоритм Витерби, что и позволило уже много лет назад создать достаточно производительные декодеры этого типа, правда, только для небольших длин свёрточных кодов, поскольку сложность АВ экспоненциально растёт с увеличением длин используемых кодов.

Хорошие возможности распараллеливания МПД алгоритма вполне очевидны. При аппаратной реализации, например, свёрточных кодов все пороговые элементы реализуются независимо и параллельно в разных частях БИС и, таким образом, сложность МПД в аппаратной версии совпадает с обычным ПД, где главные затраты связаны с реализацией именно пороговых элементов. Это многократно, в 20–50 раз ускоряет работу аппаратного МПД по сравнению с прочими алгоритмами, поскольку для многих других высокоэффективных при большом шуме декодеров проблема реального ускорения работы благодаря аппаратному распараллеливанию оказывается очень трудной. Но это только первый уровень распараллеливания.

Оказалось, что МПД допускает ещё одну не менее эффективную возможность ускорения вычислений. В самом деле, МПД, как и обычный ПД, в основном только подсчитывает суммы проверок. Это суммы не очень большого числа малоразрядных целых чисел и можно поставить задачу сформулировать условия на элементы декодера, параметры используемых кодов, модема и величины порогов в пороговых элементах, которые позволили бы даже при большом уровне шума реализовать функции суммирования и сравнения в пороговом элементе мак-

симально простыми и быстрыми средствами. Эта проблема также была полностью и однозначно решена. Сейчас пороговые элементы для многих видов кодов можно в целом ряде случаев сделать такими, что они будут выдавать решение на каждом такте сдвига регистров свёрточного МПД. В некоторых случаях необходимо несколько адаптировать кодовые полиномы применяемых кодов к требованиям особенно простого распараллеливания и ускорения работы пороговых элементов.

В результате такой реализации второго уровня распараллеливания операций в МПД этот декодер превращается в устройство, которое для внешнего наблюдателя как бы вообще не выполняет каких-либо вычислений. Иначе говоря, сторонний наблюдатель как бы видит, что на каждом такте сдвига данных в регистрах сдвига МПД одновременно и мгновенно формируются и все решения всех пороговых элементов о предстоящих изменениях декодируемых символов.

Но это означает, что в таком МПД как бы не производится никаких вычислений и все ограничения на производительность этого декодера связаны только с предельной скоростью продвижения данных по регистрам сдвига декодера и с количеством таких параллельно работающих в декодере регистров. Поскольку одноразрядные сумматоры по mod 2, сумматоры небольших целых чисел и стандартные регистры сдвига относятся к самым быстрым элементам цифровой техники, простые оценки показывают, что производительность такого аппаратно реализованного МПД при описанном подходе оказывается примерно на 3 десятичных порядка более высокой, чем у других алгоритмов при высоком уровне шума и может варьироваться в широких пределах. Таким образом, можно утверждать, что не только по критериям высокого энергетического выигрыша, но и по параметрам производительности МПД является очень эффективным устройством с абсолютно рекордным быстродействием. Отметим, что производительность свёрточного МПД, которая как бы вообще незаметна «со стороны», до некоторой степени похожа на ситуацию с достижением абсолютных параметров, например, абсолютного нуля в физике или 100%-го к.п.д. в теплофизике.

Вопросы приближения к предельно возможным значениям энергетики МПД алгоритмов также успешно решаются.

5.11. Характеристики МПД декодеров на ПЛИС

На рис. 5.7 представлены последние достижения в области высокоскоростных декодеров типа МПД на современных ПЛИС для кодовой скорости $R \sim 1/2$. Кривая «МПД ПЛИС Xilinx» относится к разработке свёрточного МПД на ПЛИС Xilinx [88, 102] на скорости ~100 Мбит/с, который может быть легко реализован на скоростях до 480 Мбит/с. Он существенно более эффективен по сравнению с АВ (кривая «АВ, К=7») и достаточно мало отличается от возможностей стандартной и весьма эффективной каскадной схемы декодирования с АВ и декодером кода Рида-Соломона (график «АВ+РС»), но оказывается значительно проще.

Далее график «МПД ПЛИС Altera» приведён для декодера МПД с 40 итерациями декодирования, построенного на ПЛИС Altera. Подчеркнём важнейшее свойство такого аппаратного МПД: эта обычная базовая схема декодера этого типа, т.е. она

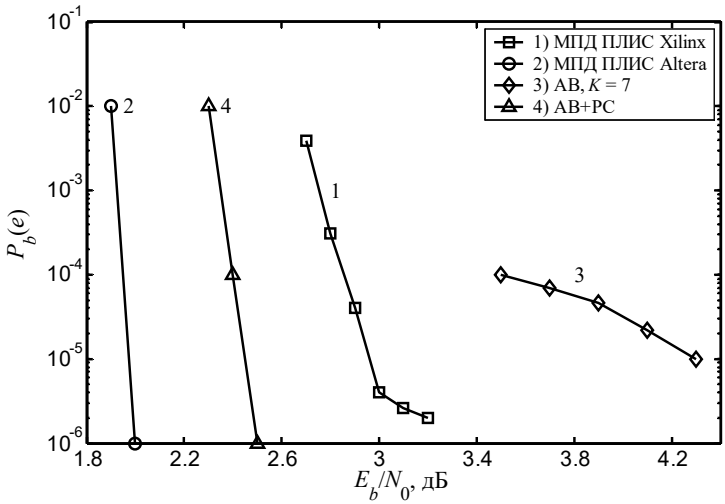


Рис. 5.7. Характеристики стандартного АВ и лучших МПД декодеров в гауссовском канале

даже не относится к каскадным конструкциям, но оказывается существенно более эффективной по уровню шума, при котором она работает, чем все предыдущие схемы на рис. 5.7. Столь высокая его эффективность обусловлена новыми реальными достижениями в поиске кодов с низким уровнем размножения ошибок при их коррекции, что в свою очередь и позволило перейти к большему числу итераций декодирования. Можно утверждать, что такая схема, безусловно, относится к лучшим некаскадным процедурам коррекции ошибок, известным в теории и технике кодирования. Разумеется, успешная работа МПД алгоритма в условиях столь большого уровня шума в соответствии с фундаментальными свойствами кодов оказывается возможной только при значительном увеличении их длины и задержки декодирования.

Данная схема реализована на ПЛИС Altera при информационной скорости более 200 Мбит/с.

5.12. ЭВК алгоритмов декодирования

Ниже на рис. 5.8 рассмотрены графики для энергетического выигрыша кодирования (ЭВК) МПД, данные для которых взяты из рис. 5.7. Предполагается, что границы областей решений в «мягком» модеме выбраны близкими к оптимальным и в дальнейшем не обсуждаются [25]. Для целей сопоставления разных методов декодирования там же представлены графики ЭВК для стандартного АВ с $K = 7$, стандартного каскадного кода (АВ и код РС), а также весьма эффективного вблизи пропускной способности канала декодера для турбо кода [1, 35]. Все коды имеют кодовую скорость $R = 1/2$, кроме каскадного кода АВ+РС, у которого скорость $R = 0{,}5 \cdot 0{,}875 = 0{,}4375$. Как следует из сравнения данных методов, характеристики МПД могут быть очень близкими к максимально возможным по энергетике. При этом МПД в своём свёрточном варианте будут, видимо, примерно на 2 порядка более быстрыми, чем другие алгоритмы. Самая верхняя кривая показывает предельные теоретически возможные величины ЭВК, соответствующие равенству $R = C = 1/2$.

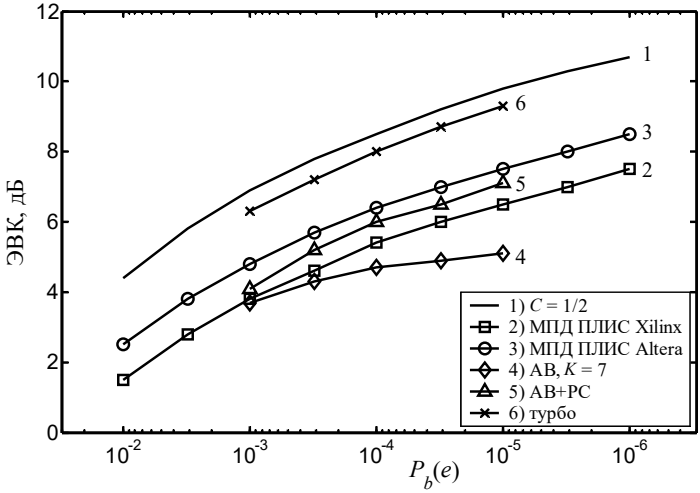


Рис. 5.8. Характеристики современных методов кодирования

На следующем рис. 5.9 для кодов с оптимальным декодированием показаны зависимости предельно возможных значений конечной вероятности ошибки на бит $P_b(e)$ при различных значениях минимального расстояния d как функции от входного уровня отношения сигнал/шум, выраженного в дБ, для гауссовского канала. Эти графики дополнены кривыми равного энергетического выигрыша, что позволяет оценивать возможности разных методов кодирования. Данный графический материал позволяет простыми способами оценить реальные значения ЭВК для любых алгоритмов кодирования в гауссовских каналах, как с «мягкими», так и с «жёсткими» модемами.

В качестве примера использования графиков на рис. 5.9 для оценки ЭВК любых методов кодирования в центре этого рисунка указана точка А при значении $E_s/N_0 = 1{,}0$ дБ и $P_b(\text{e}) \sim 2 \cdot 10^{-4}$. Эта точка находится прямо на кривой G7. Иначе говоря, эта точка соответствует «первичному» ЭВК 7 дБ. Чтобы определить, истинное значение ЭВК для того алгоритма, которому в данном примере соответствует точка А, следует вычесть из

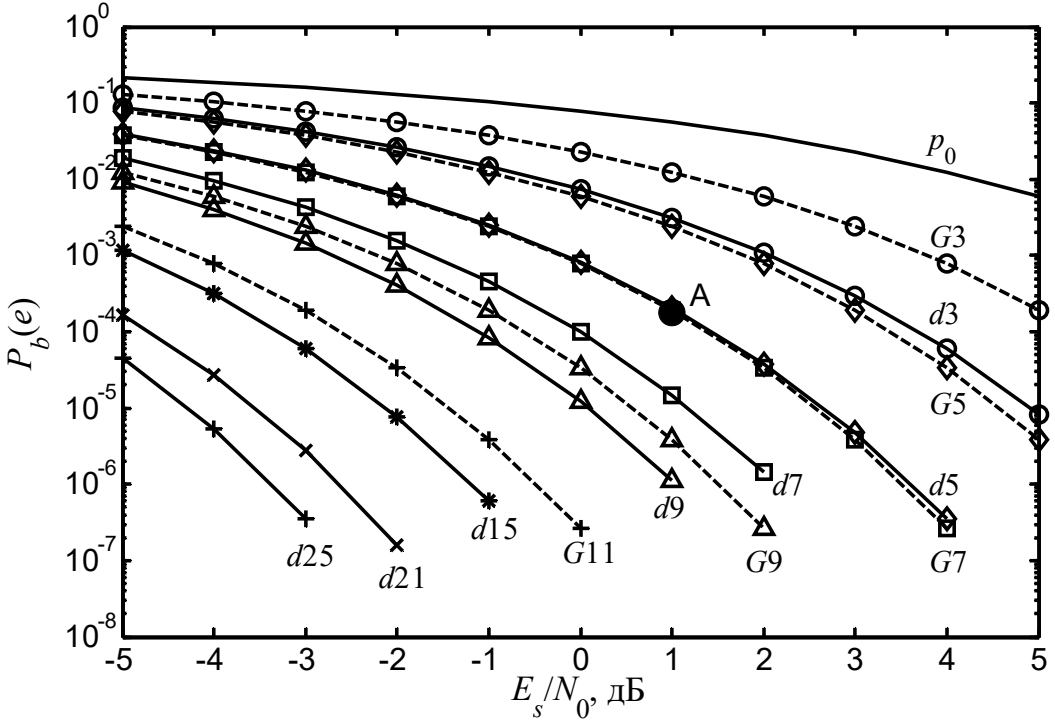


Рис. 5.9. Графики зависимости вероятностей ошибки на бит и ЭВК от кодового расстояния *d* оптимально декодируемых кодов в гауссовском канале

значения 7 дБ ту величину потерь в энергетике, которая определяется кодовой скоростью используемого кода. Например, если $R = 1/2$, то потери составят 3 дБ, что соответствует истинному уровню ЭВК в рассматриваемом примере 4 дБ, а при скорости $R = 3/4$ эти потери близки к 1,25 дБ, что приводит к величине истинного ЭВК, равной 5,75 дБ.

5.13. Адаптивность алгоритмов МПД

Рассмотренные выше свойства МПД алгоритмов позволяют сделать выводы об их высоких характеристиках, которые можно реализовать в различных системах. Следует иметь в виду, что число различных требований, которые предъявляются к системам кодирования, может превышать 10–20 позиций, часть из которых, возможно, будет весьма противоречивыми. В связи с этим весьма полезно рассмотреть взаимосвязи различных параметров кодов и декодеров типа МПД, учёт соотношений между которыми позволит выбирать наиболее подходящие их сочетания для каждой конкретной системы связи.

Отметим сначала, что высокая скорость декодирования МПД в аппаратном виде становится возможной благодаря тому, что правильный выбор кодов и декодеров позволяет максимально распараллелить операции коррекции ошибок. Для достижения столь высоких скоростей требуется выбор свёрточного кода, для которого как раз и легче всего реализовать максимально быстрый декодер. Если необходимо обеспечение работы МПД при большом шуме, то нужно увеличить число итераций и найти максимально длинный код. Все три обсуждаемых параметра декодера приводят к росту задержки решения декодера, и этот путь вполне приемлем в высокоскоростных каналах связи.

В тех случаях, когда нет необходимости добиваться максимальной производительности декодера, можно наоборот уменьшить длину кодов и количество итераций. Если оказывается, что этого недостаточно, то можно перейти к блоковым кодам. Тогда задержку решения можно резко уменьшить до величин порядка длины выбранного кода. Если при этом упадёт эффективность декодирования, то можно увеличить количество пороговых эле-

ментов, работающих параллельно, что позволит в свою очередь снизить время декодирования.

Наконец, в тех случаях, когда необходима минимальная задержка принятия решений, например, в низкоскоростных каналах, можно использовать более сложные кодовые конструкции, где допускается значительный рост вычислительной нагрузки на каждый декодируемый символ или некоторые их группы. В дальнейшем при допустимом снижении скорости декодирования следует перейти к программным методам коррекции ошибок, что, как уже отмечалось выше, вполне возможно в рамках многопороговых процедур.

Таким образом, можно сделать вывод о том, что для МПД алгоритмов между памятью декодера, задержкой решения, числом операций на бит данных, избыточностью, длиной блока кода, уровнем помехоустойчивости, формой реализации декодирования, способностью распараллеливания возможны разнообразные обменные соотношения в широком диапазоне значений. Длины блоков, задержки принятия решения, производительность и объёмы памяти могут изменяться в пределах до двухтрёх десятичных порядков, что в принципе позволяет найти приемлемые компромиссные решения при проектировании различных систем связи. Отметим, что изложенный в этой главе материал свидетельствует о действительно высоком уровне возможностей находить разумные соотношения перечисленных параметров для МПД алгоритмов, что для некоторых других алгоритмов декодирования может оказаться весьма проблематичным.

5.14. Оптимизация параметров декодеров МПД

Применение МПД в каналах с большим уровнем шума связано с использованием большого числа итераций декодирования $I \sim 5 \div 30$ и более. Как уже следовало из рассмотрения характеристик ПД и МПД из других разделов, в МПД возможен выбор различных значений порогов и весов проверок, а также разностных соотношений в структуре кодов и расстояний между пороговыми элементами, при которых остаётся справедливой основная теорема многопорогового декодирования. Поэтому были

созданы специальные программные средства для оптимизации параметров МПД по вероятности ошибки на всех итерациях декодирования. Общее число оптимизируемых параметров МПД при большом числе итераций в настоящее время составляет порядка 3000 позиций. Большой успешный опыт применения оптимизации показывает, что в сложных системах кодирования возможно достижение таких вероятностей ошибки на бит $P_b(e)$ в МПД при больших уровнях шума в канале, которые в итоге оказывались на 1–2 десятичных порядка меньшими по сравнению с приблизительно правильным выбором настраиваемых параметров МПД.

Указанные программы оптимизации включены в пакет проектирования МПД и всегда применяются при назначении настраиваемых параметров декодера.

5.15. Выводы

Представленные в этой главе данные в соответствии с фундаментальными результатами главы 2, а также оценками и рекомендациями главы 3 показали высокие характеристики алгоритмов многопорогового типа при правильном выборе кода и элементов декодера. Существенно, что МПД продемонстрировал хорошие практические возможности во всех основных типах каналов с независимыми искажениями и стираниями символов. Успешные эксперименты с МПД в наземных каналах связи с заметной пакетной компонентой шума свидетельствуют, что и в этой ситуации его возможности могут быть реализованы более чем успешно.

Проведенное краткое сопоставление МПД с алгоритмом Витерби и другими методами коррекции ошибок показывает, что при естественном сравнении таких базовых некаскадных методов МПД оказывается существенно эффективнее прочих методов, что и было показано в этой главе на примере длинных кодов и свёрточного МПД.

Как уже отмечалось выше, весьма полезно то обстоятельство, что блоковый МПД, оставаясь, например, фактически таким же по размерам декодером, что и обычный ПД, при хорошем выборе кодов обеспечивает их оптимальное декодирование.

Этим определяется преимущество МПД перед прочими процедурами коррекции ошибок. Если к этому добавить, что в основном одиночные ошибки МПД очень легко исключить с помощью простейших каскадных методов при совершенно незначительной избыточности внешнего кода, то можно ожидать хороших результатов применения МПД и в более сложных кодовых системах.

Рассмотренные вопросы сложности реализации МПД также демонстрируют высокие характеристики, как в случае аппаратной, так и программной реализации. Продемонстрированные алгоритмом возможности по скорости декодирования при его реализации на ПЛИС свидетельствуют о совершенно уникальных возможностях МПД в плане обеспечения высокой производительности.

Разумеется, необходимо отметить, что, согласно фундаментальным принципам теории кодирования, высокие характеристики МПД, как и всех других эффективных алгоритмов, достижимы только при использовании весьма длинных кодов. Учитывая, что при числе итераций декодирования $I > 10$ использование свёрточного МПД приводит к задержке решения при декодировании в тысячи, а иногда и десятки тысяч и более символов, следует помнить, что использование такой схемы кодирования возможно только в высокоскоростных трактах спутниковой и космической связи, где задержки до $10^4 \div 10^6$ битов оказываются вполне допустимыми.

Вопросы применения МПД в сложных кодовых системах рассмотрены в следующей главе.

ГЛАВА 6. ИСПОЛЬЗОВАНИЕ МПД В СЛОЖНЫХ СИСТЕМАХ

6.1. Сложные системы кодирования

Изложенные выше результаты, относящиеся к характеристикам МПД, имеют большое принципиальное значение. Впервые за достаточно длительный период развития теории и техники кодирования оказалось, что один из простейших известных методов декодирования – мажоритарный – может быть модифицирован таким образом, что в достаточно широком диапазоне уровней шума канала и кодовых скоростей на различных алфавитах при правильном выборе кодов оказывается возможным декодирование, фактически не отличающееся от оптимального для данных кодов. При этом сложность метода остаётся весьма незначительной.

Разумеется, те коды, для которых МПД оказывается неожиданно столь мощным алгоритмом, обладают формально с теоретической точки зрения серьезным недостатком: отношение d/n для используемых самоортогональных кодов блокового и свёрточного типа в 5÷100 и более раз меньше, чем это допускают теоретические границы, в частности, граница Варшамова-Гилберта. Но, с другой стороны, из теории помехоустойчивого кодирования известно, что при большом уровне шума, в частности, при $R_C < R < C$ вероятность ошибки декодирования на бит $P_b(e)$ при использовании оптимальных декодеров определяется не только свободным или минимальным расстоянием d кода, а зависит и от его спектра весов, по меньшей мере, его начальной части в области $\sim(3\div5)d$. Ясно, что ещё более сильно вероятность ошибки зависит от выбранного алгоритма декодирования, если он неоптимален. Именно поэтому при малых потенциальных возможностях АВ, поскольку он может быть реализован лишь для коротких кодов, и весьма слабых результатах использования алгебраических процедур практически оптимальные характеристики МПД для длинных кодов и определяют его большое преимущество перед абсолютно всеми другими алгоритмами и в ДСК, и в гауссовских каналах. Наконец, существует еще одно очень полезное обстоятельство, состоящее в том, что

ошибки МПД в области почти оптимального декодирования оказываются, в основном, одиночными. Все это помогает успешно решать сложные проблемы внедрения МПД в кодовые системы разнообразного назначения.

Напомним также, что невысокие отношения d/n для кодов, часто используемых в МПД, никак не ухудшают потенциальные возможности этих кодов. Как известно, энергетический выигрыш кодирования (ЭВК) в пределе при малом шуме в гауссовском канале определяется выражением (1.10).

Как следует из этого выражения, необходимо лишь некоторое не очень малое значение минимального кодового расстояния d. А это значение действительно можно сделать достаточно большим и в коде с небольшим отношением d/n. Это обстоятельство также подтверждает возможность получения хороших результатов на кодах, используемых в МПД.

Ниже рассматриваются вопросы применения алгоритмов типа МПД в различных схемах каскадирования, в специальных кодовых конструкциях, со специальными сигналами и в других системах. В конце главы обсуждаются полученные результаты.

6.2. Использование МПД в каскадных схемах

Появление каскадных кодов открыло новую главу в развитии техники кодирования [32]. Эти коды сыграли огромную роль в ускорении работ по внедрению результатов теории кодирования в технику связи, обеспечив большой простор для новых исследований тысячам исследователей, очень многие из которых получают ценные результаты [13, 26, 33, 36, 70, 73, 90, 92].

Напомним кратко, в чем заключается достоинство каскадирования. Пусть при условной сложности N_0, выраженной в некоторых единицах, для кода C_0 с параметрами (n_0, k_0, d_0) какой-то выбранный алгоритм декодирования D_0 обеспечивает при заданной кодовой скорости $R_0 = k_0/n_0$ вероятность ошибки декодирования, определяемую условной кривой 1 на рис. 6.1. Произведем замену кода C_0 на некоторый код C_1 параметрами (n_1, k_1, d_1) с кодовой скоростью $R_1 > R_0$ и того же класса с алгоритмом D_1 и добавим другой код C_2 со скоростью R_2 и параметрами (n_2, k_2, d_2), так что $R_1R_2 = R_0$. Иначе говоря, пусть одношаговая

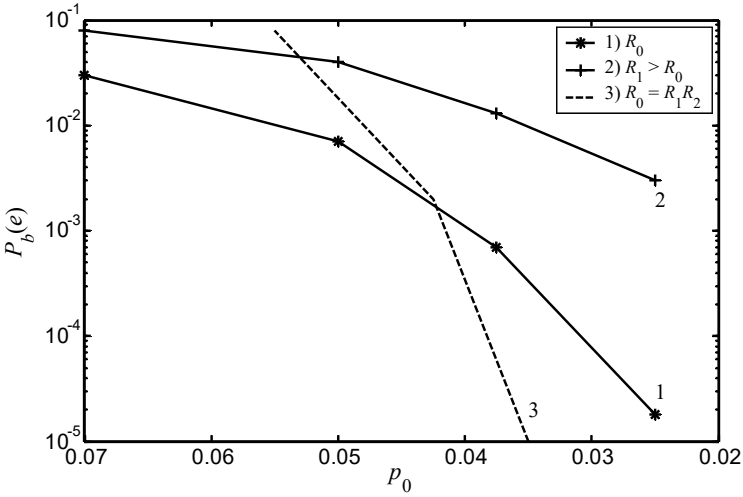


Рис. 6.1. Иллюстрация преимуществ каскадных схем перед обычными алгоритмами

процедура кодирования будет заменена на две независимые последовательные процедуры такие, что суммарная кодовая скорость R_0 останется неизменной.

