В. В. Золотарёв

ОПТИМАЛЬНЫЕ АЛГОРИТМЫ ДЕКОДИРОВАНИЯ ЗОЛОТАРЁВА

ОПТИМИЗАЦИОННАЯ ТЕОРИЯ – КОМПАКТНОЕ СОВЕРШЕННОЕ РЕШЕНИЕ ПРОБЛЕМЫ ШЕННОНА

Под научной редакцией
члена-корреспондента РАН
Ю.Б. Зубарева

Москва
Горячая линия – Телеком
2021

УДК 621.391.15
ББК 32.811.4
З-80

Р е ц е н з е н т : академик РАН *Н. А. Кузнецов*

Золотарёв В. В.

З-80 Оптимальные алгоритмы декодирования Золотарёва (Оптимизационная Теория – компактное совершенное решение проблемы Шеннона) / Под ред. чл.-корр. РАН Ю. Б. Зубарева. – М.: Горячая линия – Телеком, 2021. – 268 с.: ил.

ISBN 978-5-9912-0919-9.

На основе Оптимизационной Теории (ОТ) помехоустойчивого кодирования изложены принципиально новые методы декодирования сообщений для всех классических моделей каналов. Созданные многопороговые декодеры (МПД) с теоретически минимальной сложностью обеспечивают оптимальную достоверность даже вблизи границы Шеннона.

Представлены программные платформы, доступные читателям и позволяющие им изучать характеристики конкретных новых алгоритмов.

Обсуждаются особенности новых версий алгоритма Витерби (АВ) для блоковых кодов. Показано, что по триединому критерию «помехоустойчивость–достоверность–сложность» у алгоритмов ОТ нет конкурентов.

Указывается, что абсолютное мировое лидерство ОТ определяется синергетическим ускорением её развития, обусловленным тесным взаимодействием тонкой оригинальной теории и специального инновационного программного обеспечения, аналогов которым в мире нет.

Для специалистов в области систем связи, студентов старших курсов, а также аспирантов математических и радиотехнических факультетов и университетов.

.

ББК 32.811.4

ISBN 978-5-9912-0919-9

© В. В. Золотарёв, 2021

От научного редактора

Широкое использование систем формирования информационных потоков и их обработки, а также хранения, восстановления, сопровождения и передачи по разнообразным каналам связи является основой нашей технологической цифровой цивилизации. Её информатизация достигла уже весьма высокого уровня и продолжает интенсивно развиваться.

В этой монографии изложена полная теория и представлены масштабные высокоинтеллектуальные программные средства исследования сложных оптимизационных задач, которые позволили её автору полностью решить великую проблему Шеннона, поставленную им более семидесяти лет назад перед будущим информационным сообществом в своей исторической для судеб теории кодирования статье «Математическая теория связи». Как руководитель небольшой российской научной школы Оптимизационной Теории (ОТ) помехоустойчивого кодирования профессор В.В. Золотарёв совершил, безусловно, настоящий научный подвиг, разрешив вместе с членами своего небольшого коллектива практически все теоретические проблемы и подготовив необходимые технологии для решения главной прикладной задачи этой отрасли науки — проектирования и создания алгоритмов декодирования для всех классических моделей каналов, рассматриваемых этой сложной многокомпонентной теорией.

Простому изложению всех этих решений сложнейших, как они оценивались ранее и до сегодняшнего дня всеми специалистами, задач в сфере теории кодирования и посвящена эта столь необычная книга. Для каждой из рассмотренных в монографии проблем автор нашёл столь удобные, наглядные и теперь уже совершенно очевидные для мыслящих специалистов решения, что все технические параметры его алгоритмов естественно оказываются вообще наилучшими возможными для методов декодирования как при программном, так и при аппаратном вариантах их реализации вплоть до областей шума канала, близких к границе Шеннона. И подчеркнём, что, тем не менее, эта задача в своём полном объёме и по сей день оставалась на нашей планете абсолютно неприступной для всей многомиллионной армии специалистов в сфере кодирования в течение последних пятидесяти лет.

Однако оценить всю философскую, научную и технологическую глубину и совершенство решённой автором этой монографии проблемы можно, только поняв масштабы кризиса, в котором много десятилетий прозябала вся теория помехоустойчивого кодирования. Поэтому

вернёмся сначала к общей ситуации последнего времени в этой важнейшей для нашей цифровой цивилизации отрасли науки.

Научная информатика осваивает всё более широкие области современных цифровых технологий, активно внедряется в разнообразные системы мониторинга природы. Но проникновение цифровой идеологии во все стороны жизни современного человека сопровождается и серьёзными кризисными явлениями. Более того, масштабы этого кризиса в некоторых основных сегментах теории информации стали воистину беспрецедентными, затяжными и беспросветными.

Основные трудности информатики долго нарастали в сфере самых основ теории информации и в той её сложнейшей и, конечно же, интереснейшей (!) части, которую составляют теория, технологии и алгоритмы помехоустойчивого кодирования. Несмотря на очень большое число специалистов, которые, вроде бы, занимаются развитием методов простого декодирования цифровых потоков в очень дорогих дискретных каналах, можно считать, что, кроме полезного периода освоения алгебраических методов помехоустойчивого кодирования около 60 лет назад, все последующее полвека успехи теоретиков практически были равны нулю. Но при этом наблюдался просто вал публикаций как в виде статей, так и огромного числа монографий, которые иногда очень по-своему излагали совершенно очевидные вещи, но претендовали на большой вклад в науку, хотя их реальные прикладные результаты практически ничего не меняли по существу вопроса.

Нерешённые проблемы этой главной науки цифрового мира продолжали накапливаться, что в значительной мере определялось и тогда, и сейчас абсолютной приверженностью большого числа учёных, работающих в этой сфере, алгебраическим основам этой теории. Однако на самом деле алгебраическая теория за многие годы своего очень условного лидерства не решила вообще никаких основных проблем своего развития: не нашла простых способов коррекции ошибок выше уровня половины кодового расстояния, не преодолела трудностей декодирования блоковых кодов в гауссовских каналах, а также не вышла на линейный от длины кодов уровень сложности алгоритмов коррекции ошибок, что, конечно же, тормозило и развитие цифровой техники. Значительные трудности были у алгебраистов и при анализе свёрточных кодов. Кроме того, их неспособность уже более полувека найти хоть какие-либо методы коррекции для недвоичных кодов, которые оказались бы лучше тех, что были предложены 60 лет назад для кодов Рида — Соломона (РС), совсем разуверила инженеров-связистов в возможности появления каких-либо новых результатов и в этом кластере параметров. А ведь это исключительно важная сфера

применения кодов в вычислительных системах, поскольку цифровые фото, музыка и ТВ используют как раз недвоичные, байтовые массивы информации.

На этом фоне явного кризиса теории появление в 1967 г. алгоритма Витерби (АВ) для свёрточных кодов можно считать воистину настоящим спасением теории кодировании в своём важнейшем прикладном аспекте, поскольку схема с формально экспоненциальным с длиной кода ростом объёма вычислений декодера обеспечила сразу столь высокие характеристики, которые оказались вполне достаточными для почти всех систем связи в течение многих последующих десятилетий. Правда, АВ мог быть реализован и тогда, и сейчас только для коротких кодов.

Напомним, что полезность применения кодирования, мера его эффективности, например, в технике связи при передаче двоичных данных обычно определяется параметром энергетического выигрыша кодирования (ЭВК), который просто характеризует величину кажущегося увеличения мощности передатчика системы связи, использующей хорошие методы кодирования и, главное, последующего высокодостоверного и быстрого декодирования принятого цифрового потока. А поскольку этот эффект может достигать величины 3, 5, 10 и даже более раз (свыше 10 дБ), то становится понятной исключительная важность применения кодирования, которое просто «дарит» системе связи столь большой ресурс по мощности передатчика. Этот большой прирост доступной связистам энергетики создаёт возможность существенного повышения скорости передачи цифровых данных, значительного снижения размеров очень дорогих антенн, многократного увеличения дальности связи и улучшения на много порядков достоверности принятой информации, а также ряд других весьма важных достоинств цифровых систем связи, использующих помехоустойчивое кодирование.

К этому можно добавить и потребности в кодировании у совсем новых направлений развития цифрового мира. Занимающиеся Интернетом вещей специалисты, конечно, согласятся с тем, что реально хорошие методы кодирования потратят вообще ничтожную долю энергии автономных источников питания на коррекцию возможных ошибок по сравнению со случаем, когда коды не применяются. И это так же важно, как и работа хороших алгоритмов декодирования вблизи пропускной способности канала, т. е. при минимально возможной мощности сигнала передатчика, что также сильно экономит заряд батарей. Таких полезнейших свойств кодов очень много и все они оказываются очень кстати для всей широкой сферы приложения кодирования.

Напомним далее о том, что за полувековой сложный период своего относительно активного существования «классическая», так сказать, теория кодирования, ориентированная в своём главном прикладном аспекте на разработку методов кодирования, пыталась организовать и поиск других алгоритмов декодирования, поскольку кроме экспоненциально сложного АВ её успехи были крайне незначительны. Не вдаваясь во все второстепенные теперь детали таких смен направлений развития, интересных сейчас только для историков науки, отметим лишь некоторые черты таких алгоритмов, которые так и не стали судьбоносными для той теории. Все они являются весьма общими у турбо кодов, низкоплотностных (LDPC) и полярных кодов. Самой неудобной для всех алгоритмов декодирования этих кодов оказалась необходимость использования в своих вычислениях действительных чисел. Это сразу сильно ограничило сферу их применимости, особенно для высокоскоростных каналов. Но, более того, и решающие функции этих алгоритмов, загружавшие процессоры, реализовавшие такие алгоритмы, оказались довольно сложными сами по себе. А дополнительные высокие требования, например, к точности вычислений выражений, используемых при декодировании полярных кодов, и вообще смотрятся как неоправданно экстремальные, так как в некоторых публикациях авторы пишут о недостаточности для них обычной точности представления действительных чисел в компьютерных системах. Да и собственно объём необходимых вычислений всех этих «новых» алгоритмов оказался весьма большим.

К этому необходимо добавить, что, к тому же, за последние десятилетия фактически никакие авторские коллективы не утруждают себя такой подготовкой публикуемых материалов по алгоритмам декодирования, чтобы из них можно было получить точное и — главное (!) — правильное представление об их сложности, помехоустойчивости и достоверности. Это полностью лишает читателей таких материалов какой-либо уверенности в достоверности и применимости этих результатов. Поэтому реально доступные связистам алгоритмы декодирования нередко оказываются слишком сложными и медленными или слабыми и не представляющими интереса для техники связи. Переводные книги, в том числе и учебного типа, также многословны и обычно излагают давно устаревшие результаты.

Но, как уже более сорока лет известно, оптимальное решение (наилучший по вероятности необнаруженной ошибки результат) при декодировании кодов на самом деле может быть успешно найдено на основе оптимизационного поиска на экспоненциально растущем с длиной кода массиве возможных решений. Это стало отправной точкой воистину впечатляющих многолетних исследований автора этой

уникальнейшей монографии, получившего авторское свидетельство на такое неожиданное решение проблемы помехоустойчивого кодирования почти полвека назад. И сложность этого поиска — наилучшая из возможных, минимальная, линейно растущая с длиной кодов, что тоже всегда исключительно важно.

Многочисленные работы автора монографии и его научной школы с блеском показали, что пока лишь достижения Оптимизационной Теории (ОТ) являются основой очень простых алгоритмов поиска глобального экстремума, которые правильно декодируют принятые сообщения непосредственно вблизи границы Шеннона и с линейной сложностью, что и является конечной целью теории кодирования. Монография, в которой первоначально были представлены первые революционные результаты нового научного направления, была издана Научным советом по комплексной проблеме «Кибернетика» АН СССР и опубликована в издательстве «Наука» ещё в 1981 году.

Именно в этих условиях в течение уже многих десятилетий в России развивается Оптимизационная Теория (ОТ) помехоустойчивого декодирования, которая на совершенно новом, можно сказать, принципиально ином глубоком философском уровне успешно решает проблемы оптимального, наилучшего по достоверности декодирования, но при теоретически минимальной, линейной от длины кода сложности и в условиях максимально допустимого уровня шума цифровых каналов. А минимальная возможная сложность как раз и позволяет создавать простые и очень быстрые декодеры для очень длинных кодов. Автор и другие первооткрыватели этого направления в своих, конечно же, крайне неожиданных по стилю и результатам книгах и статьях за десятилетия напряжённой работы показали совершенно новые возможности как давно известных стандартных и улучшенных методов типа замечательного алгоритма Витерби (АВ), так и новых итеративных алгоритмов на основе многопорогового декодирования (МПД), реализующих эффективные процедуры глобального поиска экстремума функционалов.

Ключевой темой, определяющей ценность данной выдающейся монографии, являются разнообразные обширные результаты, убедительно демонстрирующие вполне удобные технологичные решения поставленной 70 лет назад Клодом Шенноном проблемы простого высокодостоверного декодирования вблизи пропускной способности канала. Совершенно непостижимо, почему за все эти годы никто не обращал внимания на то, что проблема оптимального декодирования может формулироваться и как классическая глобальная оптимизационная задача, которая в случае применения к теории кодирования приобретает, конечно, некоторые специфические особенности, не ме-

няющие сущности этой вполне понятной и давно проработанной проблематики поиска глобального экстремума. Весьма странно, что эта идея уже была опубликована научной школой ОТ ещё в том тысячелетии, но не нашла отклика у специалистов.

Стартовой установкой в большом наборе совершенно уникальных парадигм ОТ, принципиально новой во всех отношениях теории, которую сторонники школы называют «квантовой механикой» теории информации, стала Основная Теорема многопорогового декодирования (ОТМПД). Прямо в самой первой своей крайне простой, но очень точной формулировке, несущей глубочайший философский смысл, она сообщила инженерам и научному сообществу о том, что правильно организованные самые простейшие мажоритарные по своей сути итеративные алгоритмы при каждом изменении декодируемых символов строго приближаются к решению оптимального декодера (ОД), для достижения которого раньше обычно требовалось осуществлять полный экспоненциально сложный перебор, что вполне элегантно, например, делает алгоритм Витерби (АВ). Появление ОТМПД самым революционным образом поменяло постановки задач декодирования для всех видов каналов с независимыми искажениями. Теперь стало возможным использовать МПД декодеры практически для любых классов мажоритарно декодируемых кодов и при всего лишь линейной (!) от длины кода сложности алгоритма попробовать достигать решений ОД даже при большом относительном уровне шума канала. И крайне печальным обстоятельством оказывается то, что ни в одном из всего лишь нескольких реальных центров страны, в которых могла бы развиваться эта столь принципиально обновлённая и очень эффективная теория кодирования на базе ОТ, за 40 лет последующих лет её существования никто не удосужился обратить внимание на эту неожиданную возможность крайне простого декодирования с потенциально наилучшими возможными результатами по достоверности принятых декодером решений.

Автор монографии, однако, ещё в те далёкие годы сразу чётко и ясно указал, что при решении оптимизационной задачи декодирования эта исключительно точно сформулированная особая краеугольная для судеб теории ОТМПД теорема вовсе не обещает обязательного достижения решения ОД. Именно поэтому члены научной школы автора монографии, создавшие эту полную и теперь уже вполне совершенную масштабную теорию «всего» в кодировании, все эти годы были непрерывно заняты именно поиском условий, которые должны выполняться для того, чтобы процесс декодирования, т. е. поиска глобального экстремума функционала, был по возможности более долгим. Здесь очень важно, чтобы этот поиск не прекращался где-нибудь

на полпути к оптимальному решению, которым является кодовое слово, ближайшее к принятому из канала сообщению.

И эта задача также оказалась решённой в ОТ! Школа ОТ создала для этого особую теорию размножения ошибок (РО) декодирования, к которой не смог за последние 50 даже подступиться ни один научный коллектив в мире. А её главный результат оказался в том, что теория РО позволила быстро и просто строить коды, используя которые МПД декодер действительно смог уже практически всегда достигать оптимальных решений даже при экстремально большом уровне шума, т. е. вблизи пропускной способности канала.

Все очевидные, а иногда и довольно неожиданные способы достижения решения ОД на основе МПД алгоритмов и ряда других методов как раз и изложены во всём своём многообразии в данной книге. Автор доступно и понятно показывает, что для большого числа каналов и кодов уже возможно достижение очень высокого уровня достоверности при большом уровне шума на основе МПД декодеров и ряда производных от них методов. Как будет видно из последующего материала книги, эта задача действительно уже во многих случаях очень успешно решена или для некоторых кластеров параметров она будет безусловно решена уже известными в ОТ методами в непосредственной близости от пропускной способности цифрового канала. Это и даёт нам право обоснованно считать, что именно российская наука в лице автора данной монографии полностью решила проблему Шеннона для всех стандартных цифровых каналов, рассматриваемых в теории кодирования. Задача расширения списка таких кодовых кластеров (т. е. совокупностей параметров каналов, кодов и декодеров) будет теперь постоянно решаться, а поле ОТ расширяться, т. к. все условия для этого научной школой автора уже созданы.

Таким образом, по уже вполне понятным причинам можно считать, что прежняя теория кодирования передала пальму первенства ОТ — новой «квантовой механике» теории информации. Этот вывод обусловлен фактом обеспечения технологиями ОТ наилучшей достоверности при минимальной сложности декодирования вплоть до ближайших окрестностей границы Шеннона.

Подчеркнём, что автор и его научная школа получили целый ряд исключительно важных результатов и в самых различных технологических сферах, связанных с теорией кодирования. Наиболее существенным прикладным достижением ОТ является расширение области действия ОТМПД фактически на всё множество методов итеративного декодирования линейных кодов, как блоковых, так и свёрточных: это каскадные схемы разных типов, каналы со стираниями, сверхбыстрые аппаратные и программные варианты декодеров, а также,

что тоже совершенно необычно и даже абсолютно неожиданно вообще для всей теории кодирования, — символьные коды.

Эти недвоичные коды связаны с удивительными свойствами поискового человеческого мышления, которое иногда обходит своим вниманием именно те важнейшие области знания, к исследованию которых такое мышление как раз и должно было бы привлекаться. Дело в том, что символьные коды относятся к недвоичным мажоритарно декодируемым кодам. Они были открыты, как и обычные пороговые алгоритмы, основоположником этого направления, выдающимся американским учёным Дж. Месси. Он получил некоторые результаты для таких кодов и опубликовал их в своей классической книге по пороговому декодированию. Однако при анализе таких кодов он потребовал от них таких исключительно высоких характеристик, которые те в принципе не могли обеспечить. И в результате немалого вследствие этого разочарования он отказался от дальнейшего изучения таких кодовых структур. А из-за этого и исследователи всего мира, безусловно поверив мнению этого уважаемого всеми учёного, в течение последующих 50 лет даже не пытались применить мажоритарные алгоритмы к недвоичным кодам, которых как бы и не было. Но так получилось, что и все прочие недвоичные коды и декодеры, созданные «классической» наукой за этот длительный период, не стали выдающимися достижениями теории кодирования, хотя и были полезными.

А вот автор монографии и его школа очень внимательно отнеслись к кодам, когда-то отвергнутым Месси, чётко отделили их от прочих типов кодов и назвали символьными. К настоящему времени члены школы ОТ написали вообще абсолютно полную теорию для этих переоткрытых ими структур, а также для особо простых символьных МПД декодеров, реализующих функции глобального поиска экстремума на цифровых потоках с определённой кодовой структурой, причём также при минимальной линейной от длины кода сложности.

Кстати, очень полезно обратить внимание читателей этой книги на то, что для действительно триумфального шествия символьных кодов в мире систем кодирования авторы символьных алгоритмов сразу же немного поменяли и запатентовали правила работы порогового элемента (ПЭ) для этих кодов — главного активного элемента во всех МПД. Именно этот момент и решил судьбу мирового конкурса среди недвоичных алгоритмов. Он просто не состоялся, что называется, «за явным преимуществом» символьных кодов по всем параметрам эффективности и сложности, т. к. декодеры символьных МПД с линейной сложностью от длины кодов сходятся к оптимальному решению даже при очень больших уровнях шума канала. В этом можно убедиться, читая соответствующие разделы этой монографии или ра-

нее изданные книги и статьи автора и школы ОТ по этой тематике. И при этом важно подчеркнуть, что вообще все варианты МПД алгоритмов являются крайне простыми устройствами или программами с хорошо понятными принципами работы мажоритарных алгоритмов, что крайне полезно для их разработок, применения, обучения и дальнейшего прогресса этой научной тематики.

В монографии уделяется заслуженно глубокое внимание и многим другим идеям, возникшим в процессе развития ОТ: принципу дивергенции, параллельному каскадированию, кодам с выделенными ветвями и другим системам и принципам организации нового очень необычного стиля кодирования, образовавшим своё особое обширное интеллектуальное пространство парадигм ОТ. Все они действительно помогают созданию, исследованиям и реализации исключительно простых методов декодирования при большом уровне шума. Отметим, что ранее ни одного из перечисленных понятий в теории кодирования вообще не было. Но их роль в ОТ и в успешном решении проблем декодирования действительно оказалась чрезвычайно важной.

Столь же велика в ОТ и роль декодеров с прямым контролем метрики (ДПКМ). К группе ДПКМ относятся все методы с использованием МПД и АВ. Этот подход выводит исследования декодеров на основе АВ и МПД на совершенно новый уровень, работа на котором уже позволила получить ещё один чрезвычайно важный результат — создание блоковой версии алгоритма Витерби (БАВ) со сложностью, близкой к сложности классического АВ для свёрточных кодов, которую автор книги также, как и многие другие достижения, своевременно запатентовал. Этот результат для одного из самых главных алгоритмов прошлого века впечатляет и сам по себе, так как оценки сложности «прежней» теории кодирования для блоковых версий АВ фактически соответствуют удвоенному показателю экспоненты сложности по сравнению со свёрточными кодами, что, конечно, делало их совершенно недоступными для применения в реальных системах. Нелишне подчеркнуть, что школа ОТ давно и успешно развивает теперь уже и это направление прикладной теории кодирования, которое тоже было незаслуженно забыто прежней «классической» теорией на фоне турбо и прочих «достижений» теоретиков.

Во всех монографиях по МПД и ОТ для иллюстрации многих результатов МПД алгоритмов уже неоднократно использовались возможности сетевых порталов www.mtdbest.ru и www.mtdbest.iki.rssi.ru научной школы автора, первый из которых достаточно часто обновляется. Это многократно облегчает правильное понимание результатов ОТ. Использование ресурсов этих порталов в данной монографии оказывается ещё более разнообразным и полным. На этих веб-сайтах,

с общим числом информационных блоков более 600, представлено большое число демо-программ по всем наиболее известным в мире алгоритмам декодирования. Эти тематические двуязычные порталы посещают свыше 100 тысяч читателей в год из более 90 стран мира, что особенно хорошо и точно характеризует полное и безусловное признание мировым научно-техническим сообществом технологий и парадигм ОТ и её результатов.

Более того, представленные на первом из указанных сетевых ресурсов специальные программные платформы действительно позволяют любому специалисту быстро перейти к полноценной научной работе в сфере ОТ.

Автор монографии является лауреатом премии Правительства РФ по науке и технике. Европейский союз (ЕС) наградил создателя ОТ Золотой медалью «За исключительные достижения», которая в Европе вручается только за самые выдающиеся научные результаты. А на недавней Международной выставке изобретений ему была вручена Золотая медаль за патент на сверхскоростной МПД декодер.

Что же касается уровня текущей и далеко не современной теории кодирования как у нас в стране, так и в зарубежье, то единый общий драматический диагноз её состояния обусловлен крайне странным для цифровой цивилизации обстоятельством. Дело в том, что никакие главные характеристики эффективных декодеров никто не умеет рассчитывать для большого уровня шума. Наверное, этого никогда и не случится ни для каких алгоритмов. Возможно, что этого нельзя сделать просто в принципе. И никто не умеет программировать! Это можно сказать практически почти про всех специалистов в области кодов. Да и лозунг конца того тысячелетия: «программирование — вторая грамотность!» — ныне давно забыт абсолютно. Всё это и стало концом «той» чисто математической теории кодирования. Но теория кодирования — это вовсе не математическая задача! Это одна из оптимизационных проблем в дискретных пространствах со структурой массивов, корректирующих ошибки. И все их главные характеристики, возможно, всегда будут определяться только экспериментально, на программных моделях и аппаратных макетах, которые обычно выдают такие результаты по характеристикам практически мгновенно. Всё это научная школа ОТ поняла более полувека назад, что и позволило ей выиграть невероятно масштабный и важнейший научный конкурс в теории информации на самом взлёте цифровизации нашего мира.

Так что декларируемый автором этой монографии в очень мягкой форме его приоритет и абсолютное мировое лидерство, оцениваемое им весьма скромно, в 20–30 лет, действительно существует, так как

сейчас не видно даже на горизонте таких научных групп, которые хотя бы начали создавать для развития прикладной теории кодирования какие-либо программные оптимизирующие, моделирующие и проектирующие комплексы для исследования и конструирования новых очень быстрых оптимальных систем кодирования, работающих вблизи границы Шеннона. Действительно, только на создание такого программного обеспечения нужны, как это было и со школой ОТ, десятилетия напряжённого сложнейшего труда, что особенно подчёркивает способность предвидения будущего своей отрасли науки у автора этой книги, равной которой, может быть, не появится ещё очень долго. Трудный опыт школы ОТ свидетельствует, что, кроме решения о разработке тех или иных комплексов подобных интеллектуальных программных систем, нужны ещё также определённое время и большой накопленный личный опыт для того, чтобы понять, какими именно должны быть эти инновационные комплексы. А это тоже долгие напряженные годы очень упорной работы.

Свой обширный набор таких программных средств школа ОТ свободно предлагает всем специалистам. Этот набор, как полагает руководитель школы, будет непрерывно расширяться и становиться всё более доступным для всех.

Переходя к заключительным замечаниям об этой уникальнейшей в теории кодирования и вообще в истории науки книге, позволю себе напомнить, что читатель держит в своих руках действительно чрезвычайно важную монографию, которая знаменует собой, наконец, состоявшийся сильно затянувшийся переход всей прикладной теории кодирования в совершенно новую фазу своего развития, ориентированную на создание действительно доступных эффективных алгоритмов коррекции ошибок гарантированного качества. Он основан на прочном союзе теории и эксперимента. Крайне жаль, что этот переход не произошёл около 30 лет назад, когда полная теория ОТ уже была создана. Она становится уже не проблемой, а технологической задачей глобальной оптимизации функционалов от очень большого числа переменных в дискретных пространствах со структурой, учитывающей свойства корректирующих кодов. Многие из рассмотренных в монографии и глубоко исследованных алгоритмов успешно работают в непосредственной близости от границы Шеннона. И очень важно, что все методы ОТ остаются хорошо известными простейшими мажоритарным декодерами с правильно подобранными параметрами или модификациями широко распространённых декодеров, работающих по алгоритму Витерби, который любят и тоже прекрасно понимают все инженеры цифровой связи.

Ситуация, сложившаяся к настоящему времени вокруг ОТ, по

мнению уже немалого числа специалистов по теории кодирования, сильно напоминает состояние физики начала XX века, когда многие актуальные задачи оказалось невозможным решить имевшимися тогда у науки методами. И только появление ряда совершенно новых для физики парадигм, относящихся к принципам устройства нашего мира, сформировавших позже квантовую механику, позволило выйти на новые рубежи научного познания нашего физического мира. Целый ряд великих физиков своего времени был тогда заслуженно удостоен Нобелевской премии, хотя физика начала того века ещё довольно долго не относилась к сколько-нибудь актуальным отраслям знания. Её общественное признание состоялось уже в 30–40-х годах.

Важность же ОТ, её технологий и парадигм исключительно высока потому, что она уже стала новой «квантовой механикой» в прикладной теории информации. Чрезвычайно существенно и то, что ОТ создана и уже успешно завершена во всех основных своих аспектах в самый важный период начала бурного развития нашей информационной цифровой цивилизации, которая до самого последнего времени не умела обеспечивать простыми средствами необходимую ей высокую достоверность своего информационного контента. Именно поэтому для нашего современного мира значение ОТ, очень содержательной, компактной и совершенной науки, многократно превышает значимость квантовой механики для физики, какой она была в самом начале прошлого века.

Согласимся в конце нашего вводного обзора и с тем, что такая книга о полном решении проблемы Шеннона абсолютно необычна и поэтому, конечно, совершенно неожиданна для основного контингента мировой науки, занятого вопросами кодирования. Укажем также, что уже выходят публикации с участием членов РАН и специалистов в области цифровых технологий, где они подтверждают исключительную ценность результатов автора этой монографии и полагают, что алгоритмы МПД, символьные коды, а также теория размножения ошибок декодирования полностью соответствуют нобелевскому уровню исследований автора как вместе взятые, так и в отдельности. А технологии настроек параметров кодов и декодеров, алгоритмы для исправления стираний и совокупность новых парадигм ОТ, а также десятки патентов автора — большинство из них безусловно являются выдающимися открытиями в области прикладной теории кодирования. И это реально именно так, что и подтверждают сетевые порталы научной школы ОТ, которые, как я уже отмечал выше, давно читают специалисты всего мира.

Особенно наглядно совершенство ОТ подчёркивает её чрезвычайная компактность, минимальное количество формул, описывающих

возможности всех алгоритмов В.В. Золотарёва в различных каналах, и глубокая философская сущность, которая, я думаю, может обсуждаться и анализироваться историками науки ещё очень долгое время. Можно оценочно полагать, что вся ОТ имеет при этом объём, который примерно на три порядка меньше очень распухшей сейчас прежней теории, которая уже давно не приносит никаких разумных результатов, на что мы неоднократно указывали в наших новых обзорах по прикладным вопросам сферы применения теории кодирования.

Своё полное удовлетворение от выхода в свет столь необычной монографии хочется выразить ещё и в связи с тем, что 2018 год оказался юбилейным для теории кодирования. Более 70 лет назад Клод Шеннон фактически поставил эту проблему простого и эффективного декодирования перед наукой и техникой в своей замечательной статье. Очень приятно найти её успешное во всех смыслах решение именно сейчас в монографии выдающегося российского учёного. История науки не знала до сих пор такого случая, чтобы небольшая научная школа полностью развернула в принципиально новом направлении столь грандиозную и инерционную, но одновременно и такую необходимую для техники связи сложнейшую отрасль науки, практически полностью решив все ранее сформулированные для неё прикладные проблемы.

И в заключение я выражаю твёрдую уверенность, что актуальнейшие результаты ОТ — новой «квантовой механики» современной теории информации, изложенные в этой уникальной монографии, послужат масштабным достойным вкладом всей российской науки в развитие новых методов и технологий цифровой обработки данных, а также вообще всей теории информации для цифрового информационного сообщества начала нового тысячелетия.

Лауреат Государственной премии СССР,
член-корреспондент РАН,
доктор технических наук, профессор,
Заслуженный деятель науки РФ,
лауреат Государственной премии,
дважды лауреат Премии Правительства РФ

Ю.Б. Зубарев

О новом формате прикладной теории кодирования

Проблема более простого обеспечения высокой достоверности передачи, обработки, хранения и восстановления цифровых данных становится всё актуальней во всем мире. Однако до последнего времени казалось, что до успешного решения задачи создания простых и высокоэффективных даже вблизи границы Шеннона декодеров разных типов, что и является главной прикладной целью теории кодирования, ещё очень далеко. В самом деле, для этого нужно было найти методы декодирования в четырёх традиционных в классической теории каналах: в двоичном симметричном, недвоичном, гауссовском и стирающем каналах, для реализации которых ранее нередко привлекались различные и нередко довольно тяжеловесные, а также далеко не самые эффективные идеи. Но все они в итоге оказывались очень трудоемкими и далёкими от того возможного уровня эффективности, оценки которого давала теория.

На фоне этого длительного кризиса совсем иначе смотрелись все эти десятилетия работы нашей научной школы Оптимизационной Теории (ОТ) помехоустойчивого кодирования, которую около полувека назад начал развивать профессор ИКИ РАН Валерий Владимирович Золотарёв. Впервые в мире поставив задачу итеративного постепенного приближения к наилучшему оптимальному по вероятности ошибки решению, он и активные последователи нашей школы начали почти сразу получать очень высокие характеристики разрабатываемых алгоритмов по достоверности при крайне простых схемах их реализации, что было очень естественно, так как основой новых алгоритмов, названных нами многопороговыми декодерами (МПД), стали простейшие давно известные пороговые декодеры Джеймса Месси. А вот высокая достоверность МПД декодеров, практически совпадающая с оптимальным декодированием (ОД), что раньше обеспечивали лишь методы полного перебора, например алгоритм Витерби (АВ), — эти свойства для всё более высоких уровней шума наши декодеры в течение многих десятилетий приобретали медленно по мере развития ОТ вместе с очень разветвлённым и масштабным программным обеспечением (ПО). Очень помог быстрому улучшению характеристик наших алгоритмов рост производительности доступных нам вычислительных средств, а также непрерывно развиваемое нами оптимизационное ПО. Эта особенность исследований в нашей научной школе является важнейшей для прогресса самой теории ОТ и для получения новых результатов в области проектирования и анализа свойств алгоритмов

декодирования, а также для улучшения их характеристик.

Именно при такой абсолютно нетипичной для прежней теории, но очень плодотворной постановке проблемы простой высокодостоверной передачи цифровых данных по каналам с шумом В.В. Золотарёв при участии ряда энтузиастов школы издал уже много монографий по ОТ, в которых описаны решения множества крайне сложных задач, которые обеспечили достижение алгоритмами ОТ ближайших окрестностей границы Шеннона при минимальной сложности и практически наилучшей достоверности.

Предлагаемая специалистам новая монография профессора В.В. Золотарёва излагает теорию ОТ и её самые новые прикладные достижения в сфере разработки и создания алгоритмов декодирования, обеспечивающих в случае применения МПД декодеров практически оптимальное декодирование с минимально возможной от длины кодов сложностью реализации. А при использовании блоковых модификаций АВ, как следует из представленных данных, уже достижимы и все наилучшие параметры декодирования для коротких кодов, которые теперь не доступны никаким другим алгоритмам. Это определяется тем, что только все МПД декодеры и АВ во всех своих модификациях измеряют расстояния своих решений до принятого сообщения. Опыт наших исследований свидетельствует о том, что никакие алгоритмы, лишённые таких исключительно полезных свойств, не имеют никаких перспектив достичь границы Шеннона при разумной сложности их реализации.

Таким образом, утверждение абсолютного лидерства ОТ и теперь уже окончательный «уход» с реального поля науки прежней теории произошло из-за того, что по единому критерию «помехоустойчивость — достоверность — сложность» та теория не смогла за всё время своего бытия найти аналитические выражения для каждого из этих параметров критерия в условиях большого шума канала хотя бы для одного из своих алгоритмов, претендовавших на высокие характеристики помехоустойчивости. Но развивать одновременно и теорию, и экспериментальную базу адепты прежней эры просто не смогли.

А это значит, что теория кодирования в прикладном своём аспекте действительно оказалась вовсе не математической задачей. Давно осознав это, школа ОТ полностью решила проблему Шеннона для всех традиционных каналов как задачу глобальной оптимизации функционалов сложной природы в цифровых пространствах, оставшись при этом исключительно в рамках очень понятных мажоритарных алгоритмов и алгоритма Витерби. Других сопоставимых с ОТ методов за её пределами сейчас нет. Да и ожидать их появления трудно. Все характеристики алгоритмов ОТ по единому критерию сейчас

являются наилучшими и мгновенно определяются при моделировании средствами нашего инновационного оптимизационного ПО, что ещё более ускоряет развитие ОТ и помогает быстро указывать ей новые точки роста.

Полезно отметить исключительную компактность ОТ и её полноту. Технологии ОТ отлично работают и уже продемонстрировали высокие результаты примерно для ста различных кластеров параметров кодирования. Одна из ведущих ролей в текущем быстром прогрессе ОТ несомненно принадлежит автору этой монографии профессору В.В. Золотарёву, в которой изложены новейшие данные по фундаментальным научным и прикладным разработкам созданной им теории.

Сторонники научной школы ОТ полагают, что успешная теоретическая и экспериментальная работа всех специалистов, заинтересованных в дальнейшем развитии прикладных методов кодирования, в том числе в направлениях, указанных в последних главах этой монографии, позволит и далее очень быстро продвигать технику помехоустойчивого кодирования на всё более высокие уровни технологий. Именно это и нужно от передовой теории, ставшей «квантовой механикой» современной теории информации, цифровому информационному сообществу нового тысячелетия.

Заведующий кафедрой
вычислительной и прикладной математики
ФГБОУ ВО «Рязанский государственный
радиотехнический университет им. В.Ф. Уткина»,
доцент, доктор технических наук,
председатель научно-методического совета РГРТУ Г.В. Овечкин

О научном инакомыслии:
«На первых порах новая теория провозглашается нелепой. Затем её принимают, но говорят, что она не представляет собой ничего особенного и ясна, как Божий день. Наконец, она признаётся настолько важной, что её бывшие противники начинают утверждать, будто сами открыли её.»
Уильям Джеймс, философ, США

«Старайся исполнить свой долг — и ты тотчас узнаешь, чего ты стоишь.»
Лев Николаевич Толстой

От автора

Выход в свет в 1963 году 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 году алгоритма Витерби (АВ) вывело технику кодирования на принципиально новый уровень качества связи благодаря возникшей возможности существенно более эффективного кодирования, поскольку предложенный алгоритм обеспечивал в гауссовском канале оптимальное декодирование кодов небольшой длины. Это стало причиной привлечения большого числа специалистов по теории и технике кодирования к проблеме повышения именно эффективности кодирования, поскольку в те годы всем 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 более простого декодирования никогда не снималось с повестки дня.

Тем не менее, исследования алгоритмов мажоритарного типа продолжались. В 2018 году исполнилось 40 лет со дня защиты первой кандидатской диссертации по новым итеративным алгоритмам декодирования мажоритарного типа [38]. А недавно отмечались 30 лет со дня защиты докторской диссертации по этой же тематике [36], которая недавно была уже гораздо более полно представлена в новых

книгах нашей научной школы Оптимизационной Теории (ОТ) помехоустойчивого кодирования [4, 79, 90, 91, 94, 100]. Эффект от этих публикаций был достаточно сильным и положительным настолько, что это позволило издателю ряда книг по многопороговым алгоритмам декодирования (МПД) и справочника по кодированию недавно повторно выпустить в свет монографию по этой тематике [3], первое издание которой было напечатано ещё в 2006 году.

Отметим, что впервые в издательстве «Наука» результаты по многопороговым алгоритмам, включая Основную Теорему многопорогового декодирования (ОТМПД), были опубликованы ещё в 1981 году [2].

Таким образом, можно считать, что российские читатели всегда достаточно хорошо информированы о состоянии исследований по тематике эффективного декодирования на основе мажоритарных процедур, особенно простых в реализации по сравнению с другими методами. Результаты применения таких усовершенствованных алгоритмов, названных многопороговыми декодерами (МПД), оказываются к настоящему моменту уже практически совпадающими с оптимальными, т. е. мало отличающимися по выходной вероятности ошибки от характеристик переборных алгоритмов для этих же кодов даже вблизи пропускной способности канала. Это было показано участниками нашей научной школы Оптимизационной Теории (ОТ) кодирования как теоретически, так и при обширном моделировании работы соответствующих процедур для специальных кодов, удовлетворяющих ряду весьма строгих, но абсолютно понятных требований, а также при создании аппаратуры кодирования на ПЛИС в ряде организаций.

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, пять поколений которой были созданы в НИИ Радио, ведущем институте Минсвязи, и в других организациях, были получены ожидаемые автором и разработчиками систем связи характеристики. Существенно, что уже в те далёкие годы они были иногда совершенно недоступны для всех других известных алгоритмов коррекции ошибок с разумной сложностью реализации.

Напомним те основные положения, которые фактически и позволили поднять эффективность исключительно простых алгоритмов порогового типа до уровня оптимальных переборных процедур. Они состоят всего из двух пунктов, обеспечивших решение принципиально новой для теории кодирования задачи повышения качества декодеров мажоритарного типа, реализующих процедуры поиска глобального

экстремума функционалов от очень большого числа переменных.

1. Мажоритарные алгоритмы могут быть чрезвычайно эффективными. Существуют весьма простые мажоритарные алгоритмы МПД итеративного типа, которые обладают свойством строгого приближения к оптимальному решению на всех итерациях декодирования до тех пор, пока продолжается процесс изменения декодером символов принятого сообщения. При таком подходе задача декодирования превращается в проблему поиска глобального экстремума функционала от большого числа переменных в дискретных пространствах, что тысячекратно раздвигает горизонты исследований, разработок и применения принципов оптимальной коррекции ошибок.

2. Эффект размножения ошибок (РО) при пороговом декодировании действительно очень сильно ограничивает возможности мажоритарных процедур декодирования. Но этот эффект вполне управляемый. Его правильная интерпретация помогает сформировать требования и критерии, по которым можно строить на основе оптимизационных процедур коды с очень малым уровнем размножения ошибок на выходе соответствующего им декодера, что и позволяет, в конечном счёте, чрезвычайно улучшить эффективность итеративных процедур мажоритарного типа.

Первое свойство оказывается, по существу, совершенно неожиданным. Но, действительно, после незначительной, но принципиальной модификации обычного порогового декодера, превращающей его в многопороговый (МПД), новый алгоритм на самом деле приобретает уникальное свойство стремления к оптимальному переборному решению, если выполнены весьма простые условия. В этом случае алгоритм при всех изменениях непрерывно измеряет расстояние между принятым вектором и текущим решением-гипотезой о переданном векторе. А это значит, что он на самом деле реализует процедуру поиска глобального экстремума (конкретно: минимума этого расстояния!) при действительно всего лишь линейной от длины кода, т. е. минимальной теоретически возможной сложности алгоритма. Представляется правдоподобным, что никакие другие известные в настоящее время методы коррекции ошибок не обладают подобными свойствами.

Новое понимание декодирования как поиска глобального экстремума подключает к теории кодирования совершенно грандиозное число теорий, методов и стилей, созданных различными теориями оптимизации для максимально быстрого поиска этого экстремума в предельно сложных условиях большого относительного уровня шума цифрового канала, но при использовании крайне простых мажоритарных алгоритмов.

А второе из приведенных выше утверждений заслуживает се-

рьёзного обоснования, что и сделано в одной из глав этой книги. Успешное решение этой сложной проблемы РО действительно позволило создавать коды, которые особенно эффективны при их применении именно в МПД. К этой проблеме не смог за 60 лет развития теории кодирования даже подступиться ни один научный коллектив в мире. Но научная школа ОТ сформулировала проблему размножения ошибок, создала полную его теорию и действительно создала программные комплексы, которые теперь строят для любых кодовых скоростей простые мажоритарно декодируемые коды с минимальным уровнем подверженности РО. На этих кодах МПД алгоритмы достигают оптимальных решений даже в непосредственной близости от границы Шеннона и при минимальной возможной сложности. Именно создание полной теории РО позволило проявиться всем достоинствам МПД алгоритмов в полном блеске.

Вся теория РО для обширного множества классов кодов достаточно полно представлена и прокомментирована во всех предыдущих монографиях нашей школы [2–5, 90, 94]. Ознакомиться с нашей новой содержательной постановкой проблемы РО в этих книгах очень полезно. Здесь же в связи с ограниченным объёмом книги и большим числом новых теоретических и прикладных достижений ОТ этот материал существенно сокращён в объёме. Но и в нём представлены абсолютно все необходимые выводы и рекомендации по созданию кодов с малой подверженностью воздействиям РО. Это позволяет специалистам решать все вопросы построения требуемых кодов, в том числе разрабатывать программные средства для их поиска. Большую помощь в решении этой задачи, которая в принципе не могла возникнуть за пределами ОТ, могут оказать и наши сетевые порталы. По всем вопросам применения тех или иных программных систем, созданных школой ОТ, можно обращаться и к автору этой монографии.

Планируемое издание нового справочника по современным методам кодирования также будет способствовать решению этих вопросов.

Представленное в данной книге ещё более системное, чем ранее, изложение методов и парадигм ОТ, а также новых результатов, полученных на их основе, позволяет, как надеется автор и члены его научной школы, составить общее глубокое понимание о состоянии исследований в сфере ОТ. Главным новым результатом ОТ, составляющим основу монографии, является давно уже ожидаемое достижение нашими МПД алгоритмами, ключевыми в теории ОТ, области в непосредственной близости от границы Шеннона для всех традиционных в теории кодирования цифровых каналов. Технологии достижения этого главного целевого для прикладной теории информации результата в книге описаны как целый ряд различных методов и под-

ходов, использующих в том числе и уникальные оптимизационные программные средства, которые действительно позволяют реально и просто, но очень аккуратно решать эту сложнейшую в идеологическом плане задачу на вполне приемлемом уровне технологической и алгоритмической сложности предлагаемых алгоритмов.

Подчеркнём, что преимущество ОТ перед другими алгоритмами определяется тем, что найдены простые и доступные всем методы исправления ошибок в кодах с мажоритарным декодированием при минимально возможной даже теоретически сложности, растущей с длиной кода всего лишь линейно. И при этом вероятности ошибки декодирования МПД алгоритмов оказываются практически такими же, как и у оптимальных переборных алгоритмов для этих же кодов, которые могут быть очень длинными. Кроме того, оба эти свойства для заданной кодовой скорости алгоритма МПД сохраняются даже в непосредственной близости относительного уровня шума канала к его пропускной способности. А поскольку корректирующие свойства хороших длинных кодов, которые строятся для МПД декодеров, растут с их длиной, то и оптимальное декодирование на базе методов ОТ характеризуется действительно достаточно малыми вероятностями ошибки, которые уже могут далее на много порядков уменьшаться разными простыми способами, например, каскадированием. Это означает, что инженеры связи получают мощные алгоритмы простой коррекции длинных кодов во всём диапазоне основных параметров систем кодирования для кодовой скорости, меньшей чем пропускная способность канала.

Необходимо лишь напомнить, что при обсуждении главных прикладных проблем теории кодирования редко упоминается о сложности самих вычислений, выполняемых при декодировании. Поэтому подчеркнём: именно в теории ОТ все алгоритмы работают только с небольшими целыми числами, что также очень сильно влияет на возможность простой реализации быстрых декодеров. Никакие другие достаточно эффективные алгоритмы за пределами ОТ не обладают этим свойством.

Если смотреть на результаты ОТ МПД чисто формально, то иногда возможно непонимание того, почему школа ОТ столь много внимания уделяет различным разработкам программного обеспечения (ПО). Объяснение этому может быть только одно, драматическое для ОТ и чрезвычайно трагическое для «прежней» теории кодирования. Главная прикладная цель теории кодирования — создание алгоритмов декодирования, наилучших по комплексному триединому критерию «помехоустойчивость — достоверность — сложность». И 60 лет бурных математических поисков «прежней» теории ясно показали, что

при большом уровне шума (!) ни один из параметров этого обобщённого критерия вообще ни для каких алгоритмов декодирования не может быть вычислен достаточно точно. Никогда! (Слабые и короткие коды с небольшой итоговой достоверностью тут не обсуждаются из-за их бесполезности). Но тогда это обстоятельство становится чётким доказательством того, что «та» теория потерпела полное фиаско, т. к., не зная точных значений этих важнейших параметров декодеров, обсуждать какие-либо другие свойства алгоритмов бессмысленно.

И, кстати, отметим, что характеристики алгоритмов ОТ по этому критерию нельзя вычислить тоже. Но школа ОТ осознала все эти фундаментальные свойства систем помехоустойчивого кодирования очень давно, в районе 1975 года. И начала сразу создавать множество разнообразных программных комплексов для проектирования, исследований параметров и настройки элементов декодеров для всех известных в теории каналов. Как нам кажется, за последние 50 лет к этой важнейшей масштабной и исключительно трудной и долгой работе пока не приступила ни одна научная группа в мире. А мы всё это создали и продолжаем разрабатывать ПО новейшего оптимизационного типа.

И что это даёт? Наши программные модели практически мгновенно дают ответ о значении всех параметров триединого критерия. Это открывает пути для многократного увеличения возможностей теории, которая, со своей стороны, помогает указать пути развития систем оптимизационного ПО, а программные средства, с другой стороны, обеспечивают ускорение проверки достижений теории и ориентируют теорию в выборе её новых целей. Как мы понимаем, нигде в мире никаких подобных исследовательских технологий пока нет ни у одной научной группы, имеющей отношение к прикладным вопросам теории кодирования.

И если в этот момент обратить внимание на то, что все три параметра триединого критерия у МПД декодеров уже давно имеют ещё и теоретически наилучшие возможные значения, то получаем, что ОТ действительно достигла полного решения проблема Шеннона и создала абсолютно лучшие по этому критерию алгоритмы. Отсюда уже понятно, что в этом случае нет никаких причин считать, что в обозримом будущем появятся методы, которые будут значительно лучше того, что предлагает связистам и теоретикам ОТ. Это верно просто потому, что существенно улучшить характеристики алгоритмов ОТ невозможно, т. к. МПД декодеры имеют даже теоретически наилучшие значения параметров этого комплексного критерия. А создавать реальные новые алгоритмы без хорошего ПО никто не смог до нас, и никто не сможет этого делать и после нас. Причину этого мы уже назвали: никакие параметры эффективных декодеров вычис-

лить, настроить и улучшить без хорошего ПО в принципе нельзя. Так что конкурентов у нас нет. И мы очень сожалеем о том, что нам просто не с кем обсуждать дальнейшие развитие прикладной теории кодирования.

Вот и всё, что касается лидерства ОТ и ценности хорошего оптимизационного ПО, тесно взаимодействующего с оригинальной тонкой теорией.

Все несомненно важные вопросы детального количественного сопоставления возможностей и свойств алгоритмов ОТ и других методов можно найти в наших новых обзорах по прикладным вопросам теории кодирования (посмотрите для этого также Приложение 3), в основных журналах по системам связи, в наших докладах на конференциях и на портале **www.mtdbest.ru**. Часть таких обзоров можно найти по ссылке [73] и далее по всем последующим пунктам в конце этой монографии.

Таким образом, алгоритмы ОТ характеризуются тем, что они по триединому жёсткому критерию «помехоустойчивость — достоверность — сложность» являются единственной группой кодов, которые в полной степени обладают и одновременно, и по отдельности всеми наилучшими возможными свойствами, указанными в этом критерии. А именно это и является основной целью создания алгоритмов декодирования для работы вблизи границы Шеннона.

Мы надеемся, что на многие естественные вопросы по проблеме сложности, эффективности и технологичности кодирования и многопорогового декодирования, а также по методам работы с новыми версиями АВ, которые продолжают тоже интенсивно развиваться и патентоваться школой ОТ, читатели этой книги получат достаточно содержательные ответы. В случае заинтересованности они, несомненно, смогут сами продолжить весьма перспективные для всех систем связи исследования МПД процедур, а также АВ, включая их блоковые версии, которые уже нашли свое место в целом ряде проектов.

Как будет показано далее, при создании новых алгоритмов и соответствующих им кодов основной задачей исследователей становится максимально аккуратное и оптимизированное по очень многим критериям одновременное проектирование декодера и применяемого в нём кода. Иначе говоря, простота реализации МПД достигается за счёт более сложных и тщательно организованных этапов проектирования кода и конкретных алгоритмов его декодирования по уже готовым технологиям. В этом случае проблема сложности реализации алгоритма целенаправленно трансформируется таким образом, чтобы технологические задачи построения более эффективного декодера решались именно за счёт тех компонентов сложности, увеличение которых

наиболее доступно или даже полезно.

Например, в абсолютном большинстве случаев минимизации вычислительных затрат МПД объём его операций декодирования при хорошей эффективности оказывается на 2–3 десятичных порядка меньшим, чем для других алгоритмов именно за счёт значительного объёма памяти декодера, использующего весьма длинные коды. Понятно, что это иногда совершенно необходимо в высокоскоростных системах связи при большом уровне шума. Подчеркнём ещё раз то, что и вблизи пропускной способности канала алгоритмы МПД сохраняют реальную умеренную сложность, вполне доступную современным технологиям, тогда как прочие методы почти всегда оказываются в этой области параметров вообще неработоспособными.

И снова напомним, что ближайшие окрестности границы Шеннона могут быть достигнуты только в случае применения и эффективного декодирования очень длинных кодов.

Внимательный читатель, конечно, отметит, что многие свойства и возможности представленного в книге алгоритма МПД и других методов, относящихся к теории ОТ, как и в ранее изданных монографиях, многократно рассматриваются и комментируются в различных разделах книги с разных позиций. Автор признаёт, что это действительно так. И в данной монографии (как и в предыдущих) это тоже сделано с единственной целью наиболее полного, всестороннего и в то же время максимально понятного доказательства или объяснения не очень обычных свойств и возможностей многопороговых декодеров, различных модификаций алгоритма Витерби (АВ), Основной Теоремы многопорогового декодирования (ОТМПД) и многих новых парадигм ОТ. Такой способ изложения материала диктуется тем, что, хотя все ключевые результаты получены очень простыми методами, многие из них всё же не использовались ранее в публикациях по теории кодирования и являются для этой отрасли науки совершенно новыми. Это требует очень аккуратного и постепенного предъявления во многих случаях не совсем простых и иногда даже неожиданных результатов, свойств и характеристик наших алгоритмов. Разнообразные комментарии и формы изложения материала, как нам представляется, облегчают читателю задачу понимания представленных в книге результатов, для усвоения которых иногда всё-таки требуются немалые усилия и время.

Определённую, как мы думаем, немалую поддержку таким усилиям читателей окажут информационно-справочные и научно-методические материалы наших крупнейших в мире двуязычных сетевых порталов по теории кодирования, МПД алгоритмам и ОТ: **www.mtdbest.ru** и **www.mtdbest.iki.rssi.ru**. Первый из них достаточ-

но часто обновляется. Теперь на них не только размещены многие демо-программы по наиболее известным в мире алгоритмам коррекции ошибок, но и наши новые программные платформы. Читатели могут переписать на свои компьютеры эти удобные программные средства исследования МПД или АВ, а затем сразу же начать исследовательскую работу по мажоритарным алгоритмам, свёрточным АВ и по блоковым модификациям АВ (БАВ), меняя в случае необходимости и сами коды, изучая характеристики алгоритмов декодирования в весьма широких пределах, вполне соответствующих всем традициям полноценной научной работы. Достоинства такого подхода к предварительным исследованиям по ОТ уже смогли подтвердить и наши зарубежные коллеги, которые высоко оценили новые возможности, предоставляемые нашими программными платформами для более близкого знакомства с ОТ и её парадигмами, алгоритмами и технологиями. Подчеркнём снова, что использование таких программных платформ позволяет существенно расширить область параметров, которыми теперь можно управлять в экспериментах по декодированию, в том числе и самими кодами, которые стало возможным менять по желанию экспериментатора.

Опыт издания нашего справочника по кодированию [1] показывает, что он также весьма полезен многим студентам, аспирантам и специалистам. Автор надеется, что следующее издание существенно обновлённого справочника при всех текущих трудностях всё же скоро будет реализовано.

Очень способствует, как оказалось, правильному восприятию основ ОТ небольшой цветной буклет-комикс [90] ведущих авторов нашей научной школы об ОТ. Он подготовлен с использованием эмоциональных компонент восприятия весьма неожиданной (хотя и очень простой!) для всех теории. Такой подход, как и просмотр стартового мультфильма (см. далее), очень помогает дальнейшему процессу более глубокого изучения ОТ.

В качестве последнего замечания автор считает необходимым подчеркнуть, что все исходные предпосылки исследования, теоретические результаты, вытекающие из них практические следствия и выводы по-прежнему чрезвычайно просты. Они связаны только с самыми базовыми общепринятыми понятиями теории вероятностей, теории и прикладной тематики помехоустойчивого кодирования и не требуют знаний специальных разделов других сложных дисциплин. Именно эта возможность взглянуть на потенциальные возможности кодов и мажоритарных процедур, исходя только из самых простейших теоретических соображений и здравого смысла, создаёт условия для очень быстрого обучения студентов и специалистов новым возможностям

техники кодирования на основе МПД алгоритмов, простых методов достижения оптимальных решений на основе реализации поиска глобального экстремума, а также с использованием возможностей блоковых модификаций АВ. При этом остаётся крайне важным и полезным, что и МПД декодеры на базе мажоритарных процедур, и все модификации АВ уже много десятилетий хорошо известны научным работникам и инженерам, что хорошо помогает пониманию всех особенностей и тонкостей достижений ОТ — нашей «квантовой механики» теории информации.

Отметим также, что достаточно быстро просмотреть эту книгу, чтобы выразить сильное удивление от того, что в ней весьма немного формул. Но все необходимые выражения, позволяющие оценивать параметры всех кодов, декодеров и каналов, рассматриваемых в прикладной теории кодирования, в ней есть. Это обстоятельство особенно выразительно подчёркивает краткость, совершенство и информационную наполненность монографии, которую наша научная школа рекомендует читать вдумчиво и постепенно. Как отмечали некоторые специалисты при чтении рукописи монографии, глубокая философская сущность ОТ, которая уже очень давно вернула содержательную прикладную теорию кодирования на правильный путь (чего, может быть, не смогли увидеть за много прошедших десятилетий некоторые научные сотрудники, которые пишут статьи «про коды»!), заслуживает действительно очень аккуратного изучения и столь же глубокого понимания.

Так что теория кодирования — вовсе не математическая задача! Никаких главных характеристик систем кодирования при большом относительном уровне шума нельзя вычислить, причём, видимо, никогда! Та уже ушедшая теория не смогла смириться с этим. Она в реальности давно и полностью покинула огромное плодотворное поле этой отрасли науки. Судя по всему, эта прикладная и одновременно, конечно, истинно фундаментальная проблема полностью и надолго перешла в сферу интересов и достижений ОТ, т. к. успешно и полностью ею решена на базе теорий поиска экстремума функционалов, тесно взаимодействующих с интеллектуальным инновационным программным обеспечением (ПО). А поскольку ОТ создала алгоритмы со всеми самыми наилучшими возможными параметрами декодирования по триединому критерию и действительно решила проблему Шеннона, то совершено естественно, что возвращение в реальную прикладную теорию кодирования на абсолютно новом уровне простейших мажоритарных схем и известнейшего алгоритма Витерби с его различными модификациями — это факт. Мы уверены, что эта ситуация закрепилась в теории информации на весьма долгий срок!

Автор считает своим приятнейшим долгом поблагодарить всех членов нашей научной школы, многолетняя активная работа которых создала возможность написания этой книги, моего особо надёжного и всё понимающего коллегу — заведующего кафедрой РГРТУ, д.т.н., проф. Г.В. Овечкина, и воистину огромное количество наших помощников, энтузиастов и просто высокопрофессиональных специалистов, которые в течение многих лет участвовали в проведении исследований и применении полученных результатов в конкретных системах и проектах.

Большую поддержку работам по МПД и ОТ оказывали факультет ФРТК МФТИ, Научный совет по комплексной проблеме «Кибернетика» АН СССР, ОНИТ РАН, НИИ «КВАНТ», НИИ Радио, Воронежский НИИ связи, ЛЭИС им. М.А. Бонч-Бруевича, ИКИ РАН и Рязанский ГРТУ.

Значительную финансовую поддержку неоднократно оказывал нашим исследованиям Российский фонд фундаментальных исследований (РФФИ). При его участии наша школа смогла также издать целый ряд своих монографии и справочник по кодированию.

Наверное, пятидесятилетние исследования МПД не могли бы быть представлены в своём нынешнем виде, если бы не поддержка академиков АН СССР А.И. Берга и В.А. Котельникова, академиков РАН В.К. Левина, Н.А. Кузнецова и Л.М. Зелёного, члена-корреспондента РАН Ю.Б. Зубарева, профессоров Э.М. Габидулина, С.И. Самойленко, Ю.Г. Дадаева, В.И. Коржика, А.Н. Пылькина, В.В. Витязева, докторов технических наук С.В. Аверина и Р.Р. Назирова, которые высоко оценили представленные материалы исследований или участвовали в работах по исследованиям наших алгоритмов и очень способствовали их признанию научно-технической общественностью.

* * *

Для получения наглядного представления об эффективности работы МПД читателям предлагается небольшой демонстрационный мультфильм-программа, предназначенный для работы на IBM PC-совместимом компьютере под управлением ОС Windows, в котором проиллюстрированы важнейшие особенности процедур декодирования многопорогового типа при исправлении ошибок в условиях большого уровня шума двоичного симметричного канала. По опыту издания ряда предыдущих книг по тематике МПД и ОТ именно такая небольшая предварительная подготовка психологического плана с помощью предлагаемой демо-программы создаст необходимые эмоциональные и гносеологические предпосылки для плодотворной последующей работы с этой книгой над нашими новыми алгоритмами.

Предлагаемый цветной мультфильм с детальной инструкцией пользователя показывает главную особенность работы МПД алгоритма для относительно длинного кода с малым уровнем размножения ошибок: строгое уменьшение расстояний последовательности его решений до принятого вектора при каждой коррекции контролируемых символов, т. е. иллюстрирует справедливость нашей ОТМПД — Основной Теоремы многопорогового декодирования, исходного ключевого пункта всей Оптимизационной Теории.

Инструкцию по работе с демонстрационной программой и сам мультфильм можно переписать со специализированного двуязычного портала ИКИ РАН **www.mtdbest.iki.rssi.ru** на странице описания методов МПД или с аналогичного портала РГРТУ — **www.mtdbest.ru**. При копировании этих файлов с портала РГРТУ сначала надо переписать и прочесть описание[1] работы с демонстрационной программой[2], которая затем очень просто запускается.

Там же можно найти наши многочисленные обзоры по прикладным вопросам теории кодирования, самую разнообразную дополнительную оперативную информацию по МПД алгоритмам, учебно-методические материалы, большое количество статей, книг и презентаций по ОТ, её парадигмам и технологиям, а также по алгоритму Витерби и его новым модификациям, дивергентному декодированию и другим вопросам. Там же находятся файлы программных платформ для различных типов декодеров, работающих в соответствующих им каналах. Эти платформы сразу позволяют непосредственное их использование для начала исследований по тематике ОТ.

Краткий обзор ситуации в теории кодирования есть также в Приложении 3 этой монографии.

Целый ряд рисунков в книге является слайдами из нескольких презентаций и других публикаций.

Данная монография очень скоро будет размещена на одном из сайтов нашей научной школы ОТ, возможно, на **www.mtdbest.ru** или даже на каком-то ещё одном нашем новом портале. Следите за новостями!

Целый ряд проблем, относящихся к общим постановкам задач кодирования и конкретным возможностям МПД алгоритмов, также рассмотрены на наших порталах в разделах ответов на вопросы, которые позволяют более точно и образно оценивать возможности систем кодирования на основе алгоритмов МПД и АВ.

Там же представлена переписка с редакциями научных журналов,

[1] https://mtdbest.ru/articles/demoop_apr4.pdf
[2] https://mtdbest.ru/program/mtddemo.zip

что тоже помогает понять условия развития исследований в сфере ОТ.

Значительную поддержку в изучении методов декодирования на основе МПД алгоритмов нашим читателям могут оказать также три очень полезные лабораторные работы, которые можно переписать с образовательных страничек («Обучение») наших сетевых ресурсов, указанных выше (файл **labrus.zip**[3]), распаковать их и предложить радиотехническим кафедрам ВУЗов для студентов и системы профессиональной переподготовки специалистов в области телекоммуникаций.

Дополнительные сведения по многопороговым декодерам и другим полезным методам коррекции ошибок можно найти в нашем справочнике [1] и в монографиях [2–5, 94], а также в изданиях для широкого круга студентов, аспирантов и специалистов по системам связи [79, 90, 91]. Самые новые публикации можно найти по ссылке [73] и на последующих позициях ссылок на литературу в конце этой монографии.

Ваше мнение о книге и предложения по её улучшению направляйте по адресу: Россия, 117997, г. Москва, ул. Профсоюзная, д. 84/32, ИКИ РАН, в.н.с. отдела 71, В.В. Золотарёву, а также на электронную почту автора **zolotasd@yandex.ru**.

Автор В.В. Золотарёв

12.10.2020 г.

[3] http://www.mtdbest.iki.rssi.ru/labrus.zip

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 вносится теорией помехоустойчивого кодирования, создающей всё новые методы защиты от ошибок, базирующиеся на использовании корректирующих кодов.

Возможность использования тех или иных алгоритмов коррекции ошибок в системах без обратной связи, где нельзя организовать переспрос или он возможен достаточно редко, определяется весьма жёсткими 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, свидетельствует об огромной сложности и чрезвычайной актуальности проблемы эффективного декодирования.

Данная книга посвящена новому этапу развития Оптимизационной Теории помехоустойчивого кодирования и создаваемым на её основе методам коррекции ошибок в цифровых данных на базе итеративных мажоритарных алгоритмов декодирования, к которым последнее время вновь привлечено внимание специалистов в области систем связи. Новое состояние теории кодирования основано на технологиях и идеологии ОТ, а также на достижении во всех основных типах каналов с независимыми искажениями уровня помехоустойчивости, соответствующего непосредственной близости к границе Шеннона, т. е. простому высокодостоверному декодированию в таких каналах при кодовой скорости R, близкой к пропускной способности канала C: $R \lesssim C$.

Подчеркнем, что реализация высокоэффективных алгоритмов вблизи границы Шеннона требует использования только длинных ко-

дов и сложности декодирования, которая должна расти с увеличением длины кода не более чем линейно. Именно такими и оказываются МПД декодеры и другие методы на их основе, представленные в данной книге. Но достижение алгоритмами МПД решений оптимального (переборного!) декодера при линейной от длины кодов сложности их реализации полностью исключает из дальнейшего конкурса алгоритмов все процедуры, основанные на методах алгебраической теории кодирования, т. е. коды БЧХ и коды Рида — Соломона (РС), а также последовательные процедуры для свёрточных кодов. Видимо, это же относится и к некоторым последним «новым» достижениям теории кодирования — полярным и другим кодам, если они не предъявят, наконец, достаточно содержательные результаты по реальной сложности и эффективности предлагаемых ими алгоритмов декодирования. Это дополнительно повышает важность достижений ОТ.

Мажоритарные декодеры рассматривались ранее как в классических монографиях Л.Ф. Бородина [7], Дж. Месси [8], В.Д. Колесника и Е.Т. Мирончикова [9], Л.М. Финка [62], так и в книгах [10—12], изданных позднее. Существенным достоинством порогового (мажоритарного) декодирования оказалась возможность эффективного многократного улучшения решений этого декодера, которая была доказана, в частности, ещё в 1981 г. в коллективной монографии издательства «Наука» [2] на примере систематических свёрточных кодов.

Данная книга посвящена изложению различных новых аспектов Оптимизационной Теории помехоустойчивого кодирования и 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.

Основными целями предпринятого теоретического и экспериментального исследования, изложенного в данной книге, являлись

- теоретическое обоснование методов многопорогового декодирования линейных кодов, сопоставимого по эффективности с лучшими известными алгоритмами;
- анализ специальных методов кодирования с использованием парадигм ОТ и МПД, эффективно работающих вблизи пропускной способности.

Структурно монография состоит из шести глав. В первой главе введены основные понятия и определения, используемые в последующих разделах. Здесь же представлены базовые сведения по обычным пороговым декодерам (ПД) для двоичных и символьных кодов.

Во второй главе сформулированы основные принципы многопорогового декодирования для двоичных симметричных каналов, доказано стремление решений декодеров этого типа к решению оптимального декодера и указано на природу МПД алгоритма как на реализацию процедуры глобальной оптимизации функционала от большого числа переменных для частного случая дискретных математических пространств. Затем этот принцип роста правдоподобия решения МПД обобщается на двоичные гауссовские каналы при использовании «мягких» модемов, недвоичные и несистематические коды, а также на каналы со стираниями. В конце главы рассмотрены предельные возможности МПД различных типов и проблема размножения ошибок при мажоритарном декодировании, решение которой позволило многократно улучшить характеристики МПД и других связанных с ними методов.

В третьей главе на основе публикаций самого последнего времени предъявлены наиболее важные результаты по алгоритмам ОТ, включая конкретные характеристики этих алгоритмов в непосредственной близости от границы Шеннона. Материалы этой главы имеют большую самостоятельную ценность, т. к. все разделы этой главы являются законченными опубликованными работами и характеризуются очень высокой информационной плотностью излагаемого материала. Поэтому при глубокой идеологической связи этой главы с содержанием остальных частей монографии все её разделы полностью автономны, как и отдельные для каждой из них списки использованной литературы. Мы полагаем, что это окажется удобным и читателям книги, которые могут без обращения к её другим главам или иным публикациям полностью понять содержание этих самостоятельных статей-параграфов. Разумеется, ссылки на литературные источники за пределами третьей главы являются сквозными для всей книги, что соответствует сложившимся традициям.

В четвёртой главе описаны результаты, полученные с учётом новых парадигм ОТ, которые позволяют дополнительно повысить эффективность оптимизационных процедур, используемых для поиска решений оптимального декодера. Детально рассмотрены вопросы эффективности декодирования, которые и определили передачу ОТ от классической теории лидирующей роли в создании прикладных методов в этой сфере теории информации.

Пятая глава посвящена изложению основных потенциально перспективных методов, средств, систем и технологических приёмов, которые смогут ещё более повысить эффективность работы алгоритмов ОТ в ближайшем будущем. Эта глава очень важна для понимания необходимого технологического уровня, которого надо достичь для

успешного дальнейшего развития исследований МПД, АВ, дивергентного кодирования и прочих методов ОТ. Только в этом случае можно в дальнейшем достичь новых результатов в этой области. Полная неизбежная смена технологического и идеологического обеспечения исследований теории кодирования в области глобальной оптимизации функционалов уже состоялась. Сейчас только этот подход является фактически единственным средством оптимального декодирования длинных кодов вблизи границы Шеннона, что и определяет текущие возможности развития прикладных методов всей теории кодирования.

В шестой главе кратко рассмотрены перспективы новой теории, которые, как мы предполагаем, будут гораздо более масштабными, чем их описал автор.

В заключении сформулированы обобщающие выводы по проведенному исследованию.

Предполагается, что наши читатели знакомы с теорией вероятности, основами теории кодирования и базовыми методами 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 данной монографии именно на понимании свойств и возможностей изучаемых многопороговых алгоритмов и на реализации различных идей оптимизации функционалов, что, несомненно, поможет заинтересованным читателям хорошо сориентироваться в современной проблематике построения систем помехоустойчивого кодирования и с максимальной степенью уверенности выбирать пути дальнейшего повышения эффективности таких систем.

Обращаем внимание наших читателей, что в связи с ограниченным объёмом книги многие разделы изложены очень кратко, а некоторые темы, которые излагались в других наших публикациях, сокращены или опущены. При этом мы старались сделать все необходимые ссылки и краткие комментарии по поводу отсутствующего в этой книге материала. Такой подход позволил нам сосредоточиться на изложении только самых новых результатов, некоторые из которых, возможно, ещё не опубликованы достаточно полно даже в статьях по тематике ОТ. Таким образом, знакомство с вопросами итеративного многопорогового декодирования как с проблемой оптимизации специфических для теории кодирования функционалов мы старались сделать по возможности более понятным и точным.

Дополнительные информационные, научные и учебно-методические материалы по ОТ и МПД алгоритмам можно найти на специализированном веб-сайте ИКИ РАН www.mtdbest.iki.rssi.ru и на нашем постоянно обновляемом аналогичном портале РГРТУ www.mtdbest.ru.

Напоминаем также, что для более глубокого изучения ОТ, МПД декодеров, алгоритмов Витерби в их различных модификациях и каскадных схем с использованием кодов контроля по чётности (ККЧ) мы увеличили в книге количество конкретных ссылок на демо-программы этих алгоритмов, которые также можно найти на наших порталах. Обращение к наглядным примерам, которые характеризуют те или иные теоретические результаты одновременно и в практической плоскости, обычно помогает быстрее и глубже понимать оптимизационный характер абсолютно всех эффективных алгоритмов декодирования как для двоичных, так и для символьных кодов.

В данной монографии, как это можно видеть, не очень много ссылок на работы по ОТ и МПД алгоритмам, хотя самые обязательные, конечно, указаны. Гораздо большее число ссылок, включая дополнительную литературу по этой тематике есть в [3–5, 36–38]. Многие недавние публикации нашей научной школы можно найти на ресурсах [40].

Возможно, что эта обобщающая монография по ОТ, методам поиска глобального экстремума функционалов и многопороговым алгоритмам, успешно работающим непосредственно вблизи границы Шеннона, использующая простые, но иногда совершенно новые для «классической» теории кодирования парадигмы, технологии и подходы, вызовет у специалистов определённые вопросы и окажется не лишённой определённых недостатков. Автор полагает, что новые публикации нашей научной школы по тематике ОТ существенно сгладят эти недочёты.

Глава 1

Основы теории кодирования и мажоритарных алгоритмов

1.1. Линейные коды

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

$$\overline{A} = \overline{I}G. \tag{1.1}$$

Заметим, что здесь и далее операции умножения и сложения выполняются в поле $\mathrm{GF}(q)$. При $q = 2$ код называется *двоичным*. Если же $q > 2$, то код *недвоичный*.

Мы уже отмечали, что наше очень краткое введение в проблематику кодирования затрагивает не все полезные понятия, соотношения и свойства кодов. Вместе с тем мы не будем использовать сложные, хотя, может быть, и важные свойства дискретных пространств. Многие дополнительные особенности кодов, также полезные для понимания идей мажоритарных схем декодирования, можно найти в [3, 4, 8] или в нашей англоязычной монографии [5], изданной Международным союзом электросвязи.

Важную роль в оценке возможностей кодов играют кодовая скорость $R = k/n$, $0 < R < 1$, и минимальное кодовое расстояние d.

Расстоянием Хемминга между двумя векторами одинаковой длины называется число символов, в которых они отличаются. Корректирующие возможности кода в значительной мере определяет *минимальное кодовое расстояние* d. Оно определяется как минимальное по всем парам кодовых слов $(\overline{A}_i, \overline{A}_j)$, $i \neq j$, расстояние между кодовыми векторами (допустимыми сообщениями) для данного кода.

Если первые k символов в кодовом слове $\overline{A}$ совпадают с вектором $\overline{I}$, 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

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

Для технической реализации систем кодирования весьма полезен тот факт, что в поле $\mathrm{GF}(q)$ сумма двух кодовых слов линейного кода также всегда является кодовым словом. Это позволяет при кодировании обходиться весьма простыми схемами. На рис. 1.1,а представлен кодер двоичного систематического кода, состоящий из k ячеек памяти для входной информации и $(n-k)$ многовходовых сумматоров по модулю 2 (полусумматоров). Заметим, что если все ячейки памяти рассматривать как байтовые или ещё большего размера, а вместо полусумматоров подразумевать, например, использование сумматоров по $\bmod q$, $q > 2$, то представленная схема превращается в кодер недвоичного (q-ичного) линейного блокового кода. В той же мере это относится и к примеру кода на рис. 1.1,б.