Отметим, что использование двух кодов C_1 и C_2 подразумевает сначала обычное кодирование информации внешним кодом C_2**,** что приводит к увеличению общего результирующего числа символов по сравнению с исходными данными. Но вместо передачи этого сообщения в канал весь новый поток данных направляется в качестве информационной последовательности во внутренний кодер кода C_1, что приводит к еще большей избыточности сообщения по сравнению с первым этапом кодирования. Только после выполнения этой процедуры сообщение направляется в канал. На приемном конце поочередно работают декодеры внутреннего кода C_1, а затем внешнего кода C_2. Такова схема последовательного каскадирования. В настоящее время специалистами предлагаются и анализируются много различных типов схем каскадирования.

Если теперь к коду C_1, который при правильном проектировали системы можно взять существенно более коротким, применить процедуру декодирования D_1 того же класса, что и D_0, при ее условной сложности $N_1 < N_0$, то результирующая вероятность ошибки $P_b(e)$ из-за условия $R_1 > R_0$ и выбора более простого кода будет вести себя как кривая 2 на рис. 6.1. Далее, применив к информационным символам кода C_1 процедуру декодирования кода C_2 со сложностью N_2 можно получить результирующую вероятность ошибки декодирования, представленную кривой 3, которая при малом шуме будет ниже кривой 1, что обычно при выполнении условия $N_1+N_2 \le N_0$ и демонстрирует эффективность применения каскадных схем, обеспечивающих лучшее декодирование одновременно с меньшими затратами. Следует иметь в виду, что существует некоторая узкая область входных значений вероятности p_0 ДСК при большом шуме канала, где, как видно на рис. 6.1, исходный код C_0 может быть несколько эффективнее каскадного. Но это может иметь место при довольно больших фактических вероятностях $P_b(e)$ декодирования обеих кодовых систем, когда применение кодирования вообще неэффективно.

Если оба кода C_1 и C_2 двоичные, то результирующая схема кодирования чаще называется итеративной, а если C_2 – недвоичный, например, код РС, то это, собственно, и есть каскадный код с параметрами $n_0 = n_1 n_2$ и $d_0 = d_1 d_2$.

Заметим теперь, что внутренний код C_1 должен теперь удовлетворять более простым требованиям по вероятности ошибки декодирования, чем это требовалось от кода C_0. Разница в необходимых корректирующих способностях кодов может составлять несколько порядков, поскольку декодер D_2 кода C_2 обычно успешно декодирует сообщения с вероятностями ошибки, например, около $10^{-3} \div 3 \cdot 10^{-3}$, тогда как декодер кода C_0 должен был ошибаться с вероятностью не большей, чем $\sim 10^{-5}$ при одном и том же уровне шума на входе, например, при $p_0 \approx 0{,}05$ для $R = 1/2$. Разница по оси абсцисс для одной и той же вероятности $P_b(e)$, показанная на рис. 6.1 для кривых 1 и 3 и демонстрирует преимущества каскадирования.

6.3. Каскадирование при использовании кодов с проверкой на четность

Целесообразно рассмотреть такие системы кодирования, чтобы скорость внутреннего кода C_1 мало отличалась бы от скорости R_0, т.е. выполнялось соотношение $R_0 \lesssim R_1$ хотя для этого нужно повысить эффективность использования внешнего кода. Рассмотрим такую схему [93].

Пусть задан, блоковый двоичный код с нечетным d и $R = 1/2$. Допустим также, что при некоторой вероятности p_0 декодирование сколь угодно мало отличается от результата использования оптимального декодера. Выберем далее некоторый достаточно длинный (n, k, d) код с проверкой на четность (k_2+1, k_2, 2), $k_2 \le 100$. Сформируем каскадный код таким образом, что при блоковом коде ($2k_1$, k_1, d_1) декодируемом с помощью МПД по k_2 информационным блокам длины k_1, формируется (k_2+1)-й блок такой же длины k_1, биты которого являются поразрядной суммой по mod 2 соответствующих битов всех k_2 исходных информационных блоков. Полученные (k_2+1) информационных блоков кодируются мажоритарно декодируемым кодом, например, типа СОК и направляются в канал гауссовского типа, в частности, в ДСК.

Пусть далее в приемнике декодер типа МПД обеспечил вероятность ошибки на бит $P_b^{\text{МПД}}(e) << 1$, а для реализации возможностей каскадного кодирования после последней итерации $I \approx 10$ МПД запомнил также все суммы проверок относительно всех декодированных символов. Допустим, что код с проверкой на четность (ККЧ – код с контролем четности) использует предоставленную ему внутренним декодером информацию о проверках так, что для всех (k_2+1) символов блока ККЧ вычисляется достоверность решения $\Delta_i = |m_i - d/2|$, где m_i – сумма проверок, и если контроль по четности обнаруживает ошибку в блоке, то изменяется тот символ, надежность Δ_i которого минимальна. Если есть несколько символов минимальной достоверности Δ, то никакого изменения символов не производится.

Оценим вероятность ошибки такой схемы декодирования. Ошибка декодирования в ККЧ возможна при наличии двух ошибок в блоке. Вероятность такого события не более чем

$$P_{2e}(e) = \frac{(k_2+1)k_2}{2}\left[P_b^{\text{МПД}}(e)\right]^2 .$$

Другая возможность для неправильного решения декодера каскадного кода существует из-за того, что при ошибке в одном символе внешнего блока с надежностью Δ_i все другие символы декодированы верно, но есть один символ или несколько с той же или еще меньшей надежностью. В любом из этих случаев происходит ошибка декодирования каскадного кода, поскольку число ошибок в таком блоке внешнего кода, по меньшей мере, не уменьшается. Вероятность этой группы событий оценивается сверху как

$$P_{1e}(e) = k_2(k_2+1)\sum_{i=(d+1)/2}^{d} C_d^i p_0^i \sum_{j=d-i}^{(d-1)/2} C_d^j p_0^j .$$

Полагая, что в той области шумов, где решения МПД и ОД практически не отличаются, вероятности остальных сочетаний ошибок канала, приводящих к ошибкам выбранной процедуры декодирования каскадного кода, малы и ими при нижних оценках характеристик можно пренебречь. В этом случае вероятность $P_b(e)$ всей каскадной схемы оценивается как

$$P_b(e) = \frac{2[P_{2e}(e)+P_{1e}(e)]}{k_2} = (k_2+1)\sum_{i=(d+1)/2}^{d} C_d^i p_0^i +$$

$$+ 2(k_2+1)\sum_{i=(d+1)/2}^{d} C_d^i p_0^i \sum_{j=d-i}^{(d-1)/2} C_d^j p_0^j .$$

Заметим также, что если внутренний код имеет кодовое расстояние d, то предложенный алгоритм исправляет любые сочетания из d–1 ошибок, а также значительное число ошибок большего веса.

На рис. 6.2 кривыми 1 и 3 представлены графики оценки вероятности $P_b(e)$ для каскадного кода, состоящего из внутреннего СОК с кодовой скоростью $R_1 = 1/2$, $d_1 = 7$ и $R_1 = 1/2$, $d_1 = 9$ с внешним ККЧ длиной $k_2 = 49$. Данные оценки получены в предположении оптимального декодирования внутреннего СОК.

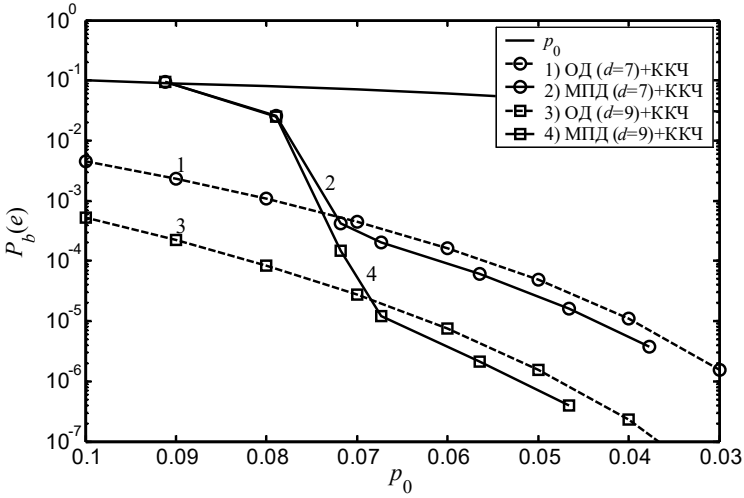


Рис. 6.2. Характеристики каскадных кодов с кодами контроля четности

Отметим, что использование (k_2+1) параллельных кодовых потоков внутреннего МПД, по крайней мере, при малых вероятностях p_0 необязательно. Это было сделано только для того, чтобы вероятности ошибочных символов в блоке внешнего кода можно было бы считать строго независимыми. Поэтому можно оставить единственный поток символов внутреннего декодера, в котором каждые 50 символов решения МПД будут блоком внешнего кода. Из-за наличия зависимости ошибок в таком коде характеристики этого гораздо более короткого каскадного кода несколько ухудшатся, но в области малых шумов канала отличие от оптимального декодирования при использовании МПД будет совершенно незначительным.

6.4. Свёрточные декодеры в каскадном коде с контролем по четности

В рассмотренных выше каскадных кодах блокового типа нигде не использовался сколько-нибудь существенным образом тот факт, что ККЧ должен как-то быть связан с параметрами блока внутреннего кода. Поэтому в соответствии с принципом однопотокового каскадирования, описанного выше для блоково-

го случая и в свёрточном внутреннем коде информационные символы разбиваются на группы по (k_2+1) символов, и для каждой такой группы формируется ККЧ с параметрами (k_2+1, k_2, 2). Заключительная процедура декодирования каскадного кода в этом случае разбивается на независимые шаги обработки каждого из подблоков с (k_2+1) символами. Оценки вероятностей критических ситуаций, оценивавшихся в предыдущем разделе через вероятности $P_{1e}(e)$ и $P_{2e}(e)$ также остаются теми же самыми. Вместе с тем, конечно, величина k_2 не должна быть слишком мала, чтобы $R_2 = k_2/(k_2+1)$ мало отличалась от единицы.

Таким образом, для свёрточных каскадных кодов совершенно независимо от длины кодового ограничения n_A и длины сообщения, которое надо передать, символы информационного потока разбиваются на группы по k_2 битов, для которых формируется дополнительный контрольный разряд и результирующий поток в $(k_2+1)/k_2$ раз большей длины поступает далее на обычный свёрточный кодер.

На рис. 6.2 кривыми 2 и 4 показаны результаты моделирования работы МПД свёрточного каскадного кода при $k_2 = 49$, $R_1 = 1/2$, $d_1 = 7$ при $n_A = 1400$ и $d_1 = 9$ при $n_A = 3000$. При получении представленных результатов использовалось до $I = 10$ итераций декодирования.

В процессе моделирования внесено одно изменение, отличающее его от процедур, для которых были выполнены вышеописанные оценки эффективности. Оно состоит в том, что внешний ККЧ использовался для декодирования не после последней итерации декодирования, как было сказано выше, а после каждого шага декодирования в МПД. Тем самым МПД для внутреннего СОК получал поддержку от внешнего декодера весьма простым способом. Именно взаимодействие декодеров и обеспечило существенное улучшение характеристик. Таким образом, свёрточные каскадные коды эффективно работают в рассматриваемой области больших шумов, позволяя строить декодеры, обеспечивающие большие значения ЭВК. В частности, точка А с объемом эксперимента $5 \cdot 10^6$ информационных символов соответствует величине ЭВК 5,8 дБ при потерях 0,10 дБ из-за кодовой скорости ККЧ $R_2 = 0{,}98$.

Предложенная методика декодирования каскадных кодов применима также и в случае работы МПД внутреннего кода с «мягким» модемом в гауссовском канале связи.

Результаты моделирования каскадного кода для свёрточного СОК с кодовым расстоянием d_1, равным 7 и 9 при $k_2 = 49$ для канала с АБГШ при использовании 16 уровневого квантования представлены на рис. 6.3 кривыми 2 и 4. Пунктиры 1 и 3 соответствуют результатам моделирования работы обычного МПД для тех же СОК без использования внешнего декодера. Как следует из результатов моделирования эффективное и простое по идее каскадирование СОК и ККЧ обеспечивает весьма существенное улучшение характеристик МПД. Кривая 5 приведена для каскадного кода с $R_1 = 1/2$ и $d_1 = 6$ и ККЧ, который работоспособен в области $E_s/N_0 \sim 1{,}5$ дБ при числе итераций до 30.

На рис. 6.4 представлены графики зависимости предельных значений ЭВК от выбранной скорости R для условия $R < C$ при $M = 2$ и $M = 16$, а также соответствующие точки каскадных кодов, экспериментальные характеристики которых были рассмотрены на предыдущих двух рисунках. Подчеркнем, что до-

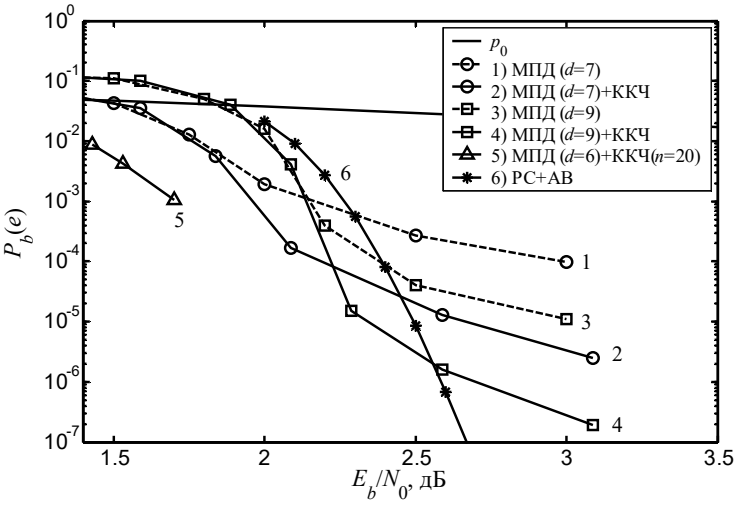


Рис. 6.3. Характеристики МПД с ККЧ в канале с АБГШ

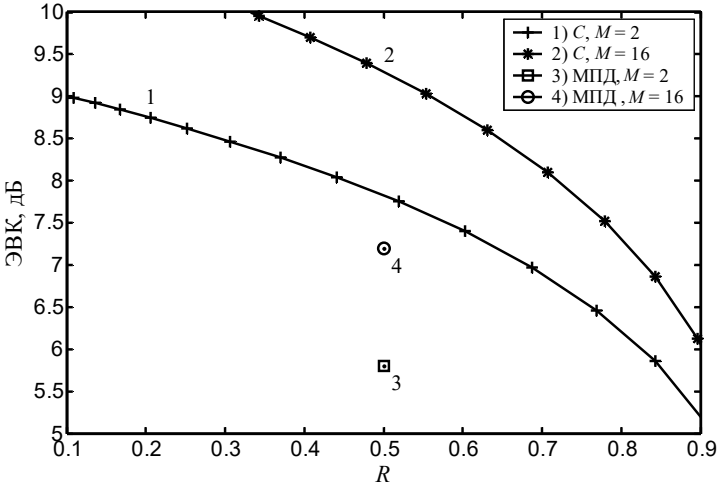


Рис. 6.4. Зависимости предельных значений ЭВК от выбранной кодовой скорости R при условии $R < C$

вольно малое, порядка 2 дБ, отличие ЭВК конкретных относительно простых алгоритмов от предельных, гарантируемых теорией, является весьма показательной иллюстрацией правильности выбора основного направления исследования. Хотя скорость $R_0 = 0{,}49$ меньше чем 0,5, отличие скоростей и предельных характеристик невелики, что позволяет считать рассмотренные очень простые каскадные коды весьма перспективными.

6.5. Использование МПД с многопозиционными системами модуляции

В [62] анализировались характеристики декодеров типа МПД при их согласовании с системами сигналов ФМ*N* и АФМ*N*. На рис. 6.5 с разрешения авторов представлены графики зависимости вероятности ошибки на бит $P_b(e)$ на выходе многопорогового декодера от отношения сигнал-шум E_b/N_0 в канале связи с квадратурной амплитудной модуляцией (аналог АФМ*N*) при 4, 5 и 6 бит/символ [63]. При этом выполнялось от 10 до 15 итераций декодирования блокового СОК с кодовой скоростью

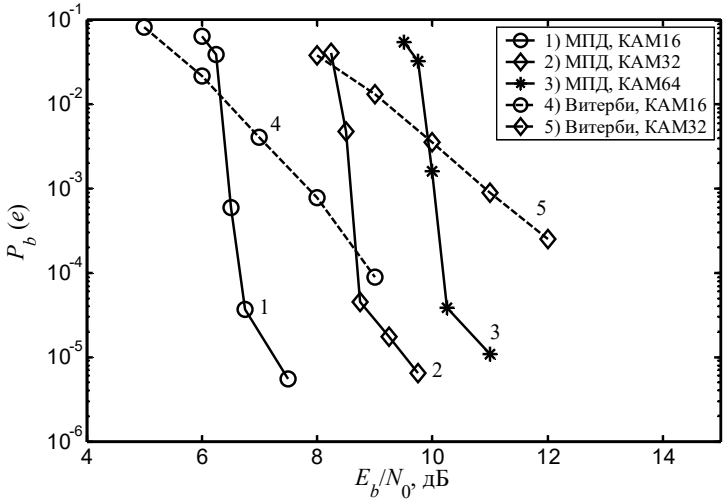


Рис. 6.5. Эффективность МПД в каналах с КАМ*N*

$R = 1/2$, кодовым расстоянием $d = 9$ и длиной n порядка 8000. Представленные результаты получены для случая использования «жесткого» модема. На данном рисунке также представлены характеристики декодера Витерби для кода с длиной кодирующего регистра $K = 7$. Как видно, декодер Витерби существенно уступает многопороговому декодеру в данных условиях.

На следующем рис. 6.6 представлены характеристики МПД для того же блокового кода, что и на рис. 6.5, в канале с многопозиционной фазовой модуляцией (ФМ*N*). Видно, что соотношения между характеристиками многопорогового декодера, декодера Витерби сохраняются и при данном виде модуляции.

А если учесть, что при этом сложность практической реализации многопороговых декодеров оказывается на два и более порядков меньшей, что допускает применение многопороговых декодеров в высокоскоростных системах передачи данных, в которых накладываются значительные ограничения на расширение используемой полосы частот.

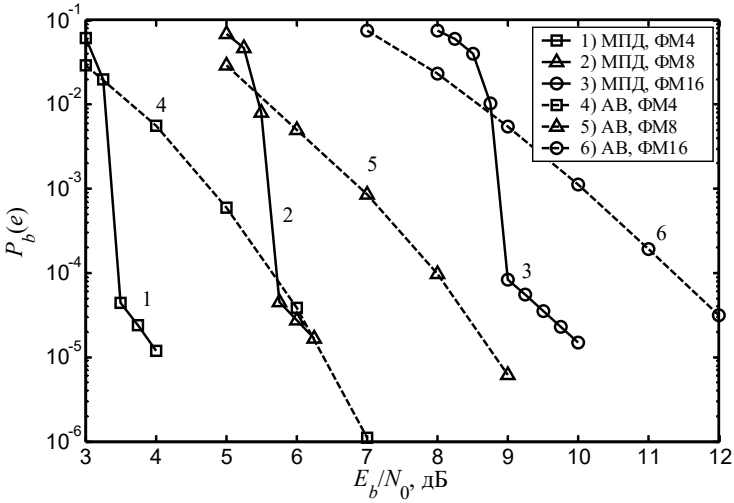


Рис. 6.6. Эффективность МПД в каналах с ФМ*N*

6.6. Использование МПД для кодов с неравной защитой символов

Внимание многих исследователей, работающих в области кодирования, привлекают коды с неравной защитой символов (КНЗС), характеризующиеся тем, что разные группы символов, например, в блоковом систематическом коде, оказываются входящими в различное число проверочных символов в качестве слагаемых [43, 95].

Это приводит, в свою очередь, к тому, что информационные двоичные символы в таких кодах, например, при оптимальном декодировании, будут декодироваться ошибочно с весьма различной вероятностью, определяемой кодовым расстоянием между кодовыми словами, отличающимися только символами, входящими в одну из подгрупп.

Применение МПД для декодирования кодов с $R = k_0/n_0$, $k_0 = 2, 3, \ldots$, попутно решает и вопросы декодирования таких КНЗС. Поскольку, например, при построении обычного СОК с $d = 7 \div 11$ и $R = k_0/(k_0+1)$ необходимо иметь k_0 полиномов, определяющих вид (k_0+1)-ой проверочной ветви кода по первым k_0

информационным, то переход к КНЗС может быть осуществлен путем использования таких полиномов для блоковых и свёрточных СОК, которые имели бы вместо, например, семи различное число ненулевых коэффициентов в порождающих полиномах – от 5 до 9. Важно, что при этом уменьшается и отношение сигнал/шум в канале, при котором возможна эффективная работа МПД с той же самой кодовой скоростью.

На рис. 6.7 представлены характеристики МПД для двоичного кода с $R = 3/4$ и $d = 7$ в ДСК (кривая 1), а также предельные для малого шума вероятности ошибки кодов с $d = 5$, 7 и 9.

Графики 2–4 соответствуют результатам использования МПД для декодирования свёрточного КНЗС типа СОК с кодовыми расстояниями по первой-третьей ветвям, равными 5, 7 и 9. Число итераций декодирования во всех случаях равно $I = 6$.

Как следует из вида графиков, предельные по $P_b(e)$ характеристики достигаются при несколько большей вероятности канала p_0, чем $p_0 \approx 0{,}017$ для первого кода. Использование предложенного кода для передачи (в данном случае) трехзарядных це-

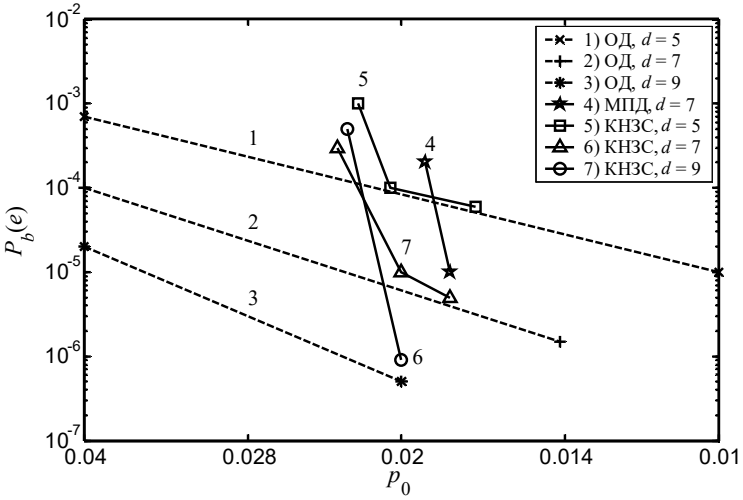


Рис. 6.7. Характеристики кодов с неравной защитой символов

лых чисел может существенно снизить среднеквадратичную ошибку.

6.7. Применение МПД в схемах параллельного кодирования

Как уже отмечалось в этой главе, возможности применения многих методов коррекции ошибок, в том числе и МПД, ограничены кодами с не очень большой корректирующей способностью. Конкретные значения и проявления этих ограничений оказываются для разных алгоритмов также весьма специфическими. Если, например, в АВ очень жесткие ограничения на эффективность возникают из-за сложности реализации, т.е. объема вычислений и памяти, то в МПД ограничение на рост ЭВК с увеличением минимального кодового расстояния d проявляется в ухудшении эффективности использования проверок, поскольку рост размерности этих проверок ведет к тому, что вероятности ошибочности этих проверок при достаточно большом шуме быстрее приближаются к 0,5, обесценивая их использование в мажоритарных схемах. Такое объяснение ограничений и свойств мажоритарных схем со стороны признанных авторитетов [4, 6] на длительный период исключило мажоритарные методы из списка перспективных направлений развития теории и техники кодирования. Хотя развитие исследований по тематике МПД раздвинуло границы эффективности мажоритарных методов, это ухудшение эффективности проверок с ростом d снова, как и в обычном мажоритарном декодере, но при существенно большей вероятности p_0 для ДСК проявляется и в многопороговом алгоритме.

Одним из наиболее традиционных способов компенсации этого ограничения, как было показано выше, оказывается использование МПД в каскадных схемах кодирования. Вместе с тем использование последовательных схем каскадных кодов усложняет решение задачи синхронизации. Кроме того, необходимость компенсации потери ЭВК из-за скорости $R_1 < 1$ внешнего кода, которая может составлять 1 дБ и более при общем ЭВК около 7÷9 дБ, приводит к уменьшению прироста ЭВК такого каскадного кода по сравнению с исходными некаскадными кодами при малых и средних уровнях достоверности.