На рис. 1.1,б изображен кодер двоичного систематического блокового кода, соответствующий порождающей матрице вида

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

Этот кодер содержит регистр сдвига на 3 бита и один двухвходовый полусумматор. В трёх информационных ячейках находятся данные, подлежащие кодированию. В этом положении на выходе полусумматора формируется первый из трёх 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* [3–5, 13]. В линейном коде минимальное кодовое расстояние d равно минимальному весу ненулевого кодового слова. Если полагать, что операции с матрицей G проводятся в группе по сложению, например, по $\bmod q$, то она стано-

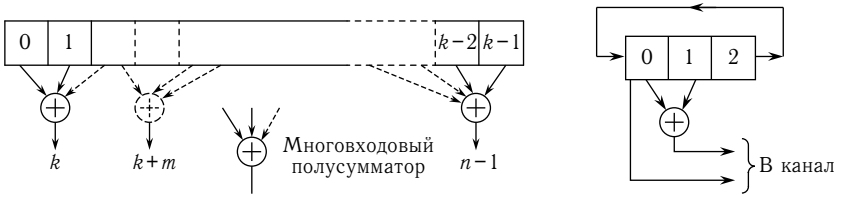

Рис. 1.1. Общий вид кодера двоичного систематического линейного блокового кода (*а*); кодер систематического квазициклического блокового кода с $R = 1/2$, $n = 6$, $d = 3$ (*б*)

вится порождающей матрицей для q-ичного линейного кода.

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

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

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

$$\overline{A} = \overline{I}G, \tag{1.3}$$

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

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, $0 \leqslant j < k_0$, не равен нулю.

Обеспечение максимальной помехоустойчивости возможно при полной реализации потенциальных возможностей используемых кодов. В этом случае корректирующие возможности свёрточного 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 d и d_f одновременно являются и минимальными весами ненулевых кодовых слов. Как следует из определений, всегда справедливо неравенство $d \leqslant d_f$.

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 $H = (P^T : I_{n-k})$. В случае свёрточных кодов с фиксированными связями начальная часть подматрицы P^T превращается в совокупность треугольных матриц, полностью определяющих код.

На рис. 1.2,а представлен пример кодера для двоичного систематического свёрточного кода с $R = 1/2$, $d = 5$ и длиной кодового ограничения $n_A = 14$, заданного порождающим полиномом

$g(x)=1+x+x^4+x^6$. Параметр n_A определяет интервал последовательности свёрточного кода, в пределах которого информационные символы кода влияют на кодовую последовательность. На каждом такте работы кодера в регистр сдвига поступает один информационный символ, который передается в канал вместе с проверочным символом с выхода четырёхвходового полусумматора. Этому коду соответствует проверочная матрица

$$H=\left(\begin{array}{ccccccc:c}
1 & & & & & & & \\
1 & 1 & & & & & & \\
0 & 1 & 1 & & & & & \\
0 & 0 & 1 & 1 & & & & I \\
1 & 0 & 0 & 1 & 1 & & & \\
0 & 1 & 0 & 0 & 1 & 1 & & \\
1 & 0 & 1 & 0 & 0 & 1 & 1 & \\
\multicolumn{7}{c:}{\cdots\cdots\cdots\cdots\cdots} &
\end{array}\right). \qquad (1.4)$$

Отметим, что подмножество 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 подмножества. Это свойство, согласно Месси, обеспечивает для такого кода минимальное расстояние $d=5$ и, следовательно, возможность исправлять любые две ошибки в начальной части длины n_A сообщения, закодированного свёрточным кодом.

В случае использования несистематических кодов в кодовом слове нельзя выделить информационную часть сообщения. Важно, что

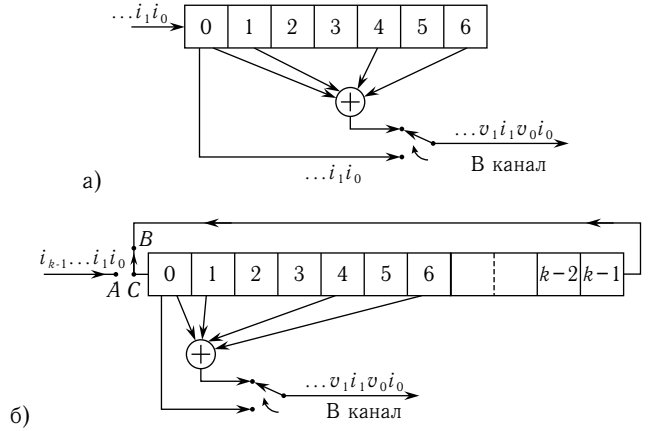

Рис. 1.2. *а* — кодер свёрточного самоортогонального кода с $R=1/2$, $d=5$, $n_A=14$; *б* — преобразование этого кодера в квазициклический блоковый кодер

в таких свёрточных кодах корректирующая способность оказывается существенно более высокой, чем в систематических.

При декодировании кода можно его проверочную матрицу умножить на принятый из канала вектор $\overline{Q} = \overline{A} + \overline{E}$, 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. В рассматриваемой проверочной матрице (1.4) множество компонент s_j синдрома $\overline{S}$, содержащих в качестве слагаемого ошибку e_0 в первом информационном символе i_0, будет иметь вид

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

Это множество проверок, благодаря отмеченному выше свойству матрицы H, содержит как в информационных, так и в проверочных символах (помеченных в выражениях (1.5) 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.

Отметим также, что возможно и более компактное описание блоковых и свёрточных СОК, используемое далее. Из вида матрицы (1.4) 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 рассмотренного примера определяет и свёрточный, и блоковый коды. Причём длина блокового кода должна быть не менее 26 (в общем случае $2n_A - n_0$), что необходимо для сохранения самоортогональности.

1.2. Единство блоковых и свёрточных кодов

Единство свойств блоковых и свёрточных кодов установлено уже достаточно давно [15, 16] и было дополнительно рассмотрено в [17]. Более детально для целей данной книги этот вопрос рассмотрен в [3–5], и напомним, что полиномы известных самоортогональных блоковых кодов [13] могут быть, наоборот, использованы в свёрточных кодах, причём длина кодового ограничения свёрточного кода n_A будет не больше, чем длина n исходного блокового СОК.

Укажем ещё на важную особенность использования свёрточных кодов, которую мы будем учитывать при обсуждении методов декодирования. Если свёрточным кодом передавать сообщения конечной длины, то для сохранения его корректирующих возможностей и при передаче последних символов сообщения необходимо в конце каждого такого сообщения введение $(n_A R - k_0)$ нулевых информационных символов. Такая процедура ресинхронизации превращает код в блоковый с особой «диагональной» структурой, когда ненулевые символы проверочной матрицы сосредоточены вблизи диагонали в той её части, которая умножается на информационные символы принятого сообщения, как показано на рис. 1.3.

$$H = \left(\begin{array}{cccccccc:c}
1 & & & & & & & & \\
1 & 1 & & & & & & & \\
0 & 1 & 1 & & & & & & \\
1 & 0 & 1 & 1 & & & & & \\
 & 1 & 0 & 1 & 1 & & & : & I \\
 & & 1 & 0 & 1 & 1 & & & \\
 & & & 1 & 0 & 1 & & & \\
 & & & & 1 & 0 & & & \\
 & & & & & 1 & & &
\end{array}\right)$$

Рис. 1.3. Формирование блокового кода со скоростью R_W усечением свёрточного кода с R_0, $R_W < R_0$.

Укажем на существенное обстоятельство при таком превращении свёрточного кода в блоковый. Как видно из представленного рисунка, для систематического свёрточного кода с $R_0 = 1/2$ с порождающим полиномом (пишем только показатели при ненулевых степенях) $P = (0, 1, 3)$, при усечении он в данном конкретном варианте превращается в блоковый код с таким же, как у свёрточного кода, минимальным расстоянием $d = 4$. Но его кодовая скорость уже равна $R_W = 6/18 = 1/3$, что, конечно же, очень важно. В пределе для достаточно длинного случайного кода с хорошими корректирующими способностями те близкие к оптимальным возможности получивше-

гося блокового кода будут соответствовать именно коду с $R_W < R_0$. При изменении места усечения скорость блокового кода может быть и большей, но она всегда останется меньшей, чем скорость исходного свёрточного кода с $R_0 = 1/2$.

Для нашего дальнейшего изложения важно, что при достаточно большом уровне шума при правильном завершении передачи сообщения теперь уже усечённым свёрточным кодом, хорошим по вероятности ошибки декодирования, сообщение оказывается закодированным и столь же хорошим блоковым кодом. При этом всегда оказывается, что в этом случае длина свёрточного кода n_A существенно меньше той задержки, которая необходима для того, чтобы наилучший оптимальный декодер мог выносить наиболее правдоподобное, самое правильное по вероятности ошибки решение при использовании свёрточного кода. Это означает, что в области большого уровня шума при сопоставимых уровнях эффективности наилучших методов декодирования задержки в принятии решения у свёрточных и блоковых кодов будут также одного порядка, хотя длина n_A свёрточного кода может быть совсем небольшой относительно длины получившегося блокового кода, который при этом будет ещё иметь и меньшую кодовую скорость R. Это давно известное соотношение между главными кодовыми структурами детально рассмотрено в [15, 16] в терминах функций надёжности.

Указанные свойства кодов случайной структуры не могут непосредственно переноситься на коды с мажоритарным декодированием, которые мы и будем далее в основном рассматривать. Однако несомненно, что по мере продвижения в область больших шумов мы увидим, что длины блоковых кодов при использовании достаточно эффективных мажоритарных алгоритмов декодирования будут быстро расти, а при реализации свёрточных кодов с ростом уровня шума канала будет резко увеличиваться задержка декодирования, что для алгоритмов мажоритарного типа может выражаться в очень быстром возрастании числа необходимых итераций (многократных попыток) декодирования. Таким образом, большая задержка при декодировании свёрточных кодов с уменьшением энергетики шумящего канала должна рассматриваться как проявление глубоких фундаментальных свойств кодовых структур при реализации на их основе процедур глобального поиска экстремума.

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 со-

общений 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. Модель такого двоичного симметричного канала без памяти (ДСК) (рис. 1.4) достаточно хорошо соответствует многим высокоскоростным высокочастотным каналам спутниковой и космической связи [1, 18, 19], например, с системой фазовой модуляции ФМ-2, что придает особенную ценность результатам, полученным в этой области, хорошо изученной теоретически.

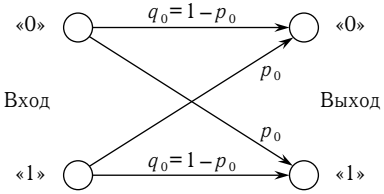

Рис. 1.4. Модель двоичного симметричного канала с квантованием выходного сигнала на $M = 2$ уровня, жёсткий модем

Достаточно часто оказывается, 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 или с другими системами модуляции. Поэтому излагаемые далее многие из результатов исследований относятся, в основном, к каналам, в которых действует аддитивный белый гауссовский шум (АБГШ), воздействующий на информацию, передаваемую, например, по спутниковым каналам связи.

В канале с АБГШ можно использовать не только жёсткие модемы, которые образуют цифровой канал без памяти типа ДСК и принимают решение «0» или «1» о принятых двоичных символах. Можно потребовать, чтобы модем был мягким, т. е. не только принимал двоичные решения, но и оценивал их надежность. При этом выходной сигнал уже будет квантоваться на $M = 4$, 8 или 16 уровней, а решения модема становятся, например, последовательностями из двух, трёх или четырёх битов, как показано на рис. 1.5 для $M = 4$. Использование мягких решений модема для декодеров оказывается чрезвычайно полезной возможностью, поскольку при этом повышается пропускная способность канала связи [1, 19] — важнейший параметр, определяющий потенциальные возможности кодовых схем. Это, в свою очередь, позволяет декодировать принятые цифровые потоки

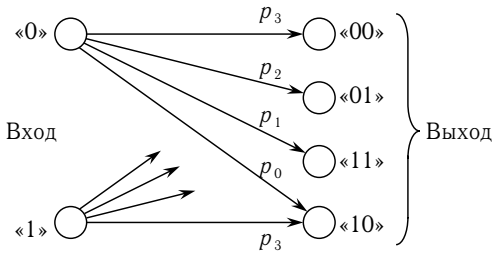

Рис. 1.5. Модель двоичного симметричного гауссовского канала с квантованием выходного сигнала на $M = 4$ уровня, мягкий модем

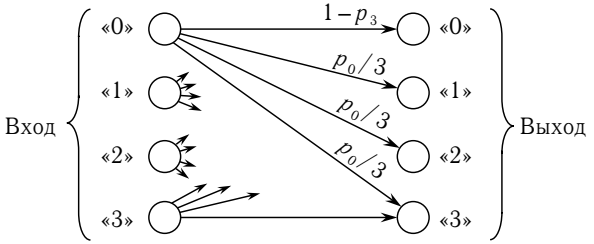

Рис. 1.6. Модель q-ичного симметричного канала, $q = 4$

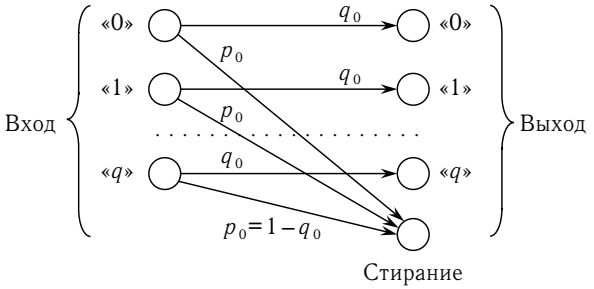

Рис. 1.7. Модель q-ичного симметричного стирающего канала, СтСКq

более эффективно по сравнению с обычным жёстким модемом, если алгоритмы коррекции ошибок предусматривают удобный способ учёта надежности принимаемого двоичного потока. Например, переход к $M = 16$ в двоичном канале с АБГШ позволяет обеспечить с помощью декодирования по алгоритму Витерби [1, 19, 20] высокую эффективность кодирования при уровне шума, примерно на 2 дБ более высоком по сравнению с жёстким модемом, когда $M = 2$. Именно это резкое увеличение энергетической эффективности при фактическом сохранении той же сложности АВ и создает условия для широкого использования мягких модемов в системах высокоэффективной цифровой связи.

Следующий важный класс каналов соответствует передаче q-ичных ортогональных сигналов. Модель данного канала для $q=4$ представлена на рис. 1.6. В этом случае при передаче каждого q-ичного символа, независимо от других, на приемной стороне с вероятностью $1-p_0$ происходит его правильное определение и с вероятностью $p_0/(q-1)$ принимается то или иное ошибочное решение о его значении. Все ошибочные решения в этом случае оказываются естественным образом равновероятны. Такие каналы мы будем в дальнейшем называть *q-ичными симметричными* и сокращенно обозначать QCK.

В случае симметричного канала с независимыми стираниями при любом основании q (рис. 1.7) 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.

О более сложных системах сигналов можно прочесть во многих книгах, например в [1, 3, 4].

1.4. 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. Её 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.А. Котельникова [21] и К. Шеннона [14] показало специалистам в области связи, на каких путях можно обеспечить повышение качества передачи. Это позволило довольно быстро пройти непростой путь от первых простейших кодов до важнейших алгебраических кодовых конструкций типа блоковых кодов Боуза — Чоудхури — Хоквингема (БЧХ) [23, 24]. С ними наступил период конструктивного развития теории помехоустойчивого кодирования, в которой сначала были доказаны только интереснейшие теоремы существования. 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 известнейшего американского специалиста Дж. Месси [8, 25]. Пороговые (мажоритарные) методы были тогда 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 комбинаторными и вероятностными методами построения и оценки характеристик кодов, которые не использовали алгебраическую теорию кодирования, основанную на свойствах конечномерных дискретных пространств. К сожалению, корректирующие возможности ПД оказались недостаточно высокими. Поэтому специалисты продолжили поиск новых подходов к реализации эффективных декодеров.

Наибольшее влияние на развитие техники помехоустойчивого кодирования на её начальном этапе оказало открытие алгоритма декодирования Витерби для свёрточных кодов [1, 18—20]. Он также не подразумевал использования методов алгебраической теории кодирования. Полученные даже для коротких свёрточных кодов с длинами кодирующего регистра $K = 5 - 7$ при кодовых скоростях $R = 1/3 - 3/4$ уровни помехоустойчивости передачи данных по спутниковым, т. е. гауссовским, каналам сразу оказались столь внушительными, что АВ на многие годы, вообще говоря, вполне обоснованно был признан наиболее подходящей процедурой для коррекции ошибок в реальных космических и спутниковых каналах связи [1, 19].

Чрезвычайно значимым этапом в развитии теории и техники кодирования стали также каскадные коды [26]. Этот действительно революционный для того времени принцип кодирования на долгие годы вместе с АВ определил направления развития техники декодирования. Каскадные коды значительно 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, а на внешних — недвоичных кодов Рида — Соломона. Они стали лучшими достижениями алгебраической теории кодирования прошедших лет [1, 19, 27]. Интенсивное развитие различных каскадных процедур является основой и текущего прогресса в технике декодирования.

Наряду с перечисленными методами коррекции ошибок, сейчас активно развиваются многопороговые декодеры самоортогональных кодов, являющиеся объектом исследования и в последующих главах

книги [1–6]. Данные алгоритмы характеризуются очень малой сложностью реализации и при этом обладают высокой энергетической эффективностью. Как будет показано далее, МПД позволяют обеспечить высокую достоверность передачи данных при высоком уровне шума, вплоть до непосредственной близости к границе Шеннона и при практически неограниченном аппаратном быстродействии. МПД также обладают уникальным свойством переходить только к строго более правдоподобным решениям в течение всего процесса исправления ошибок. Во многих случаях разрабатываемые с 1972 года МПД алгоритмы достигают оптимального (т. е. самого правдоподобного) решения при очень высоком уровне шума с линейной от длины кода сложностью декодирования [28]. Эти результаты оказалось возможным получить при рассмотрении проблемы декодирования как задачи поиска глобального экстремума функционалов от очень большого числа переменных.

Общая теория таких методов названа Оптимизационной Теорией помехоустойчивого кодирования [4, 5]. Для большого числа основных кластеров параметров кодирования (типичных сочетаний параметров кодов, декодеров и каналов) в настоящее время оказалось возможным обеспечить эффективную работу МПД и ряда других связанных с ним алгоритмов в непосредственной близости от границы Шеннона. Изложению методов и технологий ОТ и посвящена остальная часть книги. Представленные в ней результаты позволяют сделать вывод об успешном решении с помощью ОТ главной научной и технологической проблемы цифрового мира, сформулированной Шенноном — простого высокодостоверного декодирования в непосредственной близости от пропускной способности канала связи.

1.5. Эффективность декодирования

Как известно, при передаче данных по двоичному симметричному каналу существует такое значение пропускной способности канала, равное [1, 11]

$$C = 1 + p_0 \log_2 p_0 + (1 - p_0) \log_2 (1 - p_0), \tag{1.6}$$

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

$$P_B(e) = a \exp(-\alpha_B n), \tag{1.7}$$

где α_B — положительный параметр, зависящий от R и C, называемый *функцией надежности*; a — некоторая константа. Аналогичный 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 приеме в канале типа ДСК [1, 19]. Это обстоятельство активнейшим образом используется во многих системах связи для более эффективной передачи цифровых потоков именно с помощью мягких модемов и соответствующих методов (алгоритма Витерби, МПД и других).

Таким образом, существуют такие коды, для которых при $R < C$ вероятность ошибки их декодирования при использовании достаточно эффективных методов будет с ростом длины кода n экспоненциально стремиться к нулю. К сожалению, абсолютное большинство методов декодирования, доступных до недавнего времени для цифровых технологий, было существенно менее эффективно, поскольку они недостаточно полно реализовали потенциальные возможности применяемых кодов.

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

Рассмотрим первый критерий относительной энергетики сигнала. При проектировании 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 с сохранением заданной информационной скорости, которая позволит реализовать систему помехоустойчивого кодирования с умеренной сложностью аппаратуры декодирования принятых сообщений на приемной стороне.

Кроме того, всегда полезно знать величину конкретного отношения битовой энергетики сигнала к спектральной плотности мощности шума в канале 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 систем 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 график для предельных соотношений R и E_b/N_0 [3–5] (рис. 1.8). В качестве примера на график помещена точка A, соответствующая декодеру Витерби с длиной кодирующего регистра $K = 7$, для которого $R = 1/2$ и $E_b/N_0 = 4{,}5$ дБ при выбранной традиционной для него вероятности ошибки декодирования на бит $P_b(e) = 10^{-5}$.

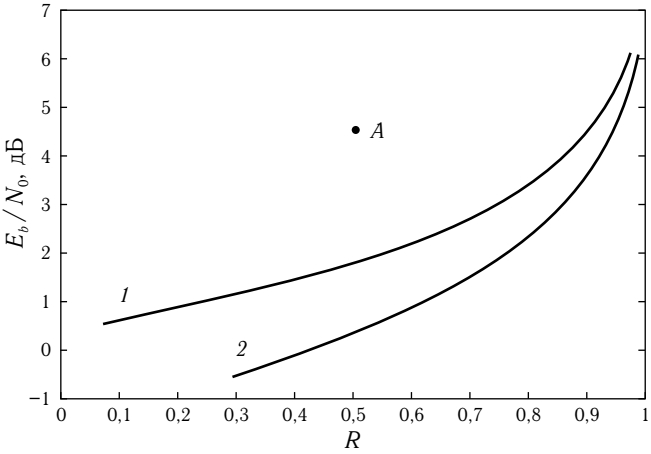

Рис. 1.8. Зависимость минимально возможного отношения битовой энергетики сигнала к спектральной плотности мощности шума E_b/N_0 в двоичном гауссовском канале от выбора кодовой скорости R для мягкого и жесткого модемов: *1* — жёсткий модем, $M=2$; *2* — мягкий модем, $M=16$

Как видно из представленных на рис. 1.8 графиков предельно возможной энергетики гауссовского канала для жесткого и мягкого модемов, разница по этому главному для теории кодирования параметру при $R=1/2$ близка к 1,5 дБ. Особенно существенно для многих приложений, что с ростом кодовой скорости R теоретическая граница для предельной энергетики E_b/N_0 перемещается вверх. Это является серьезным ограничением в 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 для мягкого модема при $R=1/2$ и квантовании принятого сигнала на 16 уровней (4-битовое квантование) минимально возможный из условия $R=C$ уровень $E_b/N_0=0{,}2$ дБ, а при $R=4/5$ $E_b/N_0=2{,}1$ дБ.

Таким образом, допустимый уровень расширения спектра сигнала и требуемый уровень энергетики сигнала E_b/N_0 при использова-

нии кодирования 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 допустимого снижения энергетики сигнала, т. е. отношения энергии передачи, приходящейся на 1 бит передаваемых данных E_b к спектральной плотности мощности шума N_0, т. е. $a = E_b/N_0$ в случае использования кодирования по сравнению с обычной передачей без применения кодов [1, 19]. Из определения ЭВК следует, что это разностный критерий, связанный с условиями выбора заданной достоверности передачи без кодирования и требуемой для этого величины $a = E_b/N_0$. Из этой величины затем вычитается или теоретически минимально достижимая величина a, определяемая, например, при условии $R = C$ из графика на рис. 1.8, или величина a, определяемая конкретным алгоритмом коррекции ошибок. Таким образом, ЭВК можно рассматривать как кажущееся увеличение мощности передатчика цифровой линии связи. Этот ресурс, определяемый кодом и эффективностью системы декодирования приёмника, можно использовать в реальной линии для повышения скорости передачи, уменьшения размеров дорогих антенн и других целей.

Оценить максимально возможные значения ЭВК можно из графиков на рис. 1.9 зависимости предельных значений ЭВК от требуемой результирующей вероятности ошибки на бит $P_b(e)$ при двоичной передаче без учёта сложности реализации декодера и вносимой задержки, т. е. только при выполнении условия $R < C$. Для каждой кривой указана кодовая скорость R и число уровней квантования M в гауссовском канале.

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 можно получить дополнительный 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, т. к. достижимый с помощью кодов и хороших алгоритмов декодирования ЭВК быстро растет, что хорошо видно из представленных на рис. 1.9 зависимостей. А это значит, что ценность и обязательность применения кодирования действительно безусловны и в дальнейшем его важность будет только быстро расти.

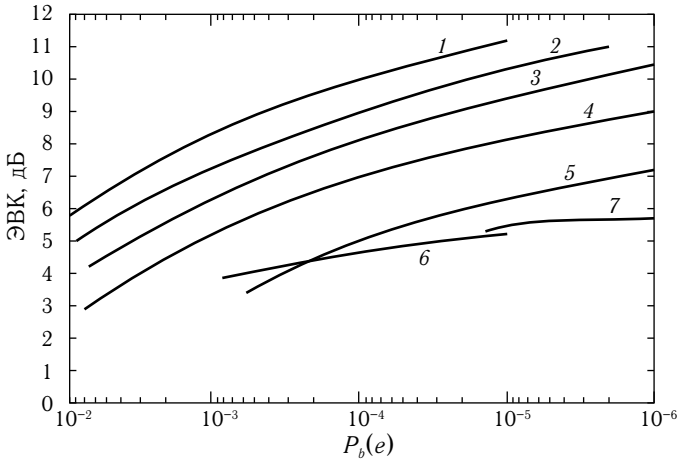

Рис. 1.9. Предельные значения ЭВК из условия $R < C$ в гауссовском канале для различных кодовых скоростей и числа уровней квантования сигналов в двоичном модеме:
1 — $R \to 0$, $M \to \infty$; *2* — $R = 1/4$, $M = 8$; *3* — $R = 1/2$, $M = 8$;
4 — $R = 1/2$, $M = 2$; *5* — $R = 4/5$, $M = 2$; *6* — АВ; *7* — МПД

Полезно также оценить, какие значения ЭВК обеспечивают конкретные коды и алгоритмы. Кривая *6* на рис. 1.9 показывает возможности алгоритма Витерби для стандартного свёрточного кода с длиной кодирующего информационного регистра $K = 7$ и $R = 1/2$, который широко используется 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 гг. прошлого века, когда эти декодеры были разработаны. Но заметим, что около 2 дБ от этого уровня ЭВК, как отмечалось выше, получены при декодировании именно за счёт мягкого модема.

Кривая *7* на обсуждаемом рис. 1.9 представляет возможности декодирования свёрточного кода на основе очень простой версии многопорогового декодера, развиваемого в рамках ОТ, который и будет основным предметом изучения в последующих главах этой книги [29]. Существенно, что этот график соответствует работе МПД с жёстким модемом, т. е. при передаче по ДСК при $M = 2$, и обеспечивает при $R = 1/2$ и $d = 11$ ЭВК$= 5{,}6$ дБ для $P_b(e) = 10^{-5}$. Этот пример очень наглядно показывает, насколько эффективно применение очень длинных кодов, используемых в МПД, поскольку с ними даже с жёстким модемом можно достаточно простыми методами получать более высокие характеристики, чем у мягкого АВ. Подчеркнём, что столь высокий результат МПД обеспечивает благодаря тому, что во многих случаях

результаты его декодирования совпадают с решениями оптимальных декодеров. Обычно ОД требуют объёма вычислений, экспоненциально растущего с увеличением длины кода, тогда как сложность МПД растёт с длиной кода лишь линейно, что соответствует минимально возможной с точки зрения теории сложности. Представленный в качестве примера МПД при $P_b(e) \leqslant 10^{-5}$ тоже осуществляет оптимальное декодирование всего при $I = 10$ итерациях коррекции ошибок.

Как видно на рис. 1.9 из сопоставления графиков для предельных возможностей и реальных характеристик некоторых не очень длинных кодов, до границы $R = C$, достижение которой допускает теория, ещё очень далеко. Способы достижения больших уровней ЭВК по возможности более простыми методами будут рассмотрены в последующих главах предлагаемой читателям книги.

Третий критерий эффективности кодирования основан на естественном понятии, который можно так и называть *эффективностью* или, например, просто «КПД», поскольку его смысл полностью соответствует обычному параметру КПД для различных физических процессов.

Понятие «КПД использования канала» непосредственно связано с предельными значениями $a = E_b/N_0$, которые соответствуют равенству $R = C$. При вычислении КПД 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 в проценты, то это и будет искомый КПД — полный аналог КПД 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, превышающем a_0 на 3 дБ. 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. Это и означает, что КПД использования канала данным декодером по энергетике составляет 50%. А если найдется 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 КПД составит 89%.

Наконец, сформулируем четвёртый критерий эффективности декодирования относительно границы Шеннона, в котором учитывается и близость рабочей области алгоритма коррекции ошибок к пропуск-

ной способности канала C, и достоверность осуществляемого им декодирования. Наиболее полезно его использовать для АБГШ каналов. Назовём его *коэффициентом совершенства Золотарёва* (КСЗ) для конкретных анализируемых алгоритмов. Он весьма удобен в связи с тем, что обычно измеряемые по логарифмической (сильно искривлённой!) шкале энергетические параметры кодов оцениваются слишком грубо и односторонне. Это особенно заметно именно в области больших шумов канала. Рассмотрим его применение для мягкого МПД алгоритма в АБГШ канале при кодовой скорости $R = 1/2$. При $C = 1/2$, как известно, $E_b/N_0 = 0{,}2$ дБ. Возьмём один из лучших опубликованных вариантов МПД декодера с $R = 1/2$, который работает при $E_b/N_0 = 1{,}2$ дБ и обеспечивает в этом случае $P_b(e) \sim 3 \cdot 10^{-7}$ [22, 58]. Обращаясь к известным табличным данным [3], находим, что такую высокую достоверность передачи можно обеспечить без применения кодирования при обычной двоичной модуляции, если $E_b/N_0 = 11$ дБ. Получаем, что декодер работает при энергетике, на $1{,}2 - 0{,}2 = 1$ дБ или на 26%, т.е. в 1,26 раз большей, чем если бы он работал при $R = C = 1/2$. Без использования кодирования энергетика передачи была бы на $11 - 0{,}2 = 10{,}8$ дБ или в 12,1 раз большей, чем в случае $R = C = 1/2$. Значит, если $12{,}1 - 1 = 11{,}1$ разделить на $1{,}26 - 1 = 0{,}26$, то получим КСЗ $= 11{,}1/0{,}26 = 42{,}7$. Эта величина показывает, во сколько раз рабочая энергетика декодера ближе к границе Шеннона по сравнению со случаем неиспользования кодирования. Как видим, в КСЗ учтена и итоговая достоверность результатов декодирования. Очевидно, что КСЗ ~ 43 является очень большой величиной, подчёркивающей эффективность кодирования в рассмотренном примере. При уменьшении вероятности ошибки, обеспечиваемой декодером, КСЗ естественно растёт, т. к. достоверность результатов кодирования увеличивается. А при устремлении рабочей энергетики декодера в нашем примере к $E_b/N_0 = 0{,}2$ дБ, когда $C = R = 1/2$, КСЗ устремится к бесконечности, что тоже естественно, т. к. сама граница Шеннона, как, например, и скорость света, недостижима.

Совсем простую содержательную интерпретацию критерия КСЗ можно получить из таких наглядных соображений, представленных на рис. 1.10.

Нарисуем числовую ось, на которой будем откладывать уровни

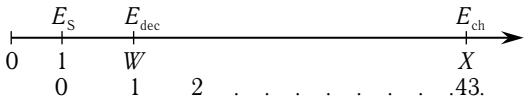

Рис. 1.10. Графическая интерпретация критерия КСЗ для алгоритмов декодирования, работающих в гауссовских каналах

энергий передачи, которые мы обсуждали выше, естественно отметив нулём слева на оси её нулевой уровень. Уровень энергетики, соответствующий границе Шеннона E_S, обозначим как 1, т. е. этот уровень выбираем в качестве условной масштабной единицы для других энергий, которые тоже будут наноситься на энергетическую ось. Далее уровень рабочей энергетики E_{dec} конкретного оцениваемого алгоритма с определённой гарантируемой им достоверностью декодирования обозначим как W. И, наконец, ту весьма большую энергетику канала E_{ch}, которую надо обеспечить без кодирования, чтобы достичь такую же достоверность передачи, как у оцениваемого нами декодера, отметим как X. Из смысла КСЗ следует, что он просто равен отношению длин отрезков $(1, X)$ и $(1, W)$. А если поменять точку отсчёта и масштаба так, как показано на рис. 1.10 мелким шрифтом ниже энергетической оси, то точка X будет как раз соответствовать тому числу на оси, которое равно отношению длин этих отрезков, в нашем примере КСЗ ≈ 43. Это последнее преобразование масштабов мер вдоль оси энергий дополнительно повышает наглядность предложенного параметра КСЗ, хотя и не является обязательным.

Таким образом, КСЗ — удобный и информативный критерий близости области работы декодера к пропускной способности канала C, учитывающий и его итоговую достоверность декодирования.

Использование параметров ЭВК, КПД и КСЗ для оценки эффективности работы декодеров вблизи границы Шеннона позволяет рассматривать возможности реальных кодов и алгоритмов их декодирования с позиций, которые более полно характеризуют методы кодирования для гауссовских каналов.

Для более точного понимания ценности критерия КСЗ определим его значение ещё для одного примера: классического варианта АВ при $K = 7$ и той же кодовой скорости $R = 1/2$. Пусть анализируется типичный вариант его работы, когда $P_b(e) \sim 10^{-5}$, что без использования кодирования требует энергетики 9,6 дБ. Но заданную через $P_b(e)$ достоверность этот АВ обеспечивает при рабочей энергетике $E_b/N_0 \sim 4{,}2$ дБ. Тогда получаем, что рабочая энергетика АВ на $4{,}2 - 0{,}2 = 4{,}0$ дБ или в 2,5 раза больше энергетики по Шеннону. А без кодирования разность в энергетике между АВ и границей Шеннона равна $9{,}6 - 0{,}2 = 9{,}4$ дБ, т. е. в 9,1 раз больше. Тогда КСЗ $= \frac{9{,}1 - 1}{2{,}5 - 1} = 5{,}4$ раза, что хорошо соответствует полезности применения классического АВ, весьма далёкого по своим параметрам от первого примера с МПД декодером, который уже может быть реализован на имеющейся элементной базе. Таким образом, КСЗ действительно удобен и информативен для оценки эффективности работы декодеров в непо-

средственной близости от границы Шеннона.

Далее при анализе характеристик алгоритмов декодирования различных кодов полезно знать также предельные достижимые величины ЭВК, соответствующие этим методам. Оказывается, что эти величины для канала с АБГШ и двоичной модуляции просто равны при малом уровне шума канала произведению Rd при приеме в целом, т. е. для числа уровней квантования $M \to \infty$, что соответствует уровню ЭВК, равному

$$G_\infty = 10 \lg[Rd] \tag{1.8}$$

по традиционной логарифмической шкале, т. е. в децибелах [1, 19].

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

$$G_2 = 10 \lg[R(t_0 + 1)] \tag{1.9}$$

где t_0 — максимальное целое число, меньшее $d/2$; d — минимальное кодовое или свободное расстояние применяемых кодов. Из сопоставления (1.8) и (1.9) видно, что в асимптотике при улучшении отношения сигнал/шум прием в целом для канала с АБГШ 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 [18, 19].

Сделаем ещё одно важное замечание относительно свойств кодов и их эффективности. ЭВК действительно давно стал одним из главных критериев, характеризующих необходимость и пользу применения кодирования. И при этом иногда оказывается, что инженеры и студенты, изучающие эту науку, с удивлением замечают, что в формуле для ЭВК нет отношения d/n — параметра, к увеличению которого очень долго стремились специалисты в области алгебраических методов кодирования. Поэтому мы обращаем ваше внимание на то, ЭВК действительно не зависит от этого отношения. Разумеется, при этом нужно всегда помнить, что выражения (1.8) и (1.9) достаточно точны только в асимптотике при очень малом уровне шума. Но во многих реальных случаях можно подобрать коды и алгоритмы их декодирования так, что эти параметры будут с приемлемой точностью близкими к реальным значения ЭВК и при довольно высоких уровнях шума. В частности, приведённый в пример МПД алгоритм для ДСК и свёрточного кода с $d = 11$ достиг своего максимально возможного значения ЭВК = 5,6 дБ при весьма большом уровне энергетики канала 4 дБ, что удалось получить благодаря правильному выбору декодера и кода.

1.6. 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 разрешенные кодовые комбинации, что и будет обеспечивать их правильное, в конце концов, определение хорошим декодером на приемной стороне линии связи. На рис. 1.11 представлены нижние оценки средней вероятности ошибки наилучшего декодирования на блок $P_B(e)$ для блоковых кодов, иногда также обозначаемой как $P_W(e)$, в ДСК при $R = 1/2$ и разных длинах n этих кодов для разных вероятностей ошибки в канале p_0. Отметим, что $R = C = 1/2$ при $p_0 = 0{,}11$, т. е. вертикальная ось графика совпадает с границей Шеннона. Как видно из представленных кривых, для получения действительно небольших вероятностей ошибки декодирования при большом уровне шума в ДСК без памяти следует выбирать весьма большие значения n. В противном случае достижение хорошей достоверности передачи при вероятности ошибки в ДСК $p_0 \lesssim 0{,}11$, т. е. когда $R \lesssim C$, окажется невозможным.

Из графиков $P_W(e)$ видно, что даже при $n \approx 10\,000$ битов значения вероятности ошибки канала p_0, при которых гипотетический наилучший переборный декодер мог бы обеспечить достаточно ма-

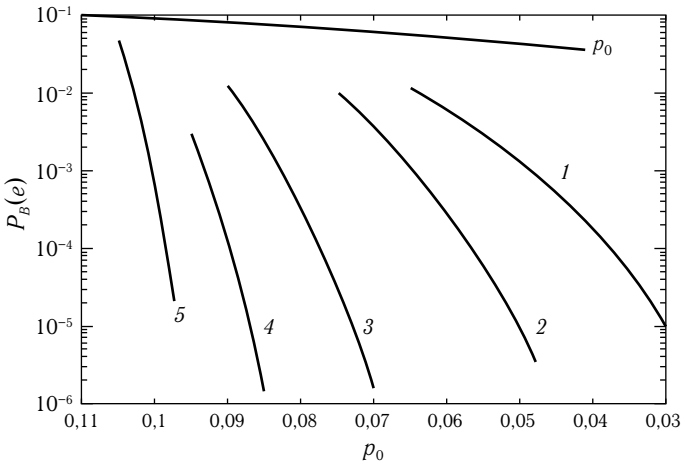

Рис. 1.11. Нижние оценки средней вероятности ошибки на блок $P_B(e)$ в ДСК без памяти для кодов с различной длиной n при $R = 1/2$:
1 — $n = 100$; *2* — $n = 300$; *3* — $n = 1000$; *4* — $n = 3000$; *5* — $n = 10\,000$

лые вероятности ошибки принятия решений относительно вида переданного блока, меньше чем $p_0 = 0{,}1$. А это примерно ещё на 0,5 дБ меньше по уровню шума канала, чем разрешает граница $R = C = 1/2$ при $p_0 = 0{,}11$, совпадающая на рис. 1.11 с вертикальной осью графика. Таким образом, даже представленные существенно заниженные оценки для вероятности ошибки декодера, полученные из известных границ сферической упаковки, показывают, что очень эффективные системы кодирования должны использовать и весьма длинные коды с $n \approx 10^5 - 10^7$. Это обстоятельство дополнительно подчеркивает, 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.

Очень важно сосредоточить внимание на правильном понимании того, что высокоэффективные коды вблизи пропускной способности канала связи, т. е. при условии $R \lesssim C$, должны быть очень длинными. При этом условии даже, казалось бы, небольшая сложность декодирования порядка n^2 оказывается недопустимой роскошью, т. к. декодирование единственного кодового блока может потребовать нескольких минут или, может быть, многих лет даже при использовании очень быстрой элементной базы микроэлектроники. Именно поэтому необходимо даже при большом уровне шума канала искать алгоритмы со сложностью, как можно более близкой именно к линейной от длины кода. Эта необходимость следует ещё и из того, что представленные на рис. 1.11 оценки являются существенно нижними (т. е. реальные коды всегда будут гораздо менее эффективными), и, кроме того, в непосредственной окрестности пропускной способности C даже эти неоправданно хорошие характеристики по мере увеличения разности $C - R$ будут улучшаться очень медленно. Это связано с тем, что упоминавшаяся в разделе 1.2 функция надёжности для блоковых кодов в показателе надёжности для вероятности ошибки декодирования изменяется как $\sim (C - R)^2$ [15, 20]. Легко видеть, что и сама вероятность $P_W(e)$ в области $C \sim R$ ведёт себя точно так же.

Для иллюстрации этой непростой ситуации, которая во многих случаях (однако далеко не всегда автоматически!) приводит к большей предпочтительности свёрточных кодов, на рис. 1.12 показано точное поведение этой нижней оценки для вероятности ошибки наилучшего декодирования $P_W(e)$ при $R = 1/2$ в окрестностях $R \approx C$. Она тоже построена на известной как сферическая упаковка идее максимально полного разделения областей решений оптимального декодера, которое для длинных кодов на самом деле невозможно.

На рисунке показана нижняя оценка для вероятности ошибки де-

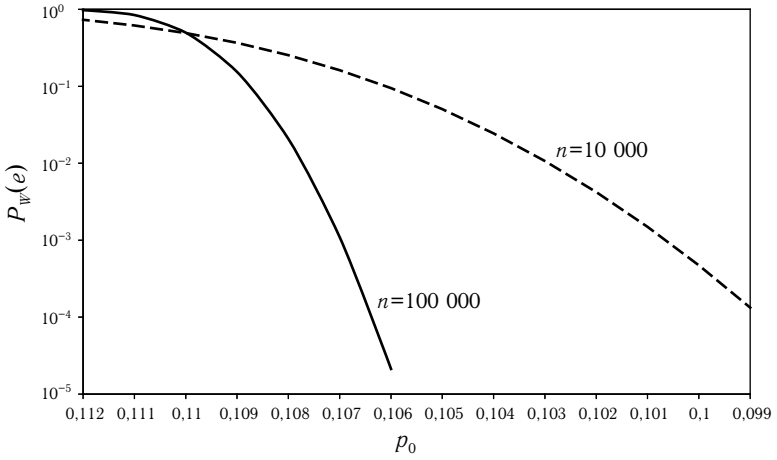

Рис. 1.12. Нижние оценки эффективности оптимального декодирования двоичных блоковых кодов в ДСК канале

кодирования кодовых слов $P_W(e)$ для кодов с $R=1/2$ длины $n=10\,000$ и $n=100\,000$ в ДСК канале. При вероятности ошибки $p_0=0{,}11$ в канале оба длинных кода ведут себя совершенно одинаково и совершают свои ошибки в принятии решения о блоке с вероятностью $\sim 0{,}5$, что достаточно естественно, т. к. это точка, в которой $R=C=1/2$. Но и по мере снижения вероятности p_0 вероятности ошибки декодирования на блок $P_W(e)$ сначала уменьшаются очень медленно именно из-за отмеченной выше квадратичной зависимости показателя надёжности от разности $C-R$.

Рассмотренная выше зависимость надёжности декодирования от уровня шума является причиной того, что, по меньшей мере, в некоторых случаях в системах кодирования предпочтительнее использовать именно свёрточные коды, т. к. необходимые длины блоковых кодов могут в области $R \lesssim C$ оказаться чрезмерными и вносить недопустимые задержки в процедуры декодирования. Это определяется тем, что для свёрточных кодов функция надёжности растёт гораздо быстрее, почти линейно с ростом разности $C-R$, что и позволяет в сопоставимых условиях применять именно свёрточные коды гораздо меньшей длины. Но при этом задержка решения для успешного декодирования свёрточного кода должна быть при $R \lesssim C$ много больше, чем его длина. Именно эта ситуация и имеет место при использовании МПД для свёрточных кодов, когда количество итераций декодирования при увеличении уровня шума возрастает многократно. Такое свойство алгоритмов МПД отражает фундаментальные структурные и алгоритмические отличия блоковых и свёрточных кодовых структур.

1.7. Пороговое декодирование и повторная коррекция

Перед тем, как заняться анализом вопросов, относящихся к МПД алгоритмам, следует вспомнить о том, что собой представляет собой прототип этого алгоритма — мажоритарный (пороговый) декодер, который когда-то разработал известнейший американский учёный Дж. Месси [8]. Данный метод может использоваться для декодирования как свёрточных, так и блоковых самоортогональных кодов. Пример схемы ПД для свёрточного кода с кодовой скоростью $R = 1/2$ и кодовым расстоянием $d = 5$, заданного порождающим полиномом $g(x) = 1 + x + x^4 + x^6$, представлен на рис. 1.13. Отметим, что ПД является простейшим устройством, состоящим только из регистров сдвига, сумматоров по модулю 2 и порогового элемента (ПЭ). Он осуществляет обычное суммирование проверок, относящихся к текущему декодируемому информационному биту, и сравнение полученной суммы с порогом, на основании чего он и принимает решение о необходимости коррекции контролируемого на ПЭ символа, если более половины проверок, поступивших на ПЭ, оказываются ошибочными. К сожалению, эффективность этой схемы коррекции ошибок оказывается довольно невысокой.

Среди самых простых и очевидных способов улучшения эффективности методов исправления ошибок, которые предлагались в 70-х годах прошлого века, можно отметить 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 ПД [3] для указанного выше свёрточного кода приведен на рис. 1.14.

Малая эффективность подобной схемы декодирования была следствием сильного группирования, т. е. размножения ошибок в порого-

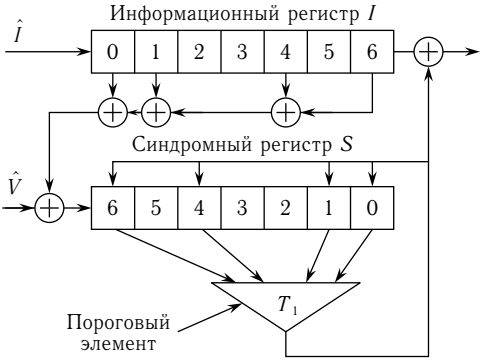

Рис. 1.13. Пороговый декодер свёрточного СОК

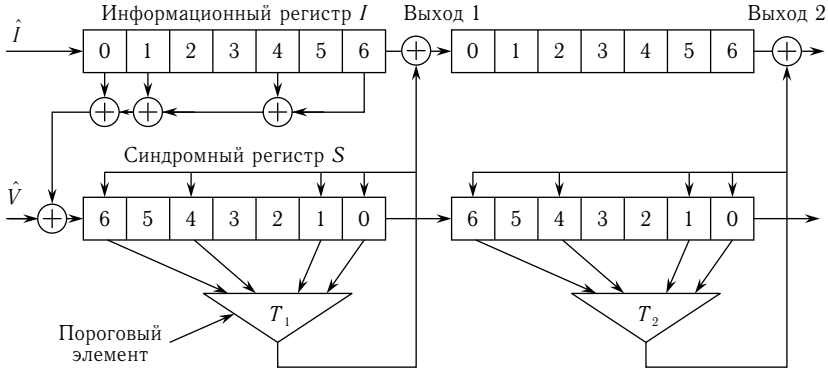

Рис. 1.14. Пример схемы повторного декодирования на основе порогового декодера свёрточного кода

вом 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 появляется очень плотный пакет ошибок. Например, пусть с выхода первого ПД (см. рис. 1.14) на вход второго поступила немного улучшенная при первой попытке декодирования последовательность. 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 длинного 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.

Подчеркнем, что коды с малым уровнем размножения ошибок в ПД в те годы были совершенно неизвестны. Поэтому попытки решить проблему роста эффективности мажоритарных методов повторной коррекцией принятого потока были в 1970-х годах прекращены. Однако позже эта проблема была полностью решена методами, описанными в [2–5, 36–38]. Только успешное решение этой сложнейшей проблемы позволило затем реализовать и все потенциальные возможности МПД, что стало началом быстрого развития идей и технологий Оптимизационной Теории.

Основная идея построения класса методов уменьшения эффекта РО будет предложена позже.

1.8. Вероятность первой ошибки порогового декодера самоортогонального кода

Очень длительное время оценки вероятностей ошибки для пороговых декодеров ограничивались единственной вероятностью ошибки декодирования первого символа кода $P_1(e)$, точно вычисленной в [8]. Умение оценивать возможности мажоритарных методов очень полезно само по себе, а также для оценки потенциальных возможностей МПД алгоритмов. Напомним процесс вычисления этого важного параметра эффективности ПД.

Рассмотрим линейный двоичный блоковый мажоритарно декодируемый самоортогональный код с кодовой скоростью $R = k_0/n_0 = 1/2$ и $d = 2t_0 + 1$, т. е. исправляющий t_0 ошибок. Изложим методику вычисления вероятности ошибки обычного порогового декодирования в первом символе такого блокового кода $P_1(e)$, повторяющую, в основном, материал, представленный в [8]. 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 [8], 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 блокового кода окажется неправильной, равна

$$p_J = 0{,}5\left[1 - (1 - 2p_0)^J\right],$$

где p_0 — вероятность ошибки в ДСК.

Тогда, вычисляя производящую функцию вероятности (ПФВ) для проверок этого ПД [8]

$$A(x) = (p_0 x + q_0)(p_J x + q_J)^J = \sum_{m=0}^{d} a_m x^m,$$

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

$$P_1(e) = \sum_{m=(d+1)/2}^{d} a_m. \tag{1.10}$$

Фактически мы нашли метод вычисления вероятности того, что более половины проверок, поступающих на вход ПЭ в ПД, будут неправильными, что и приведёт к ошибке декодирования. В общем случае при $R = k_0/n_0$ размерности проверок могут довольно сильно отличаться от рассмотренного примера с $R = 1/2$. Это определяется различными весами порождающих полиномов того или иного кода, использованием методов параллельного каскадирования, кодов с переменными связями, с выделенными ветвями (они будут рассмотре-

ны в последующих главах) или другими причинами. Кроме того, для свёрточных кодов размерность проверок не будет постоянной, т. к. они не содержат ошибок в ранее декодированных информационных символах. Поэтому правильное определение размерности проверок и управление этим параметром полезно при поиске методов повышения эффективности применения и собственно алгоритма МПД.

Важность обсуждаемых вероятностей для разных кодов определяется тем, что первоначальное уменьшение средней вероятности ошибки декодирования в итеративных алгоритмах всегда непосредственно связано с возможностями самого 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 приведенных на рис. 1.15 графиков зависимостей $P_1(e)$ от p_0, полученных с помощью (1.10) для кодов с кодовой скоростью $R = 1/2$, при мажоритарном декодировании в ДСК вероятность ошибки в первом символе кода $P_1(e)$ для свёрточных кодов с теми же значениями d и R всегда меньше, чем для блоковых. Это объясняется тем, что в блоковых кодах размерность всех проверок максимальна, а в свёрточных — увеличивается от минимальной до максимальной.

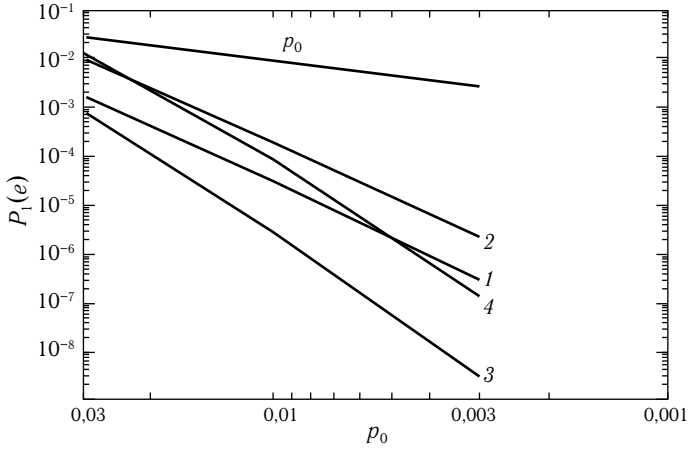

Рис. 1.15. Оценки вероятности ошибки обычных ПД в первых символах $P_1(e)$ кодов с $R = 1/2$:
1 — свёрточный, $d = 7$; *2* — блоковый, $d = 7$;
3 — свёрточный, $d = 11$; *4* — блоковый, $d = 11$

Правильная оценка вероятностей $P_1(e)$ позволяет лучше прогнозировать полезность тех или иных улучшений, которые планируется достичь при всевозможных модификациях МПД.

1.9. Пороговые процедуры для недвоичных кодов

В своей известнейшей книге [8], которая положила начало изучению мажоритарных методов декодирования первоначально для двоичных свёрточных и ряда других кодов, Дж. Месси описал и методы декодирования для недвоичных кодов. Однако никаких оценок характеристик таких кодов он не предложил. Ниже мы рассмотрим ещё один вариант декодера (по нашей терминологии — символьного ПД или QПД) для недвоичных мажоритарно декодируемых кодов, которые Дж. Месси не оценил в те далёкие годы как перспективные.

Положим, что передача идёт по q-ичному симметричному каналу (QСК) с вероятностью ошибки в принятом символе p_0. Пусть далее, аналогично двоичному случаю, используется мажоритарно декодируемый блоковый код с минимальным кодовым расстоянием d, а размерность всех проверок равна J. Именно так рассматривались эти коды в [8]. Мы только добавим для большей определённости оценок, что мы рассматриваем самоортогональные коды.

Тогда после вычисления синдрома принятого сообщения нужно определить вид решающего правила, которое должен реализовать пороговый элемент в ПД для этого символьного кода.

Необходимый результат можно получить при помощи вычисления произведения ПФВ для информационного символа и всех проверок, участвующих в его декодировании. Однако реализация данного подхода является для недвоичных кодов, т. е. при $q > 2$, слишком сложной, а полученные соотношения будут труднообозримыми. Поэтому для получения удобной оценки для вероятности первой ошибки используем более простой, хотя и немного менее точный подход, основанный на прямом перечислении тех конфигураций ошибок, которые будут приводить к неправильному решению QПД.

Далее оценим корректирующие возможности блокового символьного кода с $d = 5$, кодер для которого был представлен на рис. 1.2,б в разделе 1.1. Поскольку мы оцениваем блоковый самоортогональный код, то, как и в двоичном случае, можно выписать J выражений для символов синдрома, относящихся к некоторому выбранному информационному символу i_j, которые содержат ошибку e_j в этом информационном символе:

$$\begin{aligned} s_{0,j} &= e_j + e_{i,m_0} + \ldots - e_{v,0}, \\ &\ldots, \\ s_{J-1,j} &= e_j + e_{i,m_{J-1}} + \ldots - e_{v,J-1}, \end{aligned} \tag{1.11}$$

Здесь в каждой из J строк, определяющих выражения для значений символов $s_{h,j}$ синдрома S, $h=0,...,J-1$, содержится ошибка e_j в информационном символе i_j, есть одна ошибка в некотором проверочном символе кода $e_{v,n}$, $n=0,...,J-1$, а также присутствует некоторое количество ошибок в других информационных символах e_{i,m_k}, общее количество которых определяется порождающими полиномами кода и следующим из их числа и вида значением кодовой скорости R используемого кода. Совокупность всех символов синдрома, относящихся к некоторому информационному символу i_j, как и для случая двоичных кодов, будем называть проверками относительно этого символа. При вычислении оценок для кода, который мы взяли в качестве примера, будет естественным считать, что число прочих информационных ошибок во всех проверках для всех символов равно J. А поскольку выражение (1.11) в соответствии с нашим выбором точно соответствует выражениям, относящимся к самоортогональным кодам, то все J проверок в (1.11) таковы, что все информационные ошибки, кроме e_j, в рассматриваемом наборе проверок различны.

Но тем самым мы фактически доказали, что символьный код, построенный на базе систематического двоичного СОК с минимальным кодовым расстоянием $d=J+1$ (здесь предполагалось четное J, что, очевидно, совершенно несущественно), также имеет минимальное кодовое расстояние d.

Напомним, что 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, ошибки в декодируемом символе, более $d/2$. В q-ичном же коде можно реализовать несколько иное правило, согласно которому коррекция происходит, если число проверок с некоторым одинаковым значением превышает число любых других одинаковых по значению проверок. Тем самым определяется возможность исправления весьма 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. Полезность такого эвристического изменения решающей функции символьного ПЭ мы попробуем определить из той простой логики, что если вероятность ошибки QПД будет достаточно мала, то введённую нами решающую функцию действительно можно использовать.

Далее следует обратить внимание на то, что значения ошибок в символах в канале типа QСК могут быть разными. Именно по этой причине предлагается требовать от того значения символа, который будет принят в качестве решения о значении ошибки в i_j только стро-

гого относительного большинства его значений по сравнению со всеми другими $q-1$ возможными значениями проверок. С учётом этого важного замечания получаем, что, например, при минимальном кодовом расстоянии $d=9$ в случае правильного приема декодируемого символа можно иметь все неправильные J проверок и при этом не изменять декодируемый символ, т. е. не вносить в него ошибку. Единственное условие для реализации этой возможности состоит только в том, чтобы все значения проверок были бы различными. Тогда все возможные значения проверок появляются только один раз: $m_0=\ldots=m_{J-1}=1$. А это и обеспечивает неизменность декодируемого символа. Ясно, что в двоичных кодах такая ситуация невозможна. В то же время типичность этого случая для символьных кодов свидетельствует о гораздо более высоких корректирующих возможностях предлагаемого алгоритма QПД, поскольку он почти всегда корректирует, т. е. не изменяет правильно символы, если до $(d-1)$ проверок относительно них неправильны.

Полагая далее наличие ошибки $e_j=h$, $h>0$, в символе i_j, отмечаем, что для правильного декодирования этого символа нужно лишь наличие двух правильных проверок из J. В самом деле, если снова допустить, что все остальные проверки, содержащие ошибки в других символах, различны, то две правильные проверки имеют значения, соответствующие ошибке в декодируемом символе, что и приведет к его коррекции. Ну, и отметим в конце качественного обсуждения свойств QПД, что рассмотренные только что условия различных значений всех ошибочных проверок обычно почти всегда выполняются, если размер алфавита используемых символов достаточно велик, т. е. $q\gg 1$.

Теперь определим наиболее частые сочетания ошибок канала, приводящих к ошибкам QПД, и их вероятности. Заметим, что в недвоичном блоковом СОК с $J=d-1$ и $R=k_0/n_0$ размерность проверки равна $m=Jk_0/(n_0-k_0)$. Полагая оценку вероятности ошибочной проверки

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

где $a=1/(q-1)$, поскольку сумма нескольких ошибок может в $1/(q-1)$-й доле случаев дать правильную проверку, можно указать следующие искомые непересекающиеся события, приводящие к ошибке в первом декодируемом символе рассматриваемого блокового квазициклического кода QПД [3–5, 36, 39].

1. Все проверки и первый декодируемый символ i_0 ошибочны:

$$P_1=p_0p_v^J.$$

2. Все проверки ошибочны, среди них есть две одинаковые по

значению проверки, а i_0 правилен:

$$P_2 = \frac{(1-p_0)p_v^J J(J-1)}{2(q-1)} \prod_{i=1}^{J-2} \left(1 - \frac{i}{q-1}\right). \qquad (1.12)$$

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:

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

Таким образом, искомая оценка $P_1(e)$ вероятности первой ошибки QПД определяется суммой найденных выше вероятностей P_1, P_2, P_3 и P_4. Вероятности других типов событий несущественно влияют на результирующую вероятность. При необходимости более полный список событий, приводящих к ошибке QПД, можно найти в [36, 39].

На рис. 1.16 представлены графики оценок $P_1(e)$ вероятности первой ошибки QПД для различных недвоичных СОК. Кривая *1* на рисунке отражает оценку вероятности первой ошибки для блокового кода с $d=9$, $R=1/2$ и $q=256$. Кривой *2* здесь 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 (по меньшей мере, в первом символе) при гораздо более высоком уровне шума p_0 в QСК, чем в ДСК (сравните с рис. 1.15).

Вычисление характеристик QПД указывает на область, в которой уже после первой попытки декодирования происходит заметное снижение доли оставшихся ошибок. Ясно, что в этом случае после-

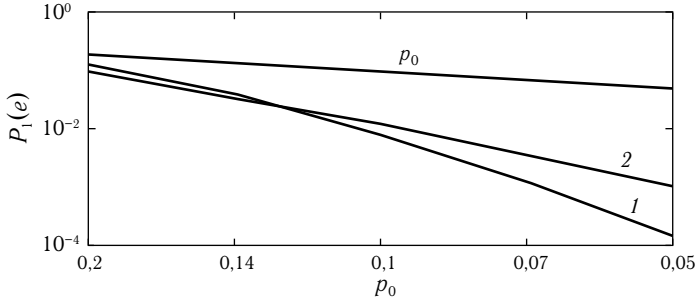

Рис. 1.16. Оценка вероятности первой ошибки блоковых QПД в QСК: *1* — $d=9$; *2* — $d=5$

дующие 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. Но основное влияние на вероятности ошибки последующих символов при первой попытке коррекции остальных символов всего принятого блока и при повторном его декодировании в недвоичных кодах оказывает эффект РО. К этому вопросу мы обратимся немного позже.

Только что полученные способы оценки возможностей QПД, показали, что символьные ПД могут работать при более высоких вероятностях ошибки в канале, чем ПД для обычных двоичных кодов. Это позволяет сделать вывод, что предложенный здесь как бы «угаданный» эвристический алгоритм их работы действительно заслуживает внимания и анализа путей повышения его эффективности. Эта тема будет рассмотрена позже.

К этому можно только добавить, что на самом деле этот алгоритм возник после успешной формулировки идеи МПД для двоичных кодов [38] при поиске в течение около 5 лет её столь же мощного аналога в недвоичных кодах. Таким образом, данный параграф является следствием того, что в процессе описания теории полезнее последовательное изложение взаимосвязанных новых результатов. Реальное же долго созревавшее внутри нашей научной школы решение о виде символьных МПД появилось гораздо раньше каких-либо идей о способах оценки $P_1(e)$ для простого одношагового QПД.

1.10. «Мажоритарное» декодирование в стирающих каналах

В [8] была предложена несложная схема для восстановления символов при передаче по шумящему каналу такому, что некоторые символы случайно оказываются неизвестными. Полагая, что они как бы стёрты, можно поставить задачу о восстановлении таких искажений в стирающих каналах. Для свёрточного кода с $R = 1/2$ там было показано, что предложенный метод будет относительно эффективен при вероятности независимых стираний в таком канале $p_s \lesssim 0{,}2$.

Следуя традиции отталкиваться в наших постановках задач и в результатах от идей, предложенных в [8], разовьём этот подход так, чтобы его можно было бы далее применить в итеративных схемах, которые сейчас занимают ведущие места в конкурсах алгоритмов. Как всегда, постараемся максимально упростить метод. И хотя он будет не совсем мажоритарный, поскольку задача при известных позициях искажений становится совсем простой (ну, конечно же, «почти простой», если $R \sim C$), оставим условно этот алгоритм в группе мажоритарных методов.

Пусть наш алгоритм для кодов типа СОК после передачи по стирающему каналу вычисляет обычным образом вектор синдрома. Пусть он в дополнение к этой стандартной операции выполняет перед началом работы подсчёт числа стёртых символов, присутствующих в каждой проверке и запоминает их, а потом передаёт для использования декодеру. Пусть далее блоковый СОК имеет некоторое значение d, $J = d - 1$ проверок, а число слагаемых в каждой проверке, без учёта самого декодируемого символа, равно m. Тем самым мы для обсуждения относительно простых, как нам кажется, идей восстановления стёртых символов не выбираем, как в предыдущих примерах декодеров, исправляющих ошибки коды с кодовой скоростью $R = 1/2$, а сразу обсуждаем достаточно общий случай произвольной кодовой скорости.

Пусть далее предлагаемый алгоритм декодирования таков, что для выбранного информационного символа, если он стёрт, просматриваются все J проверок, относящихся к нему. И если найдётся хоть одна такая проверка, что в ней есть как слагаемое только этот символ, а все остальные приняты правильно, т. е. не стёрты, то из простого уравнения $A = B + X$, где A — значение проверочного символа, B — сумма правильно принятых символов в этой проверке, неизвестное X — стёртый символ, этот символ будет восстановлен. После этого, конечно, нужно в памяти декодера уменьшить на 1 сумму стёртых символов для всех J проверок для этого восстановленного символа, после чего можно переходить к попыткам восстановления следующих символов.

Определим вероятность того, что первый же стёртый символ не удастся восстановить. При вероятности стирания в канале p_e и наличии в проверке m слагаемых вероятность p_{me} того, что некоторая проверка стёрта, т. е. содержит как слагаемое хотя бы один стёртый символ, равна

$$P_{me} = 1 - (1 - p_e)^m.$$

Но тогда вероятность того, что стёртый символ нельзя восстановить, т. к. все проверки тоже стёрты, равна

$$P_{es} = p_e P_{me}^J.$$

Это выражение и определяет возможности нашего метода восстановления стираний с подсчётом числа стираний в проверках. На рис. 1.17 представлена вероятность невосстановления для первого символа в блоковом коде с $R = 1/2$ для $d = 5$ и $d = 9$. Как следует из вида представленных данных, все методы восстановления стираний эффективны при $R = 1/2$ с вероятностью стираний $p_e < 0{,}2$. При этом метод Месси (график DM) для свёрточных кодов, как и должно быть, эффективнее нашего метода для блоковых кодов, предло-

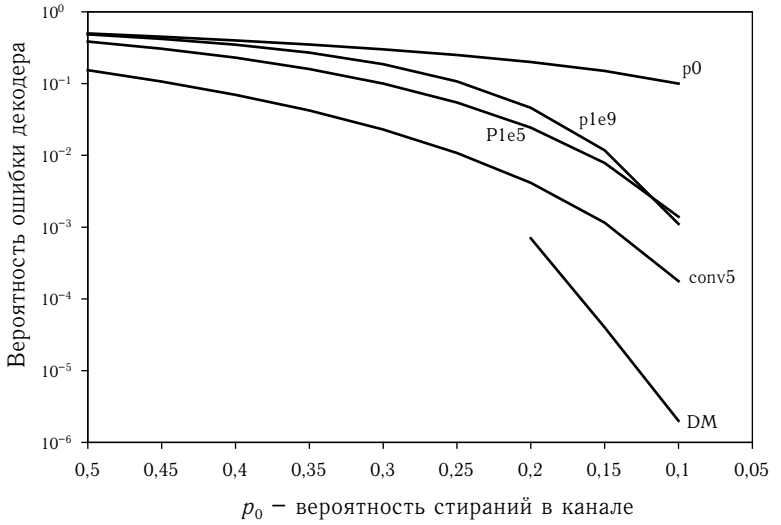

Рис. 1.17. Характеристики методов восстановления стёртых символов при передаче данных по стирающим каналам

женного выше. Поэтому мы добавили на графике нашу оценку для предложенного нами метода для варианта и его свёрточной реализации при $d = 5$ — график conv5. Как и следовало ожидать, свёрточный код обеспечивает более высокие характеристики восстановления, чем блоковый. И наш алгоритм в обоих реализациях, конечно, оказывается очень простым, контролирующим только проверки относительно декодируемого символа с целью выявления наличия таких, чтобы в них стёртым был бы только тот символ, который мы и пытаемся восстановить в данный момент.

Глава 2

Основные принципы многопорогового декодирования

Несмотря на значительные достижения техники помехоустойчивого кодирования, в этой важнейшей сфере исследований в области обработки цифровых потоков в условиях большого шума в списке серьезных нерешенных проблем по-прежнему числится недостаточно высокая эффективность простых методов коррекции ошибок и неоправданно большая сложность тех методов, которые могут обеспечить высокие значения ЭВК.

Хорошей иллюстрацией того, сколь высоких характеристик кодирования и последующего декодирования можно добиться, если почти не обращать внимания на сложность реализуемых алгоритмов, являются турбо коды [30] и многие другие методы подобного типа [31—35]. Они позволяют достичь достаточно высокой достоверности декодирования при отношениях E_b/N_0, в ряде случаев лишь на десятые доли децибела превышающих уровень энергетики, соответствующий равенству $R=C$. Но эти итеративные методы, появившиеся на двадцать с лишним лет позже многопороговых алгоритмов, нередко оказываются существенно более сложными или медленными, чем МПД декодеры. При этом за последние годы их характеристики для реализуемых вариантов построения декодеров фактически не изменились, хотя возможности микроэлектроники, в том числе и быстродействие, продолжают стремительно расти. Это не позволяет отнести такие методы к достаточно перспективным в ближайшем будущем.

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 [19, 20], а также внутренние декодеры тех каскадных схем кодирования [19, 27], которые обеспечивают большую эффективность.

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

В главе 1 указывалось, что одним из наиболее простых для реализации методов коррекции ошибок является пороговое декодирование [8]. Данный метод может использоваться для декодирования свёрточных и блоковых самоортогональных кодов. Пример схемы ПД для свёрточного кода с кодовой скоростью 1/2 и кодовым расстоянием $d = 5$, заданного порождающим полиномом $g(x) = 1 + x + x^4 + x^6$, был представлен на рис. 1.13.

Назовем две наиболее существенных причины того, что именно мажоритарные декодеры стали объектом многолетних исследований и разработок с целью создания высокоэффективных и простых методов коррекции ошибок.

Во-первых, крайне малое число операций на пороговом элементе такого декодера требует очень небольшого объема вычислений в разрабатываемых алгоритмах. При этом дополнительно оказывается, что сама процедура этих вычислений позволяет применять множество технологически удобных способов для повышения быстродействия порогового элемента, принимающего решения 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. Этот вопрос мы обсудим сразу в начале этой главы.

После обсуждения «излишней» корректирующей способности мажоритарных методов будут представлены на качественном уровне простые по своему существу, но исключительно важные для философии декодирования совершенно новые идеи, положенные в основу итеративных алгоритмов этого типа. Их главным свойством оказывается строгое приближение к оптимальному переборному (!) решению по максимуму правдоподобия при реализации коррекции символов методом многопорогового декодирования. Они положили начало оптимизационным методам декодирования как способам поиска глобального экстремума функционалов. Затем будут уже более формально рассмотрены алгоритмы этого типа для классического двоичного симметричного канала. Для систематических кодов будет строго доказана действительно уникальнейшая способность стремления решений МПД алгоритмов к решению оптимального декодера при всех изменениях контролируемых декодером символов. После этого будут сделаны некоторые обобщения этого алгоритма, существенные для техники декодирования и рассмотрены предельно возможные характеристики

двоичных СОК при оптимальном декодировании.

Затем будут описаны открытые более 30 лет назад символьные коды и соответствующие им q-ичные (символьные) многопороговые декодеры QМПД [1, 3–6, 36, 39, 40], после чего предложены нижние оценки для оптимального декодирования символьных кодов. Далее обсуждаются принципы работы МПД для каналов со стираниями и нижние оценки для вероятности ошибки оптимального декодирования в стирающих каналах. Последними будут предложены подходы к реализации идей стремления решений МПД алгоритма к решениям ОД для каналов с неравномерной энергетикой и коды с неравной защитой символов. Другие оценки и границы эффективности, реальные возможности МПД декодеров и некоторые важные прикладные вопросы будут рассмотрены в последующих главах книги.

2.1. Об «избыточной» корректирующей способности мажоритарных методов

Одной из важнейших причин выбора мажоритарного алгоритма как главного объекта исследований стала выявленная нами уже очень давно уникальная способность мажоритарных процедур исправлять во многих случаях гораздо большее число ошибок, чем это гарантируется минимальным кодовым расстоянием d используемого кода. Напомним, что в большинстве случаев для кодов на алгебраической основе (БЧХ, РС и других) исправление большего числа ошибок, чем $d/2$, является очень трудной проблемой [1]. И если многие полезные технологические достоинстъва мажоритарного (порогового) элемента для разных вариантов реализации порогового декодирования очевидны, то это выявленное нами полезнейшее обстоятельство, повлиявшее на наш выбор для глубоких исследований именно мажоритарных методов, необходимо обсудить немного более подробно.

Итак, на рис. 2.1 представлены экспериментальные результаты двукратного повторного декодирования в ДСК блокового самоортогонального кода с $R = 1/2$, $d = 11$ и $n = 1000$ с помощью обычного ПД. По оси абсцисс на графике отложено общее число ошибок канала в кодовом блоке перед его декодированием, а по оси ординат — доля правильно декодированных блоков. Кривая *1* соответствует первой попытке коррекции принятого кодового блока, а кривая *2* — второй коррекции этого же блока. Как следует из графиков, при 30 ошибках канала в блоке около 3/4 таких искажённых в канале связи типа ДСК сообщений полностью очищаются пороговым декодером от ошибок. Заметим, что гарантированно ПД обязан исправлять при $d = 11$ только 5 ошибок в блоке. Более того, даже при общем числе ошибок канала порядка 40 доля правильно декодированных блоков после пер-

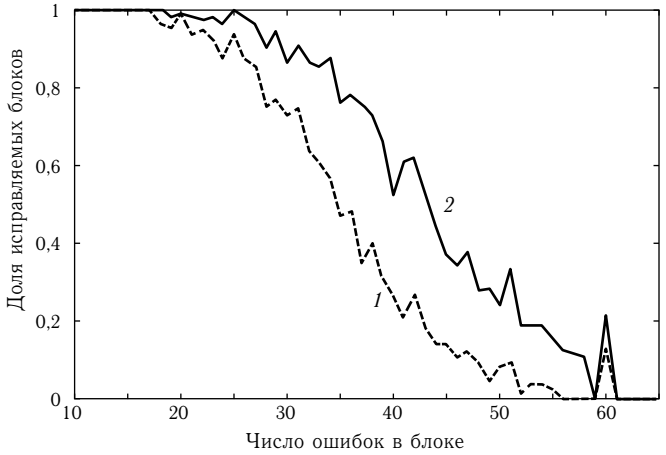

Рис. 2.1. Результаты моделирования повторного порогового декодирования СОК с $R = 1/2$, $d = 11$ и $n = 1000$:
1 — попытка 1; *2* — попытка 2

вой попытки составляет более 1/4. Далее важно отметить, что при числе ошибок в блоке порядка 50 и более пороговый алгоритм почти уже совсем не работает. Тем не менее, и при 40 ошибках ПД в заметной доле принятых блоков восстанавливает истинное сообщение, исправляя при этом в восемь раз больше ошибок, чем это гарантировано минимальным кодовым расстоянием $d = 11$. Но и этого мало! В рассматриваемом коде после второй попытки исправления ошибок число правильно декодированных блоков для исходных 40 ошибок увеличивается примерно ещё вдвое и приближается к половине. Отметим в связи с этим, что и при второй попытке коррекции ошибок пороговый декодер снова старается исправлять ошибки за пределами гарантированной корректирующей способности. Значит, и повторное декодирование в ПД тоже может быть полезным.

И хотя оказалось, что третья итерация декодирования для рассматриваемого кода практически ничего уже не дает в плане повышения доли правильно декодированных блоков, именно очень значительная «сверхнормативная» эффективность и первой, и второй попыток обычного порогового декодирования указывает на актуальность глубокой проработки потенциальных возможностей и исследования конкретных характеристик именно мажоритарных алгоритмов.

Подчеркнём, что столь большая «избыточная» корректирующая способность обычного порогового декодера и повторной попытки коррекции блока чётко указывают на то, что в этом эксперименте выявлены важные свойства мажоритарных схем, глубоким изучением

которых до сих пор почти никто не занимался. Но наша научная школа в течение длительного времени тщательно и, по нашему мнению, очень успешно исследовала это и другие интереснейшие свойства ПД. Результаты наших исследований будут представлены далее.

Итак, исходя из необходимости изучения высокоэффективных кодов при действительно минимально возможной сложности их декодирования, а также с учётом возможностей методов коррекции ошибок, рассмотренных в предыдущей главе, укажем основные причины выбора для глубоких разносторонних исследований именно мажоритарных процедур, лежащих в основе многопороговых алгоритмов:

- способность мажоритарных методов исправлять большое число ошибок за пределами гарантированной корректирующей способности;
- незначительная сложность пороговых процедур декодирования;
- способность разработанных МПД алгоритмов достигать оптимальных решений при весьма высоких уровнях шума в канале связи;
- легкость реализации МПД даже для очень длинных кодов, когда только и возможно достижение максимально возможных значений эффективности кодирования.