Рассмотрим схему кодирования и декодирования в несколько большей степени свободной от этих особенностей базового алгоритма МПД и отмеченных недостатков каскадных схем. Назовём её системой параллельного каскадирования [96]. Возможно, это одна из первых, если не первая предложенная схема каскадирования этого типа. Пусть некоторый СОК с переменными связями при $R = k_0/n_0 = 5/10$ и $d = 11$ задается $k_0 \times (n_0 - k_0) = 25$ полиномами веса 2. Каждая из пяти проверочных ветвей кода содержит $(d-1) = 10$ слагаемых, по 2 из каждой информационной ветви.

Преобразуем теперь код, выделив 4 первых проверочных ветви кода под декодер первого этапа с проверками меньшей размерности, например, по 6 от каждой информационной ветви. Остальные проверочные соотношения отнесем к пятой проверочной ветви кода.

Она будет иметь размерность проверок, равную 20. Эти проверки вместе с проверками меньшей размерности будут использоваться на втором этапе декодирования также на основе процедур типа МПД.

Сопоставим полученную схему параллельного кодирования. Отметим сначала, что при таком подходе к схемам кодирования на самом деле есть 2 кода: первый код C_1 с $R_1 = 5/9$ и $d_1 = 7$ и код с $R_2 = 5/6$, причем оба кода относятся к классу СОК, и, что существенно, их совокупность также остается СОК, исходя из самого своего принципа построения. Создание на основе одной и той же информационной последовательности двух кодов с различными скоростями передачи и позволяет назвать данный метод параллельным кодированием (ПК).

Декодирование внутренним кодом с $R_1 = 5/9$ не имеет никаких новых принципиальных отличий по сравнению с каскадными схемами и осуществляется более или менее эффективно благодаря малому увеличению R_1 по сравнению с $R_0 = 1/2$, а также меньшему кодовому расстоянию $d_1 = 7$ по сравнению с исходным кодом, имевшим исходное минимальное кодовое расстояние $d_0 = 11$. Таким образом при декодировании кода C_1 используются только обычные свойства и возможности СОК и МПД.

После того, как МПД (или, разумеется, другой эффективный алгоритм) существенно уменьшает при использовании кода C_1 вероятность $P_b(e)$ в принятом сообщении, происходит переход к главному этапу работы декодера, в котором и состоит все своеобразие и преимущества ПК: декодированию полного кода с $R_0 = 1/2$.

По сравнению с последовательными каскадными схемами, где на втором этапе декодирования на основе внешнего кода $R_2 \lesssim 1$, при ПК скорость декодируемого кода второго этапа равна R_0, т.е. в рассматриваемом примере $R_0 = 1/2$. Именно существенное уменьшение скорости кода второго этапа декодирования и составляет основу, обеспечивающую преимущество работы алгоритма параллельного каскадирования. Обычно в каскадном коде при $R_2 = 4/5$ эффективность МПД и других алгоритмов приемлема, если на его входе вероятность ошибки на символ $P_b(e)$ после первого каскада будет существенно меньше, чем 10^{-2}, то второй каскад параллельной схемы (с использованием МПД) будет работоспособен при вероятности ошибки на входе этой ступени $p_0' = (2 \div 3) \cdot 10^{-2}$ или даже выше. Эта разница в граничной работоспособности схемы с МПД декодером с меньшей скоростью и определяет преимущества ПК.

Отметим, что невозможность использования всех проверок СОК, присутствующих в ПК, сразу, без выполнения первого этапа декодирования, обусловлена тем обстоятельством, что проверки пятой ветви имеют очень большую размерность и в ходе первого этапа при $p_0 = 0{,}06$–$0{,}07$ совершенно бесполезны, поскольку в коде с $R_2 = 5/6$ они оказываются правильными с вероятностью менее 0,54 и ошибочными с вероятностью более 0,46, т.е. не несут почти никакой информации о декодируемом символе. И лишь при снижении вероятности ошибки p_0' после первого этапа декодирования до величины $\sim 3 \cdot 10^{-2}$ оказывается, что вероятность истинности для этой проверки составляет уже ~0,35, т.е. эти проверки полезны, что и показывает МПД на втором этапе коррекции.

На рис. 6.8 представлены графики вероятности ошибки декодирования для кода типа СОК с $R = 1/2$, $d = 13$, которая дости-

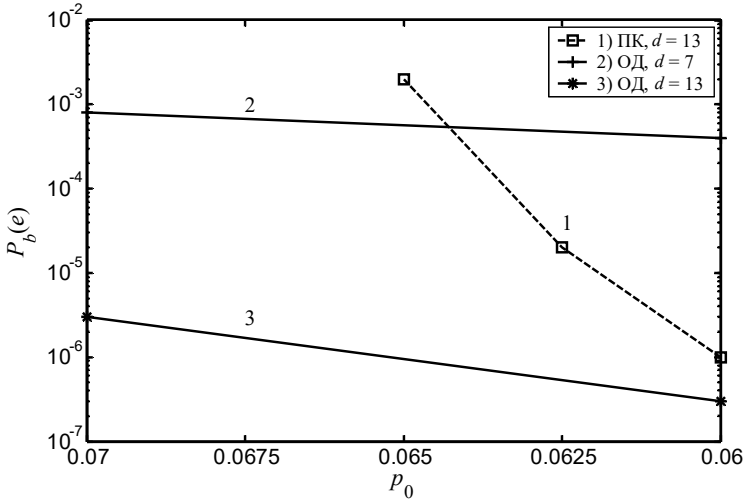


Рис. 6.8. Характеристики МПД декодера в режиме параллельного кодирования для ДСК

гается при использовании ПК на основе МПД. Кривые 2 и 3 соответствуют предельным значениям $P_b(e)$ для кодов $d = 7$ и $d = 13$ в ДСК без памяти, пунктир 1 – вероятности ошибки декодирования с внутренним кодом с $R_1 = 5/9$ и $d_1 = 7$ при $I_1 = 6$ и $I_2 = 4$ итерациях второго этапа для полного кода с $R_0 = 5/10$ и $d = 13$.

На рис. 6.9 приведены аналогичные графики для кода, работающего с «мягким» модемом при $M = 4$ в гауссовском канале. Как видно из представленных результатов, «мягкое» декодирование на базе МПД, как и в случае других схем кодирования, увеличивает ЭВК еще на величину порядка 1 дБ.

Продемонстрированное при параллельном кодировании увеличение ЭВК при фиксированной вероятности ошибки $P_b(\text{e}) = 10^{-5}$ в области уже достаточно высокой исходной эффективности МПД в ДСК без памяти и в канале гауссовского типа позволяет утверждать, что предложен полезный метод декодирования, который также может найти применение в реальных системах.

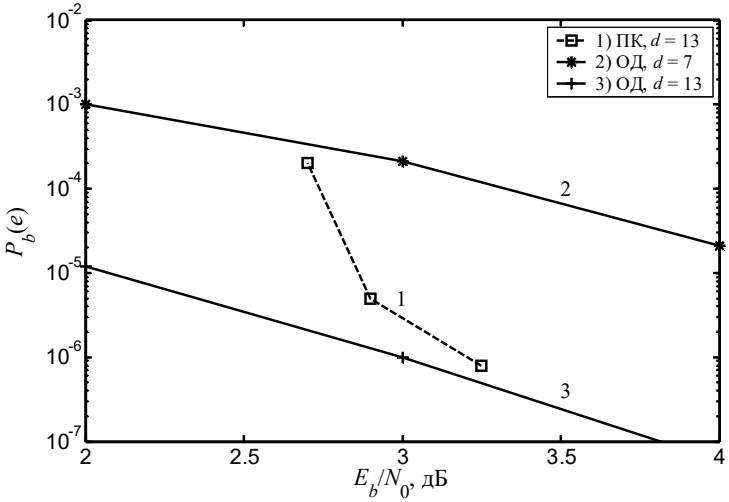


Рис. 6.9. Характеристики МПД декодера в режиме параллельного кодирования для гауссовского канала

6.8. Декодирование кодов с выделенными ветвями

Как уже отмечалось выше, рост эффективности кодирования и, главное, последующего декодирования средствами МПД линейных кодов ограничен кодами с относительно небольшим кодовым расстоянием по сравнению с наилучшими кодами достаточно большой длины. Вместе с тем прирост ЭВК для длинных СОК с малым эффектом размножения ошибок по сравнению с обычным мажоритарным алгоритмом оказывается столь значительным, что с МПД для ДСК могут быть сравнимы только весьма сложные декодеры, реализующие алгоритм Витерби для длинных кодов с $K \geq 7$ и обязательно работающие совместно с мягкими модемами.

Однако и в классе блоковых или свёрточных СОК дальнейший рост ЭВК возможен только при увеличении кодового расстояния d и сохранении почти оптимального их декодирования при большом уровне шума. Принципиальная возможность этого, как следует из допустимых значений отношения сигнал/шум канала, а также кодовых скоростей и структуры кодов, сущест-

вует. Но МПД с ростом кодового расстояния начинает достигать уровня декодирования, близкого к оптимальному, при все более высоком отношении сигнал/шум, что и определяет границу его использования в качестве базового алгоритма, который, например, может быть использован в каскадных схемах.

В некоторой степени вопросы расширения границ эффективности МПД решаются при использовании его в качестве внутренних кодов в схемах, аналогичных каскадным, как было описано в разделе 6.3. Однако каскадные традиционные схемы должны компенсировать потери ЭВК из-за наличия высокоскоростного второго кода R_2, равные $(-10\lg R_2)$ дБ, что может составлять 0,5 дБ и более. Частичная компенсация этого недостатка при параллельном декодировании увеличивает ЭВК МПД и по сравнению с традиционным использованием МПД, и по сравнению с каскадным подходом.

Как отмечалось, улучшение характеристик параллельной схемы по сравнению с каскадной оказалось возможной благодаря тому, что декодер второй ступени работал в параллельной схеме при $R_0 = 0{,}5$, а не при $R_2 \approx 0{,}8 \div 0{,}9$, как в каскадной, что и решает простейшими средствами проблему некоторого роста эффективности декодирования в рамках МПД. Ниже изложены идеи и рассмотрены пути дальнейшего совершенствования МПД путем улучшения его работы на первом этапе декодирования в параллельном декодере при $R_0 \approx 0{,}5$, что также обеспечивает рост ЭВК без обращения к другим алгоритмам коррекции ошибок повышенной сложности.

Общим свойством МПД и некоторых других алгоритмов является уменьшение граничной вероятности $p_{\text{гр}}$, например, в ДСК, ниже которой МПД работает почти оптимально, если растет размерность проверок декодера. Этим определяется уменьшение граничной вероятности ошибки приблизительно вдвое при переходе от $R = 1/2$ к $R = 2/3$, например, для СОК с $d = 7$. Если при $R = 1/2$ размерность всех мажоритарных проверок равна 6, то при переходе к $R = 2/3$ размеренность уже достигает величины, равной 12, а качество проверок, т.е. степень отличия от 0,5 для правильных и ошибочных проверок сильно уменьшается. Это и приводит при увеличении R в конкретном мажоритар-

ном алгоритме к снижению той максимальной вероятности $p_{гр}$ канала, при которой этот алгоритм еще работоспособен.

В случае, если сравниваются два систематических кода C_1 и C_2 с одинаковыми минимальными расстояниями d и $J = d–1$ проверками при $R_1 = k_0/n_0$ и $R_2 = (k_0+1)/n_0$, $k_0 < n_0–1$, то отношение размерностей проверок m_1 и m_2 для этих кодов будет равно

$$\alpha = \frac{m_2}{m_1} = \frac{(k_0+1)(n_0-k_0)}{k_0(n_0-k_0-1)} > 1 .$$

Хотя в каскадных и параллельных схемах декодирования требования к корректирующим возможностям кода C_1 много ниже, чем для всего кода C_0, что, собственно и помогает компенсировать увеличенную по сравнению с кодом C_0 скорость R_1 кода C_1, наличие этой разницы все же существенно с точки зрения получаемого итогового ЭВК.

На рис. 6.10 показаны принципы перехода от обычных кодов к кодам, предназначенным для параллельного кодирования и, наконец, к кодам с выделенными ветвями, которые еще более улучшают энергетические характеристики кодирования.

1	1	1	1	1	5
1	1	1	1	1	5
1	1	1	1	1	5
1	1	1	1	1	5
1	1	1	1	1	5

а)

1	1	1	1	2	6
1	1	1	2	1	6
1	1	2	1	1	6
1	2	1	1	1	6
2	1	1	1	1	6

б)

2	2	2	2	2	10
2	2	2	2	2	10
2	2	2	2	2	10
2	2	2	2	2	10
2	2	2	2	2	10

в)

3	3	3	3	2	14
3	3	3	2	3	14
3	3	2	3	3	14
3	2	3	3	3	14
2	3	3	3	3	14

г)

Рис. 6.1. (начало)

2	2	2	2	2	10
2	2	2	2	2	10
2	2	2	2	2	10
2	2	2	2	2	10
6	6	6	6	6	30

д)

3	1	1	1	1	7
3	1	1	1	1	7
3	1	1	1	1	7
3	1	1	1	1	7
2	10	10	10	10	42

е)

3	2	2	1	1	9
3	2	2	1	1	9
3	2	1	1	1	8
3	2	1	1	1	8
2	6	8	10	10	36

ж)

Рис. 6.2. (окончание). Принципы формирования параллельных кодов и кодов с выделенными ветвями

Пусть в качестве примера во всех случаях рассматриваются коды с $R = 5/10$. В каждой прямоугольной таблице размера 5×5 в позициях 1÷5 указано число проверок, т.е. вес одного из 25-ти порождающих полиномов кода $G_{i,j}$, соответствующего i-ой проверочной и j-ой информационной ветвям кода, $1 \le i,j \le 5$. Тогда сумма чисел, находящихся в i-й строке таблицы определяет размерность проверок СОК, построенных на i-ой проверочной ветви с учетом информационных символов всех пяти ветвей. Эти суммы проставлены в правых столбцах около каждой таблицы. Сумма чисел в j-ом столбце оказывается общим числом проверок относительно символов j-ой информационной ветви и тем самым определяет кодовое расстояние для этой ветви $d = J+1$. Везде далее в этом разделе будет предполагаться, что рассматриваются коды с одинаковой защитой всех информационных символов, так что

$$\sum_{i=1}^{5} a_{ij} = J$$

для всех $j = 1, 2,..., 5$.

Построенная таким образом таблица а) соответствует коду с размерностью всех проверок равной 5 (указано справа от таблицы) при 5-ти проверках относительно каждой информационной ветви ($d = 6$). Это обычный СОК с переменными связями. В таблице б) расписаны веса полиномов $G_{i,j}$ для $d = 7$. Так как $J = 6$ не кратно $r_0 = n_0 – k_0 = 5$, то не все проверочные ветви содержат одинаковое число слагаемых, относящихся к одним и тем же информационным ветвям, но общее число слагаемых во всех проверочных ветвях также одинаково.

Поскольку коды, относящиеся к таблицам а) и б) не могут обеспечить ЭВК более 5 дБ при $P_b(e) \sim 10^{-5}$, величину, условно, как и в других разделах, упоминаемую как достаточно высокую для текущего состояния развития техники, то в таблице в) приведены параметры кода с $d = 11$, отличающегося от предыдущих только несколько большим кодовым расстоянием, которое для достаточно длинного СОК обеспечит упомянутую эффективность. Наконец, в таблице г) приведены данные для СОК с $d = 15$, который обеспечит еще более высокий ЭВК, но лишь при малых достоверностях, например, при $P_b(e) \sim 10^{-8}$, поскольку уменьшение граничной вероятности $p_{\text{гр}}$ обычного МПД при переходе от кода а) к коду из таблицы г) в последнем случае уже столь существенно, что ЭВК кода с $d = 15$ при $P_b(e) \sim 10^{-5}$ будет несколько меньше чем даже у кода в), т.к. МПД с кодом г) в указанной точке не обеспечит эффективного декодирования кода со столь большой размерностью проверок.

Перед дальнейшим анализом таблиц на рис. 6.10 сделаем одно существенное замечание, помогающее сопоставить параллельные и последовательные каскадные коды еще в одном аспекте. Как уже отмечалось, оба кода характеризуются тем, что скорость R_1 кода C_1 первой (внутренней) ступени больше, чем результирующая скорость R_0 кода в целом. Сравним скорости кодов R_1 в каскадном и параллельном кодах. Пусть заданы $R_0 = 1/2$ и $R_2 = 5/6$ в обоих случаях. Поскольку в каскадном коде $R_1 = R_0/R_2$, то $R_1 = 3/5 = 0{,}60$. В случае же рассматриваемого па-

раллельного кода с $R_0 = k_0/n_0 = 5/10$ построенного по параллельному принципу при $R_2 = k_0/(k_0+1) = 5/6$, получаем, что $R_1 = R_0R_2/(R_2+R_0[R_2–1])$, откуда получаем $R_1 = 5/9 = 0{,}555$. Иначе говоря, уже изначально в параллельном коде заложено преимущество перед каскадным кодом по скорости кода R_1 на первом этапе декодирования, которое затем увеличивается на второй ступени декодирования, которая, как указывалось, для каскадного кода соответствует декодированию при $R_2 = 5/6$, а для параллельного кода – при $R_0 = 1/2$ для рассматриваемого примера.

Продолжим анализ таблиц на рис. 6.10. Таблица д) соответствует параллельному коду с $R_1 = 5/9$ и $R_2 = 5/6$. Верхние четыре строки таблицы относятся к коду R_1, а отделенная от них двойной чертой пятая строка – к коду R_2. Сопоставление таблиц г) и д) показывает основное различие обычного СОК с переменными связями и параллельного кода: в последнем размерности проверок m кода C_1 меньше, а кода C_2 больше, чем размерность проверок обычного СОК. Отметим, что оба кода имеют кодовое расстояние $d = 15$, поскольку в обоих таблицах сумма весов полиномов в каждом столбце равна $J = d–1 = 14$. Заметим теперь, что в параллельном коде для кода C_1 расстояние $d_1 = 9$, а $m = 10$ вместо $m = 8$ для СОК с $R = 1/2$ и тем же $d = 9$, что и является платой за использование $R_1 = 5/9$, которая ведет к уменьшению граничной вероятности $p_{гр}$ эффективной работы МПД первого каскада, хотя снижение d с величины 15 до 9 при переходе от обычного кода с переменными связями к коду с R_1 из параллельного кода наоборот увеличивает значение $p_{гр}$ и, как показали результаты предыдущего раздела, возможен такой выбор параметров параллельного кода, что для него результирующая граница $p_{гр}$ будет иметь все же немного большее значение, чем в обычном коде.

Ниже предложена методика дальнейшего перераспределения весов проверок различных ветвей в порождающих полиномах кода, являющаяся продолжением идей параллельного кодирования. Перераспределение, организация более сложных ступенчатых конфигураций весов полиномов внутри столбцов таблиц делает при этом возможным такое взаимодействие кодов, входящих в параллельный каскадный код, которое соответству-

ет их поочередному декодированию в условиях, соответствующих использованию более низкоскоростных кодов, чем скорость кода R_1 и, в некоторых случаях, чем общая скорость всего параллельного кода R_0.

Следует указать на то обстоятельство, что подобная возможность, основанная на взаимодействии кодов, уже была предложена в интересной с точки зрения теории конструкции обобщенных каскадных кодов монографии [97]. Однако в обобщенных каскадных кодах этот результат обеспечивается сложным взаимодействием нескольких, четырех, шести и более декодеров разнородных кодов, что затрудняет реализацию этого подхода на практике. В кодах с выделенными ветвями, как далее будут называться новые коды, усложнение всего процесса декодирования будет состоять лишь в том, что на пороговые элементы на разных итерациях декодирования будут поступать различные группы (из общего числа 2–4 таких групп) проверок вместо того, чтобы на каждой итерации учитывать на пороговых элементах все проверки того или иного символа полного кода C_0. Иначе говоря, некоторые проверки не используются на разных итерациях декодирования, т.е. исключаются из процедуры суммирования, что и будет составлять все усложнение методики. В частном простейшем случае двух групп проверок – только кода C_1 и всего кода C_0 коды с выделенными ветвями превращаются таким образом в параллельные коды.

Примером СОК с выделенными ветвями может быть код, веса полиномов которого представлены в таблице е) на рис. 6.10. Пусть процесс декодирования начинается с первой информационной ветви, т.е. полиномов первого столбца, и только по первым четырем из них, содержащим 3+3+3+3 = 12 проверок. Отметим снова, что код с $R = 1/2$ и $d = 13$ имел бы размерность своих проверок, равную 12, а в данном случае размерность всех проверок кода для первой ветви перед началом декодирования равна только 7. Это достигается за счет того, что полиномы других информационных ветвей имеют веса меньшие, чем полиномы первой ветви в пределах четырех первых проверочных ветвей. После того, как в первой ветви вероятность ошибки декодирования уменьшится приблизительно на поря-

док, и ошибки первой информационной ветви будут почти отсутствовать в проверках по сравнению с ошибками других ветвей, вместе с первой ветвью можно одновременно начать декодировать и все остальные информационные ветви. В этот момент можно условно считать, что для второй и прочих ветвей с $d = 5$ размерность проверок будет равна 4, поскольку вклад первой ветви в вероятность ошибочности проверок будет довольно низок и ее можно не учитывать в подсчете сумм весов по строкам таблицы е). После завершения процедуры декодирования в рамках первого кода C_1, как и в параллельном коде, декодируется полный код C_0 с $d_0 = 15$. Перед этим заключительным этапом на всех информационных ветвях средняя плотность ошибок МПД будет менее 10, хотя на первых ветвях она окажется много меньшей. В этом случае большая размерность проверок пятой проверочной ветви уже окажется несущественной, что и позволит полностью декодировать принятое сообщение почти так же, как и с помощью оптимального декодера для этого кода.

Наконец, можно рассматривать также коды с выделенными ветвями не только с одной выделенной первой ветвью, как было показано на примере таблицы е), но и с двумя или более такими ветвями. В таблице ж) указаны 4 различных типа ветвей, когда код C_1 в различной степени защищает пять информационных ветвей с числом проверок 12, 8, 6, 4 и 4 для каждой из них соответственно. При этом первая, затем две первых, три и, наконец, все пять информационных ветвей подключаются к процессу коррекции последовательно по мере снижения плотности оставшихся ошибок в предыдущих ветвях. При этом декодировании первой информационной ветви с $J = 12$ в коде с $R_1 = 5/9$ размерность проверок оказывается равной $m = 9$, т.е. даже меньше, чем в коде с $R = 1/2$ при $d = 13$, а проверки относительно второй информационной ветви (разумеется, без учета первой) при $J = 8$ равны $m = 6$, что тоже меньше, чем при $R_0 = 1/2$ и т.д. для остальных ветвей.

Разумеется, описанная ситуация с размерностями проверок в таких кодах с выделенными ветвями на самом деле непроста. При работе в больших шумах существенно снизить вероятность ошибки в первой ветви до того, как подключается к процессу

декодирования, например, вторая ветвь, не удается как из-за наличия, хотя и в небольшой степени, эффекта размножения ошибок, так и просто из-за малой эффективности проверок. Однако при правильном выборе кодов ЭВК действительно растет.

Наконец, необходимо также указать и на то, что коды с выделенными ветвями должны быть достаточно длинными, чтобы обеспечить низкий уровень размножения ошибок при тех значительных уровнях шумов канала, при которых проявляется их эффективность.

На рис. 6.11 представлены экспериментальные графики зависимости вероятности $P_b(e)$ от уровня шума канала для кодов с выделенными ветвями с полиномами $G_{i,j}$, соответствующими коду е). Общая длина этого сверточного кода C_0 равна $n_A = 5000$, кодовая скорость $R = 1/2$, кодовое расстояние $d = 15$, количество итераций $I = 14$. Кривая 1 соответствует средней по всем информационным ветвям вероятности ошибки на бит $P_b(e)$ после 7-ой итерации для кода C_1, а 2 – вероятности P_b(е) для всего кода после 14-й итерации в ДСК без памяти.