Описанию возможностей и анализу характеристик этих перспективных алгоритмов, созданных на основе ОТ, и посвящены следующие разделы этой книги.

2.2. Принцип глобальной оптимизации функционала

Развитие методов декодирования помехоустойчивых кодов в течение длительного времени совершенно удивительным образом никак не было связано с методами решения задачи глобальной оптимизации функционала от многих дискретных переменных. Тем не менее, декодирование, т. е. поиск, возможно, единственного кодового слова из экспоненциально большого числа возможных сообщений, наиболее близкого к принятому из канала зашумлённому вектору, совершенно естественно было бы рассматривать именно с таких позиций. Однако абсолютное большинство разрабатывавшихся ранее в течение многих десятилетий алгоритмов декодирования никак не использовало для поиска наилучших решений декодера широко известные разнообразные мощные оптимизационные процедуры поиска глобального экстремума. Их, несомненно, уже давно можно было бы применить к поиску кодовых слов, находящихся на минимально возможном расстоянии от принятого сообщения. Заметим при этом, что широко применяемый в технике связи алгоритм Витерби, повсеместно используемый

для декодирования по максимуму правдоподобия коротких свёрточных кодов, также не относится к классу оптимизационных процедур, поскольку он непосредственно ищет оптимальное решение на основе очень удобного в реализации метода полного перебора.

Среди других известных и используемых в технике связи алгоритмов коррекции ошибок, видимо, до недавнего времени нельзя было назвать ни одного метода, который мог бы претендовать, возможно, после некоторой модификации, на реализацию такого подхода, т. к. нам были неизвестны методы декодирования, точно измеряющие расстояние до принятого сообщения или хотя бы эффективно учитывающие это расстояние при декодировании.

Вместе с тем следует указать на то, что, в частности, классические пороговые декодеры Месси [8] уже почти обладают именно теми свойствами, которые необходимы для реализации полноценных эффективных и одновременно исключительно простых итеративных оптимизационных процедур декодирования. С помощью этих процедур, как оказалось, может осуществляться и поиск глобального экстремума функционала от очень большого числа переменных.

Для иллюстрации этого свойства ПД рассмотрим пример простейшей системы свёрточного кодирования/порогового декодирования для кода с кодовой скоростью $R = 1/2$ и минимальным кодовым расстоянием $d = 3$, показанный на рис. 2.2.

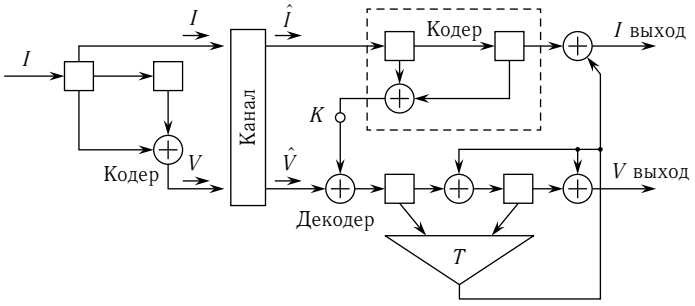

Рис. 2.2. Специальный вид системы свёрточного кодирования, поясняющий новую интерпретацию вектора синдрома

Как видим, в состав мажоритарного декодера, исправляющего в этом простейшем примере одну ошибку, входит точная копия кодера. Рисунки декодеров, в которых в качестве отдельного узла указывается такой же кодер, как и на передающем конце системы связи, можно найти в различных публикациях, в том числе в книгах [8, 11]. Эта копия формирует свои оценки проверочных символов кода по принятым из канала, возможно, с ошибками информационным символам

кода. Эти символы, содержащие теперь в качестве слагаемых ошибки в принятых информационных символах, появляются в точке K декодера и затем, после сложения на полусумматоре с принятыми из канала проверочными символами $\hat{V}$ (часть из которых тоже искажена) образуют символы вектора синдрома $\overline{S}$, который зависит только от вектора ошибок канала. Эти символы и поступают потом на пороговый элемент декодера T из синдромного регистра.

Однако до нас никто ранее не обращал внимания на следующее. 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. Обратимся к важнейшему для всей теории помехоустойчивого кодирования факту, который никогда не обсуждался для каких-либо линейных кодов ранее: в регистре синдрома декодера линейного кода 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 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. Введение в декодер порогового типа такого разностного вектора сразу решает проблему вычисления полной разности между принятым вектором и неким текущим кодовым словом, что и позволяет сразу сформулировать задачу построения правильной оптимизационной процедуры, которая будет минимизировать расстояние между последовательностью тех или иных выбираемых определённым способом кодовых слов и принятым вектором. В таком декодере (пока ещё неопределённого вида) будет содержаться текущее значение полной разности, что будет позволять измерение полного расстояния между текущим решением декодера, содержащимся в его информационном регистре, и принятым вектором. Именно это расстояние следует стремиться уменьшить самыми простыми процедурами до минимально возможного, что и будет соответствовать решению оптимального декодера, которое в современной теории кодирования обычно достигается переборными экспоненциально сложными от длины кода методами.

Такой подход к проблеме высокоэффективного декодирования и является основой развиваемых приблизительно с 1970 года специ-

альных итеративных многопороговых декодеров [2, 28, 38], весьма незначительно отличающихся от классических ПД и таких же простых в реализации, как и их прототип. Эти декодеры стали основой всей Оптимизационной Теории помехоустойчивого кодирования, которая к настоящему времени позволила создать алгоритмы декодирования, ставшие достойным решением проблемы Шеннона — простого эффективного декодирования при $R \lesssim C$.

Для дальнейшего изложения очень простого, но несколько необычного для традиционной теории кодирования материала, важно указать, что в отличие от ситуации, представленной на рис. 2.2, на вход внутреннего кодера в декодере (справа) совсем не обязательна подача именно того информационного (возможно, частично искаженного) вектора, который поступил в декодер из канала связи. На вход этого кодера, содержащегося в декодере, можно подать любой информационный поток. В этом случае вектор синдрома, конечно, будет разностью по проверочным символам принятого из канала вектора уже с тем другим кодовым словом, информационные символы которого подавались перед началом процедуры декодирования на вход внутреннего кодера. Это расширенное понимание синдрома сообщения будет активно использоваться при последующем рассмотрении свойств МПД. Существование возможности подачи любого информационного вектора на вход декодера позволяет расширить возможности алгоритма, который мы создадим для реализации очень эффективной оптимизационной процедуры. Он сможет начинать работать и решать проблему оптимизации не только с той гипотезы об информационной части, которая пришла к нему из канала, но и с любой другой исходной гипотезы о принятом сообщении. Он лишь должен начинать оптимизацию функционала из правильного состояния, для чего одновременно с вычислением синдрома в новом введённом нами в декодер разностном векторе нужно пометить те позиции, которые у произвольно выбранного информационного вектора не совпадают с информационными символами, принятыми из канала. Но у декодера сначала никогда нет более предпочтительного решения, чем принятый информационный вектор. Поэтому понятно, что в обычной ситуации всякий декодер, который возьмёт на себя решение оптимизационной задачи, начнёт декодирование именно с исходной гипотезы о том, что первая версия информационного потока, которую надо улучшить, — это принятый из канала вектор. Ясно, что исходное состояние разностного вектора будет при этом полностью нулевое. Однако очень полезно понимание того, что исходные гипотезы, по меньшей мере, для декодера, который будет оптимизировать функционал расстояний между векторами, могут быть различными! Такое свойство оптими-

зационного декодера может пригодиться, если сама оптимизационная процедура начинается после того, как принятое сообщение было сначала декодировано каким-то другим алгоритмом.

Напомним, что для двоичных кодов в канале типа ДСК нужно измерять расстояние Хемминга, т. е. число единиц в векторе синдрома, который, как мы выяснили выше, является разностью по проверочным символам между теми векторами, для которых мы создаём оптимизационную процедуру. И в это расстояние, как мы теперь понимаем, ещё обязательно включаются те единички, которые могут быть в разностном векторе $\overline{D}$, поскольку мы ввели его именно таким образом, что единички в разностном векторе ставятся там, где символы у информационных векторов — принятого и исходного стартового — для процедуры оптимизации не совпадают.

Итак, мы получили, что изменения, которые необходимо сделать в обычном ПД, чтобы преобразовать его в декодер, знающий разность между исходной гипотезой о его решении, т. е. стартовым информационным вектором, который будет улучшаться, и принятым вектором, состоят просто в том, чтобы сначала запомнить в дополнительном разностном регистре D (первоначально, возможно, нулевом) возможные несовпадения в информационном стартовом векторе и в информационном векторе, принятом из канала. Но что же должен затем конкретно делать декодер при реализации правильного процесса оптимизации?

Для поиска возможно более простого решения посмотрим сначала, что делает при декодировании самый обычный ПД. Ведь рассмотренные выше на рис. 2.1 чрезвычайно мощные корректирующие возможности ПД должны быть свидетельством каких-то очень важных свойств этого, казалось бы, очень примитивного алгоритма.

В самом деле, мы уже понимаем, что единички в разностном и синдромном векторах являются мерой расстояния по Хеммингу, его компонентами. Посмотрим далее, что происходит с векторами, которые содержатся в ПД, при обычном декодировании и изменении при этом вектора синдрома и декодируемого информационного символа. Напомним, что информационный символ будет в ПД изменён для рассматриваемого декодера, если сумма единичек на ПЭ, поступивших из проверок для декодируемого символа, больше половины, т. е. для конкретного декодера на рис. 1.13 равна 3 или 4. Но после завершения коррекции при инверсии всех проверок их сумма станет менее половины от числа проверок, т. е. 1 или 0. А чем тогда станет вектор синдрома? Легко проверить, что он станет разностью (конечно, опять только по проверочным символам!) между уже новым кодовым словом, которое теперь уже отличается от стартового исходного в том единственном информационном символе, который был инвертирован

с помощью ПД. И поскольку вес вектора синдрома, как мы только что оценили, уменьшился на 2 или на 4, то получим, что разность по проверочным символам у нового решения ПД лучше, т. е. меньше именно на столько же. Но по информационным символам новое решение может быть дальше, чем принятый вектор. Однако эта разница составляет только единичку, на которую может возрасти расстояние по информационным компонентам. Значит, новое решение обычного ПД всё равно обязательно ближе к принятому сообщению по совокупности всех информационных и проверочных символов, чем предыдущее. В этом случае после изменения соответствующего символа в разностном векторе $\overline{D}$ этот вектор и вектор синдрома снова дадут полное расстояние уже между новой гипотезой и принятым из канала вектором. Значит, после первой корректировки символа в принятом векторе мы получили такое состояние векторов в декодере, которое позволяет провести и следующую корректировку символов, после которой опять произойдёт обязательное приближение к оптимальному решению, поскольку суммарный вес векторов $\overline{D}$ и $\overline{S}$ снова строго уменьшится.

Но теперь получается, что больше ничего в процедуре декодирования изменять уже и не надо. ПД с правильно заполненным перед самым первым декодированием разностным регистром всегда будет изменять декодируемый символ тогда и только тогда, если полное расстояние нового возможного кодового слова с этим изменённым информационным символом до принятого сообщения будет меньше, чем у исходного кодового слова, которому соответствовало состояние ПД перед изменением контролируемого на этом шаге символа.

Таким образом, после каждой попытки коррекции контролируемого пороговым элементом символа содержимое всех трёх регистров — информационного, разностного и синдромного — в новом пороговом декодере точно соответствует такому же состоянию, которое было и перед первой попыткой декодирования: совокупность разностного и синдромного регистра соответствует разности между текущей гипотезой о решении декодера и принятым вектором. Но это значит, что декодер может снова просуммировать все проверки с учётом и соответствующей ячейки разностного регистра, а затем изменить декодируемый символ, если сумма проверок на ПЭ будет больше $J/2$. А в этом случае новое решение-гипотеза декодера будет всегда хотя бы на единичку ближе к принятому сообщению и т. д.

Итак, путём относительно простых рассуждений мы нашли, как нужно изменить ПД, чтобы он выполнял процедуру оптимизации функционала, который позволяет искать оптимальное решение декодера не экспоненциально сложными от длины кода способами, а про-

стыми неперебо́рными методами с минимально возможной линейной от длины кода сложностью. Подчеркнем, что содержимое соответствующей ячейки из разностного регистра нужно всегда подавать на пороговый элемент тоже. В этом случае ПЭ сразу будет точно оценивать полное расстояние сравниваемых кодовых слов до принятого вектора, а при изменении декодируемого символа он будет автоматически инвертировать и разностную ячейку. Этим и закончим описание нового метода для реализации процедуры оптимизационного декодирования на базе мажоритарных схем.

Декодер типа МПД для свёрточного СОК с $R = 1/2$, $d = 5$ и $n_A = 14$, рассмотренного ранее в качестве примера, представлен на рис. 2.3. Отметим ещё раз, что, согласно правилу работы МПД, первоначально при его обычной работе с сообщением, принятым из канала связи, в его разностном регистре D находятся только нули. Таким образом, на первой итерации коррекции ошибок МПД функционирует точно так же, как и обычный ПД. 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].

Декодер после этого достаточно простого усовершенствования приобретает новые, чрезвычайно полезные свойства [3–5, 36]. Реше-

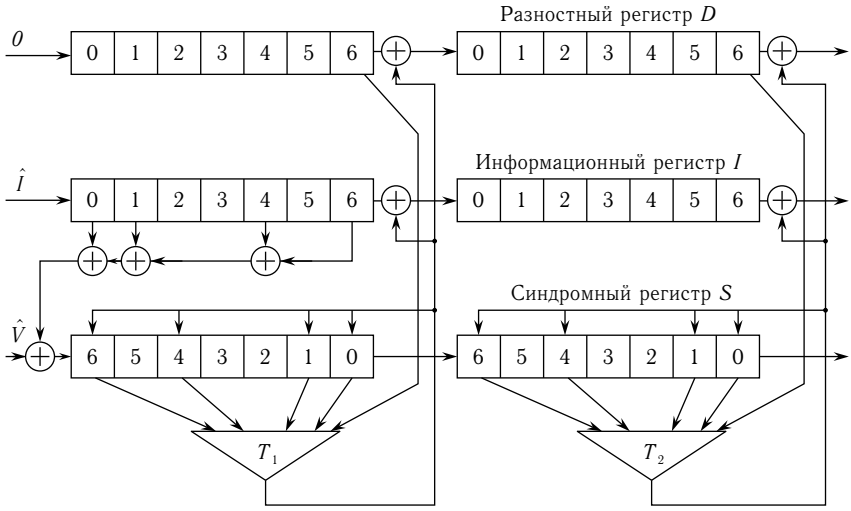

Рис. 2.3. Декодер типа МПД для свёрточного кода с $R = 1/2$, $n_A = 14$ и $d = 5$ при $I = 2$ итерациях

ния МПД при каждом изменении декодируемых им информационных символов строго приближаются к решению оптимального декодера, т. е. становятся строго более правдоподобными, обеспечивая во многих случаях реализацию этого процесса даже после нескольких десятков попыток коррекции кодового блока или потока символов свёрточного кода. Иными словами, МПД алгоритм, каждый раз измеряя расстояние своего решения до принятого вектора и уменьшая его при каждой коррекции декодируемого сообщения, фактически осуществляет поиск глобального экстремума (минимума расстояния!) при линейной сложности реализации этой процедуры.

Подчеркнем, 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 будет рассмотрен позже.

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 Хемминга $r = |\overline{Q} \oplus \widetilde{A}|$ (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 модулю 2; $|x|$ — вес Хемминга для вектора x) было бы минимальным по всему множеству кодовых

слов $\{\overline{A}\}$. Но такие алгоритмы обычно неоправданно сложны.

Для удобства доказательства последующих утверждений будем 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 проверочной частям вектора:

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

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

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

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

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 $H(\overline{0}_I, \overline{A}_V \oplus \overline{Q}_V) = \overline{A}_V \oplus \overline{Q}_V$, т. к. $\overline{A}_V \oplus \overline{Q}_V$ умножается только на единичную подматрицу I матрицы H, то вектор $\overline{S}$ равен

$$\overline{S} = \overline{A}_V \oplus \overline{Q}_V. \tag{2.3}$$

Проводя в правой части (2.1) замены с учётом (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 искаженным сообщением и определенным выше кодовым словом. ***Лемма доказана***.

Её содержание заключается в том, что разность $\overline{B} = \overline{Q} \oplus \overline{A}$ для любого кодового слова $\overline{A}$ и принятого вектора $\overline{Q}$ определяется парой векторов $(\overline{D}, \overline{S})$. 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 и при $\overline{D} \neq 0$ называть $\overline{S}$ *синдромом*, поскольку это обобщение естественно и не приводит в дальнейшем к каким-либо противоречиям.

Перебором всех возможных векторов $\overline{A}$ можно найти вектор $\widetilde{A}$, минимизирующий $|\overline{B}|$ и являющийся решением ОД. К сожалению, переборные алгоритмы декодирования слишком сложны. Поэтому рассмотрим алгоритм декодирования, единый для блоковых и свёрточных кодов, который очень близок к известному 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:

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

Напомним ещё раз, что обычно первоначально $\overline{D} = 0$, поскольку перед началом операций декодирования в памяти декодера есть только принятый вектор $\overline{Q}$, т. к. декодер не имеет никаких других более предпочтительных гипотез о переданном сообщении. Однако мы не будем использовать в доказательстве теоремы возможность того, что $\overline{D} = 0$.

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, а также i_j и d_j инвертируются при $L_j > T$ и остаются неизменными при $L_j \leqslant T$.

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, если все $d_j = 0$, совпадает с обычным алгоритмом для ПД. Будем в дальнейшем называть декодер, реализующий предлагаемый алгоритм, *многопороговым декодером*. 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 10, 50 и более раз. Разумеется, при этом часть конкретных решений декодера может быть на каких-то символах принятого сообщения ошибочной. Однако некоторые из этих ошибок могут быть исправлены при следующих итерациях декодирования тех же символов. При этом справедлива следующая теорема.

Основная Теорема многопорогового декодирования (ОТМПД) [2–5, 36–38]: 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

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

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 $L_{2j} < L_{1j}$ и, следовательно, $|\overline{B}_1| > |\overline{B}_2|$, чем доказан пункт а) теоремы.

Далее, очевидно, что 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 $\overline{S}_2 = H\left(\overline{Q}_I \oplus \overline{D}_2, \overline{Q}_V\right)$. Здесь $\overline{D}_2$ отличается от $\overline{D}_1$ в символе d_j, а 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

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

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 теперь уже и формально доказано, что МПД при каждом изменении декодируемых символов приближается к принятому вектору $\overline{Q}$, отыскивая тем самым новые текущие, все более правдоподобные векторы-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, причём 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, декодер 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 $\widetilde{A}$, ближайшему к $\overline{Q}$. Принципиально важно, что при этом сложность МПД остается такой же, как и у обычного ПД, — линейной, т. е. теоретически минимально возможной.

Итак, Основная Теорема многопорогового декодирования устанавливает, что простейшая из известных процедур порогового типа при каждом изменении декодируемых символов обеспечивает строгое приближение к оптимальному решению, т. е. строгий рост правдоподобия каждого нового решения МПД, реализуя простую эффективную процедуру поиска глобального экстремума, в нашем конкретном случае — минимума расстояния от принятого сообщения до ближайшего к нему кодового слова. При этом сложность процедуры для сообщения длины k становится пропорциональной не 2^k, а просто k. Ни для каких других алгоритмов декодирования небольшой сложности не известно аналогичное доказанное свойство строгого монотонного стремления решений алгоритма к решению ОД.

Заметим, что из доказанной теоремы следует, что применение МПД возможно для любого стартового кодового вектора, например, от результата декодирования принятого сообщения каким-либо другим алгоритмом.

Хотя для МПД алгоритма только что доказана уникальная теорема о стремлении его решений к решению ОД, не следует забывать, что речь идет 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 битах сообщения. 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 отдельных 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 и при этом относительно всего сообщения, принятого из канала, каждое новое промежуточное решение МПД, как следует из Основной Теоремы, будет всегда строго более правдоподобным.

Именно такое поведение МПД хорошо наблюдается при анализе процесса декодирования в компьютерном демо-мультфильме, который можно переписать со специализированного веб-сайта ИКИ РАН www.mtdbest.iki.rssi.ru или ресурса РГРТУ www.mtdbest.ru (гиперссылки «описание» [67] и «демонстрационная программа» [68] на странице «О методе»). В «Описании» приведена инструкция по использованию этой программы.

Наконец, заметим, что из только что доказанной ОТМПД 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. Все следующие главы этой книги будут посвящены поискам таких кодов и декодеров, для которых процесс декодирования даже для большого уровня шума действительно будет почти всегда продолжаться до тех пор, пока не будет достигнут вектор $\widetilde{A}$ — решение переборного оптимального декодера.

Допустим далее, что МПД достиг решения ОД, т. е. в информационном регистре МПД находятся символы вектора $\widetilde{A}$. Тогда справедливо **следствие**: 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, следствие доказывает один из аспектов устойчивости решения МПД относительно оптимального решения: достигнув его, МПД останется в нем. Это очень важно, поскольку алгоритм допускает возможность многократного изменения одних и тех же декодируемых символов.

Можно также заметить, что при доказательстве ОТМПД 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 из нескольких информационных символов. Формальное доказательство этого очевидного результата приведено в [3, 36].

Из целого ряда некоторых других доказанных свойств МПД, например в [3, 36], можно указать на то, что большинство случаев, когда МПД в процессе работы не может исправить оставшиеся одиночные ошибки, соответствует ситуациям, когда и ОД декодирует их неправильно. Кроме того, полезно учитывать, что МПД обладает свойством устойчивости, которое позволяет практически всегда восстанавливать редкие одиночные отклонения решений такого декодера от оптимальных. Эти и ряд других полезных особенностей МПД были ранее рассмотрены также в [38].

2.4. Гауссовский канал

Важнейшим обобщением МПД алгоритма является его способность так же, как и у алгоритма Витерби, работать в двоичном гауссовском канале с мягким модемом, который допускает при оптимальном приёме символов в канале FM-2 квантование своих решений на 4, 8 или 16 уровней. Это увеличивает пропускную способность канала в такой степени, что АВ и МПД обеспечивают с теми же кодами примерно на 2 дБ более высокий ЭВК, а для цифровых систем это весьма важное улучшение их основных параметров. График зависимости пропускной способности канала для разных значений кодовой скорости R и $M=2$ (жёсткий модем, канал ДСК), а также $M=16$ (мягкий модем) был представлен на рис. 1.8.

В чём суть трансформации МПД для мягкого модема? Это определяется тем же, почему в канале класса ДСК оптимальное решение должно отличаться от принятого сообщения в минимальном числе символов. В самом деле, если найдётся какое-то кодовое слово, которое отличается от принятого сообщения в m_0 символах, а другое будет иметь m_1 несовпадающих символов, $m_0 > m_1$, то мы тем самым допускаем, что при вероятности ошибки в канале ДСК p_0 вероятность передачи первого кодового слова в $\left(p_0/(1-p_0)\right)^{(m_1-m_0)}$ раз меньше, чем второго. Поэтому оптимальное решение и носит название «по максимуму правдоподобия», что оно для принятого из канала сообщения соответствует наиболее правдоподобному кодовому слову, т. е. самому вероятному из всего экспоненциально большого их множества. Таким образом, весом Хемминга в разностном и синдромном векторах в ДСК легко оперировать, но при декодировании на самом деле ведётся поиск наиболее вероятного кодового слова.

Так вот при переходе к гауссовскому каналу это правило поиска именно наиболее вероятного кодового слова, конечно же, сохраняет-

ся, но, согласно [3—5], для этого необходимо вычислить взвешенную функцию правдоподобия

$$L_j = W_{j\,\mathrm{inf}}(2d_{j\,\mathrm{inf}} - 1) + \sum_{j\upsilon=1}^{d-1} W_{j\upsilon}(2s_{j\upsilon} - 1), \qquad (2.5)$$

где $W_{j\,\mathrm{inf}}$ и $W_{j\upsilon}$ — веса информационных символов и проверок, небольшие целые или действительные числа. Они характеризуют надежность оценок достоверности мягкого приема символов из гауссовского канала. При этом $d_{j\,\mathrm{inf}}$ — значение 0 или 1 соответствующей ячейки в разностном регистре D, как это было и в случае жесткого МПД для ДСК; $s_{j\upsilon}$ — обычные символы регистра синдрома S, являющиеся проверками декодируемого символа i_j и равные 0 или 1.

Изменение декодируемого символа i_j происходит, если L_j в (2.5) положительно. В таком мягком МПД каждое новое решение также оказывается строго более правдоподобным, чем его предыдущее промежуточное решение, т. е. более вероятным для данной конкретной реализации принятого сообщения.

При $M = 2$ уровнях квантования (2.5) превращается в обычную мажоритарную функцию для проверок в МПД для ДСК, все веса которых $W_{\mathrm{inf}} = W_{j\upsilon} = 1$. Заметим ещё раз, что использование мягких решений модема столь же эффективно в МПД, как и в случае реализации алгоритма Витерби, позволяя при всех типичных значениях скорости R и уровня шума в канале повысить ЭВК декодера МПД примерно на 2 дБ.

2.5. Предельные возможности МПД алгоритмов в гауссовских каналах

Рассмотрим снова МПД алгоритм, осуществляющий декодирование в двоичном симметричном канале, который может быть технически реализован в гауссовском канале, когда в приёмнике используется жёсткий модем с $M = 2$ уровнями квантования.

Рассмотрим линейный двоичный мажоритарно декодируемый самоортогональный код с кодовой скоростью $R = k_0/n_0 = 1/2$ и $d = 2t_0 + 1$, т. е. исправляющий t_0 ошибок.

Оценим 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 оценка вероятности перехода решения ОД в ближайшее конкретное кодовое слово с одной информационной единицей $P_{b\mathrm{ОД}}(e)$ на заданной позиции имеет для ДСК без памяти вид, соответствующий наличию ошибок канала более чем

в половине из d ненулевых позиций этого кодового слова:

$$P_b(e) = P_{b\text{ОД}}(e) = \sum_{i=(d+1)/2}^{d} C_d^i p_0^i (1-p_0)^{d-i}. \qquad (2.6)$$

Графики зависимости вероятности ошибки на бит $P_b(e)$ от уровня шума канала для СОК, имеющих большое значение для МПД алгоритмов, приведены в [3, 4], а соответствующие данные — в табл. П-2 в Приложении 2. Эти оценки оптимального декодирования оказываются существенно нижними, поскольку никак не связаны с кодовой скоростью этих кодов, учёт которой существенно повышает вероятность ошибки при большом уровне шума. Однако при соотношениях шума канала и кодовых скоростей, близких к $R \sim R_C$, где R_C — вычислительная скорость канала, и даже при немного более высоком уровне шума выражение (2.6) дает достаточно правильные значения для предварительных оценок вероятности ошибки на бит $P_b(e)$ МПД при достаточно большом числе итераций декодирования $I \approx 10-50$ и выборе кодов, устойчивых к эффекту РО.

Для гауссовского канала и мягкого модема при приёме сигнала FM-2, квантованного на 16 уровней, также можно найти нижние оценки вероятности ошибки в СОК при оптимальном декодировании. Оценим предельные возможности мягких МПД методами, которые использовались для оценки снизу характеристик ОД в канале типа ДСК. Тут также будем вычислять вероятности ошибки при определении значения декодируемого символа в СОК 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 этих решений. В достаточно общем случае выполнения требуемых оценок можно определить ПФВ отдельного символа для мягкого модема:

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

Тогда для рассматриваемого кода с $d = J-1$ вероятность ошибки на бит при правильном выборе областей решений мягкого модема будет определяться выражением

$$P_{b\text{ОД}}(e) = \sum_{i>0} c_i, \qquad (2.7)$$

где c_i определяются из выражения

$$A_d(x) = A_M(x)^{J+1} = \sum_{\{I\}} c_i x^i \qquad (2.8)$$

и где $\{I\}$ — множество всех возможных значений показателей степени, получающихся при обычном возведении ПФВ в степень.

Нижние оценки вероятности ошибки на бит $P_{b\text{ОД}}(e)$ для ОД при $M = 16$ и различных значений d, вычисленные согласно (2.7)–(2.8), также представлены в виде графиков в [3—5] и таблицей в Приложении 2. Сопоставление этих графиков с результатами для канала ДСК показывает, что мягкие ОД на самом деле на 1,5...2 дБ более эффективны, чем жёсткие. Это весьма большое преимущество мягкого приема имело решающее значение при почти полном переходе к мягким декодерам во многих реальных системах и сетях связи, особенно при использовании в них алгоритма Витерби.

Для мягких МПД полученные выше оценки, как и в случае ДСК, также являются несколько заниженными. Их справедливость также сохраняется для большого числа вариантов МПД декодирования, если только $R \sim R_C$, где R_C — вычислительная скорость гауссовского канала. Для достижения высокой эффективности декодирования в гауссовском канале мягкий МПД также должен выполнить достаточно большое число итераций. Для эффективной работы непосредственно в области при $R \lesssim C$ может оказаться необходимым около $I \sim 50 - 100$ итераций декодирования мягкого свёрточного МПД. В некоторых случаях это число может быть и существенно большим. Но это на самом деле вполне допустимо, т. к. для некоторых других итеративных методов число выполняемых итераций декодирования при большом шуме может быть гораздо более значительным. При этом одна итерация в МПД, жёстком или мягком их вариантах, достаточно проста.

Отметим, что для СОК вероятность ошибки на бит $P_{b\text{ОД}}(e)$ для МПД и ОД на много порядков меньше, чем вероятность $P_1(e)$ ошибки обычного ПД в первом символе кода с достаточно большим минимальным расстоянием $d \gg 1$. Поэтому разработки всё более эффективных методов декодирования, в том числе и для СОК, продолжаются, как и поиск самих СОК со всё меньшей зависимостью от эффекта РО.

2.6. Символьные (недвоичные) коды

В реальных системах передачи и хранения данных, как мы уже отмечали ранее, часто сразу полезнее оперировать с данными, имеющими байтовую структуру. Например, удобнее работать с байтами и группами байтов в системах хранения больших объемов информации (оптические диски и другие носители). В подобных системах для

защиты данных от ошибок целесообразно применение недвоичных помехоустойчивых кодов.

Рассмотрим канал типа QCK, описанный в разделе 1.3, с размером алфавита $q > 2$ и вероятностью p_0 искажения символов. Для такого канала в первой главе был описан абсолютно эвристический, «угаданный» неплохой символьный пороговый декодер, реализующий для данного алфавита процедуру, аналогичную обычному двоичному ПД. Однако нам сейчас нужно создать такой алгоритм, который будет выполнять оптимизацию функционала, т. е. будет с использованием итеративных процедур искать экстремум, конкретно, минимум расстояния до принятого сообщения на множестве всех допустимых кодовых слов. Для этого нужно придумать некоторую итеративную процедуру, которая будет реализовывать именно эту функцию поиска глобального экстремума. Напомним, что расстоянием Хемминга для недвоичных векторов называется число несовпадающих символов в двух векторах равной длины.

Рассмотрим, какими свойствами должен обладать соответствующий декодер, который далее будем называть *символьным МПД* (QМПД) [1, 3–5, 36].

Пусть согласно [8] задан линейный недвоичный систематический свёрточный или блоковый код с размером алфавита q на основе самоортогонального кода с некоторым минимальным кодовым расстоянием d. Его порождающая матрица имеет вид $G = (I : P)$, а проверочная матрица H 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, т. е. $H = (P^T : -I)$. Назовем этот код символьным, т. к. на его основе можно кодировать любые байтовые, многобайтовые и многие другие данные, используемые в цифровой технике.

Пусть в соответствии с порождающей матрицей символьного кода проверочные символы рассматриваемого блокового или свёрточного кода в кодере на передающей стороне системы связи формируются как суммы по $\bmod q$ некоторого числа информационных символов. Можно реализовать и много других правил сложения q целых чисел, создавая тем самым некоторую группу по сложению. Далее полученные информационные и проверочные символы кода передаются по каналу типа QCK со средней вероятностью ошибки в каждом символе p_0.

После передачи кодового вектора $\overline{A}$ 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: $\overline{Q} = \overline{A} + \overline{E}$, где $\overline{E}$ — вектор шума канала типа QCK; «+» и «–» — операции сложения и вычитания; $\overline{A}$ — некоторое произвольное кодо-

вое слово. Здесь и далее будем полагать, что все операции сложения и вычитания матриц и векторов будут производиться в некоторой группе целых чисел, например, по модулю q.

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.

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 2.2.

$$(\overline{D},H(\overline{Q}_I+\overline{D},\overline{Q}_V))=\overline{A}-\overline{Q}. \tag{2.9}$$

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 $\overline{S}=\overline{A}_V-\overline{Q}_V$. 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, полностью аналогичное двоичному случаю [1—5, 36—38], представленному в лемме 2.1. Лемма 2.2 позволяет доказать главное свойство QМПД, 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 вычислению синдрома $\overline{S}$ принятого сообщения являются только сложениями или вычитаниями. Таким образом, для кодирования и, как мы увидим далее, декодирования не требуется не только наличия 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. Кроме того, подчеркнём, что результатом только что доказанной леммы является то, что с учётом понятия расстояния Хемминга для недвоичных символов, которое соответствует числу несовпадающих символов на соответствующих позициях двух векторов равной длины, вес синдрома S и разностного вектора $\overline{D}$ определяет расстояние между векторами: принятым из канала Q и некоторым промежуточным кодовым словом-решением. А это означает, что для уменьшения расстояния между кодовым словом и принятым сообщением в недвоичном случае, как и в двоичном, нужно

стремиться к увеличению общего числа нулей в синдроме и разностном векторе.

С учётом только что рассмотренных свойств символьных кодов и векторов $\overline{S}$ и $\overline{D}$ опишем алгоритм функционирования QМПД. Пусть при передаче по QCK кодового слова $\overline{A}_0$ в декодер поступил искаженный 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 QМПД 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 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, причём $m_0 \geqslant m_1$. Эта процедура аналогична подсчёту суммы проверок на пороговом элементе двоичного МПД.

2. Если $m_0 - m_1 > T$, где T — целое неотрицательное число, и $h \neq 0$, то из i_j, d_j и всех J проверок относительно i_j вычитается оценка ошибки, равная h_0. Этот шаг является аналогом процедуры сравнения суммы с порогом в двоичном декодере и изменения декодируемого символа и коррекции через обратную связь символа d_j и всех символов синдрома, являющихся проверками декодируемого символа.

3. Происходит выбор нового i_m, $m \neq j$ и переход к п.1.

Такие попытки декодирования по пп. 1–3 могут быть повторены для каждого символа принятого сообщения, например, три, десять и более раз. Заметим, что 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. Пример схемной реализации QМПД представлен в [1].

Для описанного алгоритма QМПД справедлива теорема.

Основная Теорема многопорогового декодирования недвоичных (символьных) кодов (ОТQМПД). Пусть декодер реализует алгоритм QМПД для описанного выше кода. Тогда при каждом изменении декодируемых символов происходит переход к более правдоподобному решению по сравнению с предыдущими состояниями декодера.

Доказательство теоремы дано в [3, 39]. При доказательстве аналогично двоичному случаю показывается, что суммарный вес Хем-

минга синдромного и разностного регистров при каждом, возможно, многократном изменении декодируемых символов в соответствии с вышеописанным алгоритмом QМПД всегда только строго уменьшается. И при этом после каждого шага коррекции векторы $\overline{D}$ и $\overline{S}$, находящиеся в памяти декодера, соответствуют разности принятого сообщения $\overline{Q}$ и очередного текущего решения-гипотезы декодера о переданном кодовом слове. А это и есть процесс последовательного перехода ко всё более правдоподобным вариантам кодовых слов, всё в меньшей степени отличающихся от принятого вектора $\overline{Q}$, которые могут быть очередным улучшенным решением QМПД, чем и реализуется процедура поиска глобального экстремума для символьных кодов. И здесь тоже можно надеяться, что во многих случаях этот поиск будет успешным, т. е. глобальный минимум (!) будет достигнут. Всё доказательство основывается на том, что символьный ПЭ изменяет декодируемый символ только в том случае, если для него есть m_0 проверок с одинаковым ненулевым значением, которые встречаются строго чаще, чем m_1, $m_0 > m_1$, других $q-1$ возможных значений. А это и гарантирует обязательное увеличение числа нулевых значений проверок, конечно, с учётом изменения соответствующего символа d_i разностного регистра, после коррекции декодируемого символа.

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 QМПД, но которые могут быть исправлены в ОД. Таким образом, QМПД также не является ОД. Поэтому основной способ повышения эффективности QМПД опять же 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 [8] (и это оказывается главным моментом в революционной смене главных алгоритмов декодирования для недвоичных кодов!), в QМПД для правильного изменения декодируемого символа достаточно наличие не абсолютного, а только относительного строгого большинства правильных проверок, как это следует из условия $m_0 - m_1 > T$ в п. 2 описания алгоритма. Таким образом, мы видим, что это очень неожиданное свойство QМПД, «угаданное» при формулировке алгоритма обычного символьного ПД, сохранилось и в QМПД. Напомним ещё раз в связи с этим, что, например, в самоортогональном коде с $d = 9$ ошибка в декодируемом

символе будет исправлена даже в том случае, если из девяти его проверок (включая и символ d_j разностного регистра) правильными будут только две, а остальные семь — ошибочными. Этого вообще невозможно представить для двоичных кодов, а для QМПД такая ситуация типична. Нужно только, чтобы алфавит символьного кода был достаточно большой, т. е. $q \gg 1$, чтобы почти всегда все поступающие на символьный ПЭ проверки имели различные значения.