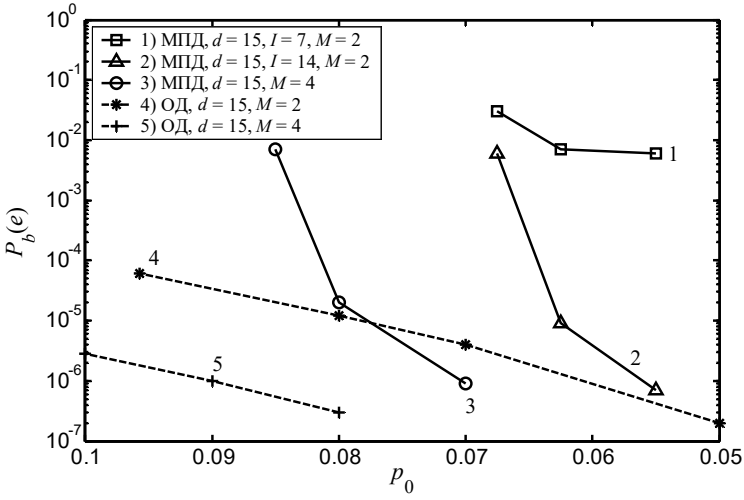


Рис. 6.11. Характеристики кодов с выделенными ветвями

Кривая 3 дает представление о коде с выделенными ветвями с той же скоростью $R = 1/2$ в гауссовском канале с $M = 4$ уровнями квантования решений на выходе модема. Дополнительное улучшение характеристик порядка 1 дБ по входному уровню шума подтверждает целесообразность использования кодов с выделенными ветвями, декодируемыми средствами МПД, и в таких каналах.

6.9. Характеристики аппаратных средств кодирования

На рис. 6.12 представлены последние достижения в области высокоскоростных декодеров типа МПД на современных ПЛИС для кодовой скорости $R \sim 1/2$. Кривая «МПД ПЛИС Xilinx» относится к разработке свёрточного МПД на ПЛИС Xilinx [88] на скорости от 80 до 480 Мбит/с с полным распараллеливанием операций. Каскадная схема с использованием того же кода и кода контроля по чётности (ККЧ) обеспечивает характеристики, показанные на графике «КК1+МПД». Они достаточно мало отличаются от возможностей стандартной и весьма эффективной каскадной схемы декодирования с АВ (кривая «АВ, K=7») и де-

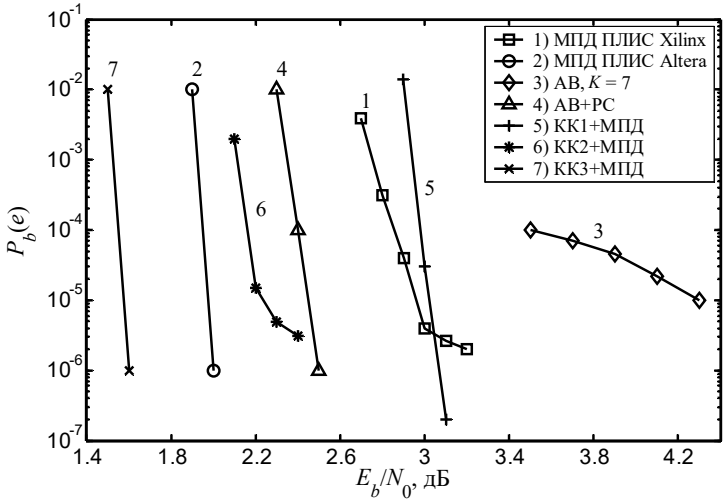


Рис. 6.12. Характеристики основных алгоритмов декодирования на ПЛИС

кодером кода Рида-Соломона (РС) (график «АВ+РС»), но оказываются значительно проще, поскольку при использовании каскадирования с МПД наличие второго кода типа ККЧ добавляет всего 2 операции на каждый бит данных по сравнению с обычным МПД. Это не идёт ни в какое сравнение со сложностью дополнительного декодера для кода РС. При этом каскадный МПД легко реализовать, как и обычный МПД декодер, для скоростей порядка 500 Мбит/с и выше.

Кривая «КК2+МПД» на рис. 6.12 соответствует МПД декодеру с объёмом памяти ПЛИС, увеличенным по сравнению с первым примером в 1,4 раза, который каскадируется с таким же ККЧ. Эта простая схема также с очень высоким потенциальным быстродействием уже существенно эффективнее каскадной схемы АВ+РС как по энергетике, так и по скорости передачи. Более того, поскольку уровень остаточных ошибок у этого каскадного МПД очень невелик, то добавление любого самого простого малоизбыточного кода в качестве внешнего каскада в эту схему приведёт к абсолютному преимуществу такой каскадной схемы относительно варианта каскадных кодов АВ+РС вплоть до вероятностей ошибки на бит $P_b(e) \sim 10^{-9}$.

Далее график «МПД ПЛИС Altera» приведён для декодера МПД с 40 итерациями декодирования. Подчеркнём важнейшее свойство такого аппаратного МПД: эта обычная базовая схема декодера, т.е. она даже не относится к каскадным конструкциям, но оказывается существенно более эффективной по уровню шума, при котором она работает, чем все предыдущие схемы на рис. 6.12. Столь высокая его эффективность обусловлена новыми достижениями в поиске кодов с низким уровнем размножения ошибок при их коррекции, что, в свою очередь, и позволило перейти к большему числу итераций декодирования. Можно утверждать, что такая схема, безусловно, относится к лучшим некаскадным процедурам коррекции ошибок, известным в теории и технике кодирования. Разумеется, успешная работа МПД алгоритма в условиях столь большого уровня шума в соответствии с фундаментальными свойствами кодов оказывается возможной только при значительном увеличении их длины и задержки декодирования.

В связи с большим преимуществом каскадных схем перед базовыми методами кодирования/декодирования применение самых лучших базовых алгоритмов МПД в каскадных конструкциях совместно с внешними кодами с минимальным кодовым расстоянием $d = 3 \div 9$ также обеспечивает значительное улучшение энергетических характеристик при декодировании. График «КК3+МПД» показывает возможности такой каскадной схемы с использованием МПД во внутренних каскадах. При этом применение каскадирования позволяет ещё и снизить в таком декодере полную задержку принятия решений примерно в 1,5 раза при сохранении высокой производительности МПД декодера и в этом варианте применения.

6.10. Кодирование в каналах с неравномерной энергетикой

Рассмотрим случай применения кодирования, также приводящий к значительной экономии энергии передачи, что обычно и требуется от кодов.

Пусть для передачи закодированных данных используются два различных канала с неодинаковой энергетикой для информационных и проверочных символов. Пусть суммарная энергия каналов фиксирована и при этом ставится задача обеспечить работу системы связи при максимальной кодовой скорости.

Ясно, что при передаче в такой системе из двух каналов нужно в канале с большей энергией передавать информационные и с меньшей – проверочные символы кода. В этом случае можно ожидать, что МПД будет более работоспособным при меньшей средней энергетике системы связи или, что тоже самое, при большей кодовой скорости.

Следует отметить, что даже при оптимальном декодировании в НЭК каналах характеристики используемых кодов будут значительно ухудшены из-за того, что ближайшие кодовые слова в СОК, находящиеся на расстоянии d, отличаются в $(d–1)$ проверочных символах, которые как раз и передаются в таких каналах при более тяжёлых отношениях сигнал/шум, а значит, и с большей вероятностью ошибки. Таким образом, в НЭК каналах граница эффективности применения МПД сместится в об-

ласть более высокого уровня шума в канале, но при этом МПД декодер значительно понизит достоверность своих решений.

Пример применения МПД в таком НЭК канале представлен на рис. 6.13, на котором даны характеристики разработанного в 2004 году МПД на ПЛИС Xilinx в обычном гауссовском канале (МПД) (кривая 2), граница снизу для эффективности применяемого кода СОК с $d = 11$ (кривая 1), а также характеристики применения этой же ПЛИС в канале с неравномерной энергетикой (кривая 4). Предполагается, что энергия канала проверочных символов уменьшена примерно вдвое, благодаря чему энергетика канала информационных символов увеличилась в ~1,5 раза. Для сравнения на рис. 6.13 также приведён график для стандартного декодера по алгоритму Витерби с конструктивной длиной кода $K = 7$ (кривая 3).

Как следует из сопоставления обычного МПД и этого же декодера, работающего в каналах с неравномерной энергетикой, последний позволяет работать при уровне шума, примерно на 1 дБ более высоком, чем в обычном случае без изменения дру-

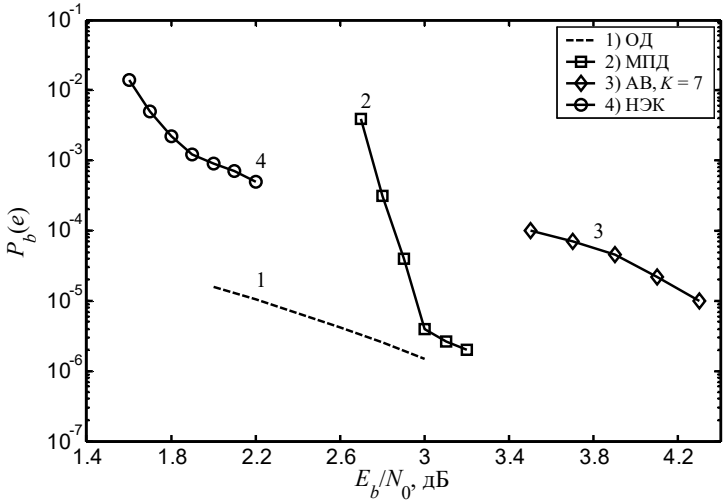


Рис. 6.13. Характеристики МПД на ПЛИС Xilinx в обычном гауссовском и в НЭК каналах

гих параметров кодирования. Изменение состоит только в том, что число итераций в МПД возрастает с 9 до 25. Но это всегда происходит, если декодер переходит к работе в области значительно более высокого уровня шума.

Отметим, что в обоих случаях сравнения МПД используется в обычном свёрточном варианте работы ПЛИС.

Очевидно также, что МПД в канале с неравномерной энергетикой обеспечивает более низкие уровни достоверности, чем в обычном канале. Вместе с тем, конечно, работа при низком уровне сигнала более чем желательна.

Анализ показал, что при $E_b/N_0 \sim 2$ дБ МПД в канале с неравномерной энергетикой уже работает с эффективностью, близкой к оптимальной для этой системы каналов и ошибки МПД фактически распределены случайно и независимо. Иначе говоря, после МПД мы имеем снова канал, очень близкий к классическому ДСК. А это значит, что второй внешний код с кодовой скоростью $R \geq 0{,}097$, создающий с МПД простую последовательную каскадную схему и вносящий потери в ЭВК не более 0,1 дБ, обеспечит доведение итоговой достоверности до уровня $P_b(e) \sim 10^{-6} \div 10^{-8}$ при совершенно незначительной сложности второго декодера.

Заметим, что формы организации НЭК каналов очень разнообразны. Конкретные методы реализации таких каналов сильно зависят от системы сигналов, с которой МПД декодер должен взаимодействовать. В целом все эти вопросы решены для многих таких систем. Этим и можно завершить обсуждение разнообразных возможностей повышения эффективности применения МПД в сложных системах связи.

6.11. Применение МПД в каналах со сложной структурой потоков ошибок

При использовании МПД в каналах с пакетной компонентой, как показали результаты применения этого алгоритма в разработках автора и ряда организаций, основным результатом работы МПД алгоритма является успешное исправление и достаточно длинных пакетов. Это в первую очередь связано с тем, что МПД в явном виде не осуществляет перемежения символов

передаваемых сообщений, но, используя коды с низким отношением d/n, как бы выполняет именно эти операции.

Полезные демопрограммы с алгоритмом МПД в своей сверхбыстрой версии можно переписать с веб-сайта **www.mtdbest.iki.rssi.ru**. Эти программы позволяют наряду с исправлением ошибок гауссовского канала одновременно исправлять и пакеты ошибок, длины которых можно в этих программах менять в широких пределах.

Таким образом, имея в виду большое разнообразие каналов со сложной структурой ошибок, можно указать, что МПД может успешно работать и в таких сетях связи, поскольку обладает весьма широкими возможностями для адаптации к конкретным условиям применения кодирования в различных системах передачи данных.

6.12. Выводы

Изложенные в этой главе методы, развивающие способы использования МПД в различных кодовых конструкциях традиционного типа, как, например, в каскадных схемах, в том числе с проверками на четность, или нового вида, как параллельное кодирование и коды с выделенными ветвями, многопозиционные системы сигналов, коды с неравной защитой символов и коды с неравномерной энергетикой демонстрируют высокие значения эффективности по важнейшему критерию кодирования – энергетическому выигрышу.

На рис. 6.14 представлены графики возможной предельной энергетической эффективности кодирования. На нём указаны кривые предельных значений отношения E_b/N_0 для кодов с алгоритмами декодирования, которые ограничены в ДСК и гауссовском канале вычислительной скоростью канала R_C, как, например, для последовательных алгоритмов. Приведены также кривые для E_b/N_0 лучших возможных алгоритмов декодирования, что в случае ДСК и гауссовского канала определяется равенством $R = C$. Кроме того, на рисунке указаны возможности для свёрточных кодов с длиной кодирующего регистра $K = 7$ и декодированием по АВ в гауссовском канале. Приведены также возможности МПД в гауссовском канале для кодовых скоростей

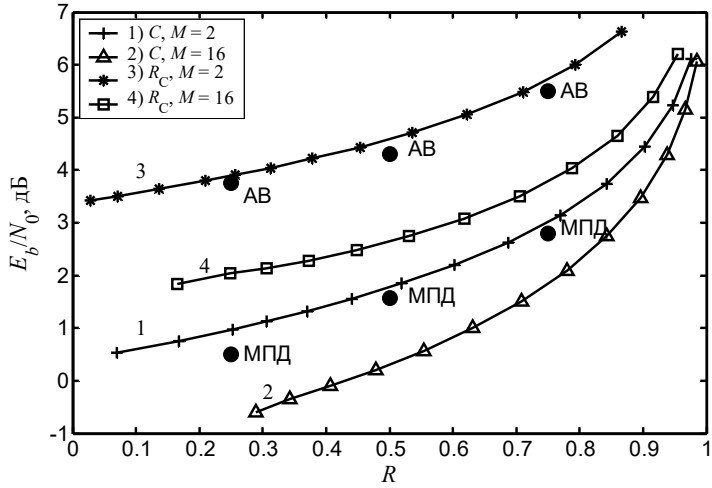


Рис. 6.14. Энергетическая эффективность АВ, МПД и лучших алгоритмов декодирования при условиях $R = R_C$ и $R = C$ в гауссовских каналах

R, равных 1/4, 1/2 и 3/4. Эти декодеры реализованы или могут быть реализованы уже в настоящее время аппаратно даже для высокоскоростных каналов связи с производительностью до сотен Мбит/с. Оставшееся расстояние до пропускной способности гауссовского канала по энергетике новые разработки МПД, видимо, смогут преодолеть путём некоторого увеличения числа операций на бит и введения новых для МПД методов каскадирования без существенного снижения производительности декодирования.

Во многих случаях полученные на базе алгоритмов МПД значения ЭВК и производительности оказываются выше аналогичных данных для весьма сложных в реализации схем, например, классических каскадных кодов и многих других кодовых конструкций.

Отметим, что новые методы параллельного кодирования, использование МПД в каналах с неравномерной энергетикой и применение кодов с выделенными ветвями позволяют решать

проблему увеличения эффективности кодирования и в рамках некаскадных схем МПД.

Представленные данные исследований по кодам и МПД успешно использованы в различных организациях, в том числе при создании многопороговых декодеров на ПЛИС и как часть программного обеспечения систем связи широкого назначения.

ЗАКЛЮЧЕНИЕ

Эта монография увидела свет в год сорокалетия издания на русском языке перевода удивительной по своей глубине и ясности изложения книги Дж. Месси «Пороговое декодирование», издательство «Мир», 1966 г. Полагая это совпадение важным и обязывающим, автор умножил усилия при подготовке к публикации совокупности своих исследований по дальнейшему развитию методов исключительно простого мажоритарного декодирования линейных кодов и в связи с этим надеется, что, по меньшей мере, некоторые из тех методов многопорогового декодирования, которые были представлены в данной книге, окажутся действительно полезными для связистов нового века.

Перечислим кратко те принципиальные новые результаты, которые выводят МПД методы на ведущие позиции в мировом конкурсе алгоритмов коррекции ошибок для каналов с большим уровнем шума.

Во-первых, книга про МПД представляет собой уникальное издание, в котором постоянно указывается на единство блоковых и свёрточных кодов. В мировой практике исследования проблем кодирования до сих пор ещё не преодолено противопоставление этих классов кодов, тогда как МПД даже своими базовыми свойствами подчёркивают их взаимосвязь, особенно на прикладном уровне.

Далее, это, несомненно, доказательство ключевых свойств МПД алгоритмов, согласно которым изменения декодируемых символов всегда приводят к строго более правдоподобным новым промежуточным решениям декодера. Никаких аналогов таких важнейших свойств для других алгоритмов коррекции ошибок до сих пор нет.

Найдены классы кодов, которые почти не подвержены эффекту размножения ошибок, т.е. группирования ошибок на выходе декодера порогового типа. Все ранее применявшиеся подходы к изучению эффекта размножения ошибок не смогли дать ничего конструктивного для идеи повторной и, тем более, многократной коррекции ошибок.

Подчеркнём, что свойство сходимости решений МПД к оптимальному и результаты принципиально нового анализа эф-

фекта размножения ошибок обеспечили одновременно с двух направлений (со стороны алгоритма и со стороны кодов) такие условия декодирования, при которых МПД декодер на самом деле во многих случаях при весьма высоких уровнях шума достигает решения оптимального декодера. В то же время, хотя достижение оптимальных решений обычно требует переборных методов, сложность алгоритма МПД растёт с длиной кода всего лишь линейно.

Тем не менее, МПД не относится к оптимальным методам и, после описания решения двух сложнейших проблем – выбора простых хороших алгоритмов и наиболее подходящих для них кодов – большая часть книги фактически посвящена методам повышения эффективности работы МПД при возможно более высоком уровне шума. Все предлагаемые для этого методы улучшения алгоритмов типа МПД всегда строго отбираются по критериям минимальной сложности как при оценке их с точки зрения числа операций, так и при расчётах быстродействия аппаратной реализации.

Для различных кодов, использованных в МПД, и большинства вариантов декодирования на основе этого метода приведены полезные оценки эффективности. Для дополнительных оценок эффективности кодов и алгоритма МПД можно обратиться к нашему справочнику по кодам, на специализированный научно-методический двуязычный веб-сайт ИКИ РАН по методам кодирования **www.mtdbest.iki.rssi.ru** , или промоделировать ту схему, которая вызывает вопросы, на компьютере.

Более того, на указанном веб-сайте можно найти развёрнутые ответы на вопросы, которые часто задают читатели, желающие улучшить своё понимание проблематики помехоустойчивого кодирования.

Оценки сложности программной реализации показывают преимущество МПД перед другими методами примерно на два десятичных порядка по числу операций на бит при сопоставимой эффективности. Это редчайший случай в истории развития методов цифровой обработки. Им надо правильно распорядиться. В канале с довольно большим уровнем шума при моделировании работы МПД на обычных ПЭВМ скорость его рабо-

ты близка к 1 Мбит/с на каждые 1 ГГц тактовой частоты процессора. Это действительно на порядки превышает производительность программных версий других алгоритмов при той же энергетической эффективности.

В настоящее время построены коды и созданы конкретные программные МПД процессоры, принятые к стандартизации для цифровых каналов специальной телевизионной системы. Трудно припомнить другие подобные решения при отечественных разработках цифровой техники связи. На специализированных микропроцессорах скорость декодирования МПД можно значительно повысить. Поэтому маловероятно, что какие-то другие достаточно эффективные методы могут быть упрощены в такой же степени.

Результаты аппаратной реализации МПД на основе ПЛИС Xilinx и Altera демонстрируют возможность достижения абсолютной степени распараллеливания вычислений. В этом случае архитектуру БИС можно выстроить таким образом, что декодер как бы вообще не тратит никакого времени на операции с данными синдромного регистра. Прямо в момент завершения цикла сдвига данных по регистрам декодера решения о величине ошибки в декодируемых символах уже всегда сформированы. Значит, эти регистры в декодере МПД могут сдвигать данные со скоростью, максимальной для выбранной технологии. А это скорости порядка сотен мегабитов в секунду на регистр. Разумеется, при этом число одновременно и параллельно работающих регистров в декодере может достигать нескольких десятков. Поэтому производительность МПД алгоритма может определяться только максимально возможной скоростью одновременного сдвига данных во всех таких регистрах памяти, из которых почти полностью и состоит этот декодер. Иначе говоря, стороннему наблюдателю представляется, будто декодер просто в большинстве случаев «угадывает» правильные решения, которые он мгновенно и подставляет в проходящие информационные потоки, двигающиеся по схемным регистрам с максимально возможной скоростью.

Эта возможность уже успешно реализована на стандартных ПЛИС за счёт создания соответствующей адаптивной схемы

порогового элемента и подбором необходимых разностных соотношений в порождающих полиномах используемого кода. Такое двухэтапное распараллеливание операций МПД и обеспечивает его сверхбыструю работу. Столь идеальное упрощение МПД в аппаратном виде довольно трудно реализовать для других алгоритмов, что позволяет считать МПД абсолютным лидером среди других методов и по производительности аппаратного декодера. Таким образом, преимущество аппаратных МПД перед другими алгоритмами по скорости на два-три десятичных порядка также может считаться уже вполне достигнутым.

Подчеркнём, что МПД просто декодируют очень длинные коды, для которых только и возможна эффективная реализация коррекции ошибок при больших шумах канала. МПД могут использовать многие типы блоковых и свёрточных кодов, из которых наиболее выделяются самоортогональные с особенно простой реализацией их декодирования.

Для недвоичных каналов более 20 лет назад предложены также очень простые МПД декодеры для недвоичных кодов. Их характеристики при близких по уровню шума условиях работы на два, три и более порядков лучше по вероятности ошибки, чем у любых декодеров кодов Рида – Соломона. Это, как и в двоичных кодах, связано с тем, что МПД успешно, очень просто и почти оптимально декодирует весьма длинные коды, такие, которые в принципе невозможно построить в классе кодов РС. Заметим, что среди недвоичных кодов очень трудно создать и эффективный алгоритм Витерби. Таким образом, недвоичный МПД является прекрасным примером совершенно уникального и чрезвычайно эффективного декодера, с которым не может даже близко сравниться никакой известный недвоичный код и декодер другого класса, которых, если исходить из реальности, фактически и нет. А поскольку сейчас известно огромное число различных вариантов применения кодов РС (и больше практически никаких других нет!), то это и означает, что потребность в недвоичных кодах чрезвычайно велика, а возможности ограничены именно кодами РС. Например, недвоичный МПД обеспечит простейшими методами повышение достоверности хранящихся на CD-ROM или переданных цифровых данных на много

десятичных порядков. Эти декодеры формируют принципиально новые уровни качества и целостности цифровых символьных потоков данных, которые недостижимы для декодеров РС. Причём, что крайне важно, недвоичные МПД тоже очень просты, как и его двоичные аналоги.

МПД можно применять и для одновременного с помехоустойчивым кодированием сжатия цифровых данных, в частности, со статистикой бернуллиевского источника. Очень важно, что для некоторых типов источников сжатие реализуется на уровне, очень близком к теоретически предельно возможному. И, что очень существенно, такие МПД не боятся даже высокой плотности ошибок в принятых упакованных потоках. Они и в этом случае восстанавливают данные с требуемым высоким качеством. При этом совершенно не обнаруживается никаких признаков «хрупкости» сжатой информации, когда искажения в переданных данных приводят к большим пакетам ошибок в восстановленной распакованной информации.

В каналах со стираниями МПД работают почти при пропускной способности такого канала, на много порядков снижая долю стёртых символов по сравнению с их исходной плотностью во входном цифровом потоке. Это, видимо, тоже практически недостижимо для других методов. Причём, восстанавливающий стёртые данные МПД оказывается даже ещё проще, чем декодер для каналов типа ДСК, хотя сложность базового МПД и так очень незначительна.

Уникальны и каскадные схемы для МПД. При каскадировании с кодами контроля по чётности иногда можно обойтись всего одной – двумя дополнительными операциями декодера на бит, сохраняя при этом все достоинства каскадных схем по эффективности. Это совершенно несопоставимо со сложностью декодирования каскадных схем с кодами РС, которые, тем не менее, иногда очень сильно уступают простейшим схемам с МПД и ККЧ.

Далее, практически всегда можно сделать так, чтобы на втором этапе декодирования каскадного кода с МПД скорость кода R_1 этого второго этапа коррекции ошибок фактически совпадала со скоростью R_0 всего каскадного кода в целом. Обычно

декодер второй очереди в последовательной каскадной схеме работает при скорости $R_1 \approx 0{,}8 \div 0{,}95$, т.е. он изначально гораздо менее эффективен, чем код с кодовой скоростью полного каскадного кода R_0. В значительной степени именно поэтому МПД для каскадных кодов особенно эффективны, оставаясь при этом почти столь же простыми, как и обычные базовые МПД алгоритмы.

Особенно удобны и эффективны МПД при параллельном каскадировании. Возможно, эти методы появились гораздо раньше всех других достаточно эффективных параллельных методов кодирования. Хорошо работает МПД также и с различными сложными многопозиционными системами сигналов, которые значительно сжимают спектр передаваемого сигнала относительно традиционной двоичной системы ФМ2.

Полезные результаты получены для МПД при использовании кодов с неравной защитой битов, с неравномерной энергетикой каналов, в случае применения МПД для кодов с выделенными ветвями. Это позволяет утверждать, что МПД декодеры легко адаптируются к различным условиям их применения в системах связи.

Заметим, что при отсутствии мягкого модема, наличие которого обязательно для применения большинства других эффективных алгоритмов, МПД существенно упростится, а некоторое снижение его характеристик по энергетике будет очень умеренным.

Важнейший шаг проектирования МПД – оптимизация многих сотен его параметров. Это – хороший пример правильного использования мощной современной компьютерной техники и тех же методов адаптации и оптимизации, которые реализует собственно МПД, в проектировании самих этих крайне полезных алгоритмов. При этом достигается дополнительное повышение результирующей достоверности декодирования благодаря очень существенному улучшению характеристик МПД, иногда на один-два порядка, без какого-либо увеличения числа операций в конечном варианте применения такого декодера после выполнения оптимизации. Никакие другие методы коррекции ошибок не имеют такого действительно мощного дополнитель-

ного средства повышения эффективности без какого-либо увеличения его итоговой сложности.

Вообще вся идеология МПД базируется именно на идеях оптимизации функционалов от очень большого числа переменных на всех трёх этапах проектирования и собственно контроля работы алгоритма.

1. Сначала при выборе кодов для МПД осуществляется поиск по целому ряду критериев таких кодов, которые в минимальной степени подвержены эффекту размножения ошибок.

2. Затем при выборе общих критериев и параметров декодирования оптимизируются путём выбора необходимых значений веса проверок, пороги решений мажоритарных элементов и отдельные разностные параметры кодов в выбранных декодерах.

3. Третьим шагом оптимизационного проектирования является контроль работы МПД, который и реализует алгоритм, минимизирующий расстояние решения МПД до принятого из канала сообщения.

Именно совокупность указанных мощных оптимизационных процедур на всех трёх главных этапах проектирования и контроля характеристик МПД обеспечивает высокие результирующие параметры эффективности алгоритма.

Очень широки возможности МПД по согласованному взаимному обмену между значениями его параметров: памяти, задержки решения, числа операций, производительности, размеров кода, избыточности, уровня шума канала и энергетического выигрыша. Всегда можно выбрать такие параметры декодера, что по любому непротиворечивому техническому заданию на его разработку можно создать требуемое устройство класса МПД. Например, для достижения максимальной скорости можно реализовать высокопроизводительный свёрточный МПД за счёт увеличения памяти декодера и задержки решения. При необходимости снижения задержки решения следует применять блоковые коды, что уменьшает производительность декодера. В случае выбора небольшой скорости передачи можно успешно нагрузить декодер мощным алгоритмом коррекции с более

сложным типом порогового элемента, который позволит работать при большем уровне шума и т.д.

И, наконец, подчеркнём, что все эти совершенно принципиальные практические результаты являются следствием серьёзных теоретических исследований. В течение многих десятилетий создавались очень мощные инструментальные стенды и программное обеспечение для разработки, испытаний и контроля работы МПД на различных ПЛИС, а также создания имитаторов цифровых каналов и макетов новых алгоритмов декодирования.

Описанная выше технология проектирования МПД декодеров представляет собой ещё один важнейший аспект тематики многопорогового декодирования. Дело в том, что параллельно с 35-летними исследованиями по тематике МПД все эти годы создавались программно-аппаратные средства. Их базовые компьютеры, цели и ориентиры, быстро преображались в соответствии со стремительным развитием цифровой техники. В настоящее время специально созданное системное программное обеспечение для исследований, оптимизации и проектирования МПД составляет эффективные пакеты прикладных программ, которые продолжают интенсивно развиваться.

Таким образом, исследования МПД базируются на идеологии современного помехоустойчивого кодирования, мощном, динамически развивающемся программном обеспечении и специальных аппаратных средствах. Это обеспечивает условия для успешного продолжения исследований и разработок, но и определяет трудности приобретения необходимого объёма знаний и опыта для специалистов, которые не работали ранее по тематике МПД. Если они готовы к сотрудничеству, то при взаимодействии с разработчиками МПД алгоритмов всегда быстро выходят на тот уровень, с которого начинается действительно серьёзная исследовательская работа по этой проблематике. Только непрерывное и интенсивное развитие всей инструментальной базы исследований и программного обеспечения для дальнейшей разработки этого метода, а также всесторонняя глубокая подготовка специалистов по исследованиям и разработкам алгоритмов МПД, которая осуществляется по многим направлениям,

позволяют продолжать успешные исследования по тематике многопорогового декодирования.

Рекомендации для дальнейших исследований

Исходя из уровня достигнутых возможностей алгоритмов МПД попробуем сформулировать те задачи, которые следует решать, чтобы развитие тематики МПД продолжалось максимально быстрыми темпами.

1. Поскольку рабочая область МПД в настоящее время выше границы Шеннона по энергетике примерно на 1 дБ, то должен быть продолжен и расширен поиск условий для работы МПД непосредственно вблизи пропускной способности канала.

2. Если рекордная производительности МПД не нужна, то полезно немного усложнить работу порогового элемента в МПД, что позволит сократить число итераций, уменьшить задержку принятия решений МПД и обеспечить работу МПД при большем уровне шума. Надо найти оптимальную по сложности функцию, намного более эффективную, чем обычный пороговый элемент.

3. Развивать каскадные методы кодирования, которые способны помочь МПД работать почти при пропускной способности канала без увеличения сложности декодирования. Нужно иметь в виду, что схемы с высокоскоростными внешними кодами, скорее всего, бесперспективны.

4. Проработать каскадные недвоичные коды, предварительно повысив эффективность обычного недвоичного МПД ещё на несколько порядков, хотя уже и сейчас его преимущество перед декодерами кодов РС более чем значительно. При этом полезно рассмотреть самые различные схемы, в том числе и с параллельными кодами.

5. Создать новые системы кодирования с мощными МПД и многопозиционными системами сигналов.

6. Продолжить разработки систем одновременного кодирования канала и различных видов источника. Это крайне важно для телеметрии.

7. Продолжить поиск и анализ эффективных методов кодирования блоковых кодов, поскольку при их обработке пока не

наилучшим образом используются вычислительные возможности МПД.

8. Продолжить развитие тематики неравномерной энергетики. Это быстрый и успешный рост ЭВК с минимальными затратами.

9. Создать эффективные декодеры для каналов с неравной защитой символов. Некоторые задачи тут довольно простые, но требуется тонкая оптимизация кодов.

10. Под все перечисленные задачи необходимо непрерывно создавать новые коды, которые только и могут помочь в дальнейшем развитии методов МПД.

11. Создать микропроцессорные МПД с большой энергетической эффективностью на лучших в настоящее время микропроцессорах.

12. Предпринять специальные усилия по дальнейшему снижению объёма вычислений в МПД при большом уровне шума. Это облегчит достижение высокоэффективной работы МПД алгоритмов при предельных отношениях сигнал/шум.

* * * * * * * *

Приглашаем также специалистов, студентов и аспирантов просмотреть специализированный веб-сайт ИКИ РАН **www.mtdbest.iki.rssi.ru**. Он регулярно обновляется. Там можно найти задачи, которые могут быть решены и стать основой для создания новых типов МПД.

На веб-сайте регулярно помещаются новые статьи, демонстрационные материалы и презентации последних результатов по МПД. Там же можно найти ответы на последние вопросы по кодированию и объявления о новых предстоящих или уже состоявшихся событиях в сфере разработок МПД алгоритмов.

Часть не рассмотренных в данной книге вопросов проанализирована в нашем справочнике по кодированию «Помехоустойчивое кодирование. Методы и алгоритмы», Москва, издательство «Горячая линия – Телеком», 2004 г. Интернет-магазины, в которых можно её купить, легко найти через поисковую систему **www.findbook.ru** или приобрести её непосредственно через издательство **www.techbook.ru**, тел.: (495)737–39–27.

THE SUMMARY

This monography was issued in 40-year jubilee of publishing in Russian surprising on the depth and simultaneously on statement clearness J. Massey's book «Threshold decoding», 1966. Believing this concurrence important and obliging, the author has increased his efforts in preparation for the publication of his research set on the further development of methods of extremely simple linear codes majority decoding. Therefore the author hopes, that at least some of those methods of multithreshold decoding (MTD) which have been submitted in the given book, appear really useful for communications of a new century.

We list briefly those basic new results which propose iterative MTD methods on leading positions in global competition of error correcting algorithms for channels with the large noise level.

First, the book about MTD represents the unique edition in which the unity of block and convolutional codes is constantly underlined.

Further, it is, undoubtedly, the proof of key MTD algorithms properties according to which decoding symbols changes always lead strictly to optimum decoder (OD) decisions. Any analogues of such significant properties for other error correcting algorithms till now are not present.

Classes of codes which are not subject almost to effect of error propagation (EP), i.e. groupings of errors at the output of the threshold decoder are found. All earlier used approaches to studying EP effect could not give anything constructive for idea of repeated error correction.

Let's emphasize, that MTD the decoder actually in many cases at rather high noise levels reaches the OD decision. At the same time, though achievement of optimum decoder decisions usually demands total search methods, complexity of algorithm MTD grows with length of a code only linearly.

Nevertheless, MTD is not an optimum method and, after the description of the two most complicated problems decision: a choice of simple good algorithms and the codes most suitable to it, – the most part of the book is actually devoted to methods of increase of overall MTD performance at possible higher noise level. Thus all methods

of improvement of algorithms offered for such MTD are always strictly selected by criteria of the minimal complexity as at their estimation from the point of view of operations number, and at calculations of hardware realization throughput.

For the various codes used in MTD, and the majority of decoding variants on the basis of this method useful estimations of efficiency are resulted. In the case of need in additional estimations of efficiency of codes and algorithm MTD it is possible to address to our reference book on codes, at specialized website SRI of the Russian Academy of Science **www.mtdbest.iki.rssi.ru** or to imitate that circuit which causes questions, on a computer.

Moreover, on the specified website it is possible to find the detailed developed answers to questions asked frequently by the readers, wishing to improve their understanding error correcting coding problems.

Estimations of complexity of program realization show MTD advantage before other methods at ~2 decimal exponents in number of operations per bit at comparable efficiency. It is a very rare case in a history of digital processing methods development. They should be used correctly. In the channel with rather large noise level at modeling MTD work with usual personal computer its throughput is more than 1 Mbit/s per 1 GHz the processor clock frequency that exceeds extremely productivity of other soft algorithms at the same signal/noise efficiency.

Now codes are constructed and created concrete soft MTD processors accepted to standardization for digital channels of special television system. It is difficult to remember other similar decisions by domestic development of digital communication techniques. For the specialized microprocessors speed of MTD decoding can be increased considerably. Therefore it is improbable, that any other effective enough methods can be simplified in the same degree.

Results of hardware realization MTD on a basis PLIS Xilinx and Altera show an opportunity of achievement of an absolute degree of parallel calculations. In this case the decoder architecture can be built in such a manner that the decoder as though does not spend for operations with the data of the syndrome register in general any time at all. Directly at the moment of shift data cycle end through registers

of the decoder the decision on error value in decoding symbols always are already ready. Therefore throughput of MTD algorithm can be determined only by the greatest possible speed of simultaneous data shift in all such memory registers of which ones almost completely this decoder will consist. This opportunity is already successfully realized on standard PLIS due to creation of corresponding adaptive majority element circuit and selection necessary differentials in generating code polynomials. Such two stage parallelism in MTD operations forms its super fast work. Thus, advantage of hard MTD before other algorithms at speed at 2÷3 decimal exponents is already achieved also.

MTD simply decode very long codes for which ones only effective realization of error correction is possible at the large noise of the channel.

The codes and their very simple MTD decoders without operations of multiplication and division for non-binary channels also were offered 20 years ago. At relatively close on noise level conditions MTD is at 2÷3 decimal exponents and better than characteristic of error probability for Read-Solomon (RS) codes. It is connected, as well as in binary codes, by that MTD successfully, very simply and almost in optimal manner decodes rather long codes, which ones cannot be constructed in a class of RS codes. We shall notice that among non-binary codes it is very difficult to create effective Viterbi algorithm also. So non-binary MTD is a fine example of completely unique and extremely effective decoder for which any other non-binary codes and the good decoders of other class really does not exist at all. And as the huge number of various variants of codes PC application now is known it also means, that the need for non-binary codes is extremely great, and all opportunities are limited by codes RS possibilities. For example, non-binary MTD will provide with the elementary methods to increase data reliability stored on CD-ROMs or the transmitted digital data at many decimal exponents. These decoders form essentially new level of quality and integrity of digital symbolical data streams that are unattainable for RS decoders at all. And, that is the extremely important, non-binary MTD is very simple also, as well as its binary analogues.

MTD is possible to apply and for simultaneous with error correcting coding data compression, in particular, with binomial source statistics. It is very important, that for some types of sources compression with MTD is realized at a level very close to theoretically limiting possibilities. And, that is very essential, such MTD are not afraid even of high error density in the accepted packed streams. In this case it restores the data with required high quality also. There are not finding out any attributes of «fragility» of the compressed information at all when distortions in the transmitted data lead to the big packets of error in the restored unpacked information.

In channels with erasures MTD work almost at the capacity of such a channel, at many decimal exponents reducing a remained number of the erased symbols in comparison with their initial density in input digital stream. It seems to be practically unattainable for other methods also. And, restoring erased data for MTD is even easier task, than for decoder in binary symmetric channel, though complexity of MTD for errors is very insignificant too.

Concatenated circuits for MTD are unique. At concatenating with parity check codes sometimes it is possible to get with one – two additional decoding operations saving very large advantages on concatenation efficiency. It is more simple in complexity than decoding of concatenated circuits with codes RS which ones sometimes are less effective too.

Further, practically always it is possible to make so that at the second stage of decoding of a concatenated code with MTD speed of code R_1 of this stage of error correction actually coincided with speed R_0 of all concatenated code as a whole. Usually the second-order decoder in the consecutive concatenated circuit works at speed $R_1 \approx 0{,}8 \div 0{,}95$, i.e. it is initially much less effective than a code with code speed of full code R_0. Substantially for this reason MTD for concatenated codes are especially effective, remaining thus almost so simple, as well as usual main MTD algorithms.

MTD are especially convenient and effective for parallel codes. Effective parallel MTD coding schemes may be have appeared much earlier in general than all others similar methods.

MTD well works with various compound systems of signals which considerably compress a spectrum of a transmitted signal with respect to traditional binary system FM2.

Useful results are received for MTD at use of codes with unequal bits protection, with non-uniform power of channels, in case of MTD application for codes with the allocated branches. So MTD decoders easily adapt for various conditions of their application in systems of communication.

Let's notice, that at absence of the "soft" modem that is necessary for the majority of other effective algorithms, MTD in this case will be very essentially simplified, and some decrease in its characteristics at signal/noise level will be very moderate.

The main step of designing MTD – optimization of its many hundreds parameters. It is a good example of correct use of powerful modern computers and technical equipment and the same methods of adaptation and optimization which realizes MTD itself, in designing these extremely useful algorithms. Thus additional increase of resulting reliability of decoding achieves sometimes 1÷2 decimal exponents without any increase in operations number in a final variant of such decoder after performance optimization is made. Any other methods of error correction have no such really powerful additional means of efficiency increase at all.

In general all MTD ideology is based on ideas of optimization functional of very large number of variables at all three design stages. First it needs at a choice of codes for MTD, at the stage of its optimization and at real work in noisy channel. Note that optimization of weight values of checks, thresholds and separate differential parameters of code polynomials in the chosen decoders requires big efforts, but gives most important results. This complex optimizing means usage provides high decoder performance.

Opportunities MTD on the coordinated mutual exchange between values of its parameters are very wide: memories, delays of the decision, number of operations, productivity, the sizes of a code, redundancy, noise level of the channel and a code gain. Always it is possible to choose such parameters of the decoder, that under any practically consistent technical requirements for its development it is possible to create good MTD device. For example, for achievement

of the maximal speed it is possible to realize high-efficiency convolutional MTD due to increase in decoder memory and delay of the decision. If it is necessary to decrease in a delay of the decision then they must to apply block codes that reduces throughput of the decoder, and at a choice of small speed of transmission it is possible to load successfully the decoder with more powerful algorithm of correction with more comprehensive threshold element which will allow to work at the greater noise level, etc.

Well, and at last, we shall emphasize, that all these fundamental results are consequence of serious theoretical researches, developments within many decades of very powerful tool, test benches and the software for development, tests and the control of work MTD in various PLIS, and also creations of simulators of digital channels and models of new decoding algorithms.

In connection with the technology of designing MTD decoders described above there is one more major aspect of subjects of multithreshold decoding. The matter is that together with 35-years researches on subjects MTD all these years were created hardware-software means which changed the base computers, the purposes and reference points, quickly changed according to fast development of digital technical equipment. Now specially created system programs for researches, optimization and designing MTD makes effective software that continues to develop intensively.

In addition full and all-round deep expert education in the field of researches and development of algorithms MTD which is carried out on many directions allows to continue successful researches on subjects of multithreshold decoding.

The part of the questions considered in the given book is analyzed in our reference book on coding «Error correcting coding. Methods and algorithms», Moscow, publishing house «Hot line – Telecom», 2004. Internet-shops in which it is possible to buy it, easily to find through search system **www.findbook.ru** or to get it directly through publishing house **www.techbook.ru**, phone number +7–495–737–39–27 in Moscow.

The latest information on MTD may be found at specialized web-site SRI RAS on codes **www.mtdbest.iki.rssi.ru**. It is upgraded permanently.

ПРИЛОЖЕНИЯ

Список сокращений, принятых в книге

АБГШ	аддитивный белый гауссовский шум
АВ	алгоритм декодирования Витерби
АФМ	амплитудно-фазовая модуляция
БЧХ	код Боуза-Чоудхури-Хоквингема
ДСК	двоичный симметричный канал
QСК	q-ичный симметричный канал
ККЧ	код с контролем по четности
МПД	многопороговый декодер (алгоритм декодирования)
НЗ-коды	коды с неравной защитой символов
ОД	оптимальный декодер
ПД	пороговый декодер
ПДД	пороговый декодер с «джином»
ПК	параллельный код, параллельное кодирование
ПФВ	производящая функция вероятности
РО	размножение ошибок
РС	код Рида-Соломона
СМПД	многопороговый декодер для стирающих каналов
СОК	самоортогональный код
СтСК	симметричный стирающий канал
ФМ	фазовая модуляция
ЭВК	энергетический выигрыш кодирования
QМПД	q-ичный многопороговый декодер

Таблица уровня шумов в гауссовском канале

Отношение сигнал/шум E_s/N_0, дБ	Вероятность ошибки в канале p_0	Пропускная способность канала C_{16}, «мягкий» модем	Пропускная способность канала C_2, «жесткий» модем
1	2	3	4
–15,00	4,01e–001	0,0365	0,0286
–14,50	3,95e–001	0,0412	0,0321
–14,00	3,89e–001	0,0466	0,0359
–13,50	3,83e–001	0,0526	0,0402
–13,00	3,76e–001	0,0594	0,0450
–12,50	3,69e–001	0,0670	0,0504
–12,00	3,61e–001	0,0755	0,0563
–11,50	3,53e–001	0,0851	0,0630
–11,00	3,45e–001	0,0958	0,0704
–10,50	3,36e–001	0,1077	0,0786
–10,00	3,27e–001	0,1209	0,0878
–9,50	3,18e–001	0,1356	0,0980
–9,00	3,08e–001	0,1518	0,1093
–8,50	2,98e–001	0,1696	0,1217
–8,00	2,87e–001	0,1892	0,1356
–7,50	2,75e–001	0,2105	0,1508
–7,00	2,64e–001	0,2337	0,1676
–6,50	2,52e–001	0,2588	0,1860
–6,00	2,39e–001	0,2857	0,2062
–5,50	2,26e–001	0,3145	0,2283
–5,00	2,13e–001	0,3452	0,2524
–4,50	2,00e–001	0,3776	0,2785
–4,00	1,86e–001	0,4116	0,3067
–3,50	1,72e–001	0,4472	0,3371
–3,00	1,58e–001	0,4841	0,3696
–2,50	1,44e–001	0,5221	0,4042
–2,00	1,31e–001	0,5610	0,4408
–1,50	1,17e–001	0,6004	0,4792
–1,00	1,04e–001	0,6400	0,5192
–0,50	9,09e–002	0,6794	0,5605
0,00	7,86e–002	0,7180	0,6026
0,50	6,71e–002	0,7554	0,6451
1,00	5,63e–002	0,7911	0,6875
1,50	4,64e–002	0,8247	0,7291

1	2	3	4
2,00	3,75e–002	0,8556	0,7693
2,50	2,97e–002	0,8835	0,8073
3,00	2,29e–002	0,9082	0,8427
3,50	1,72e–002	0,9295	0,8747
4,00	1,25e–002	0,9474	0,9031
4,50	8,79e–003	0,9620	0,9273
5,00	5,95e–003	0,9734	0,9474
5,50	3,86e–003	0,9821	0,9635
6,00	2,39e–003	0,9885	0,9758
6,50	1,40e–003	0,9930	0,9847
7,00	7,73e–004	0,9959	0,9909
7,50	3,99e–004	0,9978	0,9949
8,00	1,91e–004	0,9989	0,9974
8,50	8,40e–005	0,9995	0,9987
9,00	3,36e–005	0,9998	0,9995
9,50	1,21e–005	0,9999	0,9998
10,00	3,87e–006	1,0000	0,9999
10,50	1,08e–006	1,0000	1,0000
11,00	2,61e–007	1,0000	1,0000
11,50	5,33e–008	1,0000	1,0000
12,00	9,01e–009	1,0000	1,0000
12,50	1,23e–009	1,0000	1,0000

Типичные вопросы о кодировании

Здесь приводятся ответы на типичные наиболее часто встречающиеся вопросы по тематике помехоустойчивого кодирования. Представленный ниже материал позволит техническим специалистам более точно ориентироваться в вопросах исправления ошибок в каналах с шумами.

Вопрос 1. Зачем в системах связи необходимо кодирование, если при этом на самом деле увеличивается вероятность ошибки при передаче цифровых данных, поскольку нужно пересылать за то же время ещё и проверочные символы кода?

Ответ. Правильно, вероятность ошибки передачи каждого бита данных растёт, поскольку при этом приходится за определённое время отправить большее число символов в канал связи. Если для примера возьмём код с $R = 1/2$, то энергия на передачу одного кодового символа будет на 3 дБ (вдвое) меньше, чем без кодирования, и вероятность ошибки на каждый двоичный символ весьма заметно возрастёт. Но, тем не менее, если используется код с достаточно большим кодовым расстоянием, например, с $d = 11$, то результирующая вероятность ошибки после успешного декодирования может быть на несколько порядков меньшей, чем вероятность ошибки в том же канале связи без использования кодов.