Указанные свойства QМПД существенно расширяют возможности этого алгоритма по сравнению с одношаговой процедурой при работе в больших шумах, сохраняя при этом весьма малую сложность реализации.

Другая особенность предложенного QМПД алгоритма заключается в том, что его решения стремятся к решению ОД, но при этом сложность их реализации линейно зависит от длины кода, в то время как обычно оптимальные методы характеризуются экспоненциально нарастающей с длиной кода сложностью. Поэтому применение недвоичных МПД представляется особенно желательным.

Заметим, что за более чем полувековой период развития теории и техники кодирования из недвоичных кодов в реальных системах связи фактически использовались только коды Рида — Соломона, прекрасно изученные и реализованные во множестве своих модификаций. 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 очень далеки от потенциальной шенноновской границы их корректирующих возможностей при $R = C$ просто потому, что реально в технике связи можно использовать только короткие коды РС. При этом ориентировочно сложность декодирования кодов РС можно оценить как $\sim n^2$ (правда, в асимптотике она несколько меньшая), что существенно больше, чем линейная от n сложность QМПД, который во многих случаях ещё и обеспечивает наилучшее решение, эквивалентное по вероятности ошибки переборному. Поэтому задача реализации максимально простых недвоичных алгоритмов для кодов, гораздо более длинных, чем коды РС, остается чрезвычайно актуальной, поскольку для выбранного основания кода q максимальная длина n недвоичного кода РС обычно не может превышать q символов. В связи с этим в настоящее время коды РС длины более 256 применяются достаточно редко. Для QМПД такого ограничения по длине кода нет в принципе, т. к. параметры n и q в символьных кодах никак не связаны. Таким об-

разом, QМПД алгоритмы могут полностью взять на себя все задачи, решаемые сейчас на основе кодов РС, причём при меньшей сложности и большей достоверности. Но ещё более существенно то, что в случае больших значений основания кода $q \gtrsim 10$, практически абсолютно невозможно создать никакие истинно оптимальные эффективные декодеры, в том числе и алгоритм Витерби, поскольку при этом, аналогично двоичной передаче, их сложность в большинстве случаев, видимо, будет иметь порядок q^k или q^{n-k}, где k — длина кодирующего регистра, выраженная числом q-ичных символов, n — длина кода. Поэтому даже для $q = 16-64$ реализация ОД для кодов длиннее $k \approx 5$ очень проблематична, а их эффективность для таких малых длин будет совершенно незначительной. С другой стороны, например, код РС для $q = 256$ при любой избыточности работоспособен только при весьма малых уровнях шума. Это и определяет особую ценность применения QМПД, которые, как будет показано далее, действительно оказываются значительно более эффективными, чем декодеры кодов РС, и могут при любых вариантах размера алфавита q использоваться с кодами сколь угодно большой длины [1, 3—5]. При этом сложность реализации QМПД будет всегда весьма незначительной и иметь тот же порядок, что и в двоичном случае, т. е. расти с увеличением длины кода только линейно.

2.7. Нижние границы эффективности символьных МПД

Рассмотрим потенциальные возможности символьных МПД при использовании СОК кодов. Как и при анализе корректирующих возможностей простого QПД, мы можем повторить все рассуждения о проверках, которые контролирует его пороговый элемент, и затем посмотреть, в каких ситуациях будет ошибаться даже оптимальный (переборный!) декодер, поскольку QМПД стремится к оптимальному решению как к результату процедуры поиска глобального экстремума.

Для оценки потенциальных возможностей QМПД через нижние оценки вероятности ошибки ОД несколько удобнее выявлять наиболее часто встречающиеся условия 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 декодируемого символа i_0. Выпишем вероятности таких наиболее частых событий, которые всегда приводят к ошибкам ОД для СОК с минимальным кодовым расстоянием $d = J + 1$.

К искомым векторам ошибки относятся следующие [1, 3–5].

1. Все проверочные символы и декодируемый символ i_0 ошибочны:

$$P_1 = p_0^{J+1}. \tag{2.10}$$

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

$$P_2 = \frac{(1-p_0)p_0^J J(J-1)}{2(q-1)} \prod_{i=1}^{J-2} \left(1 - \frac{i}{q-1}\right). \tag{2.11}$$

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

$$P_3 = J(1-p_0)p_0^J. \tag{2.12}$$

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

$$P_4 = \frac{(1-p_0)^2 p_0^{J-1} J!}{6(q-1)^2 (J-4)!} \prod_{i=1}^{J-4} \left(1 - \frac{i}{q-1}\right). \tag{2.13}$$

Таким образом, нижняя оценка вероятности ошибки оптимального декодирования определяется суммой найденных выше вероятностей P_i, $i = 1-4$.

Более полное перечисление событий, приводящих к ошибкам недвоичного ОД, и оценки их вероятностей, а также вероятностей ошибки в первом символе недвоичного ПД приведены в [3, 4, 39]. Разумеется, перечисленных здесь событий, приводящих к ошибке ОД, также вполне хватает для того, чтобы определяемые ими вероятности ошибки ОД были достаточно точны для всех предварительных оценок.

А поскольку QMПД на каждом шаге поиска экстремума расстояния стремится к решению ОД, можно ожидать, что при некотором достаточно высоком уровне шума он в большинстве случаев также будет достигать искомого оптимального решения, потенциальные характеристики которого мы получили выше.

2.8. Итеративные «мажоритарные» процедуры 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,

если её выражать в символах используемого кода, равна $C = q_s$. 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 точно 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. Но количество ошибок, т. е. невосстановленных стираний в решении декодера должно быть уже на много порядков меньшим, чем в принятом сообщении.

В первой главе мы уже рассмотрели возможности простого одношагового метода восстановления неопознанных модемом символов, переданных по стирающему каналу с вероятностью приёма таких стёртых символов p_s. Он дал вполне приемлемые результаты. Однако желательно рассмотреть вопрос о возможности его улучшения на основе многократного применения описанной ранее очень простой процедуры для декодера, т. е. в результате введения нескольких итераций такого декодирования.

Но при ближайшем рассмотрении вопроса оказывается, что метод многопорогового, точнее, многошагового декодирования в стирающих каналах (СтМПД) не требует такого же очень строгого обоснования, как, скажем, в ДСК или в QCK. Знание местоположения того символа, значение которого было невозможно определить в модеме, принципиально упрощает алгоритм, что и показал уже простейший одношаговый алгоритм МПД для этого канала.

В рассматриваемом случае поиска итеративной процедуры МПД для стирающего канала достаточно отметить только то, что после первой попытки коррекции обычно ситуация складывается так, что часть информационных символов, которые были стёрты, не удалось восстановить. При этом по смыслу самого алгоритма он вообще не вносит никаких ошибок в декодируемое сообщение и некоторую часть стёртых символов всегда только правильно восстанавливает. Но тогда попытка повторного декодирования сообщения, в котором количество стираний стало меньше, безусловно, всегда 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 i_n для нескольких других стёртых символов в их проверках число оставшихся стираний уменьшается на единичку. Если в такой проверке единственным оставшимся стиранием будет именно стирание некоторого другого декодируемого информационного симво-

ла i_m, то в этом случае опять появится дополнительная возможность исправления уже 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 i_n достаточно всего одного соответствующего правильно принятого проверочного символа без прочих стёртых информационных символов, входящих в проверку для этого конкретного символа i_n, то и СтМПД будет работать в канале со стираниями при гораздо более высоких допустимых вероятностях канального стирания передаваемых битов по сравнению с теми каналами, в которых происходят ошибки.

Таким образом, новый алгоритм, конечно, сохраняя полное тождество между всеми правильно принятыми из канала кодовыми символами и восстановленным (может быть, не полностью) сообщением, вообще не требует каких-либо изменений в процедуре, предложенной для одношагового декодера.

Ясно, что на второй итерации при таком алгоритме снова будут последовательно исправляться, точнее, восстанавливаться и некоторые другие информационные символы. Но тогда и на следующих итерациях очень возможны новые успешные попытки восстановления. Если будет восстановлена ещё некоторая часть информационных символов, что создаст новые проверки, способствующие восстановлению других символов, то итеративный процесс будет продолжать оставаться успешным. Но если в проверке стёрт проверочный символ, такая проверка никогда не будет полезной для восстановления каких-либо символов. Отсюда следует, что любой информационный символ точно не будет восстановлен, если он стёрт, как и все J проверочных символов, относящихся к нему. Это определяет очень простую нижнюю оценку для невосстановления символов даже в оптимальном переборном декодере:

$$P_{s\text{ОД}}(s) = p_s^d.$$

На рис. 2.4 представлены графики вероятности невосстановления стёртых символов $P(s)$ кода с $R = 1/2$ и $d = 7$ для одношагового декодера (кривая *1*) и в оптимальном декодере — $P_{s\text{ОД}}(s)$ (кривая *3*) для стирающего канала с вероятностями стираний p_s (кривая «p_s»). Кроме того, тут представлены экспериментальные результаты для многошагового МПД декодера при совсем небольшом числе итераций $I = 8$ (кривая *2*). Как видно из графиков, многошаговая процедура восстановления стираний хорошо работает даже непосредственно вблизи пропускной способности канала при $p_s \approx 0{,}45$.

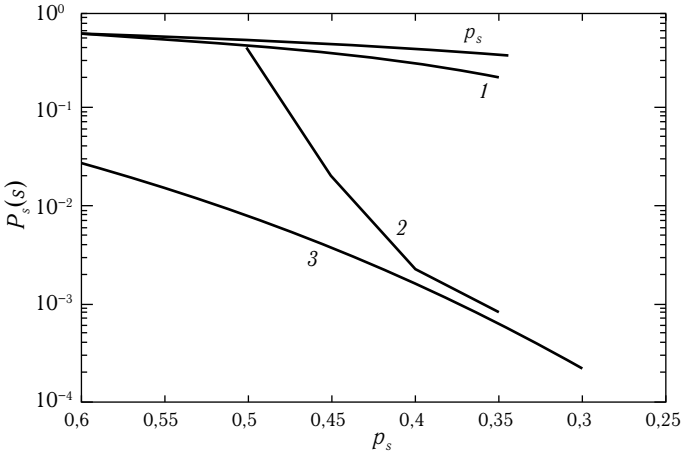

Рис. 2.4. Характеристики блоковых МПД декодеров на потоках стираний в каналах со случайными замираниями при $d=7$ и $R=1/2$: *1* — МПД, $I=1$; *2* — МПД, $I=8$; *3* — ОД

2.9. Несистематические коды

Рассмотренные выше алгоритмы МПД позволяют находить последовательность все более правдоподобных решений на основе очень простых вычислений, проводимых над непрерывно изменяемыми вектором синдрома $\overline{S}$ и разностным вектором $\overline{D}$. Выше было показано, что пара векторов $(\overline{D},\overline{S})$ является разностью между текущим решением-гипотезой декодера и принятым сообщением. При этом следует отметить, что на самом деле между векторами $\overline{S}$ и $\overline{D}$ нет вообще никакого 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 $g_1(x)=1+x^{P_1}+\ldots+x^{P_{j-1}}$, а другой — $g_2(x)=1$, т. е. код был систематическим. Принципиальным обстоятельством оказывается только то, что процедура вычисления синдрома соответствует просто вычислению разности между некоторой первоначальной гипотезой о переданном кодовом слове и принятым сообщением. Этой стартовой для МПД гипотезой в систематическом коде всегда оказывается то кодовое слово, информационные символы которого приняты из канала. Разумеется, никаких более предпочтительных «догадок» у такого 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 [3–5, 36]. 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 к последующим все более правдоподобным решениям. Кроме того, как уже неоднократно подчеркивалось, к используемым в МПД кодам предъявляются весьма строгие дополнительные требования по уровню размножения ошибок при пороговом декодировании, которые для несистематических кодов будут особенно сложными.

Таким образом, не требуются формулировка и доказательство каких-либо новых утверждений о существовании МПД для несистематических кодов. Для них после генерации абсолютно любого кодового слова используемого кода и вычитания из него принятой из канала последовательности тоже формируется вектор, который удобно называть *синдромом* и для которого с учётом сделанного выше 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. Успешные варианты решения проблемы МПД декодирования несистематического кода описаны в [36, 41].

2.10. Многопозиционные системы сигналов

Принципы использования МПД для систем сигналов на плоскости типа КАМN и ФМN также разработаны уже достаточно давно [3, 4, 36]. Это позволяет считать, что возможность применения МПД с этими обширными типами сигналов в настоящее время уже также стала вполне очевидной. 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.

Наш опыт разработок и сопоставления процедур декодирования показывает, что алгоритмы, успешно работающие в каналах с ФМ-2, всегда эффективны и в случае многопозиционных систем модуляции. Разумеется, при этом следует очень аккуратно решать стандартную задачу согласования системы сигналов, кода и алгоритма декодирования. Решение многих вопросов этого уровня представлено в [4, 40].

2.11. Расширение области приложения принципов МПД

Хотя в этой главе были рассмотрены основные классические каналы связи, в которых возможно успешное применение МПД, потребности техники связи становятся все более разнообразными, а сфера приложения кодирования стремительно расширяется и условия их применения все 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) [4]. Они обеспечивают более эффективную, чем традиционные методы, защиту передаваемых численных данных в среднеквадратичном смысле путем обеспечения 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 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 и применяться другие парадигмы ОТ, в частности принцип дивергенции, являются различные *каналы с неравномерной энергетикой* (НЭК) [4]. К таким каналам можно перейти от обычных систем модуляции, если изменить соотношение энергий и, следовательно, расстояний между различными сигнальными точками многих традиционных систем модуляции, например, ФМN или КАМN. Возможны и другие варианты вариации энергетики передачи между символами кода. Это приводит к очень заметному росту достоверности передачи одних групп символов и уменьшению достоверности других и означает, что, например, при вычислении функций правдоподобия L_j веса проверок будут во многих случаях вычисляться несколько иначе. Остальные принципы МПД и ОТ остаются вполне работоспособными и в этом случае.

Наконец, вполне эффективным оказывается и *комбинирование* рассмотренных в этой главе методов и подходов к применению кодирования и декодирования с использованием идеологии ОТ. Разуме-

ется, при этом эффективность применения кодирования будет только возрастать. Подчеркнём, что все идеи и принципы сходимости решений МПД к решениям ОД и поиска глобального экстремума во всех подобных случаях вполне успешно реализуются при совершенно минимальных вычислительных затратах.

Обратим внимание на то, что при обсуждении методов МПД мы рассмотрели важнейший класс оптимизационных процедур, которые положили начало Оптимизационной Теории помехоустойчивого кодирования, реализующей, как уже довольно давно стало ясно, поиск глобального экстремума в цифровых пространствах. В следующем разделе будет рассмотрена другая идеологически сложнейшая проблема теории кодирования — размножение ошибок при пороговом декодировании. Без её всеобъемлющего решения вопрос о высокой эффективности МПД алгоритмов нельзя было бы даже поднимать. Проблема РО была преодолена на основе постановки и решения другой оптимизационной задачи, которая вместе с теоремой ОТМПД обеспечила мощный синергетический эффект в достижении высоких характеристик декодирования на базе МПД алгоритмов и правильного выбора используемых кодов.

2.12. Размножение ошибок в мажоритарных схемах декодирования

Результаты предыдущих разделов этой 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 при описании новых итеративных методов коррекции ошибок было много раз особо указано, что для многих каналов и конкретных кодов существуют такие конфигурации ошибок канала, которые не будут исправлены при любом числе итераций в МПД, но которые исправляются оптимальным декодером по максимуму правдоподобия. Таким образом, МПД не является ОД ни в каких из рассмотренных выше каналов.

Тем не менее, уже сам факт стремления МПД к решению ОД, т. е. его готовность к использованию для поиска глобального экстремума, но при линейной от длины кода сложности стимулировал поиск таких решений проблемы декодирования, которые позволяли бы почти всегда реально достигать решений ОД даже при очень большом уровне шума.

Наиболее плодотворным подходом к решению проблемы максимально эффективного применения МПД оказывается оптимизация параметров МПД по порогам, весам проверок и разностным соот-

ношениям в порождающих полиномах, а также выбор кодов с минимальным уровнем размножения ошибок при пороговом декодировании. В этом случае существенно снижаются число и вероятность появления комбинаций ошибок, которые исправляются в ОД, но не корректируются в МПД. Напомним, что мы уже обсуждали выше проблему РО как задачу снижения уровня пакетирования ошибок на выходе ПД.

Понятие РО и методы его анализа неодинаково трактуются разными авторами. Анализ общих свойств кодов, влияющих на РО, проводился в [36, 37, 42–50]. Отметим также, 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 в 70-х годах прошлого века состояли 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 [46–49] 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 РО и изучения свойств ПД в те годы.

Но, с другой стороны, такой искусственный подход к алгоритму и к каналам просто в принципе не мог обеспечить качественный анализ поведения декодера в реальном канале при большом уровне шума. В связи с этим ниже предлагается достаточно общий метод оценки размножения ошибок декодирования, полезный для повышения эффективности МПД. Как оказалось, выбор кодов, при использовании которых группирование ошибок ПД действительно гораздо меньше, чем у обычных СОК кодов, принципиально улучшает сходимость МПД к решению ОД, что и определяет в конечном счёте возможность алгоритмов этого класса работать в непосредственной близости от границы Шеннона, что является главной задачей разработки всех алгоритмов.

Предлагаемый ниже метод основан на использовании производящих функций вероятности [3, 4, 8, 37], которые применяются к

свёрточным и блоковым кодам, допускающим мажоритарное декодирование. Эти оценки непосредственно зависят от уровня шума канала и не требуют изменения параметров самого канала или алгоритма декодирования, как это предполагалось в ранних исследованиях РО в 70-х годах прошлого века. Такой подход позволяет сделать реальные оценки характеристик и выработать действенные рекомендации по минимизации исследуемого эффекта РО. Именно в такой постановке и решается далее задача приближения эффективности МПД к возможностям ОД. Заметим, что данный подход применим и к некоторым другим классам кодов [3, 36].

При решении проблемы РО нужно, вообще говоря, различать две совершенно различные причины группирования ошибок декодера. Первая в каналах без памяти обусловлена выбранным алгоритмом декодирования и его особенностями: наличием в ПД обратной связи на регистр синдрома декодера, правилом принятия последовательных решений о необходимости коррекции, способом ортогонализации проверок или выбором величины порогов. Для других типов декодеров причины группирования могут быть весьма отличными от указанных для ПД.

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

Вышеприведённые обстоятельства и определяют те большие трудности в улучшении характеристик МПД, когда надо 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 некоторого увеличения числа совершенно одинаковых операций и выбором хороших кодов.

Указанный подход к явлению РО сначала оказался достаточно продуктивным для свёрточных СОК [3, 36]. Позднее эта методика была применена для анализа других кодов и каналов. На основе многомерных производящих функций вероятности новый метод позволяет вычислить условные вероятности ошибки ПД декодирования $P(e_j = 1 | e_0 = 1)$ или их оценки в j-м символе, $j > 0$, если имеет место неправильное решение декодера относительно символа i_0. Полученные результаты, в свою очередь, оказались полезными при поиске

особых кодов с малым РО и создании МПД с низким уровнем группирования ошибок на первых пороговых элементах декодера, что и обеспечило достижение алгоритмами МПД высоких характеристик, во многих случаях совпадающих с возможностями ОД даже при очень большом уровне шума.

Ниже будут рассмотрены основные результаты, относящиеся к анализу РО в свёрточных кодах для двоичных каналов. Это позволит сформулировать главные критерии поиска кодов с наиболее подходящими для МПД свойствами и сравнить затем уровни РО в различных кодах.

Далее при получении оценок РО будет использовано основное свойство СОК, согласно которому каждая ошибка канала может входить не более чем в одну проверку относительно любого из декодируемых символов. Применим многомерные версии производящих функций вероятностей, введенные в [8, 37], которые позволили найти оценки вероятностей совместных ошибок в информационных символах i_0 и i_j, $j>0$, при мажоритарном декодировании свёрточных кодов.

Рассмотрим свёрточный СОК с некоторыми значениями кодовой скорости R, длины кодового ограничения n_A и минимального кодового расстояния d. Введем производящую функцию вероятности вида $A_{m,k}(x,y)=p_0x_my_k+q_0$ 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, $l=1,2,\ldots$. Если некоторая ошибка e_x канала отсутствует в проверках относительно i_0 или i_l, то её ПФВ имеет соответственно вид $A_k(y)=p_0y_k+q_0$ или $A_m(x)=p_0x_m+q_0$.

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.

Метод ПФВ был успешно адаптирован для вычисления вероятности ошибки в первом символе свёрточного кода в классической книге Дж. Месси [8]. Но там был использован одномерный вариант этого мощного средства вероятностных вычислений. Применяемые в данном разделе ПФВ все будут только многомерными, что и позволит получать необходимые 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, причём показатели степеней переменных с одинаковыми индексами суммируются по модулю 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 превышать 1, а добавление новой ошибки увеличивает вероятность того, что проверка будет искажена.

Сделаем ещё 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 [3], то для последующих вычислений будем условно 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, ПФВ для ошибки e_0 символа i_0 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, с учётом перечисленных особенностей, 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

$$A_{0,1}(x, y) = \prod_{m,k=0}^{J} A_{m,k}(x, y) = \sum_{k=0}^{2^{2d}} a_k \prod_{i=0}^{J} x_i^{m_i} \prod_{j=0}^{J} y_j^{n_j}, \qquad (2.14)$$

где показатели степени m_i и n_j равны 0 или 1.

Общее число ненулевых слагаемых в (2.14) 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 (2.14) важно только 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 будет j ошибок. Тогда получаем, что

$$P(e_0 = 1, e_1 = 1) = \sum_{i,j>T} a_{i,j}. \qquad (2.15)$$

Опишем теперь метод вычисления нижней оценки вероятности $P(e_0 = 1, 0)$, т. е. вероятности появления одиночной ошибки декодирования, которая оказывается наиболее существенной для дальнейшего анализа. Применим полученные методы оценки группирования ошибок к СОК с $R = 1/2$, $n_A = 14$ и $d = 5$ с порождающим полиномом

$P=(0,1,4,6)$, декодер для которого представлен на рис. 1.13.

В соответствии с предложенной технологией вычисление $P(e_0=1,e_1=1)$ для этого кода следует проводить, используя ПФВ вида

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

Тогда в соответствии с (2.14) при не очень большом шуме канала задача вычисления $P(e_0=1,e_1=1)$ сводится к суммированию слагаемых вида

$$p_0^3\prod_i x_i^{m_i}\prod_j y_j^{n_j}, \tag{2.16}$$

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

Проводя аналогичные расчёты для $P(e_0=1,e_j=1)$, $2\leqslant j\leqslant 4$, можно вычислить и 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

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

Так как рассчитанная в соответствии с методикой из [8] вероятность ошибки в первом символе рассматриваемого свёрточного кода равна $P_1(e)=P(e_0=1)=85p_0^3$, то нижняя оценка вероятности одиночной ошибки в первом символе

$$P_{1H}(e_0=1,0)=P_1(e)-P(e_0=1,1)=34p_0^3.$$

Поскольку вероятность $P(e_0=1,e_1=1)$ выше была вычислена точно, то вероятность появления одиночной ошибки оценивается сверху соотношением

$$P_B(e_0=1,0)=P_1(e)-P(e_0=1,e_1=1)=58p_0^3.$$

Следовательно, вероятность появления одиночной ошибки ПД лежит между $34p_0^3$ и $58p_0^3$. Поскольку лучшие СОК с $d=5$ имеют вероятность ошибки оптимального декодирования, которая, как можно проверить, при малых значениях p_0 равна $10p_0^3$, то получаем, что оди-

ночные ошибки в рассматриваемом ПД можно и полезно исправлять, т. к. такие ошибки в ОД возникают в 4–5 раз реже, чем в ПД.

Отметим, однако, что при увеличении длины свёрточного СОК с $d = 5$ нельзя уменьшить совместную вероятность ошибки в двух первых символах кода для малого шума ниже уровня $23p_0^3$. Поведение совместных вероятностей при больших значениях d подобно рассмотренному случаю с $d = 5$. Увеличение длины кодов снижает вероятность появления пакетов в очень ограниченных масштабах.

Дальнейшее уменьшение размножения ошибок возможно при переходе к переменным во времени кодам. Например, среди кодов длины $n \approx 1000$ 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 теперь величину порядка p_0, т. е. падает с уменьшением уровня шума, а условная вероятность одиночных ошибок вообще стремится к 1. Иначе говоря, при использовании в ПД таких кодов при достаточно малом шуме все его ошибки окажутся одиночными. Это обстоятельство очень необычно для простого ПД, ошибки которого обычно заметно группируются. Аналогичные характеристики уровня размножения ошибок в кодах могут быть получены и для более высоких значений d при любом выборе R.

Заметим, что для МПД алгоритмов коды с переменными связями эквивалентны кодам с кратными скоростями $R = mk_0/mn_0$, $m = 2, 3, 4, \ldots$. Оценки их характеристик проводятся по единой рассмотренной выше методике.

В [3, 36] проводился анализ РО для равномерных свёрточных кодов, блоковых кодов максимальной длины, блоковых СОК, символьных и несистематических кодов, а также для ряда других кодовых конструкций: декодеров с «джинном» и дефинитных алгоритмов. По итогам выполненных исследований эффекта РО в условиях реальной работы ПД в каналах с независимыми ошибками были формализованы критерии РО, по которым затем были построены мощные оптимизационные процедуры поиска кодов с многократно сниженной подверженностью РО, т. е. группированию ошибок на выходе ПД. Программы могут быть настроены на уменьшение числа таких ошибок, которые попадают одновременно во все или некоторые возможные пары проверок. Такие коды имеют длины в тысячи и сотни тысяч битов, что, как это было отмечено в главе 1, является абсолютно неизбежным при организации эффективного декодирования вблизи границы Шеннона.

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

Отметим, что подход к РО через многомерные ПФВ оказывается довольно общим и позволяет при переходе к ПФВ ещё более высоких размерностей оценивать и вероятности появления групп из трёх, четырёх и большего числа ошибок декодера на любых конкретных позициях блока. 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 методами многомерных ПФВ определять, наоборот, вероятности одного, двух и более подряд правильных решений ПД.

Несколько вариантов наших оптимизационных программных средств построения кодов с минимальным РО имеет порядок сложности от d^3 до d^5, что позволило во многих случаях решить все проблемы создания кодов, наилучшим образом соответствующих алгоритмам МПД. Комплексы оптимизационного поиска хороших кодов позволяют сейчас строить коды до длин порядка 10^6 и значений кодового расстояния $d = 41$ для диапазона кодовых скоростей $R = 0{,}02...0{,}98$. Их цель состоит в том, чтобы всемерно уменьшать те множества ошибок канала передачи данных, которые одновременно попадают во множества проверок для двух или более декодируемых символов. Синергетический эффект от идей ОТМПД и оптимизации кодов по критерию РО обеспечил новому направлению в теории кодирования успешное решение её главной задачи — простого и эффективного декодирования на базе оптимизационных процедур при $R \lesssim C$.

Следует ещё раз специально подчеркнуть, что полученные выше оценки РО выполнены не для многопорогового декодера, изучению которого были посвящены предыдущие разделы этой главы, а для обычного порогового алгоритма. Проведение достаточно полного и точного анализа РО на выходе последующих — 2-го, 4-го или 10-го пороговых элементов, — например, в свёрточном МПД сопровождается такими объективными трудностями, как быстрое увеличение размерности решаемой задачи, что не позволяет получать простые, но достаточно точные и обозримые оценки.

Однако чрезвычайно важно, что весь проведенный анализ выполнен для порогового элемента, который стоит на первой позиции и в блоковом, и в свёрточном МПД. Этот ПЭ 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 и всего алгоритма в целом.

Как следует из проведенного в этой главе анализа, наиболее важным полученным результатом является создание МПД алгоритмов для разных кодов и каналов, а также выяснение и минимизация причин РО в ПД. Для уменьшения РО нужно сокращать в максимальной степени число пересекающихся множеств ошибок, которые есть в проверках относительно любых пар символов кода или, что ещё полезнее, в совокупностях трёх и более проверок для декодируемых символов. Реальная минимизация числа таких ошибок возможна 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 дает, тем не менее, незначительный эффект, если алгоритм работает в области больших шумов канала. В таких случаях нужно проверять достаточно много условий, выполнение которых обязательно. В ряде случаев вполне эффективным может быть компромиссное использование и других кодов с большой длиной, но всё же существенно более коротких, чем наилучшие коды по критерию РО.

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 [3]. Полезными иногда оказываются и дополнительные веса проверок, которые могут назначаться для них на некоторых итерациях декодирования.

Вместе с тем поиск хороших кодов для МПД требует достаточно аккуратного анализа и довольно большого объема 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 итоговое число операций, выполняемых уже построенным декодером, что и оправдывает сложность самой процедуры создания такого предельно простого кодека.

Именно гарантии, которые даёт ОТМПД, и простые критерии РО как числа общих ошибок в парах и тройках проверок решают проблему выбора лучших кодов и высококачественного декодирования на основе оптимизационных процедур. 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 теорема ОТМПД для разных каналов, нижние оценки эффективности МПД и 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 при использовании таких кодов в МПД. Полученные результаты и выработанные критерии сравнения кодов по РО позволили разработать мощные оптимизационные методы построения достаточно длинных кодов с минимальным уровнем эффекта размножения ошибок при их декодировании оптимизационными алгоритмами.

Но, видимо, именно здесь надо указать на ещё одну, третью оптимизационную проблему, решение которой оказалось совершенно необходимым для того, чтобы алгоритмы МПД и связанные с ними как бы производные от них методы, в частности каскадирование, смогли продемонстрировать действительно выдающиеся результаты и достижение практически абсолютно лучших характеристик в прикладной теории кодирования. Дело в том, что при изучении МПД почти сразу оказалось необходимым создать и непрерывно совершенствовать третью группу оптимизационных процедур. Выяснилось, что дополнительная точная настройка тысяч весов проверок, значений порогов на ПЭ и разностных соотношений между полиномами порождающих кодов ещё более повышают уровень сходимости решений МПД к решениям ОД. Эта работа по совершенствованию таких очень трудоёмких, но крайне полезных оптимизирующих процедур третьего типа для параметров МПД продолжается и сейчас.

Успешное использование трёх уже рассмотренных оптимизационных методов при поиске, исследованиях и наладке МПД алгоритмов, наконец, действительно решило все вопросы эффективного декодирования вблизи границы Шеннона. Дальнейшее развитие алгоритмов МПД позволит существенно расширить уже сформировавшееся совершенно новое обширное интеллектуальное пространство современной теории кодирования.

2.13. Особенности контроля уровня размножения ошибок

Правильность понимания проблемы размножения ошибок (РО) исключительно важна потому, что, во-первых, только минимизация этого воздействия на процесс декодирования позволяет действительно обеспечить эффективное МПД декодирование при большом уровне шума. А во-вторых, необычность этой темы, которую не смогла осилить и решить как проблему ни одна научная группа в мире, опреде-

ляет и её довольно непростое (но только на первый взгляд!) решение, полученное нашей научной школой ОТ.

Именно поэтому для правильного понимания основ теории размножения ошибок декодирования и определяемой ею причин эффективности МПД мы предлагаем рассмотреть на нескольких простых примерах реальные доступные всем способы оценки эффекта РО. Это поможет настойчивым исследователям методов кодирования успешно и правильно применять технологии выбора кодов, устойчивых к воздействию РО, что и обеспечит для них в дальнейшем создание действительно эффективных декодеров для условий большого шума канала. Понимание просто изложенных ниже ситуаций позволит читателям правильно воспринимать и глубокую сущность явления РО. А это уже будет основой для самостоятельной разработки требуемого программного обеспечения, оценивающего РО любых заданных кодов и конструирующего по определённым требованиям новые коды с необходимым уровнем РО. Ведь среди известных и опубликованных в научной литературе (не относящейся к школе ОТ) миллиардов кодов нет ни одного с небольшой степенью подверженности РО при мажоритарном декодировании. Но те коды совершенно не нужны для ОТ и МПД декодеров.

Начнём с простого примера двоичного самоортогонального свёрточного кода с $R = 1/2$, $d = 5$, порождающим полиномом $P = (0, 1, 4, 6)$ и $n_A = 14$, представленного на рис. 1.2, *а*. А далее аккуратно напишем так, как показано на примере системы проверок (1.5), конкретное множество из четырёх проверок именно этого кода для первого символа i_0. Конкретные номера ошибок в информационных символах в системе (1.5) свидетельствуют о том, что в проверках для i_0 присутствуют все возможные информационные ошибки в пределах длины кодового ограничения n_A. А если далее выписать систему проверок для следующего символа i_1, то понятно, что в этой системе не будет ошибки e_0, появится следующая ошибка e_7 в i_7, и останутся все прочие информационные ошибки с номерами от 1 до 6, которые были в системе проверок для i_0.

Если же теперь при декодировании символа i_0 произошла ошибка, то это значит, что среди проверок относительно этого символа есть не менее трёх ошибочных проверок и, значит, в пределах длины кодового ограничения n_A присутствуют 3 или 4 и даже большее число ошибок, пришедших из канала. А тогда получается, что в проверках относительно i_1 присутствуют, в основном, те же ошибки. Их достаточно много и, значит, после ошибки в символе i_0 очень вероятно ошибочное решение и относительно i_1. Это и есть проявление эффекта РО: после ошибки порогового декодера в некотором символе

ошибки и в нескольких последующих символах становятся очень реальными событиями. Конкретные оценки вероятностей таких событий и были выполнены в предыдущем разделе.

Но на самом деле ситуация гораздо сложнее и труднее для анализа. Если для этого кода посмотреть, какие именно проверки искажаются теми или иными ошибками в информационных символах, то увидим, что, например, информационные ошибки с номерами 1, 4 и 6 все входят в различные проверки первого набора относительно i_0. Но во втором наборе проверок эти же ошибки, оказывается, также находятся в разных проверках. А это значит, если они привели к ошибке при декодировании i_0, то как раз их наличия может быть достаточно, чтобы именно эти ошибки в каком-то сочетании привели ещё к ошибке декодирования и символа i_1. Это уже более конкретное указание на то, что группирование ошибок декодера очень вероятно. Чтобы оценить вероятность такого события более точно, посмотрите внимательно конкретные выражения для вероятности двух таких ошибок порогового декодера (ПД) этого кода в предыдущем разделе. Там этот анализ выполнен на основе двумерных производящих функций вероятностей (ПФВ) и там аккуратно пройдены все шаги формирования оценок группирования ошибок ПД. Очень полезно также и просто рассмотреть все комбинации из трёх ошибок канала, которые приведут к двойной ошибке того ПД, который мы сейчас обсуждаем. Этого и будет сначала достаточно для понимания реальности и конкретики группирования ошибок декодера в обычном двоичном симметричном канале (ДСК). Реальное число различных комбинаций из трёх ошибок, которые приводят к двум последовательным ошибкам обычного ПД в символах i_0 и i_1, также может быть определено из преобразований (2.16), которые показывают далее, что число таких комбинаций для анализируемого кода равно 27.

Первым шагом к пониманию того, что РО является управляемым процессом, может быть оценка РО для какого-либо другого более длинного кода. Попробуйте почти случайным образом найти такой код с $d = 5$ и степенью полинома порядка 40, например, $P = (0, 3, 16, 39)$. Как известно, для того, чтобы это был полином самоортогонального кода (СОК), все возможные разности этих четырёх чисел в полиноме должны быть различными [1]. При самостоятельной оценке РО для этого кода методами, предложенными в предыдущей главе, вполне возможно, что число возможных комбинаций из трёх ошибок, приводящих к двум последовательным ошибка декодера, будет меньшим, чем 27, что было точно выяснено для первого короткого кода. Но, к сожалению, снижение степени группирования ошибок, представленное через вероятность появления двух таких

ошибок декодера даже для очень длинных кодов с $d=5$, не получится сделать меньшим, чем 23 комбинации из трёх ошибок канала. Если рассматривать более длинные коды с $d=7$ и более, то разница в степени группировании ошибок будет больше, но всё равно изменится не очень заметно, чтобы считать это хорошим способом снижения РО.

Более сильное снижение степени группирования ошибок, т. е. эффекта РО для СОК кодов, в том числе и с бóльшими значениями d, чем $d=5$, оказывается возможным, если переходить к кодам с переменным связями или, что тоже самое, с кратными скоростями, например $R=2/4$. В этом случае вероятности появления двух и более близких ошибок декодера можно снизить до весьма малых уровней, что приведёт в конечном счёте к тому, что при малых вероятностях ошибок в канале ошибки декодера будут происходить почти независимо друг от друга. Это и считается в настоящее время требуемым низким уровнем подверженности РО, а выбранные таким образом коды действительно наиболее полезны в случае их использования в МПД декодерах, которые в этом случае успешно работают при существенно более высоких вероятностях ошибок в канале. Но столь уже заметное снижение эффекта РО произойдёт только для таких кодов, длины которых будут равны сотням и тысячам битов.

Рассмотрим те конкретные свойства, которыми должны обладать наиболее подходящие для использования в МПД коды. Как было показано в предыдущем и обсуждалось на простых примерах в этом разделах, в хорошем коде все проверки для всех кодов должны быть такими, чтобы число всех возможных наборов ошибок в проверках для всех попарно рассматриваемых символов было минимальным. Отсюда получаем, что число рассматриваемых пар пропорционально квадрату числа символов в блоковом коде или числа символов в свёрточном коде в пределах длины кодового ограничения. В зависимости от параметров (n, k, d) кода число всех возможных сочетаний наборов одинаковых символов в различных парах проверок может быть очень разным и не поддаваться поэтому точным оценкам из-за их большого разнообразия. Понятно, что в некоторых кодах есть определённое количество пар проверок, в которых есть по 3 общих ошибки в символах, т. е. таких, которые входят в проверки и в первом символе, и во втором, причём эти информационные символы пары необязательно находятся рядом. А возможны и коды, которые не имеют, например, ни одной пары проверок, в которых бы число общих ошибок было равно 5 и т.д. Эти конфигурации сочетаний невозможно просчитать, что случается довольно часто при решении разных технологических задач улучшения помехоустойчивости МПД декодеров.