Численный пример: пусть исходная вероятность ошибки в каждом переданном бите без кодирования передаваемой последовательности по некоторому обычному ДСК равна $p_1 = 0{,}01$. Из-за кодирования при $R = 1/2$ при уменьшении символьной энергетики вдвое, что происходит при удвоении скорости передачи, так как необходимо сохранить ту же информационную скорость, вероятность ошибки на символ в гауссовском канале будет уже $p_0 \sim 0{,}05$. Но поскольку нижняя достаточно точная оценки вероятности ошибки, например, после МПД или какого-то оптимального декодера (ОД) для этого кода имеет вид $P_b(e) \sim 462 p_0^{(d+1)/2}$, то именно большой показатель степени при p_0, равный 6 при $d = 11$, обеспечивает малую итоговую вероятность ошибки декодера на бит $P_b(e)$ порядка 10^{-5}. Сравнивая исходную вероятность $p_1 = 10^{-2}$ и результирующую $P_b(e) \sim 10^{-5}$

при одинаковой битовой энергетике сигнал и той же спектральной плотности мощности шума, видим, что кодирование оказалось весьма полезным, поскольку энергетический выигрыш кодирования для этих параметров кода будет порядка 5 дБ (~3 раза).

Вопрос 2. Почему вообще следует применять коды? Ведь при их использовании расширяется спектр сигнала передачи или растёт время связи.

Ответ. Да, дополнительные символы надо как-то передавать тоже. Считается, что именно энергетика в большинстве случаев является решающим параметром, который нужно минимизировать. В расчётах эффективности кодирования действительно происходит расширение спектра частот, поскольку при этих оценках считаются равными периоды передачи полезной информации при наличии кодирования и без него. Но именно экономия энергетики сигнала приносит очень большую экономическую выгоду, исчисляемую миллионами долларов. Результатом применения кодирования могут быть уменьшение размеров антенн, увеличение дальности или повышение скорости передачи, а также многие другие достоинства кодов. Этим и определяется ценность кодирования для систем спутниковой связи.

Вопрос 3. Как написать правильное Техническое задание на систему кодирования?

Ответ. Ниже приведён достаточно типичный вариант рассматриваемого заказчиком и исполнителем списка параметров системы кодирования, которые они должны согласовать в процессе разработки ТЗ.

Перечень

основных и дополнительных параметров кодов и декодеров при подготовке ТЗ на разработку системы кодирования

1. Основные параметры.

1.1. Блоковые или свёрточные коды.
1.2. Двоичные или недвоичные коды.
1.3. Длина кода n (число кодовых символов).
1.4. Задержка решения L (число кодовых символов).
1.5. Кодовая скорость R (избыточность).
1.6. Кодовое расстояние d (минимальное или свободное).
1.7. Энергетический выигрыш кодирования (ЭВК) G, дБ.

1.8. Выходная вероятность ошибки декодера $P_b(e)$, ($\sim 10^{-5}$ или другая).
1.9. Система сигналов модуляции (двоичная, круговая ФМ, квадратурная (например, АФМ 4х4) и т.д.).
1.10. Формы контроля качества канала.

2. Дополнительные и взаимосвязанные с основными параметры кодирования.

2.1. K – длина кодирующего регистра при реализации выбранного кода.
2.2. E_b/N_0 – отношение битовой энергии канала к спектральной плотности мощности шума.
2.3. p_0 – вероятность ошибки на входе декодера (на выходе канала).
2.4. E_s/N_0 – отношение символьной энергии канала к спектральной плотности мощности шума.
2.5. Тип модема: жёсткий или мягкий.
2.6. Применимость или необходимость каскадирования.

3. Общие технические характеристики создания системы связи.

3.1. Задержка при передаче блока, (мсек).
3.2. Задержка решения декодирования, (мсек).
3.3. Виды и способы взаимодействия декодера с системами синхронизации (ветвевая, символьная, блоковая, кадровая, …..).
3.4. Реализация: программная/аппаратная.
3.5. Общая характеристика канала.
3.6. Возможность распараллеливания функций в декодере.
3.7. Скорости обработки (декодирования) (Мбит/с).
3.8. Сроки разработки проекта.
3.9. Предмет исследования в процессе проведения разработки (неясные моменты проекта).
3.10. Сложность разработки (объём работ, сложность схемы, необходимое время, технологичность, способы тестирования, виды и объемы тестирования, необходимая инфраструктура для разработки, виды взаимодействия с модемом).
3.11. Наличие аппаратуры тестирования (имитатор цифрового шума, макеты узлов и систем модема, содержащего кодек и т.д.).
3.12. Формы и способы обслуживания кодеков в процессе эксплуатации.
3.13. Объёмы эксплуатационной документации.

3.14. Необходимость сертификации и других разрешительных документов.

4. Оргвопросы.

4.1. Порядок финансирования.
4.2. Возможные виды договоров.
4.3. Предмет договора (что именно сдаётся).
4.4. Обучение персонала.
4.5. Формы испытаний, порядок.
4.6. Этапность выполнения работ.
4.7. Ответственность сторон.
4.8. Охрана интеллектуальной собственности.
4.9. Содействие продолжению научных изысканий.

Вопрос 4. Как протестировать возможно большее число лучших из известных алгоритмов в процессе проектирования системы связи?

Ответ. Желательно постоянно работать в этой сложной и интересной области проектирования систем связи. Это позволит быть в курсе всех основных результатов в технике кодирования. Большинство лучших алгоритмов должно моделироваться и непрерывно сравниваться друг с другом. Кроме того, нужно следить за публикуемыми обзорами в области кодирования.

Мы решили облегчить проектировщикам проблему выбора метода кодирования и создали имитатор цифрового спутникового канала связи, который содержит все основные наиболее эффективные методы кодирования.

Его описание есть на специализированном веб-сайте ИКИ РАН **www.mtdbest.iki.rssi.ru**.

В случае необходимости мы дополнительно включим в состав программного обеспечения имитатора и те, возможно, специальные методы кодирования/декодирования, которые необходимо рассмотреть именно в вашей организации.

С помощью такого компьютерного имитатора с лучшими современными алгоритмами кодирования можно отслеживать и прогнозировать развитие техники кодирования на много лет вперёд.

В настоящее время подготовлена новая версия цифрового имитатора, которая позволяет проверять работу аппаратных версий различных декодеров.

Вопрос 5. Почему нижние оценки вероятности ошибки декодирования МПД даже при относительно небольших значениях кодового расстояния оказываются очень маленькими? Это слабые оценки?

Ответ. Нет. Если характеристики алгоритмов декодирования соответствуют возможностям оптимального декодера или близки к ним, то, действительно, реальные вероятности ошибки декодирования даже при кодовом расстоянии используемых кодов $d \sim 7 \div 9$ оказываются достаточно маленькими. Но характеристик оптимального декодера ещё надо достичь! МПД во многих случаях это может. А про другие алгоритмы этого утверждать нельзя. Здесь нужно всё аккуратно проверять.

Вопрос 6. Почему оптимальные декодеры обычно формируют решения с группирующимися ошибками? Если это эффект размножения ошибок декодирования, то можно ли от него избавиться? Другие декодеры тоже группируют ошибки? А как ведёт себя в этой ситуации МПД?

Ответ. Оптимальные декодеры характеризуются тем, что они в той или иной форме реализуют полный перебор решений и затем выбирают лучшее из них. Но для них нужно выбирать и лучшие, плотно упакованные коды с максимально возможными значениями кодового расстояния d. А в таких кодах много кодовых слов веса d. Но тогда в таком коде всегда будут слова минимального веса со многими единичками в информационных позициях. Это хорошо известная и давно проанализированная ситуация. В случае оптимального декодирования с группированием ошибок мирятся, потому что сами ошибки происходят достаточно редко благодаря как раз большим значениям кодового расстояния d используемых для оптимальных декодеров кодов и наилучшему возможному декодированию.

А вот если декодер неоптимальный, то группирование ошибок декодирования может быть ещё и свойством самого алгоритма декодирования. В этом случае можно говорить о размножении ошибок декодирования. Таким образом, группирование ошибок всегда зависит и от алгоритма, и от вида используемого кода. Это и надо учитывать при выборе таких алгоритмов, осо-

бенно если они предназначаются к использованию в каскадных схемах кодирования.

В МПД можно сделать размножение ошибок очень небольшим при правильном выборе кодов. Обо всём этом много материала для размышлений в третьей главе.

Вопрос 7. Почему кодирование требует очень больших задержек решений?

Ответ. На самом деле это не всегда так. Если требования к способности кода работать при очень большом уровне шума нет, то всегда можно найти алгоритмы с достаточно умеренной задержкой. А вот при работе вблизи пропускной способности канала C по Шеннону действительно необходимо применять только длинные коды. Иллюстрацией этого обязательного свойства являются графики для границы сферической упаковки, которые есть в наших презентациях на веб-сайте ИКИ РАН **www.mtdbest.iki.rssi.ru**, а также в этой книге на рис. 1.11, стр. **Ошибка! Закладка не определена.**.

Вопрос 8. Различных каналов, в которых практически вообще нет ошибок, очень много. Зачем вообще применять кодирование, если можно просто увеличить энергию передачи?

Ответ. Если соединить два компьютера, стоящих на одном столе, кабелем и переписывать данные с одного диска на другой, то помех в кабеле обычно нет и применять очень мощные коды нет необходимости. Заметим, что коды контроля передачи с обнаружением ошибок применяют и тут. Но ситуация в плане защиты от ошибок здесь действительно достаточно простая, необходимости экономить энергию сигнала нет.

А вот если в спутниковом канале нет ошибок даже без применения кодов, то это только значит, что мощность сигнала очень велика, потрачены очень большие средства на создание канала и его пропускная способность C используется примерно на один процент или даже намного меньше. Если система коммерческая, то предприятие гарантированно разорится, потому что в других каналах такого же типа конкуренты передадут в 100÷1000 раз больше информации именно благодаря применению кодирования.

Заметьте, что бесспорной истиной при решении проблемы правильного проектирования системы связи в гауссовских (и многих других) каналах является исключительно парадоксальная (но только на первый взгляд!) фраза: в правильно спроектированном спутниковом канале связи должна быть достаточно большая средняя вероятность ошибки на бит. Но как раз это гарантирует, что в такой системе связи благодаря применению кодирования будет выполняться фундаментальное соотношение $R < C$ (кодовая скорость меньше пропускной способности канала), причём значения R и C будут весьма близки. Вполне неплохим результатом можно считать, если окажется, что $R \sim 0{,}7C$. Именно из-за большой стоимости каналов связи и ведутся работы по увеличению кодовой скорости при передаче по цифровым каналам, что как раз и ведёт к декодированию при всё более высоком уровне шума.

Вопрос 9. Чем отличаются различные корректирующие коды и методы их декодирования? Почему их так много?

Ответ. Если посмотреть ответ-пример (ТЗ на коды) на вопрос №3, то легко заметить, что проект на систему кодирования содержит до трёх десятков пунктов, которые надо учесть и рассмотреть. Причина этого проста: требования к кодам по многим параметрам могут быть очень и очень разными. И от этого сильно зависит, в свою очередь, выбор и самого метода коррекции ошибок, т.е. алгоритма декодирования, и его сложность.

Но и этого мало. Коды нужны для исправления ошибок. Сами ошибки при передаче цифровых данных могут возникать из-за очень разных причин. Но тогда они описываются и различными моделями генерации ошибок. Это тоже приводит к специфическим методам коррекции ошибок, т.е. к новым алгоритмам.

Более того, возможны и разные системы формирования передаваемых сигналов. Они также являются причиной дальнейшего изменения модели возникновения ошибок.

Отметим, наконец, что успехи в построении, например, алгоритмов декодирования для двоичных каналов существенно помогают продвижению и методов коррекции ошибок для мно-

гих других систем сигналов: например, для многопозиционной ФМ, для системы типа АФМ16 и т.д.

Таким образом, наличие разных методов декодирования для различных сигналов – это нормально. В частности, алгоритм МПД существует в различных модификациях: для двоичных, недвоичных и стирающих каналов, для метрик Хемминга и Евклида, для круговых ФМ, для АФМ*N* и некоторых других моделей.

Вопрос 10. Чем принципиально отличается МПД от обычного порогового декодера Месси?

Ответ. Только тем, что решения всех пороговых элементов в МПД запоминаются в дополнительном разностном регистре памяти декодера и используются затем при формировании решений на следующих итерациях коррекции ошибок. Этого достаточно, чтобы строго доказать совершенно уникальное свойство сходимости решений МПД к решению оптимального (переборного!) декодера. Ни один другой алгоритм коррекции ошибок не обладает таким чрезвычайно полезным свойством, которое становится особенно важным в итеративных схемах декодирования, к которым и относится МПД. Более того, сложность МПД – линейная от длины кода n, причём, с очень небольшим коэффициентом пропорциональности при n.

Нелишне также напомнить, что в МПД должны применяться только специальные коды с очень низким уровнем размножения ошибок. Этот эффект был всесторонне теоретически рассмотрен в ряде публикаций по МПД, а также в настоящей книге и в материалах, представленных на веб-сайте ИКИ РАН по методам кодирования **www.mtdbest.iki.rssi.ru**.

Вопрос 11. Можно ли создать МПД для недвоичных каналов?

Ответ. Вся теория МПД для недвоичных кодов и каналов была написана и опубликована более 20 лет назад. Построены оценки характеристик и найдены соответствующие коды, позволяющие достичь высокой эффективности декодирования. Недвоичные МПД (далее QМПД) столь же легки в реализации, как и обычные пороговые декодеры. Они представлены и в данной книге.

Оценки результатов моделирования QMПД свидетельствуют, что эти декодеры также очень просты алгоритмически и имеют характеристики, которые существенно лучше, чем у единственно используемых до сих пор кодов Рида-Соломона.

Это неудивительно, так как решения QMПД также строго сходятся к решению недвоичного оптимального (разумеется, переборного!) декодера, а используемые в QMПД коды в отличие от кодов Рида-Соломона могут быть достаточно большой длины, что существенно увеличивает эффективность многопорогового алгоритма и одновременно упрощает его.

Учитывая, что ОД для недвоичных кодов создать практически невозможно, QMПД – абсолютный монополист среди недвоичных кодов, потому что он гораздо проще декодеров для кодов Рида-Соломона и несравненно более эффективен из-за простого применения длинных кодов.

Вопрос 12. Если в рассматриваемом проекте для относительно низкоскоростных каналов не требуется большая скорость декодирования, то следует ли и в этом случае реализовать именно метод МПД? Может быть, следует применять другие алгоритмы?

Ответ. Алгоритмы МПД на 2 десятичных порядка проще других при сопоставимой эффективности методов. При невысоких скоростях можно увеличить количество итераций и применить более сложные пороговые функции. Тогда вычислительные ресурсы МПД будут использованы полностью и наиболее эффективно.

Вопрос 13. Если в нашем конкретном случае необходимо реализовать систему кодирования с малой задержкой принятия решения, то какой может быть процедура выбор правильного метода декодирования?

Ответ. Маленькая задержка требуется в низкоскоростных каналах, когда даже несколько лишних миллисекунд принятия решения являются критическими для всего проекта в целом. Если задержка очень мала, то сначала её следует сопоставить (снова!) с границами сферической упаковки и посмотреть, чтобы эти характеристики были теоретически возможны.

Первое впечатление при этом состоит в том, что эта ситуация сразу соответствует необходимости применения алгоритма Витерби (АВ). Однако следует помнить, что АВ – переборный алгоритм. Как известно, в 70-х годах прошлого века разработчики очень быстро сумели достичь такого уровня, что стандартом для систем связи стал АВ с длиной кодирующего регистра $K = 7$. Через 30 лет существования АВ при чрезвычайно быстром прогрессе элементной базы только недавно автору пришлось проконсультировать работы по созданию АВ для кода с $K = 11$. Причём, как известно, характеристики АВ с $K = 11$ не намного лучше, чем при $K = 7$. А вот усложнение такого АВ – весьма немалое. Причина снова та же – экспоненциальный рост его сложности! Так что быстрого прогресса от АВ ожидать не стоит.

Но хорошо известно, что МПД может обеспечить характеристики эффективности, которым соответствуют только лучшие коды с $K \sim 15$. А поскольку АВ с разумной производительностью для $K = 15$ пока создать нельзя, то получается, что МПД перехватывает у АВ инициативу и при малых задержках решения. Правда, при этом увеличивается число необходимых итераций декодирования. Но при постановке задачи в данном вопросе производительность не является критическим параметром. Да и каждая итерация в МПД требует всего нескольких операций.

Подчеркнём ещё раз, никакие другие методы декодирования не позволяют столь же легко манипулировать практически всеми параметрами алгоритмов, как это возможно в случае МПД. Это позволяет многопороговым декодерам выигрывать практически все реальные конкурсы на объективно организованных чемпионатах алгоритмов.

Вопрос 14. Можно ли достичь на практике тех реальных преимуществ МПД перед другими методами по эффективности и быстродействию на несколько десятичных порядков, которые формально следуют из оценок для аппаратной реализации?

Ответ. Да. Несомненным является безусловная правильность предложенного нами подхода к оценкам аппаратной эффективности декодирования. Он состоит просто в том, что по сравнению со всеми другими методами МПД состоит как бы

только из регистров сдвига, которые относятся к наиболее быстрым элементам любых БИС. Кроме того, таких параллельно работающих регистров в МПД много: от 4 до 20 и более. А поскольку обычно скорости регистров сдвига на ПЛИС – это десятки Мбит/с, то МПД декодеры действительно являются устройствами, которые легко обрабатывают потоки на скоростях в сотни Мбит/с.

Так что всё написанное ранее про возможности МПД исходило из самых реальных оценок и обстоятельств проектирования аппаратуры кодирования.

Вопрос 15. Сколько итераций декодирования требуется МПД для достижения решения, близкого к оптимальному?

Ответ. Число итераций, требуемое для полной реализации корректирующих способностей кода, зависит от близости отношения сигнал/шум, при котором происходит работа многопорогового декодера, к пропускной способности канала. В результате оказывается, что чем ближе к пропускной способности канала приходится работать, тем большее число итераций декодирования требуется выполнить. Например, если при работе примерно в 1÷1,5 дБ от пропускной способности канала необходимо выполнить порядка 20÷40 итераций декодирования, то при отношении сигнал/шум в канале, большем пропускной способности на 3÷4 дБ, может потребоваться всего 5 итераций.

Вопрос 16. Какова задержка декодирования МПД?

Ответ. Задержка декодирования зависит от вида используемого кода. В случае применения блокового кода задержка будет совпадать с длиной кодового блока. При этом за время приема кодового блока предыдущий кодовый блок успевает декодироваться. Если же используется свёрточный код, то задержка определяется как произведение длины кода на число итераций декодирования. Но и здесь много вариантов дополнительной адаптации параметров.

Вопрос 17. Возможно ли применение МПД в каскадных схемах кодирования, например, с декодером Витерби?

Ответ. Замечательной особенностью МПД является то, что при правильно выбранных кодах (с минимальным размножением ошибок) ошибки декодирования оказываются одиночными.

Это позволяет использовать МПД в простых каскадных схемах кодирования. Например, использование совместно с МПД во внешнем каскаде кодов с контролем четности или кодов Хэмминга позволяет практически без усложнения схем кодирования и декодирования на несколько порядков уменьшить вероятность ошибки декодирования по сравнению с базовым МПД.

Результаты исследований таких каскадных схем отражены в публикациях, представленных на веб-сайте ИКИ РАН по методам кодирования **www.mtdbest.iki.rssi.ru**, а также в этой книге.

Вопрос 18. Почему приходится всё время слышать о невероятной эффективности применения кодирования? Можно привести такие примеры?

Ответ. Да, именно очень высокая ценность кодирования стимулирует широкие исследования в этой области. Экономическая эффективность применения кодирования совершенно грандиозна. Поскольку при этом в каналах связи можно применять гораздо менее мощные передатчики, то получается, что при использовании кодов значительно уменьшаются размеры всей аппаратуры связи, или, если необходимо, многократно повышаются скорость или дальность передачи, а также во много раз уменьшаются размеры чрезвычайно дорогих и во многих случаях просто огромных антенн. При этом аппаратура связи приобретает ещё очень много и других полезных свойств, которые совершенно нереальны в аналоговых системах.

Всё это означает, что кодирование просто более полно использует пропускную способность каналов систем и сетей связи. В самом деле, достоверная цифровая связь без кодирования использует всего несколько процентов ёмкости каналов связи, тогда как кодирование приводит к тому, что пропускная способность каналов используется уже на 30%, 50% и более процентов. Пусть некоторая сеть спутниковой связи использует малоэффективны методы кодирования, которые используют канал на ~20%, а стоит, к примеру, 5 млрд. долл. Допустим далее, что на разработку нового метода кодирования потрачено около 0,1% от стоимости такой сети, что привело к увеличению к.п.д. до 80%. Но это обеспечивает рост реальной пропускной способности сети в 4 раза и, значит эквивалентно запуску на орбиту ещё трёх

таких сетей общей стоимостью 15 млрд. долл.!!! Но реально были потрачены только средства на разработку системы кодирования в объёме всего лишь 5 млн. долл., В этом и состоит экономическая ценность кодирования: применив относительно недорогие (относительно стоимости сети в целом) методы кодирования, получаем огромный выигрыш по стоимости сетей (в нашем примере – 15 млрд. долл.) и по их пропускной способности. И эти цифры вовсе не являются предельными.

Вопрос 19. Зачем вводить новый термин «к.п.д.» для эффективности использования каналов, если уже есть такие критерии, как отношение сигнал/шум и энергетический выигрыш кодирования (ЭВК)?

Ответ. Он тоже удобен и, несомненно, полезен.

Попробуем сначала обсудить полезность критерия «сигнал/шум». Более точно, сначала рассмотрим отношение $a = E_b/N_0$, т.е. отношение битовой энергии сигнала к спектральной плотности мощности шума. Чем он меньше, тем, естественно, код и алгоритм декодирования лучше. Но при этом надо учитывать кодовую скорость и знать предельно возможное значение для a, определяемое условием равенства выбранной кодовой скорости R и пропускной способности канала C. Только в этом случае будет достаточно ясно, на сколько ещё можно, в принципе, улучшать характеристики декодера.

Обратимся к ЭВК. Этот критерий – разностный. Берём требуемую достоверность приёма данных и смотрим соответствующее ему отношение a. А потом смотрим эту же величину $a = E_b/N_0$ для конкретного алгоритма декодирования. Их разность есть ЭВК. И опять для понимания того, как далёк энергетический выигрыш данного алгоритма от предельно возможного уровня ЭВК, нужно знать для конкретной кодовой скорости R её предельный ЭВК, определяемый условием $R = C$. Эти графики представлены в нашей статье о новом МПД на ПЛИС Xilinx в журнале «Электросвязь» №2 за 2005 год и в данной книге.

Таким образом, рассматриваемые критерии полезны, но предполагают знание некоторых дополнительных, предельно возможных своих значений.

А понятие к.п.д. непосредственно связано с предельными значениями $a = E_b/N_0$, которые соответствуют равенству $R = C$. Берём отношение a для этого равенства и определяем рабочее значение a для обсуждаемого алгоритма. Их разность и есть мера эффективности использования канала в децибелах. А если преобразовать эту разность к процентам, то это и будет искомый к.п.д.

Например, пусть равенству $R = C$ соответствует конкретное значение a_0, а анализируемый алгоритм декодирования при этой же кодовой скорости R работает при уровне a, на 3 дБ более высоком, чем a_0. Вот эти 3 дБ и есть та величина, которая непосредственно указывает на отличие возможностей выбранного декодера от предельно возможных теоретических значений a_0. Но 3 дБ – это 2 раза. Во столько раз энергетика передачи для этого декодера больше, чем это возможно по теории. Но это и означает, что к.п.д. использования канала данным декодером по энергетике составляет 50%. Если найдётся декодер, который будет работать с превышением энергетики от предельной только на 0,5 дБ, то легко найти, что его к.п.д. равен 89%. Удобно? Конечно! И совсем не нужно отказываться от первых двух критериев. Но понимать смысл к.п.д. для цифрового канала тоже полезно.

* * * * * * * *

Ряд дополнительных вопросов по кодированию и ответы на них можно найти также на сайте ИКИ РАН по МПД алгоритмам **www.mtdbest.iki.rssi.ru**.