Из этой ситуации нечёткого определения качества цели, т. е.

свойств кода, который надо построить, вытекает, что одним из способов, который здесь можно применить, состоит в том, что код наращивается до требуемого число ветвей, заданного веса полиномов и степени устойчивости к РО постепенно. При этом для каждого нового значения позиции очередного кодового полинома проверяются все пары проверок, которые существуют в коде с учётом нового элемента, а затем позицию этого нового элемента полинома меняют и снова производят проверку. Если спектр общих ошибок в проверках не меняется, то производят ещё несколько попыток найти более хорошую позицию элемента. Если же ни одна из таких попыток сдвига нового элемента полинома не приводит к улучшению спектра общих ошибок канала, то самая первая позиция элемента полинома принимается как выбранная и с этим новым значением элемента приступают к поиску следующего элемента для, может быть, другого полинома. Конечно, если поиск привёл на каком-то шаге к улучшению спектра общих ошибок, то эта позиция принимается за новую стартовую и далее снова начинается процесс поиска улучшенной конфигурации полиномов строящегося кода.

Данная технология построения хороших кодов была реализована с учётом ряда дополнительных требований и показала достаточно быстрое достижение цели — конструирования хорошего кода по критерию минимизации РО. Разумеется, здесь пришлось реализовать ряд процедур, ускоряющих решение этой типичной оптимизационной задачи, что существенно подняло производительность программы на C++, которая затем в течение многих лет позволяла нам строить требуемые коды наилучшего или, если необходимо, компромиссного качества для кодовых скоростей R в диапазоне от 0,01 до 0,99 с шагом 0,01 и минимальным кодовым расстоянием $d \lesssim 25$, что оказалось вполне достаточным для решения всех текущих задач построения и применения хороших в плане РО кодов.

Для более полного удовлетворения запросов на исследования в подобных программах полезно вводить средства более гибкого назначения параметров, так как при этом также сильно меняются характеристики, связанные с РО. К таким параметрам относятся различные планируемые веса полиномов, особые меняющиеся правила поиска кодов по мере увеличения уже построенных до этого частей кода, введение ограничений на длины приемлемых для будущих исследований кодов и некоторые другие второстепенные детали, например, исключение из рассмотрения заранее назначенных конкретных полиномов с определенными номерами их информационных и проверочных ветвей.

Таким образом, как часть общего весьма массивного комплекта программных оптимизационных средств проектирования МПД, про-

граммы поиска кодов с малым уровнем РО всегда должны во всех разработках занимать своё обязательное место, важнейшее для получения требуемых характеристик МПД алгоритмов с хорошей сходимостью к решениям ОД. Только точный выбор необходимого кода по уровню подверженности РО может обеспечить хорошие результаты декодирования соответствующего МПД. Созданные комплексы научной школы ОТ успешно выполняют в таких наших проектах свою миссию создания кодов с лучшими характеристиками для реализации МПД декодеров при работе непосредственно в ближайшей окрестности границы Шеннона.

Однако, обсудив содержание этого очень важного технологического раздела, о ценности которого до сих пор просто не догадываются (увы!) тысячи других научных сотрудников, пишущих статьи по теории кодирования, наиболее заботливые сторонники нашей научной школы решили, что читатели, впервые соприкоснувшиеся с проблемой РО, после прочтения данной главы всё равно могут не прочувствовать исключительную важность именно проблемы группирования ошибок на выходе мажоритарных алгоритмов. Это ослабит их внимание к качеству используемых кодов для МПД, что может значительно снизить итоговую эффективность МПД алгоритмов, которые они будут потом создавать.

Поэтому мы добавляем ещё несколько шагов в процедуру предварительного обучения технологиям РО. Выполнив и эти шаги, наши будущие коллеги сразу уже реально ощутят ключевую роль РО в ограничении эффективности методов ОТ. Добавим, что мы позаботились о том, чтобы первичные затраты на освоение идей теории РО были у читателей этой книги сначала минимальными. Нам представляется, что лучше осознав результаты экспериментов с МПД декодерами на следующих простых этапах, наши будущие последователи с гораздо большим энтузиастом будут развивать экспериментальную базу ОТ, без которой, как мы уже много раз писали, нельзя получить никаких основных характеристик любых алгоритмов декодирования при большом уровне шума.

Итак, перепишите по гиперссылке [102] статью автора за 1986 год. Обратите внимание на графики, отражающие характеристики свёрточного МПД для разного числа итераций и различных полиномов в ДСК канале. Её можно также найти на портале **www.mathnet.ru** по контекстному поиску «многопороговое декодирование». Далее на портале **www.mtdbest.ru** на странице «Обучение» внизу справа из раздела демо-программ надо переписать компактную программную платформу «Программа моделирования работы многопорогового декодера». Подчеркнём, что она позволяет моделировать блоковые варианты

МПД алгоритмов в ДСК. Она также доступна по гиперссылке [111].

А далее после прочтения простой инструкции для этой программной платформы попробуйте запустить алгоритм МПД со входными данными, уже записанными во входные файлы для программного модуля на языке C++. Затем после быстрого завершения работы МПД декодера с теми полиномами, которые даны в качестве примера в описании и в этих уже заполненных файлах входных данных, просмотрите и оцените все основные параметры «помехоустойчивость — достоверность — сложность» по единому критерию эффективности декодирования.

Более интересным будет следующий цикл работы с этой программной платформой. Прочтите инструкцию внимательно ещё раз и попробуйте, используя полиномы свёрточного кода из той статьи 1986 г., запустить МПД декодер (повторим: блокового кода!) со всеми вариантами кодов, описанными в той статье. Программа сама настроит длину блока в соответствии с выбираемыми вами полиномами. Сравните ваши результаты и статью. Разберитесь, почему блоковые алгоритмы всегда немного слабее свёрточных, если все их параметры выбираются идентичными. И, самое главное, оцените, как всё же сильно влияет РО на итоговую достоверность при разном выборе кодов, которые, однако, все имеют одинаковое значение кодового расстоянии $d = 11$. Эти примеры, которые вы уже сами наработаете, окажут вам важную поддержку в изучении эффекта РО и создании собственных способов его минимизации. Отметим далее, что полезно также научиться избегать собственных пакетов кодов, на что было ясно указано в той статье. Это можно делать на основании теорем 2.3, которые есть в [3, 4]. Для этого девятый пороговый элемент надо настроить на собственный пакет длинного последнего кода. Тогда МПД практически всегда убирает его, если такой пакет появится. Но это уже тонкости ещё более высокого уровня, которые не заложены в обсуждаемую программную платформу. Но его всегда надо иметь в виду.

Ну, и очень полезно воспользоваться для оценки эффекта РО возможностью того, что, например, эта программная платформа позволяет использовать коды с кратными скоростями, например $R = 4/8$. Такие коды эквиваленты кодам с переменными связями, и выше специально указывалось, что у таких кодов при достаточной их длине эффект РО может быть значительно меньшим. Один код с таким значением R даётся в предварительно заполненных файлах данных для программы, которую мы предлагаем вам использовать. А другие коды вы вполне можете построить и попробовать запустить их сами. Попробуйте выбирать достаточно длинные коды. Тут — вопрос поиска и удачи.

Ну, и наконец, поскольку статья написана для свёрточных МПД, после столь немалых усилий по изучению РО на примере блокового МПД вполне можно потратить совсем небольшое время и написать самостоятельно программу уже именно для свёрточного многопорогового алгоритма, снова ввести в теперь уже вашу программу полиномы из статьи и убедиться, что в некоторых случаях свёрточные версии алгоритмов МПД работают при большем уровне шума, чем блоковые. Посмотреть «вживую» на эффекты РО для одинаковых значений d, как мы уверены, будет также очень полезно и в этом случае анализа свёрточных кодов.

Напомним, что именно здесь очень вовремя будет напомнить о реальной предельной лёгкости реализации мажоритарных алгоритмов. В МПД единственный активный элемент, который, собственно, и надо запрограммировать, — пороговый элемент. На его реализацию требуется затратить не более 5–7 команд языка C++. А весь остальной объём программы на 99 % — удобный именно для вас интерфейс вашей программы с вашим же принтером, который позволит вам самому удобно прочитать результаты работы моделируемого вами мажоритарного алгоритма. Так что МПД — это абсолютно просто!

Если вы выполните, хотя бы в основном, предлагаемую нами программу изучения труднейшего, очень неожиданного и важнейшего во всей ОТ эффекта РО, то ваше дальнейшая жизнь в современной теории кодирования будет весьма успешной и плодотворной.

2.14. Об особых свойствах МПД и ОТ

На этом и заканчивается в целом рассмотрение фундаментальных основ совершенно нового и, вообще говоря, абсолютно не прогнозируемого и очень неожиданного проекта по созданию технологий конструирования декодеров, работающих в непосредственной близости от границы Шеннона. Этот, без сомнения, фантастический с точки зрения прежней теории (полностью закончившей своё бытие в прикладном аспекте) проект основан на исключительно тесном взаимодействии новой оригинальной тонкой теории и инновационного оптимизационного программного обеспечения (ПО).

А теперь можно позволить себе немного менее академические, но, тем не менее, столь же точные и полезные качественные комментарии особенностей этой принципиально новой ситуации в проблеме эффективной организации высокодостоверной обработки цифровой информации. В самом деле, найденные, как вдруг оказалось, действительно наипростейшие решения великой проблемы Шеннона лежат вообще вне сферы каких-либо масштабных математических достижений прежней эпохи. Это обстоятельство сразу полностью изъ-

яло бывшую как бы «классическую» теорию кодирования и близкие к ней направления из научной сферы. Да, решение этой важнейшей прикладной задачи лежало действительно совсем «не там». И основы нового подхода, все его ключевые результаты, базирующиеся на использовании совершенно особого сплава теории и эксперимента, были компактно и очень точно изложены в этой главе. Это и даёт нам возможность взглянуть на возможности ОТ ещё и с других, немного особых точек зрения, что, как мы надеемся, поможет и в дальнейшем чаще анализировать ОТ и её приложения с разных позиций. Несомненно, это обеспечит дальнейшее ускорение развития и разнообразных версий МПД, и многих будущих модификаций БАВ, а значит, и в целом всей ОТ.

Итак, начнём с того, что один из наших студентов долго смотрел на схему блокового МПД (рис. 2.5), которую вы можете увидеть на слайде из одной нашей презентации.

А затем он в течение минуты нарисовал вот такую картинку (рис. 2.6), которую мы тоже взяли из этой же презентации.

Когда мы спросили его, что это такое, он нам объяснил, что так он видит процесс работы МПД. Пришлось попросить его прокомментировать его сюжет. И вот что он рассказал.

Поскольку обсуждаемый двоичный код линеен, то можно полагать, что при какой-то большой вероятности искажений при передаче символов кода посылается нулевое сообщение. Ведь все знают, что выбор передаваемого сообщения, которое является кодовым словом, не влияет на вероятность ошибки решения декодера. При передаче к кодовому вектору $\overline{A}$ добавился вектор шума $\overline{E}$, вес которого равен $|\overline{E}|$. В нашем случае вес — число единичек в двоичном векторе. В декодер поступит вектор $\overline{X}=\overline{A}+\overline{E}$. ОД должен найти кодовое слово такое, что оно среди всех возможных было бы самым близким к вектору $\overline{X}$. Так как $\overline{A}$ — нулевой вектор, то вес $\overline{X}$ такой же, как у $\overline{E}$: $\overline{X}=\overline{E}$ и $|\overline{X}|=|\overline{E}|$. И пусть сообщение $\overline{A}$ — ближайшее к $\overline{X}$, т. е. $\overline{A}$ — решение ОД.

Мы тут же спросили студента, а как он будет комментировать нам свою картинку, если вектор шума имеет столь большой вес, что $\overline{A}$ — уже не решение ОД. И он почти мгновенно порадовал нас чётким ответом, что в этом случае совершенно ничего не изменится вообще, так как он рассказывает о процессе сходимости решений МПД к решению ОД, а не к правильному решению. Так что для того, чтобы не мешать хорошему пониманию картинки, наш студент сразу предложил считать, что вектор $\overline{E}$ не столь «тяжёл» и отправленное сообщение $\overline{A}$ — это именно решение ОД.

А далее у него оказалось ещё интереснее. Как известно, в МПД, как во многих других декодерах, сначала выполняется простейшая

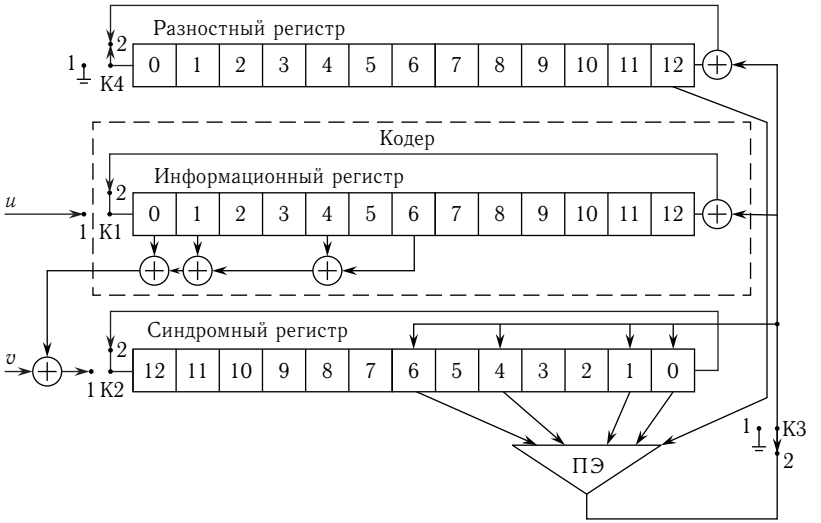

Рис. 2.5. Блоковый многопороговый декодер для кода с $R = 1/2$, $d = 5$

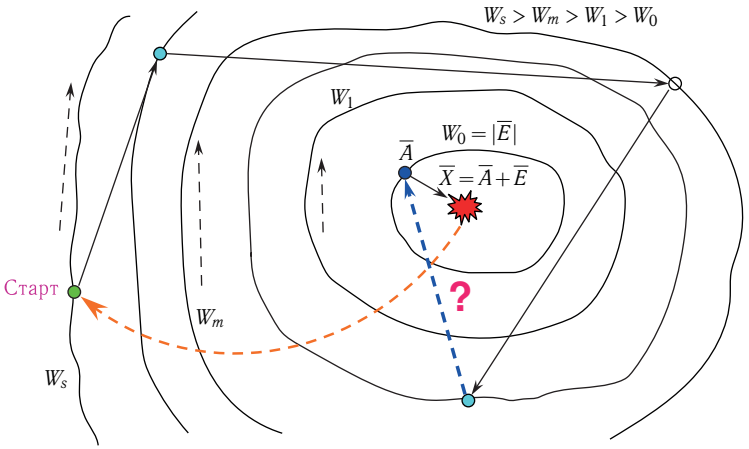

Рис. 2.6. Сходимость процедур глобального поиска для МПД декодеров

процедура вычисления вектора синдрома для принятого сообщения (посмотрите про эту важную операцию в книгах). И после этого получается некоторый стартовый (исходный) вариант решения МПД, от которого начинается процесс поиска решения ОД. Этот вариант показан точкой «Старт» на краю рисунка, дополнительно помеченной символом W_s. Этим знаком обозначен вес разности точки «Старт» и принятого вектора $\overline{X}$. И эта точка лежит на некоторой «круговой» линии, на которой находятся решения, у которых вес разности с $\overline{X}$ равен W_s. Вес W_s всегда реально много больше, чем $|\overline{E}|$, $W_s \gg |\overline{E}|$.

Просто так устроены все коды. Но зато символы синдрома не зависят от значений информационных символов. Синдром — вектор, который есть функция только от ошибок, которые пришли из канала связи. На внутренних кругах лежат другие решения, расстояния W_m до которых от вектора $\overline{X}$ уменьшаются по мере их приближения к $\overline{X}$. Общее количество решений декодера, лежащих на различных кругах, достаточно велико и растёт с увеличением длины кода.

В этом случае процесс декодирования становится таким, что, согласно слайду с блоковым МПД, данные в нём двигаются во всех регистрах синхронно и циклически, а пороговые элементы при этом постепенно корректируют контролируемые крайние правые информационные символы. На обсуждаемой диаграмме в процессе коррекции ошибок декодер последовательно просматривает на некотором текущем круге веса W_m (но начинает он свою работу, конечно, на крайне внешнем круге веса W_s) возможность перейти с него на один из внутренних кругов, каждый из которых является геометрическим местом части таких решений, которые находятся на некотором одинаковом расстоянии W_n от $\overline{X}$, причём $W_m > W_n$. И при этом пороговые элементы в МПД таковы, что переход на внутренний круг возможен только тогда, когда новое решение на этом внутреннем круге меньшего веса будет отлично от предыдущего решения точно в одном информационном символе. И в этом условии заключается та величайшая проблема мажоритарных алгоритмов, которая была сформулирована и потом полностью решена теорией размножения ошибок (РО). Но если она не решена, то обычно декодер будет с какого-то момента бегать по кругу некоторого веса W_m, $W_m > W_0$. Возможность такой неудачи показана последней пунктирной стрелкой к решению $\overline{A}$, которая подчёркивает вопросительным знаком отсутствие гарантии достижения алгоритмом в конце процесса декодирования итогового правильного решения $\overline{A}$. Но если использовать все возможности теории РО и строить только правильные коды по критериям РО, то даже при большом шуме непростой по своим условиям поиск на кругах диаграммы студента будет почти всегда продолжаться до момента попадания декодера в правильное решение $\overline{A}$, ближайшее к принятому вектору $\overline{X}$, как мы договорились об этом перед началом рассмотрения студенческого слайда.

А ещё наш студент сказал, что текущее условие о единственности изменённого символа в очередном решении МПД после каждого события коррекции блока является очень жёстким, но совсем необязательным. Он предложил найти другое решающее правило для МПД и менять символы блока группами или даже ещё каким-то другим способом, что может улучшить характеристики декодирования при

большом уровне шума. Вполне очевидно, что главное условие тут — сохранение линейной от длины кода сложности — можно выполнить. А вот конкретный вид новой решающей функции — это очень непростая задача. Её, возможно, скоро решит наш студент, участники научной школы ОТ или другие удачливые исследователи. Это будет и очередным шагом дальнейшего развития теории размножения ошибок (РО) в МПД.

Итак, очередная новая задача в теории ОТ сформулирована. А когда будет решение?

2.15. О компактности и совершенстве ОТ

И ещё один важнейший качественный итог создания ОТ следует всегда иметь в виду. Речь идёт о соотношении ОТ с прежней «классической» теорией кодирования. Очень условной качественной картинкой, иллюстрирующей эти отношения, является приводимый ниже слайд (рис. 2.7), который даёт вполне простые ответы на эти вопросы.

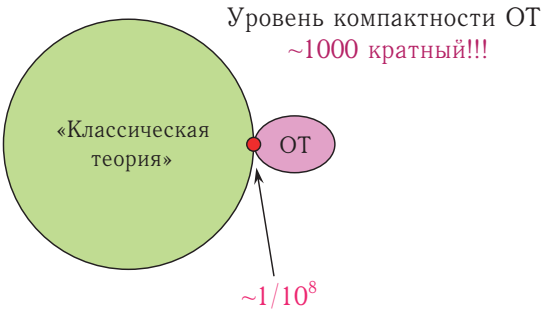

Рис. 2.7. Размеры «классической теории» и ОТ

Анализ всех монографий по ОТ, которые были изданы нашей научной школой в этом тысячелетии, показывает, что все они являются системно-философскими трактатами по теории информации с крайне ограниченным использованием сложной математики. Для всех типов каналов в ОТ нужно уметь определять вероятности ошибки в первом символе кода, что давно уже является простой задачей даже для студента, сдающего курсовую работу по теории кодирования. Некоторым исключением являются те разделы ОТ, которые относятся к основам теории размножения ошибок (РО) и её приложениям к конкретным кодам. Совершенно ясно, что столь новый важный и очень оригинальный раздел теории кодирования, который не смогли за прошедшие 40 лет открыть, исследовать и хоть как-то понять никакие научные группы в России и в зарубежье, и не мог быть очень простым. И, тем не менее, после полного анализа и описания столь сложного явле-

ния, как РО, последовавшие из его понимания выводы и технологии оказались также вполне понятными и естественными. РО показала, что надо строить коды с самой минимально возможной зависимостью всех пар проверок относительно декодируемых символов между собой. Этот вывод, который невозможно сделать без теории РО, привёл ко вполне простым алгоритмам создания таких кодов, которые тоже укладывались в концепцию доступных методов с ясными и понятными итоговыми критериями качества кодов. Именно этот вопрос и был ещё раз рассмотрен в предыдущем разделе, из которого видно, что теория РО действительно помогает искать столь необходимые для МПД специальные мажоритарные коды. Остальное же в ОТ — тоже очень просто. Специалисты, разрабатывающие алгоритмы декодирования, должны ещё найти, в основном, кроме символьных кодов, по биномиальным распределениям вероятности ошибки для оптимального уровня декодирования используемых кодов. Их даже не требуется как-то выводить. Но это и вся математика! Если все заложенные в проект данные правильные, то далее уже оптимизационное ПО доведёт проект до запланированного решения с оптимальным декодированием используемого кода. Так что данный раздел этой монографии, как и нескольких предыдущих книг, — полное, очень компактное и абсолютно логичное описание идеологии решения проблемы Шеннона самыми простейшими методами с наилучшей возможной результирующей достоверностью.

Общее число новых математических соотношений в характеристиках методов ОТ оказалось совершенно небольшим и ограничено теперь буквально несколькими десятками новых формул, вывод которых нигде не занимает более страницы текста. А из прежней прикладной теории кодирования в ОТ используются только несколько простых преобразований, которые позволяют вычислять вероятность ошибки в первом символе используемого двоичного блокового или свёрточного кода $P_1(e)$ для двоичного симметричного канала (ДСК), а также для гауссовского и стирающего каналов. Всё это, тем не менее, позволяет рассчитывать абсолютно все необходимые характеристики декодирования методами ОТ во всех классических каналах, рассматриваемых в теории кодирования для любых алгоритмов нашей новой «квантовой механики» теории информации. Это и есть конкретное безусловное подтверждение высокого совершенства ОТ.

Именно такая ситуация и представлена на слайде (рис. 2.7), где изображены почти абсолютно независимые прежняя «классическая» и новая оптимизационная часть современной прикладной теории кодирования, нашей ОТ. Соединяющее их маленькое пятнышко, которым мы обозначили несколько выражений, — это как раз предложенный

Дж. Месси метод вычисления вероятности $P_1(e)$. Но это — вообще всё, что их объединяет. Наша ОТ — полностью от нуля переписанная новая отлично работающая вся прикладная теория кодирования. И указанные на слайде соотношения для размеров этих двух теорий действительно (очень условно, конечно!) соответствуют разнице в три десятичных порядка по объёму информации. Так же ничтожна и доля формул для $P_1(e)$ по отношению к очень пухлой и не очень плодотворной прежней теории кодирования. Указанная их часть, равная 10^{-8}, — это просто их качественная оценка. Ну, и отметим, наконец, что вся ОТ очень наглядна и абсолютно понятна. Так что учить собственно теоретическую часть ОТ почти и не требуется. Это простейшие аккуратно спроектированные МПД декодеры или столь же хорошо известный алгоритм Витерби с какими-то его модификациями. Для создания алгоритмов ОТ не нужны, кроме оценок $P_1(e)$ и вероятности ошибки на бит $P_b(e)$ для ОД, никакие другие методы расчёта чего-либо, так как истинные параметры триединого критерия всегда быстро достигаются на основе моделирования работы МПД и АВ. Вероятности $P_b(e)$ обычно определяются биномиальными или ещё более простыми выражениями. Да и все вероятности ошибки для недвоичных кодов, достаточно точно выражаемые суммой нескольких простых выражений — тоже вполне простые и логичные. Обслуживающая ОТ теория РО также привела к понятным итоговым правилам поиска лучших кодов для МПД.

И далее все эти задачи проектирования декодеров решаются комплексами программных систем, которые на основе идей оптимизационных теорий доводят, конечно, при участии квалифицированного исследователя-проектировщика параметры систем декодирования до требуемых уровней значений параметров критерия. Сложность таких алгоритмов минимальная, а эффективность в плане достоверности — наилучшая.

Добавляя к этому наши новые результаты по различным модификациям АВ, получаем, что ОТ охватывает теперь уже все сферы применения кодирования, с использованием как длинных, так и коротких кодов. А вычислять параметры критерия, как показали 60 лет существования «классики», никто не умеет. Оценить их аналитически нельзя. И это — навсегда! Так что теория кодирования — вовсе не математическая задача. Профессиональные математики, как мы надеемся, найдут возможность просмотреть все результаты прежней теории кодирования, не связанные с методами декодирования. Здесь-то обсуждать нечего. Нуль! А вот проанализировать наличие действительно ценных результатов в той теории именно для математики — такую задачу надо бы решить. Мы будем не меньше других специ-

алистов довольны, если окажется, что какие-то ценные для науки задачи действительно были решены за эти 60 лет её «бурного» существования. Этот итог будет хорошим завершением подготовительного математического периода к решению проблемы Шеннона, пусть даже при этом та прежняя теория ни на шаг не продвинулась за эти годы к хорошему решению поставленной задачи. Но независимо от итогов обязательного, как мы настаиваем, пересмотра математиками научных итогов той теории, научная школа ОТ приглашает абсолютно все высококвалифицированные научные кадры в сфере «цифры» к дальнейшему развитию новых информационных систем с использованием инновационных компьютерных технологий высокодостоверной обработки данных в условиях высокого уровня шума.

Так что ОТ — это действительно мощная системная философия решения проблемы Шеннона на основе теорий оптимизации. Найти здесь место для малоэффективных алгоритмов декодирования, созданных прежней теорией, теперь уже нельзя.

2.16. Выводы

В этой главе представлена довольно неожиданная для прежней теории полная системная философия цифровой обработки, которая позволила крайне небольшими ресурсами и в очень ограниченные сроки буквально «с нуля» создать теоретические и технологические средства решения чрезвычайно актуальной для современного информационного сообщества проблемы обеспечения высокой достоверности цифрового контента нашей цивилизации. Это и есть абсолютно исчерпывающее решение проблемы Шеннона, сформулированной в его действительно великой работе [14], для всех моделей каналов, рассматриваемых в теории кодирования.

Материал последующих глав описывает уже конкретные технические достижения, которые стали возможными именно благодаря дальнейшей разработке и формулировке совокупности принципиально новых руководящих парадигм ОТ, представленных в этой главе. Созданные на их основе мощные оптимизационные методы и конкретные программные средства теперь на самом деле обеспечивают достижение всех тех высоких параметров систем кодирования/декодирования, которые ещё совсем недавно были абсолютно далёкими и совершенно недоступными целями науки.

Глава 3

Основные достижения Оптимизационной Теории

В данной главе рассмотрены наиболее значимые результаты последнего времени, которые показывают основные достижения ОТ в области обеспечения высокой эффективности и технологичности декодирования при большом уровне шума, в том числе вблизи границы Шеннона, т. е. при $R \lesssim C$. Основной особенностью этой главы является представление всего материала по ОТ и МПД алгоритмам так, как он был изложен в недавних принципиальных публикациях в ведущих российских журналах по этой тематике. Фактически параграфы данной главы — это главные статьи последних трёх лет, 2017–2020 гг., в которых были изменены только отдельные фразы и даже сохранены все внутренние списки литературы со своими собственными номерами ссылок и рисунков. Это никак не влияет на сквозную для всей монографии нумерацию ссылок и рисунков за пределами третьей главы и совершенно не мешает рассмотрению помещённых здесь отдельных параграфов-статей, каждая из которых является законченным уникальным научным трудом сотрудников нашей научной школы. Эти статьи точно соответствуют тематике и структуре книги, в которой последовательно излагаются различные важнейшие достижения ОТ, связанные единым планом описания общего состояния идей и технологий ОТ, а также её лучших достижений.

Сейчас ОТ, по меньшей мере в своём прикладном алгоритмическом аспекте, полностью сменила классическую алгебраическую теорию кодирования, которая довольно неспешно, в течение нескольких десятилетий передавала Оптимизационной Теории пальму абсолютного первенства во всех прикладных вопросах, связанных с разработкой алгоритмов декодирования на основе процедур поиска глобального экстремума функционалов. Как теперь уже можно уверенно полагать, этот процесс передачи атрибутов лидерства, явно начавшийся приблизительно в 1985 г. и вполне завершившийся в целом в районе 2010 г., показал недосягаемость характеристик фактически оптимального декодирования алгоритмов МПД на базе ОТ по эффективности и по небольшой сложности реализации, растущей лишь линейно с длиной кода во всём диапазоне параметров систем кодирования в окрестностях границы Шеннона. Иллюстрацией вступления теории кодирования в новую фазу ОТ, которая успешно реализует простейшие процедуры поиска глобального экстремума (минимума расстояния!) и безо

всяких оговорок стала своеобразной «квантовой механикой» в теории информации, и являются статьи-параграфы этого ключевого раздела настоящей монографии.

В конце главы сделаны обобщающие выводы по проделанным исследованиям.

3.1. Принципы дивергентного кодирования

Представленные в [1, 2] основные достижения Оптимизационной Теории помехоустойчивого кодирования свидетельствуют о том, что построенные на новых постулатах этой теории многопороговые декодеры к настоящему моменту достигли уже весьма высокого уровня эффективности при довольно умеренной сложности. Текущие возможности МПД таковы, что в гауссовских каналах эти алгоритмы работают с вероятностью ошибки на бит $P_b(e) < 10^{-5}$ при $R = 1/2$ и уровне битовой энергетики $E_b/N_0 \sim 1{,}2$ дБ. Организовать столь же эффективную работу декодеров низкоплотностных (LDPC) кодов, которые до недавнего времени оставались единственными конкурентами МПД алгоритмов в гауссовских каналах, при таком уровне шума уже весьма сложно, а для высокоскоростных каналов просто невозможно. Гораздо сложнее для этих алгоритмов и задача декодирования свёрточных кодов. С другой стороны, возможность реализации декодеров МПД на основе технических решений [3] полностью снимает для них проблему скорости работы, т. к. позволяет сохранять высокие энергетические характеристики аппаратного декодирования вообще на любых скоростях передачи канала, в том числе выше 1 Гбит/с [4, 5]. К тому же ресурсы улучшения характеристик для МПД алгоритмов ещё не полностью исчерпаны, что позволяет и в дальнейшем ожидать от них дальнейшего значительного улучшения эффективности работы при больших уровнях шума. При этом можно напомнить, что эффективность МПД при их использовании в недвоичных каналах с символьными кодами или в каналах со стираниями (везде при очень малой сложности) была уже изначально при создании этих алгоритмов столь значительна по сравнению с алгебраическими декодерами, что для таких приложений никаких конкурирующих методов для МПД декодеров не оказалось и в обозримый период, наверное, не будет. Для этого до сих пор нет никаких серьёзных оснований.

Важнейший вопрос о сложности декодирования средствами МПД полностью снимается, если проанализировать скорость работы известных в настоящее время демо-программ всех популярных методов декодирования (алгоритма Витерби, декодеров кодов LDPC, БЧХ и Рида — Соломона, МПД, символьных декодеров QМПД и ряда других с инструкциями по их использованию). Все они доступны на на-

ших порталах www.mtdbest.ru и www.mtdbest.iki.rssi.ru. В абсолютном большинстве случаев оказывается, что все модификации МПД алгоритмов обеспечивают на несколько порядков более высокие достоверности декодирования, чем прочие методы, и одновременно (!) демонстрируют также на несколько десятичных порядков бóльшие скорости работы, чем их бывшие потенциальные конкуренты. В значительной доле случаев при этом оказывается, что для заданных уровней шума и избыточности используемых МПД алгоритмов нельзя найти никаких других методов декодирования с таким же уровнем эффективности при декодировании. Главная причина столь высокой степени преимущества МПД декодеров всегда заключается в том, что и для весьма высоких уровней шума канала они обеспечивают такое же декодирование, как и оптимальные переборные методы, но при линейной от длины кода сложности, выполняя при этом только самые простейшие операции уровня сложения небольших целых чисел. При этом очень важно, что весьма многие технические решения для этих МПД декодеров запатентованы [6, 7]. Все эти обстоятельства позволяют МПД алгоритмам легко использовать и быстро декодировать очень длинные коды, что и определяет их превосходство над АВ, LDPC и прочими процедурами [1, 2]. И, наконец, особенно важно, что для многих сочетаний характеристик кодов и основных типов каналов эффективность МПД разных модификаций при малой энергетике канала столь значительна, что других методов, которые работоспособны в этих условиях, вообще назвать нельзя. Таким образом, существенно преодолев уровень эффективности реальных декодеров LDPC кодов, алгоритмы МПД фактически заявили о своём первенстве по эффективности и сложности реализации вообще для всех значимых приложений в системах передачи, хранения, контроля и восстановления цифровых данных при наличии независимых случайных потоков искажений.

Однако в настоящее время недостаточно применения в декодерах итеративного типа только самых простых средств обработки цифровых потоков на базе мажоритарной логики, хотя эти методы сами по себе обеспечивают реализацию процедур глобальной оптимизации. То, что при снижении энергетики канала для обеспечения той же высокой эффективности по достоверности необходимо наращивать объём вычислений, специалистам уже давно очевидно. Но использование только привычного стиля применения мажоритарной логики, видимо, не даст МПД алгоритмам и далее столь же быстро приближаться к пропускной способности канала, хотя текущее расстояние до границы Шеннона для гауссовского канала, соответствующее 1 дБ, и так уже достаточно мало.

Ниже предлагаются новые направления развития методов итера-

тивного декодирования, которые могут помочь значительно приблизить реальные характеристики алгоритмов на базе ОТ к пропускной способности каналов.

Рассмотрим схему простого свёрточного кодирования с кодовой скоростью $R = 1/2$, представленную на рис. 3.1. Она состоит, условно говоря, из регистра сдвига, в левой части которого сгруппированы ячейки, с выходов которых поступают значения их содержимого на входы полусумматора (mod 2 сумматор), после которого проверочные символы кода отправляются в канал. Для упрощения описания будем полагать код систематическим. Поэтому вместе с проверочным символом кода в канал на каждом такте работы кодера уходит и один информационный символ из нулевой ячейки регистра сдвига. Принципиальным моментом для описания работы данного кодера является наличие далеко в правой части кодирующего регистра ещё одной ячейки, содержимое которой также поступает на вход полусумматора, с которого данные уходят в канал. Конечно, код может быть и несистематическим, а ячеек в правой части регистра, с которых отправляются данные во многовходовой полусумматор, может быть в общем случае достаточно много. Но пока ограничимся анализом представленных здесь более простых схем.

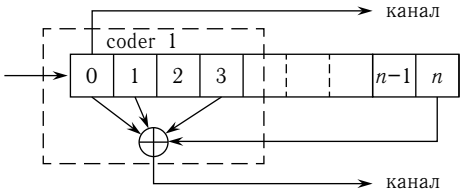

Рис. 3.1. Кодер дивергентного кода

На рис. 3.2 показан декодер свёрточного кода, соответствующий кодеру на рис. 3.1. Он построен по идеям функционирования обычных МПД и содержит два пороговых элемента, находящихся в левой и правой частях декодера. Левый ПЭ и соответствующие части информационного и синдромного регистров, с которыми он взаимодействует, выделены пунктирным квадратом и называются далее Decoder1 (D1).

Полный декодер со вторым ПЭ2 в правой части регистров декодеров подобен D1. Но на вход ПЭ2 поступает ещё и дополнительная проверка кода, которая появляется в декодере намного позже символов компактной группы проверок, связанных с первым ПЭ1.

При работе в канале первый ПЭ1 принимает решения об информационных ошибках на основании только своей компактной группы

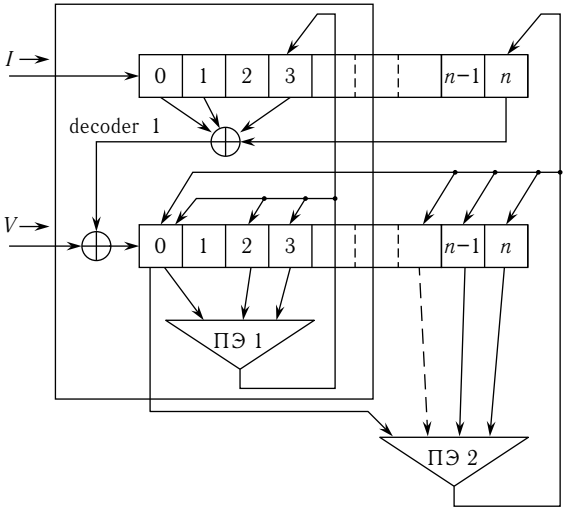

Рис. 3.2. Декодер дивергентного кода

проверок. Если шум канала и код выбраны правильно, то после первого ПЭ1 плотность таких ошибок будет меньше, чем до этого порога, а достигнув второго ПЭ2, эти ошибки согласно принципам работы МПД будут подчищены. А поскольку на входы ПЭ2 поступает на одну большее число проверок, чем в ПЭ1, то и корректирующие возможности второго ПЭ2 будут более высокими, что позволит усилить процесс коррекции, т. к. второй ПЭ2 работает с кодом, у которого минимальное расстояние d как бы выросло на единичку по сравнению с первым ПЭ1. Важно, что этого удалось добиться без привлечения методов каскадирования, которые отнимают избыточность у первого кода (и первого ПЭ1), что заметно уменьшает корректирующие возможности первого декодера.