СПИСОК ЛИТЕРАТУРЫ

1. Золотарёв В.В., Овечкин Г.В. Помехоустойчивое кодирование. Методы и алгоритмы. Справочник. М.: Горячая линия – Телеком, 2004. 126 с.
2. Финк Л.М. Теория передачи дискретных сообщений. М.: Советское радио, 1970.
3. Бородин Л.Ф. Введение в теорию помехоустойчивого кодирования. М.: Советское радио, 1968.
4. Месси Дж. Пороговое декодирование. М.: Мир, 1966.
5. Колесник В.Д., Мирончиков Е.Т. Декодирование циклических кодов. М.: Связь, 1968.
6. Касами Т., Токура Н., Ивадари Е., Ипагаки Я. Теория кодирования. М.: Мир, 1978.
7. Галлагер Р. Теория информации и надежная связь. М.: Советское радио, 1974.
8. Блейхут Р. Теория и практика кодов, контролирующих ошибки. М.: Мир, 1986.
9. Самойленко С.И., Давыдов А.А., Золотарёв В.В., Третьякова Е.Л. Вычислительные сети. М.: Наука, 1981, 278 с.
10. Золотарёв В.В. Устройство для декодирования линейных сверточных кодов // Авторское свидетельство СССР №492872.
11. Золотарёв В.В. Многопороговое декодирование в недвоичных каналах // Вопросы радиоэлектроники, серия ЭВТ. 1984. Вып.12.
12. Цифровое телевидение. Под редакцией Кривошеева М.И. М.: Связь, 1980.
13. Зюко А.Г. Фалько А.И., Панфилов И.П., Банкет В.Л., Иващенко П.В. Помехоустойчивость и эффективность систем передачи информации. М.: Радио и связь, 1985.
14. Towsend R.L., Weldon E.J. Self-Orthogonal Quasi-Cyclic Codes // IEEE Trans. On Inform. Theory. 1967. Vol.IT-13. №2.
15. Зяблов В.В. Кусочно-циклические коды и схемы их декодирования по большинству // Проблемы передачи информации. 1968. Т.IV. Вып.1.
16. Forney G.D. Convolutional codes. II. Maximum-likelyhood decoding // Information and control. 1974. Vol.25. №3.

17. Нейфах А.Э. Сверточные коды для передачи дискретной информации. М.: Наука, 1979.

18. Solomon G., van Tilborg C.A. A connection between block and convolutional codes // SIAM journal of applied mathematics. 1979. Vol.37. №2.

19. Робинсон Дж.П. Размножение ошибок и прямое декодирование сверточных кодов // В сб.: Некоторые вопросы теории кодирования. М.: Мир, 1970.

20. Robinson J.P., Bernstein A.J. A class of binary recurrent codes with limited error propagation // IEEE Trans. On inform. Theory. 1967. Vol.IT-13. №1.

21. Tong S.Y. Systematic construction of self-orthogonal diffuse codes // IEEE Trans. On Inform. Theory. 1970. Vol.IT-16. №5.

22. Wu W.W. New convolutional codes. Parts I. 1975. Vol.COM-23. №9.

23. Wu W.W. New convolutional codes. Parts II, III. 1976. Vol.COM-24. №1, №2.

24. Klieber E.R. Some difference triangles for constructing self-orthogonal codes // IEEE Trans. On Comm. Technology. Part II. 1971. Vol.COM-19. №5.

25. Heller J.A., Jacobs J.M. Viterbi decoding for satellite and space communication // IEEE trans. on comm. techno1ogy. Part IIю 1971. Vol.COM-19. №5.

26. Кларк Дж., Кейн Дж. Кодирование с исправлением ошибок в системах цифровой связи. М.: Радио и связь, 1987.

27. Котельников В.Л. Теория потенциальной помехоустойчивости. М-Л.: Госэнергоиздат, 1956.

28. Шеннон К.Э. Математическая теория связи // В сб.: Работы по теории информации и кибернетике. М.: Иностранная литература, 1963.

29. Bose R.C., Ray-Chaudhuri D.K. On a class of error correcting binary group codes // Information and control. 1960. №3.

30. Hocquenghem A. Codes correcteures derreurs // Cheffres. 1959. Vol.2.

31. Витерби А.Дж. Границы ошибок для сверточных кодов и асимптотически оптимальный алгоритм декодирования // В сб.: Некоторые вопросы теории кодирования. М.: Мир, 1970.

32. Форни Д. Каскадные коды. М.: Мир, 1970.

33. Хацкелевич Я.Д., Готлиб В.М. Эффективность каскадного кода при декодировании с метками надежности // Труды НИИР. 1981. №1.

34. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. М.: Мир, 1976.

35. Berrou C., Glavieux A., Thitimajshima P. Near Shannon Limit Error-Correcting Coding and Decoding: Turbo Codes // in Proc. of the Intern. Conf. on Commun. (Geneva, Switzerland). 1993. May. P.1064–1070.

36. Немировский Э.Э., Портной С.Л. Методы расчета и оптимизации параметров декодеров на основе каскадных кодов // Электронная техника. Серия 10. Микроэлектронные устройства. М., 1982. Вып.1 (31).

37. Massey J.L. Catastrophic error propagation in convolutional codes // Proc. 11th midwest circuit theory symp. University Notre Dame. Ind.. May. 1968.

38. Massey J.L., Sain M.K. Inverses of linear sequential circuits // IEEE trans. on computers. 1968. Vol.C-17. №4.

39. Sullivan D.D. Control of error propagation in convolutional codes // Technical report №EE-667. University of Notre Dame. Indiana. 1966.

40. Elahi-Teleghani A., Costello D.J. Quick-look in codes // Proc. National Electronics Conf. Chicago. 1974.

41. Штарьков Ю.М. Методы кодирования источников дискретного времени с заданным критерием качества // В сб. Информационный обмен в вычислительных сетях. М.: Наука, 1980.

42. Штарьков Ю.М. Проблема сокращения избыточности дискретных данных в теории информации // В сб.: Кодирование в сложных системах. М.: Наука, 1974.

43. Бояринов И.М. Об одной конструкции линейных кодов с неравной защитой информационных символов // Проблемы передачи информации. 1960. №2.

44. Блох Э.Л., Зяблов В.В. Линейные каскадные коды. М.: Наука 1982.

45. Брауде-Золотарёв Ю.М., Золотарёв В.В. Пороговое декодирование в каналах с неравномерной энергетикой // В сб.:

«VII Конференция по теории кодирования и передачи информации». Доклады, Ч.II, Теория помехоустойчивого кодирования. М.: Вильнюс, 1978.

46. Золотарёв В.В. Мягкие многопороговые декодеры // В сб.: «Труды V Всесоюзной школы-семинара по вычислительным сетям». Тезисы докладов. Ч.4. М.: Владивосток, 1980.

47. Золотарёв В.В. Об оптимизации мягких многопороговых декодеров // В сб.: «VIII Всесоюзная конференция по теории кодирования и передачи информации». Ч.II. М.: Куйбышев, 1981.

48. Cain J.B., Clark G.G. Some results on error propagation of convolutional feedback // IEEE trans. on inform. theory. 1972. Vol.IT-18. №5.

49. Bahl L., Jelinek P. On the Structure of Rate 1/n Convolutional Codes // IEEE Trans. Inform. Theory. 1972. Vol.IT-18. №1. P.192–196.

50. Massey J.L., Bin R.W. Application of Lyapunov's Direct Method to the Error-Propagation Effect in Convolutional Codes // IEEE Trans. Inform. Theory. 1964. Vol.IT-10. №4. P.248–250.

51. Massey J.L., Sain M.K. Inverses of Linear Sequential Circuits // Trans. Computers. 1968. Vol.C-17. №4. P.330–337.

52. Габидулин Э.М., Ларин А.Д. Размножение ошибок при декодировании равномерных сверточных кодов // Проблемы передачи информации. 1969. Т.V, Вып.3. С.73–77.

53. Ларин А.Д. О максимальной длине размножения ошибок при пороговом декодировании равномерных сверточных кодов // Известия ВУЗов, Радиоэлектроника. 1972. Т.XV. №4. С.507–510.

54. Reddy S.U. Linear Convolutional Codes for Compound Channels // Informationand Control. 1971. Vol.19. №5. P.387–400.

55. Wyner A.D., Ash R.B. Analysis of Recurrent Codes // IEEE Trans. Inform. Theory. 1963. Vol.IT-9. №3. P.143–156.

56. Феллер В. Введение в теорию вероятностей и ее приложения. М.: Мир, 1964.

57. Золотарёв В.В. Эффективные многопороговые алгоритмы декодирования // Научный совет по комплексной проблеме «Кибернетика» АН СССР. Препринт. М., 1981. 76 с.

58. Klieber B.R. Some Difference Triangles for Constructing Self-0rtogonal Codes // IEEE Trans. Inform. Theory. 1970. Vol.IT-16. №2. P.237–238.

59. Брауде-Золотарёв Ю.М., Золотарёв В.В. Оптимизированные пороговые декодеры сверточных кодов // В сб.: «Труды IV Всесоюзной школы-семинара по вычислительным сетям», М., 1979.

60. Золотарёв В.В. Верхняя оценка вероятности ошибки декодирования равномерных кодов // V Конференция по теории кодирования и передачи информации. Москва-Горький, 1972. С.70–73.

61. Берлекэмп Э. Алгебраическая теория кодирования. М.: Мир, 1971.

62. Банкет В.Л., Золотарёв В.В. Эффективность многопозиционных систем модуляции и многопорогового декодирования // В сб.: ЕС Всесоюзная школа-семинар по вычислительным сетям». М.-Пушкино, 1984. Ч.3.2.

63. Денисова М.А., Овечкин Г.В., Овечкин П.В. Применение многопорогового декодера в системах передачи данных с многопозиционными системами модуляции // Мат. 13-й Межд. науч.-техн. конф. Рязань: РГРТА, 2004. С.58–59.

64. Золотарёв В.В. Недвоичные многопороговые декодеры // Цифровая обработка сигналов. 2003. №3. С.10–12.

65. Золотарёв В.В. Использование многопорогового декодера вместо алгоритма Витерби // Вестник РГРТА, 2002. Вып.10. С.117–119.

66. Зигангиров К.Ш. Процедуры последовательного кодирования, М.: Связь, 1974.

67. Зиновьев В.А., Зяблов В.В. Декодирование обобщенных каскадных кодов // IV Международный симпозиум по теории информации. Тезисы докладов. М.-Л., 1976. Ч.II.

68. Файзулаев Б.Н. Теория матричных БИС и СБИС ЭВМ // В сб.: ЭВТ. Радио и связь. М., 1987.

69. Самойленко С.И., Золотарёв В.В. Итеративное декодирование сверточных и биноидных кодов // В сб.: «Труды IV Всесоюзной школы-семинара по вычислительным сетям». М., 1979.

70. Золотарёв В.В. Многопороговое декодирование в каскадных схемах // В сб.: «VIII Симпозиум по проблеме избыточности в информационных системах». Л., 1983. Ч.2.

71. MacKay D.J.C., Neal R.M. Near Shannon limit performance of low density parity check codes // IEEE Electronics Letters. Aug. 1996. Vol.32. №18. P.1645–1646.

72. Richardson T., Shokrollahi M., Urbanke R. Design of capacity-approaching irregular low-density parity-check codes // IEEE Trans. Inform. Theory. Feb. 2001. Vol.47. P.638–656.

73. Press Release, AHA announces Turbo Product Code Forward Error Correction Technology. 1998. Nov.2.

74. Jin H., Khandekar A., McEliece R. Irregular repeat-accumulate codes // Proc. 2nd Int. Symp. on Turbo Codes and Related Topics (Brest, France). 2000. Sept. P.1–8.

75. Li J., Narayanan K.R., Georghiades C.N. Product accumulate codes: A class of capacity-approaching, low-complexity codes // submitted to IEEE Trans. Inform. Theory. 2001.

76. Золотарёв В.В. Алгоритмы многопорогового декодирования линейных кодов // Мобильные системы. М., 2005. №12. С.56–62.

77. Золотарёв В.В. Верхние оценки эффективности мажоритарных алгоритмов // Вопросы радиоэлектроники. Серия ЭВТ. 1986. Вып.12.

78. Залманов А.Л., Золотарёв В.В. Мажоритарные декодеры недвоичных блоковых кодов // В сб.: XII Всесоюзный семинар по вычислительным сетям. Тезисы докладов. М.-Одесса, 1987. Т.3.

79. Вентцель Е.С. Теория вероятностей. М.: Физматгиз, 1962.

80. Zierler N., Brillhart J. On primitive trinomials (mod. 2) // Information and control. 1968. Vol.14. №6.

81. Голенко Д.И. Моделирование и статистический анализ псевдослучайных чисел на ЭВМ. М.: Наука, 1965.

82. Полляк Ю.Г. Вероятностное моделирование на ЭВМ. М.: Сов. радио, 1971.

83. Кнут Д. Искусство программирования для ЭВМ. М.: Мир, 1977. Т.2.

84. Форсайт Д., Малькольм М., Моулер К. Машинные методы математических вычислений. М.: Мир, 1980.

85. Песошин В.А. Устройства вычислительной техники для генерирования случайных и псевдослучайных последовательностей и чисел. Докторская диссертация. 1986.

86. Веб-сайт ИКИ РАН **www.mtdbest.iki.rssi.ru**.

87. Золотарёв В.В., Овечкин Г.В. Многопороговые декодеры для каналов с предельно высоким уровнем шума // Телекоммуникации. М., 2005. №9. С.29–34.

88. Зубарев Ю.Б., Золотарёв В.В., Овечкин Г.В., Строков В.В., Жуков С.Е. Многопороговые декодеры для высокоскоростных спутниковых каналов связи: новые перспективы // Электросвязь. М., 2005. №2. С.10–12.

89. Золотарёв В.В., Овечкин Г.В. Эффективные алгоритмы помехоустойчивого кодирования для цифровых систем связи // Электросвязь, 2003. №9. С. 34-37.

90. Золотарёв В.В., Овечкин Г.В. Использование многопорогового декодера в каскадных схемах // Вестник РГРТА, 2003. Вып.11. С.112-115.

91. Золотарёв В.В. Использование помехоустойчивого кодирования в технике связи //Электросвязь. 1990. №7. С.7–10.

92. Зяблов В.В. Теория обобщенного каскадного кодирования и проблема сложности в помехоустойчивом кодировании. Докторская диссертация. М., 1978.

93. Золотарёв В.В., Минина Н.Г. Устройство для декодирования линейных свёрточных кодов // Авторское свидетельство СССР №1291984.

94. Банкет В.Л., Портной С.Л., Салабай А.В. Помехоустойчивое кодирование в канале с многопозиционной ФМ // Труды НИИР. 1985. №1.

95. Ma H.H., Wolf J.K. Binary unequal-protection block codes formed from convolutional codes by generalized tail-biting // IEEE trans. on inform. theory. Vol.IT-32. №06.

96. Золотарёв В.В. Параллельное кодирование в каналах СПД // В сб.: «Вопросы кибернетики». ВК-120. М., 1986.

97. Блох Э.Л., Зяблов В.В. Обобщенные каскадные коды. М.: Связь, 1976.

98. Золотарёв В.В. Размножение ошибок при пороговом декодировании самоортогональных сверточных кодов // В сб.: Труды МФТИ, серия «Радиотехника и электроника». 1976.

99. Золотарёв В.В., Овечкин Г.В. Сложность реализации эффективных методов декодирования помехоустойчивых кодов // Проблемы передачи и обработки информации в сетях и системах телекоммуникаций: Мат. 12-й Межд. науч.-техн. конф. Рязань: РГРТА, 2003.

100. Золотарёв В.В., Овечкин Г.В. Сложность реализации эффективных методов декодирования помехоустойчивых кодов // 6-я межд. конф. и выст. «Цифровая обработка сигналов и ее применение». М., 2004. Т.1. С.220–221.

101. Золотарёв В.В. Недвоичные многопороговые декодеры эффективнее кодов Рида-Соломона // Проблемы передачи и обработки информации в сетях и системах телекоммуникаций: Мат. 12-й Межд. науч.-техн. конф. Рязань: РГРТА, 2004. С.9–11.

102. Золотарёв В.В., Овечкин Г.В. Аппаратная реализация многопороговых декодеров // 7-я межд. конф. и выст. «Цифровая обработка сигналов и ее применение». М., 2005. Т.2. С.451–454.

103. Золотарёв В.В. Субоптимальные алгоритмы многопорогового декодирования. Докторская диссертация. М., 1990.

Дополнительный список литературы по методам многопорогового декодирования

1. Zolotarev V.V. The Multithreshold Decoder Performance in Gaussian Channels // 7–th International Symposium on Communication Theory and Applications (7–th ISTA'03). St. Martin's college. Ambleside. UK. 13–18 July 2003. P.18–22.

2. Бабкин В.Ф., Золотарёв В.В. Многопороговое декодирование вблизи границы Шеннона и возможности его микроминиатюрной реализации // Сборник докладов выездного семинара ИКИ «Вопросы миниатюризации в современном космическом приборостроении». М., 2005. С.282–304.

3. Бабкин В.Ф., Золотарёв В.В. Современные методы помехоустойчивого кодирования для систем дистанционного зондирования Земли // Сборник научных статей «Современные

проблемы дистанционного зондирования Земли из космоса». М., ИКИ РАН, 2005. Т.I. С.199–202.

4. Банкет В.Л., Золотарёв В.В. Эффективность свёрточного кодирования с многопороговыми декодерами в каналах с АФМ // В сб.: «Республиканская научно–техническая конференция. Проблемы создания и внедрения автоматизированной системы технической эксплуатации первичной магистральной и вторичных сетей связи страны». Тезисы докладов. Киев, 1983. С.42–43.

5. Брауде–Золотарёв Ю.М., Золотарёв В.В. Пороговый декодер свёрточного кода // Авторское свидетельство СССР №708934.

6. Брауде–Золотарёв Ю.М., Золотарёв В.В. Пороговый кодек свёрточного кода // Авторское свидетельство СССР №777814.

7. Брауде–Золотарёв Ю.М., Золотарёв В.В. О методах согласования систем модуляции и кодирования // В сб.: «IX Симпозиум по проблеме избыточности в информационных системах». Тезисы докладов. 1986. Ч.1. С.45–47.

8. Брауде–Золотарёв Ю.М., Золотарёв В.В. Оптимизация порогового декодирования // Труды НИИР. М., 1979. №1. С.25–31.

9. Брауде–Золотарёв Ю.М., Золотарёв В.В. Оптимизированный пороговый алгоритм декодирования и сжатие источника // Труды НИИР. М., 1979. №2. С.45–48.

10. Брауде–Золотарёв Ю.М., Золотарёв В.В. Характеристики аппаратуры кодирования на матричных БИС // Труды НИИР. М., 1986. №2. С.35–38.

11. Брауде–Золотарёв Ю.М., Золотарёв В.В., Шанина Н.И. Перспективные методы помехоустойчивого кодирования // Труды НИИР. М., 1980. №1. С.38–42.

12. Брауде–Золотарёв Ю.М., Золотарёв В.В., Красносельский И.Н., Шанина Н.И. Пороговый алгоритм и оптимальные приемники малоизбыточных сигналов // Труды НИИР. М., 1979. №4. С.21–25.

13. Брауде–Золотарёв Ю.М., Золотарёв В.В., Лернер А.А., Трофимов Ю.К. Повышение эффективности связи широкопо-

лосными сигналами путем оптимизированного порогового декодирования // Труды НИИР. М., 1983. №1. С.28–31.

14. Брауде–Золотарёв Ю.М., Золотарёв В.В., Хацкелевич Я.Д. Перспективные пути развития помехоустойчивого кодирования // В сб.: «Вопросы кибернетики», ВК–65, АН СССР, Научный совет по комплексной проблеме «Кибернетика». М., 1980. С.45–51.

15. Брауде–Золотарёв Ю.М., Путрин В.С., Золотарёв В.В. Формирователь сигнала коррекции порогового декодера свёрточного кода // Авторское свидетельство СССР №646451.

16. Гаврилов А.Н., Золотарёв В.В., Овечкин Г.В., Пылькин А.Н. Устройство для декодирования линейных кодов // Патент на изобретение РФ №2212766.

17. Гринченко Н.Н., Овечкин Г.В. Перспективные методы коррекции ошибок для высокоскоростных спутниковых систем связи // Мат. 14-й Межд. науч.-техн. конф. «Проблемы передачи и обработки информации в сетях и системах телекоммуникаций». Рязань: РГРТА, 2005. С.48–49.

18. Гринченко Н.Н., Овечкин Г.В., Овечкин П.В. Развитие многопороговых алгоритмов декодирования помехоустойчивых кодов // Мат. науч.-практ. конф. «Научные исследования и их практическое применение. Современное состояние и пути развития». Одесса: Черноморье, 2005. Т.7. С.13–14.

19. Гринченко Н.Н., Овечкин Г.В., Овечкин П.В. Разработка каскадных схем коррекции ошибок на основе многопороговых декодеров // 8-я межд. конф. и выст. «Цифровая обработка сигналов и ее применение». М., 2006.

20. Дмитриева Т.А., Золотарев В.В. Разработка алгоритма декодирования на основе многопорогового декодера // Мат. 14-й Межд. науч.-техн. конф. «Проблемы передачи и обработки информации в сетях и системах телекоммуникаций». Рязань: РГРТА, 2005. С.50–52.

21. Епишина Т.А. Разработка компьютерной учебной среды, моделирующей системы помехоустойчивого кодирования // Современные информационные технологии в образовании: Мат. 5-й Межрегиональной науч.-практ. конф. Рязань, 2004.

22. Епишина Т.А., Овечкин Г.В., Овечкин П.В. Имитатор цифрового спутникового канала // Новые информационные технологии в учебном процессе и производстве: Мат. межвуз. науч.-техн. конф. студентов, молодых ученых и специалистов. Рязань: РИМГОУ, 2004. С.77–79.

23. Золотарёв В.В. Каскадное декодирование в стирающих каналах // Вопросы радиоэлектроники. Серия ЭВТ. 1985. Вып.9. С.109–113.

24. Золотарёв В.В. Недвоичные мажоритарные алгоритмы декодирования // В сб.: «Республиканская научно–техническая конф. «Помехоустойчивость и эффективность систем передачи информации». Тезисы докладов. Одесса, 1986. С.56–58.

25. Золотарёв В.В. Алгоритмы коррекции символьных данных в вычислительных сетях // В сб.: «Вопросы кибернетики», ВК–105, АН СССР, Научный совет по комплексной проблеме «Кибернетика». М., 1985. С.54–62.

26. Золотарёв В.В. Асимптотические свойства мажоритарных алгоритмов // В сб.: «IX Всесоюзная школа–семинар по вычислительным сетям». Тезисы докладов. М.–Пущино, 1984. Ч.3.1. С.42–44.

27. Золотарёв В.В. Высокоскоростное устройство многопорогового декодирования линейных кодов // Патент на полезную модель РФ №44216.

28. Золотарёв В.В. Использование принципа каскадного кодирования в технике связи // В сб.: «Вопросы кибернетики», ВК–77, АН СССР, Научный совет по комплексной проблеме «Кибернетика». М., 1982. С.45–52.

29. Золотарёв В.В. Использование устойчивости пороговых декодеров для уменьшения вероятности ошибки декодирования // В сб.: «IV Международный симпозиум по теории информации». Доклады. М.– Л., 1976. Ч.II. С.45–47.

30. Золотарёв В.В. Исследование способов эффективного кодирования каналов и источников на основе оптимизированных многопороговых декодеров. Отчет Научного совета по комплексной проблеме «Кибернетика» АН СССР. 1977. 62 с.

31. Золотарёв В.В. Каскадные мажоритарные схемы для гауссовских каналов // В сб.: «XI Всесоюзный семинар по вы-

числительным сетям». Тезисы докладов. М.–Рига, 1986. Т.2. С.58–60.

32. Золотарёв В.В. Коды и кодирование // Радиоэлектроника и связь, М.: Знание, 1990. №9. 64 с.

33. Золотарёв В.В. Мажоритарные методы дл кодирования каналов и источников // «Вопросы радиоэлектроники», Серия «Электронная вычислительная техника». 1991. Вып.8. С.65–70.

34. Золотарёв В.В. Многопороговое декодирование в стирающих каналах // Вопросы радиоэлектроники. Серия ЭВТ. 1983. Вып.10. С.67–70.

35. Золотарёв В.В. Многопороговое декодирование для каналов с дефицитом энергетики // В сб.: «Межд. науч.–техн. конф. «Проблемы передачи и обработки информации в сетях и системах телекоммуникаций». Тезисы докладов. Рязань, 2004. С.7–9.

36. Золотарёв В.В. Многопороговое декодирование // Проблемы передачи информации. М., 1986. Т.XXII. Вып.1. С.104–109.

37. Золотарёв В.В. Многопороговые декодеры могут быстрыми и эффективными // 6–я Межд. конф. и выставка «Цифровая обработка сигналов и её применение». М., 2004. Доклады 1. С.96–98.

38. Золотарёв В.В. О выборе направлений развития кодирования // В сб.: «Республиканская научно–техническая конференция «Помехоустойчивость и эффективность систем передачи информации». Тезисы докладов. Одесса, 1986.

39. Золотарёв В.В. О задержке принятия решения при использовании помехоустойчивых кодов // «Вопросы радиоэлектроники», Серия «Электронная вычислительная техника». 1992. Вып.8. С.70–74.

40. Золотарёв В.В. О методах улучшения порогового декодирования свёрточных кодов // В сб.: «VI Конференция по теории кодирования и передачи информации». Тезисы докладов. Томск, 1975. Ч.II. С.60–63.

41. Золотарёв В.В. О полной реализации помехоустойчивости свёрточных кодов // Труды семинара «Помехоустойчивое кодирование в сложных системах», АН СССР, Научный совет

по комплексной проблеме «Кибернетика». Деп. №2838–74 от 12.02.74. 36 с.

42. Золотарёв В.В. О субоптимальном декодировании свёрточных кодов // В сб.: «VI Симпозиум по проблеме избыточности в информационных системах». Тезисы докладов. Ленинград, 1974. Ч.I. С.34–36.

43. Золотарёв В.В. О технологически доступных алгоритмах для исправления ошибок вблизи теоретических границ. – «Вопросы радиоэлектроники», Серия «Электронная вычислительная техника». 1991. Вып.8. С.71–75.

44. Золотарёв В.В. Обзор перспективных методов помехоустойчивого кодирования // В сб.: «Методы исследования эффективности и перспективные средства передачи и обработки информации». Рязань, 1985. С.39–43.

45. Золотарёв В.В. Повышение эффективности пороговых декодеров при помехоустойчивом кодировании в вычислительных сетях // В сб.: «Вопросы кибернетики», ВК–28, АН СССР, Научный совет по комплексной проблеме «Кибернетика». М., 1977. С.88–91.

46. Золотарёв В.В. Предельные возможности кодов и характеристики перспективных декодеров // «Вопросы радиоэлектроники», Серия «Электронная вычислительная техника». 1992. Вып.8. С.75–78

47. Золотарёв В.В. Простые методы исправления ошибок в каналах с большим уровнем шума // «Радиотехника». М., 1991. №10. С.79–82.

48. Золотарёв В.В. Развитие техники кодирования для каналов с большим уровнем помех // «Вопросы радиоэлектроники», Серия «Электронная вычислительная техника». 1993. Вып.4. С.160–165.

49. Золотарёв В.В. Реальный энергетический выигрыш кодирования для спутниковых каналов // В сб.: 4–я Международная конференция «Спутниковая связь–2000». М., 2000. Т.2. С.20–25.

50. Золотарёв В.В. Сложность эффективных методов каскадного кодирования в каналах с большим шумом // В сб.: «Республиканская научно–техническая конференция. Проблемы соз-

дания и внедрения автоматизированной системы технической эксплуатации первичной магистральной и вторичных сетей связи страны». Тезисы докладов. Киев, 1983. С. 56–58.

51. Золотарёв В.В. Сравнительные характеристики алгоритмов помехоустойчивого кодирования // Техника средств связи. Серия ТРС. 1986. Вып.4. С.21–24.

52. Золотарёв В.В. Улучшение характеристик МПД в гауссовских каналах // LVIII Научная сессия РНТОРЭС им. А.С.Попова, посвящённая дню радио. Труды. М., 2003. Т.2. С.82–84.

53. Золотарёв В.В. Устранение пакетов ошибок при многопороговом декодировании // В сб.: «VII Всесоюзный симпозиум по проблеме избыточности в информационных системах». Доклады. Ленинград, 1977. Ч.1. С.82–84.

54. Золотарёв В.В. Устройство для декодирования линейных кодов // Патент на изобретение РФ №2035123.

55. Золотарёв В.В. Характеристики декодеров для гауссовских каналов с большим шумом // В сб.: «VII Всесоюзная школа–семинар по вычислительным сетям». М.–Ереван, 1982. Ч.3. С.67–70.

56. Золотарёв В.В. Характеристики каскадирования многопороговых декодеров для спутниковых каналов связи // 5-я Международная конференция и выставка «Цифровая обработка сигналов и её применение». М., 2003. Доклады–2. С.353–356.

57. Золотарёв В.В. Характеристики эффективных алгоритмов декодирования в сетях ЭВМ // В сб.: «Вопросы кибернетики», ВК–98, АН СССР, Научный совет по комплексной проблеме «Кибернетика». М., 1983. С.34–38.

58. Золотарёв В.В. Энергетическая эффективность новейших методов помехоустойчивого кодирования // В сборнике ИКИ РАН: Всероссийская конференция «Современные проблемы дистанционного зондирования Земли из космоса». М., 2003. С.119.

59. Золотарёв В.В. Энергетическая эффективность новейших методов помехоустойчивого кодирования // Сборник докладов выездного семинара ИКИ РАН «Современные и перспек-

тивные разработки и технологии в космическом приборостроении». Россия, Таруса, 2003. С.312–318.

60. Золотарёв В.В. Эффективность лучших методов кодирования для спутниковых каналов // Труды LVI Научной сессии РНТОРЭС им. А.С.Попова, посвященной Дню радио. М., 2001. Т.2. С.379–382.

61. Золотарёв В.В. Эффективность лучших методов кодирования для спутниковых каналов // В сб.: «LVI научная сессия РНТОРЭС им. А.С.Попова, посвящённая Дню радио». Труды. М., 2001. Т.2. С.359–362.

62. Золотарёв В.В., Жуков С.Е. Многопороговые декодеры для систем спутниковой связи с большим уровнем шума // Труды НИИР. М., 2004. С.88–98.

63. Золотарёв В.В., Минина Н.Г. Каскадные схемы с мажоритарными кодами // В сб.: «9-я Всесоюзная конференция по теории кодирования и передачи информации». Тезисы докладов. Одесса, 1988. Ч.3. С.155–158.

64. Золотарёв В.В., Минина Н.Г. Мажоритарные декодеры с малой задержкой // В сб.: «IX Симпозиум по проблеме избыточности в информационных системах». Тезисы докладов. 1986. Ч.1. С.48–50.

65. Золотарёв В.В., Минина Н.Г. Микропроцессорная реализация алгоритмов помехоустойчивого кодирования // В сб. «Всесоюзная научно–техническая конференция «Микропроцессоры–85». М., 1985. С.61–63.

66. Золотарёв В.В., Минина Н.Г. О проектировании систем декодирования для сложных каналов // Вопросы радиоэлектроники. Серия ЭВТ. 1987. Вып.9. С.45–48.

67. Золотарёв В.В., Минина Н.Г. О соотношении корректирующих способностей кодов в каскадных схемах // «Вопросы радиоэлектроники», Серия «Электронная вычислительная техника». 1990. Вып.6. С.82–84.

68. Золотарёв В.В., Минина Н.Г. Устройство для декодирования линейных свёрточных кодов // Авторское свидетельство СССР №1291984.

69. Золотарёв В.В., Минина Н.Г. Устройство для декодирования свёрточных кодов // Авторское свидетельство СССР №1345356.

70. Золотарев В.В., Овечкин Г.В. Имитатор цифрового канала передачи данных (ChannelSim) // Свидетельство РОСПАТЕНТ №2005611304 от 31.05.05 о регистрации программы для ЭВМ.

71. Золотарёв В.В., Овечкин Г.В. Модификация многопорогового алгоритма декодирования // В сб.: «3-я Международная научно–техническая конференция «Космонавтика. Радиоэлектроника. Геоинформатика». Рязань, 2000. С.231–232.

72. Золотарёв В.В., Овечкин Г.В. Применение многопорогового декодера в схемах с параллельным кодированием // Труды РНТОРЭС им. А.С.Попова, Серия: Научная сессия, посвящённая Дню радио. М., 2004. Вып.LIX–2. С.121–123.

73. Золотарёв В.В., Овечкин Г.В. Сравнение турбоподобных кодов и многопорогового алгоритма декодирования // 10-я Межд. науч.–техн. конф. «Проблемы передачи и обработки информации в сетях и системах телекоммуникаций». Материалы конференции. Рязань, 2001. С.193–195.

74. Золотарёв В.В., Овечкин Г.В. Устройство многопорогового декодирования линейных кодов для гауссовских каналов // Патент на полезную модель РФ №44215.

75. Золотарёв В.В., Овечкин Г.В., Овечкин П.В. Многопороговые декодеры: новые достижения // 14-я Международная научно–техническая конференция «Проблемы передачи и обработки информации в сетях и системах телекоммуникаций». Рязань, 2005. С.57–58.

76. Золотарёв В.В., Овечкин Г.В., Овечкин П.В. Современные методы помехоустойчивого кодирования для высокоскоростных спутниковых систем связи // В сб.: «Новые информационные технологии в научных исследованиях и в образовании, НИТ–2005». Материалы 10-й Всероссийской научно–технической конференции. Рязань: РГРТА, 2005. С.2–3.

77. Золотарев В.В., Овечкин Г.В., Пылькин А.Н. Эффективность многопороговых алгоритмов декодирования помехо-

устойчивых кодов в высокоскоростных спутниковых системах связи // Космонавтика 2003. С.353–355.

78. Золотарёв В.В., Овечкин Г.В. Борьба с пакетами ошибок на выходе много порогового алгоритма декодирования // Межвузовский сборник научных трудов «Математическое и программное обеспечение вычислительных систем». Рязань: РГРТА, 2002. С.88–90.

79. Золотарёв В.В., Овечкин Г.В. Каскадирование многопорогового алгоритма декодирования с кодами с проверкой на чётность // Межвузовский сборник научных трудов. Новые информационные технологии. Рязань: РГРТА, 2002. С. 88–90.

80. Золотарёв В.В. Помехоустойчивое кодирование в спутниковой связи на основе многопороговых алгоритмов // Доклад на научно–технической конференции, посвящённой 55-летию НИИР. «Прогрессивные технологии для инфокоммуникаций России. НТТР–55. Новые перспективы». Тезисы докладов. М., 2004. С.30.

81. Зубарев Ю.Б., Золотарёв В.В. Многопороговые декодеры: перспективы аппаратной реализации // 7-я Межународная конференция «Цифровая обработка сигнала и её применение», М., 2005. С.68–70.

82. Зубарев Ю.Б., Золотарёв В.В. Новые технологии обеспечения высококачественной связи по радиоканалам с большим шумом на основе многопороговых декодеров // 6-я Международная конференция и выставка «Цифровая обработка сигналов и её применение». М., 2004. Доклады–1. С.3–8.

83. Зубарев Ю.Б., Золотарёв В.В., Жуков С.Е. Многопороговые декодеры для систем спутниковой связи // Сборник докладов выездного семинара ИКИ «Вопросы миниатюризации в современном космическом приборостроении». М., 2005. С.305–314.

84. Зубарев Ю.Б., Золотарёв В.В., Кумыш Э.И., Липатов А.А., Петров М.С., Плотников А.А. Многопороговые декодеры – новые технологии помехоустойчивого кодирования // Труды РНТОРЭС им. А.С.Попова. Научная сессия, посвящённая Дню радио. М., 2004. Вып.LIX-2. С.118–120.

85. Зубарев Ю.Б., Золотарёв В.В., Кумыш Э.И., Липатов А.А., Петров М.С., Плотников А.А. Применение многопороговых алгоритмов в каналах с большим уровнем шума // 6-я Межд. конф. SCTB. Тезисы докладов. М., 2004. С.30.

86. Колупаев А.В., Кондрахин А.В., Овечкин Г.В. Система имитации цифровой передачи данных по спутниковым и иным каналам связи // Межвуз. сб. науч. тр. «Математическое и программное обеспечение вычислительных систем». Рязань: РГРТА, 2005. С.109–111.

87. Овечкин Г.В. Алгоритмы и процедуры обработки и многопорогового декодирования в телекоммуникационных системах. Кандидатская диссертация. Рязань: РГРТА, 2003.

88. Овечкин Г.В. Методы улучшения эффективности многопорогового декодера самоортогональных кодов // Вестник РГРТА. Рязань, 2004. С.54–58.

89. Овечкин Г.В. Эффективность прямого исправления ошибок в системах передачи данных // Материалы 37-й науч.-техн. конференции. Рязань: РГРТА, 2002. С.24.

90. Овечкин Г.В., Золотарёв В.В. Перспективы применения многопороговых декодеров в высокоскоростных системах передачи данных // Сети и системы связи: Материалы Всероссийского научно-практического семинара. Рязань: РВВУС, 2005. С.52–55.

91. Овечкин Г.В., Овечкин П.В. Построение самоортогональных кодов устойчивых к эффекту размножения ошибок // Мат. 14-й Межд. науч.-техн. конф. «Проблемы передачи и обработки информации в сетях и системах телекоммуникаций». Рязань: РГРТА, 2005. С.70–71.

92. Овечкин Г.В., Овечкин П.В. Эффективность каскадной схемы кодирования на базе многопорогового декодера и кодов Хэмминга // Математическое и программное обеспечение вычислительных систем: Межвуз. сб. науч. тр. Рязань, 2004. С.79–82.

93. Овечкин Г.В., Овечкин П.В. Эффективность применения многопорогового декодера в каскадных схемах // Новые информационные технологии в научных исследованиях и в обра-

зовании: Материалы 8-й Всероссийской науч.-техн. конф. Рязань: РГРТА, 2003. С.131–132.

94. Овечкин П.В., Цыплаков Д.А. Разработка методов декодирования помехоустойчивых кодов на базе многопороговых декодеров // Материалы всероссийского смотра-конкурса научно-технического творчества студентов высших учебных заведений «Эврика-2005». Новочеркасск, 2005. Ч.1. С.140–144.

95. Пылькин А.Н., Золотарев В.В., Овечкин Г.В. Вопросы применения многопороговых декодеров в каскадных схемах кодирования // мат. всеросс. конф. «Информационно-телекоммуникационные технологии». Сочи, 2004. С.234–236.

ОГЛАВЛЕНИЕ

Имитатор цифрового спутникового канала связи с современными системами повышения достоверности – «Салют»

Институт космических исследований РАН предлагает разработку – уникальный компьютерный исследовательский и технологический стенд – имитатор цифрового спутникового канала связи с современными системами повышения достоверности «Салют». В имитатор включены практически все современные наиболее эффективные методы и алгоритмы повышения достоверности, используемые в реальных сетях связи или опубликованные за последнее время в специализированных научных изданиях по телекоммуникациям.

Имитатор «Салют» и многочисленные системы помехоустойчивого кодирования, включенные в состав его программного обеспечения, необходимы при разработке цифровых сетей передачи данных. Имитатор позволяет оценить возможность применения в разрабатываемых системах различных декодеров корректирующих кодов, что создаёт возможность правильного проектирования всех узлов создаваемых новых коммуникационных систем с учётом требуемых уровней энергетической эффективности, сложности, скорости и надёжности реализации, задержки принятия решения и других критериев выбора систем повышения достоверности. Современные системы кодирования стали настолько сложными и трудными для специалистов, занимающихся смежными вопросами, что из-за этого принятие правильных решений об этих важнейших компонентах сетей связи стало очень непростой задачей. Применение имитатора в процессе проектирования систем связи полностью снимает эту проблему.

Аналогов имитатора, хотя бы приблизительно сопоставимых с ним по качеству и объёму представления результатов анализа, удобству работы и, – главное! – разнообразию реализованных в нём наиболее эффективных методов кодирования в настоящее время **нигде в мире просто не существует**.

Подчеркнём, что очень многие возможности исследования и анализа методов кодирования, которые обеспечивают применение «Салюта», являются действительно абсолютно уникальными. Это относится к особенностям моделирования алгоритма Витерби с длиной кодирующего регистра до K~20 (!!!), к возможности анализировать прямо на экране характеристики многих турбо кодов и рассматривать применимость многопороговых и некоторых других наиболее мощных алгоритмов при задержках принятия решений до миллиона и более битов.

Применение «Салюта» обеспечивает возможность заглянуть примерно на 5–10 лет вперёд в будущее техники кодирования, проанализировать потенциальные возможности ещё только проектируемых систем и алгоритмов, которые опубликованы в самых последних журналах по кодированию. Подчеркнём в связи с этим, что программное обеспечение имитатора постоянно обновляется, что позволяет отслеживать уровень лучших мировых достижений в технике и технологии помехоустойчивого кодирования.

Среди большого числа методов, включенных в программное обеспечение имитатора «Салют», можно выбрать и быстро опробовать в моделируемом канале обычные мажоритарные декодеры, имитаторы декодеров кодов БЧХ, стандартные и специальные версии алгоритма Витерби, разнообразные варианты систем кодирования с применением каскадирования последовательного и параллельного типа, в том числе большое число различных версий декодеров турбо кодов с настраиваемыми параметрами как образующих их кодов, так и применяемых перемежителей. Много внимания разработчиками уделено созданию и реализации различных декодеров для низкоплотностных кодов.

Важнейшее место в программном обеспечении имитатора занимают алгоритмы многопорогового декодирования (МПД). Эта интереснейшая многолетняя разработка ИКИ РАН сейчас успешно завершена и готова к применению в самых разнообразных системах передачи информации с высокими требованиями к достоверности обмена данными и производительности алгоритма. По совокупности критериев простоты реализации и энергетической эффективности методы МПД далеко опережают многие другие известные разработки и продолжают успешно развиваться дальше. Все основные наиболее эффективные версии алгоритма МПД также включены в качестве возможных вариантов алгоритмов повышения достоверности передачи данных в состав программного обеспечения «Имитатора» и демонстрируют очень высокие реальные характеристики этого уникального алгоритма, который полностью разработан российскими специалистами.

Для более полного ознакомления с МПД алгоритмами и возможностями «Имитатора» предлагаем прочитать материалы, представленные на специализированном двуязычном веб-сайте ИКИ РАН **www.mtdbest.iki.rssi.ru**, а также в публикациях журнала «Электросвязь», 2003, № 9, и 2005, №2. Можно также переписать с этого вебсайта демоверсию имитатора «Салют», которая позволит потенциальным пользователям оценить удобство и полезность применения имитатора в процессе разработки.

Перечислим для краткости некоторые из важнейших характеристик «Салюта», предназначенного для исследований эффективности различных алгоритмов декодирования помехоустойчивых кодов в каналах различного вида.

Программное обеспечение «Салюта» обеспечивает специалисту, работающему с ним, интуитивно понятный пользовательский интерфейс. В процессе работы все результаты моделирования отображаются в текстовом виде в окне просмотра результатов. Предусмотрена возможность отображения графиков зависимостей вероятности ошибки декодирования от отношения сигнал/шум в канале связи.

Реализована также удобная возможность экспорта полученных графиков в Microsoft Excel и автоматизированного построения графиков эффективности декодирования.

Имитатор «Салют» создан на базе высокоскоростного переносного компьютера со следующими основными параметрами:

– IBM-совместимый компьютер на базе процессора с тактовой частотой 1 ГГц;

– объем оперативной памяти 256 Мбайт;

– операционная система Windows XP.

Перечислим некоторые наиболее эффективные методы коррекции ошибок, включенные в программное обеспечение имитатора «Салют»:

1) алгоритм декодирования Витерби сверточных кодов с конструктивной длиной до $K = 20$ и кодовой скоростью $R = 1/2$ и выше (для получения более высоких кодовых скоростей необходимо применять выкалывание);

2) многопороговый алгоритм декодирования блоковых и свёрточных самоортогональных кодов с кодовой скоростью R от 1/11 до 10/11 и кодовым расстоянием d от 1 до 20;

3) каскадные схемы кодирования на базе многопорогового декодера;

4) алгоритмы декодирования турбо кодов с кодовой скоростью 1/3 и выше (большие кодовые скорости достигаются применением выкалывания); предусмотрена возможность настройки параметров составляющих кодов и алгоритмов их декодирования, длины и типа перемежителя, количества итераций декодирования.

Исследование методов коррекции ошибок можно проводить в следующих моделях каналов:

1) канал с аддитивным белым гауссовским шумом и двоичной фазовой модуляцией; в данной модели возможна настройка следующих параметров:

– отношение сигнал/шум E_s/N_0, дБ (от –10 до 10 дБ);

– число уровней квантования решения демодулятора (от 2 до 64);

– границы областей решения мягкого модема;

– соответствующее каждой области квантования значение выхода демодулятора (используемая метрика);

2) канал с аддитивным белым гауссовским шумом и *M*-ичной фазовой модуляцией; в данной модели возможна настройка следующих параметров:

– отношение сигнал/шум E_s/N_0, дБ (от –10 до 10 дБ);

– количество точек сигнального множества (от 2 до 64);

– возможность формирования мягких решений демодулятора.

3) канал с аддитивным белым гауссовским шумом и квадратурно-амплитудной модуляцией; в данной модели возможна настройка следующих параметров:

– отношение сигнал/шум E_s/N_0, дБ (от –10 до 10 дБ);

– количество точек сигнального множества (от 2 до 64);

– возможность формирования мягких решений демодулятора.

Для обеспечения необходимой точности моделирования в имитаторе «Салют» предусмотрено тестирование моделей канала, а также доступны широкие возможности настройки параметров эксперимента, в частности:

– объем эксперимента;

– вид передаваемой информационной последовательности (нулевая, единичная, случайная и определяемая пользователем);

– количество ошибок на выходе декодера, после которого следует прекратить моделирование.

По желанию заказчика в «Салют» могут быть оперативно включены любые методы коррекции ошибок, специальные модели каналов связи, необходимые для конкретных проектных работ протоколы связи и иное программное обеспечение, повышающее эффективность работы исследователей и разработчиков новых систем связи.

Все доработки имитатора по заданным заказчиком параметрам канала и алгоритмов декодирования производятся оперативно с соответствующими изменениями в эксплуатационной документации на договорной основе.

Для консультаций по применению и приобретению нашего уникального стенда – имитатора «Салют» – предлагаем обращаться по адресу:

Москва, ИКИ РАН, тел. (495) 333–45–45, 333–23–56, e-mail: zolotasd@yandex.ru, моб.: 8–916–518–86–28, В.В. Золотарёв, или e-mail: g_ovechkin@mail.ru, моб.: 8–920–952–02–26, Г.В. Овечкин.

Демонстрационно-испытательный стенд аппаратуры помехоустойчивого кодирования на базе многопороговых алгоритмов исправления ошибок «Стиль-МПД»

В ИКИ РАН разработан программно-аппаратный комплекс «Стиль-МПД» для испытаний аппаратуры помехоустойчивого кодирования на базе многопороговых алгоритмов декодирования при передаче цифровых потоков по каналам с большим уровнем шума.

В состав стенда «Стиль-МПД» входят имитатор спутникового канала связи с возможностью подключения «мягких» и «жёстких» модемов передачи и приёма цифровых данных с системами контроля параметров канала, измеритель потери достоверности с различными методами формирования информационных потоков и рабочий модуль, выполненный на базе ПЛИС, содержащий устройство коррекции ошибок с параметрами, обеспечивающими высокую, до 200 Мбит/с производительность декодера класса МПД в каналах различного типа.

Аппаратно-программные средства стенда «Стиль-МПД» могут быть доработаны с учётом требований заказчика по параметрам помехоустойчивости испытываемых алгоритмов, видов систем сигналов, используемых в канале и способов формирования потоков ошибок, отличных от спутниковых каналов связи, а также по видам и классам используемых для реализации МПД ПЛИС или по видам собственно алгоритмов декодирования других типов, реализованных на этих ПЛИС.

В случае необходимости в состав стенда включаются основные цепи и узлы, отвечающие за реализацию различных видов синхронизации, применяемых в модемах.

Все доработки стенда по заданным заказчиком параметрам канала, измерителя потерь достоверности и алгоритмов декодирования производятся оперативно с соответствующими изменениями в эксплуатационной документации на договорной основе.

* * * * * *

Для консультаций по применению и приобретению стенда «Стиль-МПД» предлагаем обращаться по адресу: Москва, ИКИ РАН, тел. (495) 333–45–45, 333–23–56 или e-mail: zolotasd@yandex.ru, моб.: 8–916–518–86–28, В.В. Золотарёв.