Очевидно, что предложенный код сам может быть первой частью ещё более длинного кода с подобной же структурой. Тогда на двух таких условных «каскадах» кодирования/декодирования минимальное расстояние d уже будет увеличено на 2 и т. д. Действительно, такие схемы успешно работают, соответствуют принципам работы МПД и Основной Теоремы, показывая при этом вполне удовлетворительные результаты.

Но на самом деле получившаяся схема декодирования стала в плане идеологии и оценок характеристик намного более сложной, т. к. эффект роста кодового расстояния, крайне ценного ресурса, не может быть получен просто так, из ничего. Первый декодер на рис. 3.2 часть ошибок, которые он не исправил, пропускает направо ко второму ПЭ2.

И тогда с ячейки n через два полусумматора эти ошибки попадают в синдромный регистр. Значит, первый ПЭ1 работает при немного возросшем уровне шума, что ухудшает его характеристики по сравнению со случаем, если бы отдельной дополнительной проверки не было. Но если ПЭ1 справляется с этим возросшим потоком ошибок и ухудшает свои характеристики немного, а второй ПЭ2 помогает первому, то можно ожидать, что вместе они всё же справятся с таким лишь немного более сложным потоком ошибок, что и позволяет продолжить анализ этой схемы для определения её возможностей при высоком уровне шума.

Рассмотрим возможности такой дивергентной схемы (с растущими, «расходящимися» значениями d) с помощью рис. 3.3. На нём представлены приближённые зависимости вероятности ошибки декодеров $P_b(e)$ от уровня шума канала для алгоритма Витерби (АВ) и для МПД декодеров с кодами, имеющими некоторое кодовое расстояние d и $d+1$. Характеристики имеют типичные изгибы, которые находятся в точках, где вероятности ошибки МПД при уменьшении уровня шума (вправо) достигают оптимальных минимальных значений для используемых кодов. Левее точек перегибов алгоритмы уже не могут работать из-за высокого шума канала. Рисунок демонстрирует принцип дивергентного кодирования, при котором МПД, работающий в такой схеме с кодом, имеющим расстояние $d+1$, обеспечивает декодирование при уровне шума $\sim 1{,}7$ дБ, хотя сам МПД работает в обычном режиме только при уровне шума порядка 1,8 дБ.

Для анализа ситуации возьмём МПД с кодом, имеющим минимальное расстояние d. Его характеристики близки к оптимальным до энергетики 1,6 дБ. Установим уровень шума для него 1,7 дБ. Это точка 1 на рис. 3.3. Теперь подключим в кодере и декодере дополнительную далёкую проверку, влияние которой мы обсуждали по рис. 3.1 и 3.2. Если дополнительный шум от этой проверки невелик и может

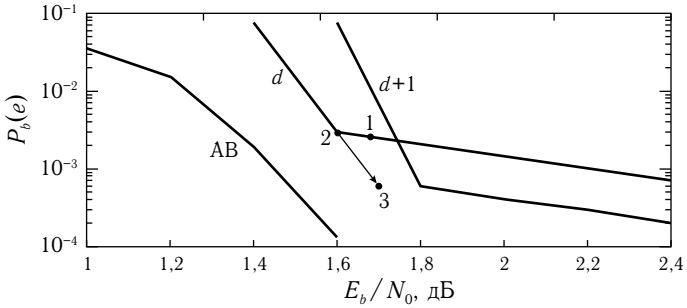

Рис. 3.3. Иллюстрация принципов дивергентного кодирования

быть выражен как увеличение шума канала примерно на 0,1 дБ, с которым первый МПД с кодом, имеющим расстояние d, ещё справляется, то характеристики этого МПД сместятся из точки 1 в точку 2 и пока останутся оптимальными. Но тогда во второй декодер с ПЭ2 действительно попадает поток информационных ошибок из первого декодера с гораздо меньшей плотностью, чем вероятность ошибок в канале. А это и создаёт условия, при которых второй ПЭ2 действительно тоже дополнительно снизит плотность ошибок, пришедших к нему от первого ПЭ1 (точка 3). Но это произойдёт уже при уровне шума, примерно на 0,1 дБ большем, чем тот, при котором ПЭ2 мог работать без поддержки ПЭ1. Разумеется, применяя этот принцип несколько раз, можно значительно продвинуться в область более высоких шумов канала.

Обращаясь к графику для АВ, приведённому на рис. 3.3, можно заметить, что он не имеет таких перегибов, как кривые для МПД. Кроме того, обычно графики для длинных, но ещё реализуемых в плане сложности декодеров АВ лежат левее графиков для МПД, как это и показано на рис. 3.3. Это значит, что если вместо первого ПЭ1 поставить достаточно эффективный декодер АВ, то применение принципа дивергенции может быть ещё более эффективным. Проверка показала, что такие решения действительно работоспособны.

Что касается АВ, разнообразные сопоставления эффективности многих алгоритмов декодирования показали также, что единственной группой методов, которые точно измеряют расстояние своих решений до принятого сообщения, являются только МПД, QМПД (декодеры символьных кодов) и алгоритм Витерби, а также его блоковая модификация [4–7]. Они объединены нами в особый класс декодеров с прямым контролем метрики и уже успешно применяются совместно, в том числе для дивергентного кодирования. Работы в этом направлении расширяются.

Блоковая модификация АВ рассматривается в следующем параграфе.

Исследования дивергентного кодирования с МПД алгоритмами и АВ получили поддержку РФФИ (грант 14-07-00859).

Большинство использованных в докладе материалов можно найти на нашем сетевом ресурсе **www.mtdbest.ru**.

На способ дивергентного кодирования получено положительное решение о выдаче патента на изобретение.

Список литературы

1. *Золотарёв В.В., Зубарев Ю.Б., Овечкин Г.В., Аверин С.В., Овечкин П.В.* 25 лет Оптимизационной Теории кодирования: новые перспективы. — Пленарный доклад // Научно-техническая конференция РГРТУ, 2017.
2. *Золотарёв В.В., Зубарев Ю.Б., Овечкин Г.В.* Многопороговые декодеры и оптимизационная теория кодирования / Под ред. академика РАН В.К. Левина. — М.: Горячая линия — Телеком, 2012. — 238 с.
3. *Золотарёв В.В.* Способ декодирования помехоустойчивого кода: патент на изобретение РФ № 2377722 от 27.12.2009.
4. *Золотарёв В.В., Зубарев Ю.Б., Овечкин Г.В.* Высокоскоростной многопороговый декодер для систем передачи больших объемов данных // Научно-технический сборник «Техника средств связи», серия «Техника телевидения», юбилейный выпуск. — МНИТИ, 2010. — С.41–43.
5. *Золотарёв В.В., Овечкин Г.В.* Применение многопороговых методов декодирования помехоустойчивых кодов в высокоскоростных системах передачи данных // Электросвязь. — 2014. — № 12. — С.10–14.
6. *Золотарёв В.В., Овечкин Г.В.* Способ реализации символьного порогового элемента в символьном мажоритарном декодере: патент РФ № 2573741.
7. *Золотарёв В.В., Овечкин П.В.* Способ кодирования и декодирования блокового кода с использованием алгоритма Витерби: патент на изобретение РФ № 2608872 от 25.01.2017.

3.2. Блоковая модификация алгоритма Витерби

Фундаментальная научная проблема повышения достоверности передачи цифровых данных по каналам с шумами решается с использованием методов помехоустойчивого кодирования. Среди них лучшими по эффективности являются оптимальные декодеры, которые всегда находят наиболее близкое и, значит, наиболее правдоподобное к принятому сообщению кодовое слово. Оптимальные декодеры при декодировании принятых сообщений осуществляют полный перебор всех возможных вариантов кодовых слов, поэтому их сложность экспоненциально растёт с длиной используемого кода. Среди оптимальных алгоритмов декодирования в настоящее время наиболее широкое распространение получил алгоритм декодирования свёрточных кодов, предложенный А. Витерби в 1967 г. [1]. Данный алгоритм позволяет изящно и весьма экономно выполнить полный перебор всех возмож-

ных кодовых слов и выбрать среди них то, которое находится на минимальном расстоянии от принятого сообщения.

Однако при создании технических средств с системами помехоустойчивого кодирования на основе декодеров, реализующих алгоритм Витерби и другие методы, часто приходится реализовывать процедуры ресинхронизации. Они состоят в том, что при завершении передачи некоторого блока данных, который следует отправить получателю по каналу связи, в кодер вводится нулевая информационная последовательность, равная по длине размеру памяти кодера. Эта процедура необходима для того, чтобы помехозащищенность последних информационных символов кода не ухудшилась из-за отсутствия необходимых кодовых символов, если передачу кодовых символов блока прекратить в момент поступления в кодер последнего информационного символа в этом блоке. При этом очень неудобно, что дополнительные нулевые информационные символы в конце сообщения конечной длины меняют кодовую скорость исходного свёрточного кода. Например, при длине исходного сообщения, равного 100 битам, для кода с кодовой скоростью $R = 1/2$ в канал должны уходить не только 200 двоичных кодовых символов, а ещё $2(K-1)$ символов, где K — конструктивная длина кода (длина кодирующего регистра). Поэтому, например, в частном случае при $K = 7$ в канал дополнительно уходят ещё 12 кодовых символов. Это значит, что реальная кодовая скорость равна не $R = 1/2$, что было бы крайне удобно при формировании управляющих воздействий (тактовых импульсов) для аппаратуры, использующей АВ, а $R = 100/212 \approx 0{,}47$, что неоправданно усложняет разработку систем с аппаратурой кодирования.

Именно поэтому возникает задача разработки такого способа кодирования и последующего декодирования сообщений при помехоустойчивом кодировании, когда обеспечивается работа декодеров для блоковых кодов при той же кодовой скорости R, что и у свёрточного кода, выражаемой обычно отношением небольших целых чисел. Иначе говоря, нужны блоковые коды с хорошим удобным декодированием, имеющие те же простые значения кодовых скоростей, что и у свёрточных кодов, например, $R = 1/2$, $R = 1/3$, $R = 3/4$ и т. д. Это существенно упрощало бы применение кодирования с использованием АВ для конечных по длине сообщений, т. е. для блоковых кодов.

Ниже предлагается эффективное решение этой проблемы.

На рис. 3.4 представлено устройство кодирования информации с использованием известного способа кодирования, превращающего свёрточное кодирование в блоковое с той же кодовой скоростью. Этот метод позволяет на приемном конце линии связи применить для декодирования различные алгоритмы, в том числе и мажоритарные.

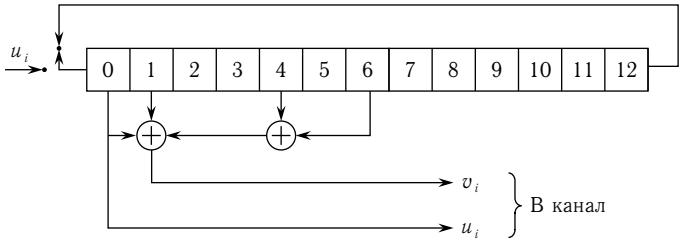

Рис. 3.4. Кодер квазициклического блокового кода

Данный блоковый код задается порождающим полиномом $g(x) = 1 + x + x^4 + x^6$ и характеризуется параметрами: длина кода $n = 26$, длина информационной части кода $k = 13$, кодовая скорость $R = 1/2$, кодовое расстояние $d = 5$. Он построен на основе более короткого свёрточного кода с конструктивной длиной $K = 7$, с тем же $d = 5$ и тем же порождающим полиномом. Важно, что для этого правая часть регистра кодера, не содержащая отводов на полусумматоры, должна быть такой же или больше, чем максимальная степень свёрточного полинома (в данном случае шестая). Подчеркнем, что такое преобразование свёрточного кода в блоковый квазициклический код хорошо известно и давно используется в технике кодирования [2–5]. Дополнительную информацию по этим методикам, часто называемым циклическим усечением свёрточных кодов и анализируемым с помощью циклических решеток, можно найти в [6]. Там же приведены ссылки на других авторов, занимающихся этой темой.

Представленное выше устройство кодирования (кодер) информации блоковым квазициклическим кодом работает следующим образом. В кодер сначала некоторым образом записываются информационные символы, предназначенные для их помехоустойчивого кодирования и последующей передачи по каналу связи. Далее производится главная процедура кодирования, в результате которой получается блок кодовых символов для передачи по каналу связи с шумом. В этой процедуре после каждого циклического сдвига кодирующего регистра и вычисления проверочных символов кодовые символы (в рассматриваемом примере символы u_i и v_i) направляются в канал. Процесс формирования кодовых символов заканчивается, когда после ряда циклических сдвигов регистра сдвига кодера он оказывается в исходном состоянии. После этого можно приступить к кодированию следующего информационного блока. Подчеркнем, что такая же схема кодирования может использоваться для формирования несистематического блокового кода, который также легко декодируется с помощью АВ.

Пусть на приемном конце линии связи декодирование происходит так, что АВ (или какой-то другой алгоритм декодирования) сразу

начинает работать точно так же, как и при обычном декодировании исходного длинного (возможно, бесконечного) свёрточного кода с произвольного места, например, прямо с первых символов квазициклического блокового кода, поступивших в декодер. После приема и обработки последнего кодового подблока принятого сообщения в декодер снова в соответствии с видом циклической решетки блокового кода подаются так же циклически первый подблок кодовых символов этого кода, затем второй и т. д. В зависимости от длины кода и уровня шума таким образом можно циклически подать на вход декодера, работающего согласно АВ, снова 2–5 или более раз все кодовые символы принятого кодового блока. Отметим, что поскольку у квазициклического кода нет «начала», то декодер, как и в бесконечном свёрточном коде, будет выходить на правильное (т. е. с малым числом ошибок) решение только после прихода в декодер примерно первых $D \sim (3-20)K$ кодовых подблоков. После обработки этих кодовых подблоков, когда декодер уже принимает достаточно достоверные решения относительно декодируемых символов, решения декодера обязательно повторяются также с периодом, очевидно, равным размеру блокового кода. Значит, получателю информации (приемнику) нужно передать от декодера только очередной двоичный информационный блок, соответствующий переданному кодовому слову, т. е. часть последовательности решений декодера, который, например, в случае кодера на рис. 3.4 имеет длину 13 битов. При этом из декодера его надо взять за пределами первых D принятых декодером кодовых подблоков, где, как уже указывалось выше, эти решения, в основном, неправильны. С другой стороны, для АВ также хорошо известно (см. [2]), что другое условие достаточной достоверности решений состоит в том, что обычно такие правильные решения декодера формируются не ранее, чем после приема $L = (5-25)K$ кодовых подблоков, конкретное число которых тоже зависит от кода и уровня шума в канале. Таким образом, АВ (или другой алгоритм декодирования) должен как бы «принять» несколько циклически завязанных одинаковых (!) кодовых блоков и затем передать приемнику двоичные информационные символы, находящиеся приблизительно в середине этой циклической последовательности решений декодера, т. к. решения, находящиеся близко к месту приема очередного кодового подблока и близко к месту приема самых первых кодовых подблоков, малодостоверны по сравнению с потенциальными возможностями применяемого кода.

Очевидно, что корректирующая способность декодера блокового кода остается почти такой же, как и у декодера свёрточного кода, если длина блокового кода по сравнению со свёрточным оказывается существенно, в 10–30 раз большей. При укорочении блокового

кода и при сохранении длины составляющего свёрточного кода характеристики декодера блокового кода, конечно, обязательно должны несколько ухудшаться. Однако простота и привычность (конечно же, условные) декодирования с использованием АВ при сохранении кодовой скорости исходного свёрточного кода позволяют считать, что оптимальное декодирование блоковых кодов на основе блокового АВ [13–16] позволит намного проще решать практически все задачи коррекции ошибок в блоковых кодах. Подчеркнем теперь, что полученный блоковый АВ столь же прост (условно, конечно), как и его свёрточный прототип, а предложенная схема декодирования работоспособна как в канале гауссовского типа, так и в ДСК. Это приводит к тому, что с учётом возможностей МПД для таких же каналов из списка конкурентоспособных методов для блоковых кодов исключаются фактически абсолютно все алгебраические декодеры для этих двух основных моделей каналов связи. Во всех случаях проектирования декодеров для этих каналов можно брать МПД, АВ и, иногда, самые простые каскадные схемы с этими алгоритмами.

Рассмотрим характеристики декодирования блоковых кодов на базе блоковой модификации АВ. На рис. 3.5 представлены результаты для декодеров блоковых кодов, которые были получены на персональном компьютере описанными выше методами коррекции ошибок в квазициклических кодах на основе классического АВ. По вертикальной оси отложены оценки вероятности ошибки на бит BER и на блок WER для декодеров указанных далее кодов. На горизонтальной оси указано битовое отношение сигнал/шум E_b/N_0 в канале с аддитивным белым гауссовским шумом для кодовой скорости $R = 1/2$.

График VA7 соответствует декодеру, реализующему обычный АВ для стандартного свёрточного кода с $K = 7$, а график VA15 соответствует декодеру свёрточного кода с $K = 15$. Последний декодер на современной элементной базе уже легко реализуем. Можно напомнить, что впервые столь длинный код при небольшой кодовой скорости R был использован ещё в прошлом тысячелетии для проекта NASA «Кассини».

Для остальных графиков, представляющих характеристики декодеров блоковых кодов, используются обозначения в виде XK-n. Здесь X соответствует типу вероятностей, которые представляют графики (B — BER, W — WER), K определяет конструктивную длину свёрточного кода, выбранного за основу блокового (7 или 15), а n — длину использованного блокового квазициклического кода (40, 100 и 200 битов).

Выполним анализ представленных результатов моделирования. Как уже отмечалось выше, чтобы вероятности BER при декодирова-

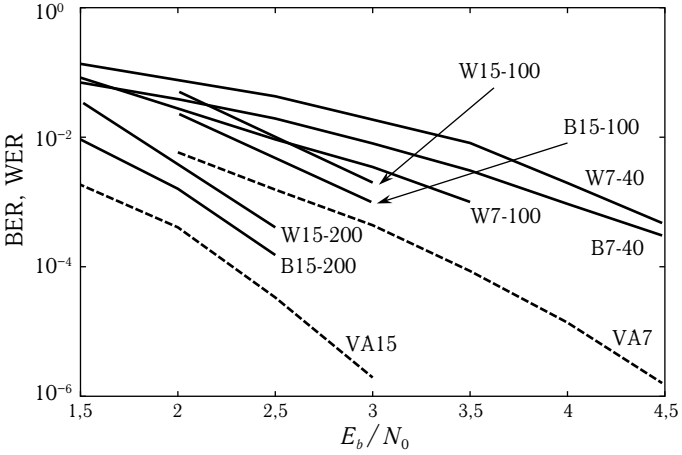

Рис. 3.5. Характеристики декодеров для свёрточных и блоковых кодов в канале с АБГШ

нии блоковых кодов были близки к характеристикам декодеров исходных свёрточных кодов, нужно, чтобы длины создаваемых квазициклических блоковых кодов существенно превосходили длины исходных свёрточных кодов, причём с увеличением параметра K эта разница также должна расти. Например, график VA7 почти совпадает с вероятностью BER для блокового кода длины $n = 100$ с образующим его свёрточным кодом с $K = 7$. Поэтому этот график не потребовалось рисовать отдельно. При использовании этого же свёрточного кода в блоковом коде с $n = 40$ разница между параметрами K и n достаточно мала. Поэтому характеристики декодера этого блокового кода при том же значении $K = 7$, что и в предыдущем случае, оказываются слабее: оба графика B7-40 и W7-40 находятся существенно выше, чем графики VA7 и W7-100 для первого кода.

Аналогичное соотношение характеристик наблюдается и в случае базового свёрточного кода с $K = 15$. Для декодера этого варианта блокового кода BER будет мало отличаться от BER для декодера свёрточного кода только при длинах n, превышающих, видимо, $n \sim 300 - 400$ битов. Графики BER и WER при $K = 15$ приведены на рис. 3.5 для $n = 100$ и $n = 200$. Они показывают, что с уменьшением n возможности блокового кода с декодированием по АВ заметно уменьшаются, как и должно быть для любого блокового кода, сравниваемого со свёрточным при сопоставимых длинах.

Отметим, что обсуждаемые блоковые коды, аналогично их свёрточному прототипу, легко декодируются при переходе к варианту АВ с неполным просмотром путей [7]. Однако тут надо проводить очень точные настройки параметров.

Нелишне напомнить, что предложенные блоковые модификации свёрточных кодов легко включаются в различные параллельные и последовательные схемы каскадирования. Этим снимаются многие вопросы разработки и использования различных блоковых кодов, которые нередко объявляются безо всяких (пока что!) на то оснований революцией в технике кодирования и декодирования. Анализ некоторых методов такого «уровня» приведен в [8]. Сопоставление представленных там полярных кодов [9] и других методов носит предварительный характер из-за очень ограниченного фактического материала по этим алгоритмам, объявленным перспективными. Там же показано, что декодеры, реализующие АВ, и многопороговые декодеры даже без какой-либо адаптации к условиям сопоставления методов, близки к ним по эффективности. Все заявляемые преимущества кодов [9] при небольших длинах блоков и, вследствие этого, их невысокие, в принципе, характеристики легко достижимы декодерами Витерби, МПД и декодерами каскадных схем с их участием при весьма небольшой сложности [2–5, 10].

Из принципа построения блоковых модификаций АВ ясно, что сложность предложенных декодеров переборного типа, о чем не следует забывать, оказывается приемлемой для многих приложений, т. к. свёрточные версии АВ всесторонне проработаны уже несколько десятилетий назад, а блоковая модификация почти ничем не отличается от исходной свёрточной.

Вместе с тем полезно указать на некоторые особенности блоковой модификации АВ и её возможности. Необходимость для каждого кодового блока декодировать повторяющуюся последовательность символов несколько большей длины, чем размер блока, не очень усложняет алгоритм. В абсолютном большинстве случаев можно ограничиваться декодированием «свёрточного» кода, длина которого, например, в представленных выше экспериментах никогда не превышала размеров блокового кода более чем в 5 раз. Обычно в рамках эксперимента оказывалось возможным ограничиться трёхкратной разницей в длинах кодов и эту величину ещё можно снизить примерно в полтора раза.

При программной реализации значительные вычислительные затраты необходимы на сопровождение выживших путей, число которых, как известно, растет экспоненциально с ростом конструктивной длины K свёрточного кода. При этом возможна экономия в вычислениях по переформированию этих путей на каждом шаге декодирования за счёт двойного роста памяти, которая используется для запоминания ссылок на предыдущие позиции выживших путей. Возможна и значительная экономия памяти путей, за счёт чего появляется

возможность реализовать блоковый АВ для кодов с $K \sim 28$ или даже для несколько бóльших значений конструктивных длин базового свёрточного кода. При этом несколько увеличиваются вычислительные затраты, которые могут возрасти до 2–4 раз. Наконец, напомним, что блоковый АВ должен лишь однажды просмотреть лучший путь после завершения всей процедуры декодирования и выбрать при этом среднюю часть из последовательности своих решений в как бы «свёрточном» коде. Это тоже существенно снижает объем вычислений.

Большинство указанных обстоятельств было рассмотрено и проанализировано в процессе моделирования блоковых и свёрточных версий АВ как для одинаковых, так и для различных параметров используемых кодов. При этом глубокие процедуры оптимизации вычислений для повышения скорости декодирования не проводились. Очевидно, что эта полезная задача заслуживает отдельного внимания и рассмотрения. Оказалось, что для типичных вариантов декодирования производительность свёрточных и блоковых версий АВ отличалась не очень сильно. Для кодов с $K = 7$ при одном из вариантов АВ, выполняющемся на персональном компьютере с процессором Core-i7 с тактовой частотой порядка 3 ГГц, декодирование в свёрточном классическом варианте происходило со скоростью около 100 Кбит/с, а в блоковой версии — порядка 60 Кбит/с. При использовании блоковых кодов, основанных на свёрточных с $K = 15$, скорость декодирования была равна 1,0 Кбит/с, а при использовании свёрточного варианта составила около 600 бит/с. Эти данные свидетельствуют о хорошем уровне декодирования в программе для блоковой версии АВ, не содержащей явных недостатков при реализации каких-либо её компонент. Основные возможности улучшения разработанной версии блокового АВ были рассмотрены выше.

Наконец, укажем на то, что близкие скорости работы свёрточных классических версий АВ и их новых блоковых модификаций при моделировании свидетельствуют о том, что сложность блокового АВ, конечно, в пересчёте на информационные биты осталась пропорциональной 2^K. Это следует и из описания предложенного алгоритма, который просто совпадает с исходным методом.

В связи с этим чрезвычайно полезно обратить внимание на то, что почти все методы «циклического усечения хвостов» при переходе от свёрточных кодов к их блоковым версиям, в том числе и методы, представленные, например, в [6], характеризуются тем, что предлагаемые там декодеры имеют сложность, близкую к 2^{2K}. Очевидно, что настолько большая сложность таких модификаций АВ является совершенно неприемлемой. Авторы этих методов и оценок их характеристик в связи с этим вполне обоснованно указывают на то,

что тут возможны существенные упрощения. Некоторые из таких методов упрощения для блокового АВ ими были предложены, однако никаких оценок для сложности подобных улучшений в удобном для интерпретации виде мы нигде не увидели. Более того, такие «упрощения» столь разрушительно воздействуют на сам исходный практически идеальный однородный вычислительный алгоритм, который «улучшается», что предлагаемые улучшения сразу смотрятся как абсолютно неактуальные.

Таким образом, предложенный блоковый вариант АВ является достаточно простой и очень понятной модификацией классического АВ для свёрточных кодов и имеет сложность, как это следует из его описания, превышающую сложность исходного алгоритма не более чем в 2–3 раза. Возможно, что некоторые его модификации окажутся ещё более простыми. Этим определяются его возможности по использованию в системах связи самого широкого назначения.

В связи с вышеизложенным представляется очень правдоподобным, что в настоящее время наилучшие характеристики по быстродействию и эффективности декодирования пока что могут обеспечить только декодеры с прямым контролем метрики. К ним относятся различные МПД алгоритмы, все модификации АВ, а также дивергентные схемы коррекции ошибок [11], построенные на их основе. Все эти методы объединяет простота и однородность вычислений, а также важнейшее их свойство точного измерения расстояний от решений этих декодеров до принятых из канала сообщений, которым не обладают никакие другие повсеместно публикуемые сейчас методы декодирования. Подчеркнём, что если декодер не учитывает и не измеряет ни в каком виде точное расстояние до принятого сообщения, то такие алгоритмы коррекции становятся неработоспособными при большом уровне шума, а в случае малых вероятностей ошибок в канале всегда можно использовать другие совсем простые методы.

Создание описанной здесь модификации блокового АВ, который, разумеется, также относится к декодерам с прямым контролем метрики, применение вместе с ним методов дивергентного кодирования, алгоритмов МПД, классических и параллельных методов каскадирования [3, 4], создает условия для ещё более широкого использования различных методов кодирования, представленных на порталах [12]. Там же можно найти некоторые публикации, на которые даны ссылки при изложении этого материала, а также другие статьи, презентации и книги по теории кодирования и её прикладным вопросам.

Исследования по новым блоковым версиям алгоритма Витерби проводились при финансовой поддержке ИКИ РАН, РГРТУ и РФФИ (грант 15-07-06348).

Большинство использованных здесь материалов можно найти на нашем сетевом ресурсе **www.mtdbest.ru** [12].

Список литературы

1. *Viterbi A.* Error Bounds for Convolutional Codes and an Asymptotically Optimum Decoding Algorithm // IEEE Trans. — 1967. — IT-13. — P.260–269.
2. *Золотарёв В.В., Овечкин Г.В.* Помехоустойчивое кодирование. Методы и алгоритмы. Справочник. — М.: Горячая линия — Телеком, 2004. — 126 с.
3. *Золотарёв В.В.* Теория и алгоритмы многопорогового декодирования. — М.: Радио и связь, Горячая линия — Телеком, 2006; второе издание — 2014.
4. *Zolotarev V., Zubarev Y., Ovechkin G.* Optimization Coding Theory and Multithreshold Algorithms. — Geneva, ITU, 2015. — 159 p.
5. *Золотарёв В.В., Зубарев Ю.Б., Овечкин Г.В.* Многопороговые декодеры и оптимизационная теория кодирования / Под ред. академика РАН В.К. Левина. — М.: Горячая линия — Телеком, 2012. — 238 с.
6. *Кудряшов Б.Д.* Основы теории кодирования. — СПб.: БХВ-Петербург, 2016. — 393 с.
7. *Овечкин Г.В., Овечкин П.В.* Алгоритм декодирования Витерби с продолжением только наиболее вероятных путей // Материалы 18-й Международной научно-технической конференции «Проблемы передачи и обработки информации в сетях и системах телекоммуникаций». — Рязань, 2015. — С.39–42.
8. *Золотарёв В.В., Овечкин Г.В., Овечкин П.В.* О сопоставлении новых методов помехоустойчивого кодирования // Доклады 18-й Международной конференции «Цифровая обработка сигналов и её применение». — М., 2016. — Т.1, С.59–64.
9. *Arikan E.* Channel Polarization: A Method for Constructing Capacity-Achieving Codes for Symmetric Binary-Input Memoryless Channels // IEEE Transactions on Information Theory. — 2009. — Vol. 55, No. 7. — P.3051–3073.
10. *Золотарёв В.В.* Использование многопорогового декодера вместо алгоритма Витерби // Вестник Рязанской государственной радиотехнической академии. — 2002. — Вып. 10. — С.117–119.
11. *Золотарёв В.В., Овечкин Г.В.* Дивергентное кодирование свёрточных кодов // Материалы 18-й Международной научно-технической конференции «Проблемы передачи и обработки информации в сетях и системах телекоммуникаций», 2015. — С.27–32.

12. Ресурсы www.mtdbest.ru и www.mtdbest.iki.rssi.ru.
13. *Золотарёв В.В., Овечкин П.В.* Способ кодирования и декодирования блокового кода с использованием алгоритма Витерби: патент на изобретение РФ № 2608872 от 25.01.2017.
14. *Zolotarev V.V., Ovechkin G.V., Ovechkin P.V.* Modified Viterbi Algorithm for Decoding of Block Codes // 6th Mediterranean Conference on Embedded Computing MECO'2017, Bar, Montenegro.
15. *Золотарёв В.В., Овечкин П.В.* Характеристики декодирования блоковых кодов по алгоритму Витерби для систем ДЗЗ // XIII Всероссийская открытая конференция «Современные проблемы дистанционного зондирования Земли из космоса»: Тезисы докладов. — М.: ИКИ РАН, 2015.
16. *Золотарёв В.В., Мурзин С.Н.* Исследование методов ускорения работы алгоритма Витерби в каналах связи ДДЗ // XII Всероссийская открытая конференция «Современные проблемы дистанционного зондирования Земли из космоса»: Тезисы докладов. — М.: ИКИ РАН, 2014.

3.3. О синергетическом взаимодействии дивергентности и каскадирования

Принцип дивергенции при проектировании кодов и алгоритмов их декодирования (см. раздел 3.1) создан в процессе развития Оптимизационной Теории помехоустойчивого кодирования [4, 5], позволяющей реализовать новый уровень эффективного исправления ошибок в шумящих каналах на основе многопороговых декодеров и других алгоритмов. Дивергентные методы построения кодов и формирования алгоритмов их декодирования создают принципиально новый стиль постепенного некаскадного наращивания кодового расстояния в свёрточных кодах при использовании простейших итеративных, например, многопороговых или ещё каких-либо алгоритмов. Этот подход оказывается особенно важным при большом уровне шума канала. При этом всегда сохраняется небольшая сложность реализация исходных методов, а также реализуется более высокая результирующая эффективность кодирования, если, например, при этом используются коды, допускающие многопороговое декодирование [1–5]. В этом случае фактически оказывается возможным столь эффективное декодирование, что даже при большом шуме канала оно оказывается совпадающим по вероятности ошибки с оптимальным декодированием для используемых длинных кодов, которое обычно создаётся только на основе полного перебора, как это успешно реализуется, например, в случае алгоритма Витерби. Однако сложность МПД, которые

и при дивергентном кодировании оказываются простейшими схемами с мажоритарным декодированием, остаётся теоретически минимально возможной, линейной от длины кода. Именно использование длинных кодов и их практически оптимальное декодирование, обеспечиваемое методами МПД, приводит к наилучшим на сегодняшний день характеристикам их эффективности при очень большом уровне шума. Высокая достоверность декодирования МПД в этих условиях впервые позволила в [7, 9] и других исследованиях и разработках алгоритмов декодирования сделать уже вполне обоснованный вывод об успешном решении Оптимизационной Теорией проблемы Шеннона, сформулированной им 70 лет назад, как задачи простого высокодостоверного декодирования непосредственно вблизи пропускной способности канала C, т. е. при $R \lesssim C$.

Существенной особенностью дивергентного стиля декодирования является постепенное структурное усложнение декодера, например, мажоритарного типа, а также многократное применение этого подхода. В этом случае при построении кода и его декодера уже созданная структура декодера снова рассматривается как некоторый исходный декодер, который далее снова сам включается во внешнюю схему дивергентного декодирования ещё более высокого уровня. В этом многократном (трёх-, пяти- и более кратном) постепенном наращивании кодового расстояния, которое затем полностью реализуется, например, МПД алгоритмом, и состоит эффективное применение рассматриваемого дивергентного принципа организации процедуры декодирования. При правильном проектировании процедуры декодирования на дивергентных принципах декодер МПД в процессе выполнения процесса коррекции ошибок доводит, как и при использовании обычных кодов, достоверность своих решений до уровня оптимального декодирования используемых кодов.

Рассматриваемый подход к организации процедуры МПД декодирования, очевидно, ведёт к значительному увеличению длительности и сложности процесса проектирования, исследования и настроек создаваемых декодеров такого типа, заметному росту длины используемых кодов, а также к увеличению задержек принятия решений, т. к. количество необходимых итераций декодирования, в том числе и при использовании МПД, тоже заметно растёт. Однако, как уже было указано в первой главе и неоднократно отмечалось в литературе по кодированию последнего времени [7–9], все реальные методы декодирования с увеличением уровня шума канала требуют некоторого усложнения самих методов, процедур их проектирования и, что самое главное, значительного увеличения длины используемых кодов как в блоковых, так и в свёрточных вариантах своей реализации.

Что касается дивергентного стиля декодирования, то исключительно важным его свойством является то, что после окончания проектирования и настройки алгоритма, использующего этот весьма эффективный подход, созданный метод декодирования во всех случаях на самом деле остаётся фактически столь же простым, как и исходный алгоритм, взятый за его основу. В частности, если за такую основу проектируемого декодера дивергентного типа взят МПД алгоритм, то результирующая схема традиционного для свёрточных алгоритмов декодера со многими пороговыми элементами практически всегда остаётся таким же простейшим МПД декодером со вполне понятными принципами работы, что тоже всегда очень важно при обучении специалистов, которые будут контролировать и сопровождать далее работу таких систем кодирования. Фактически единственным отличием дивергентного МПД от его стандартного обычного классического вида обычно оказывается то, что используемые на различных итерациях декодирования пороговые элементы принимают свои решения только по некоторой части из полного множествах проверок. Декодер принимает эти решения на основе их значений и затем выполняет всё те же простые операции изменения символов синдрома и декодируемых символов. Количество таких различных групп проверок может для различных ПЭ достигать 3–5 вариантов при общем полном числе проверок порядка 20, что никак не усложняет суть МПД алгоритма. Более того, поскольку на первых итерациях пороговые элементы, как это следует из описания принципов дивергенции, используют лишь небольшую часть из общего набора проверок, созданный МПД алгоритм на таких новых принципах выполняет даже немного меньшее число суммирований проверок на общей совокупности ПЭ, чем если бы все ПЭ использовали полные наборы проверок. Таким образом, дивергентные МПД остаются действительно очень простыми системами декодирования, но, как и предполагалось при их создании, понимание сути дивергентного декодирования и правильное проектирование соответствующих декодеров позволили действительно создать алгоритмы многопорогового типа, которые успешно работают вблизи границы Шеннона, т. е. при тех почти максимально возможных уровнях шума, когда $R \lesssim C$.

Рассмотрим наиболее эффективные новые результаты применения принципа дивергентности, полученные для каналов с большим уровнем шума. На рис. 3.6 представлены характеристики МПД алгоритмов для гауссовских каналов, а также АВ декодера с $K = 7$ и каскадной схемы АВ с кодом Рида — Соломона, которые были взяты из [7]. Как было указано там же, МПД декодер, отмеченный как MTD1, характеризуется теоретически максимально возмож-

ным быстродействием в аппаратном варианте [10]. Кроме того, имея вполне технологичную реализацию, что подтверждается представленным в [7, 8] макетом МПД декодера на ПЛИС Altera на информационную скорость декодирования более 1 Гбит/с, этот МПД эффективно работает на расстоянии всего лишь 1 дБ от пропускной способности канала. Это позволяет утверждать, что оптимизационная Теория и алгоритмы МПД действительно стали доступным технологичным решением проблемы Шеннона — эффективного и простого декодирования при максимально допустимом уровне шума.

Обращаясь к графику MTD1 для кода, успешно работающего при кодовой скорости $R = 1/2$ в двоичном гауссовском канале при $E_b/N_0 = 1{,}2$ дБ, т. е. на расстоянии всего лишь 1 дБ от границы Шеннона, укажем, что он является результатом реализации трёхуровневой дивергентной схемы для самоортогонального систематического кода с минимальным расстоянием $d = 21$. В случае, если бы мажоритарно декодируемый код с таким же кодовым расстоянием был реализован без учёта идей дивергентного декодирования, то даже при использовании методов параллельного каскадирования или других полезных кодовых конструкций из обширного множества технологий ОТ было бы возможно обеспечить работоспособность алгоритма МПД в гауссовском канале только при уровне энергетики более 2,9 дБ. Отметим, что декодеры для кодов МПД2 и МПД3, представленные в [7], также использовали дивергентные структуры.

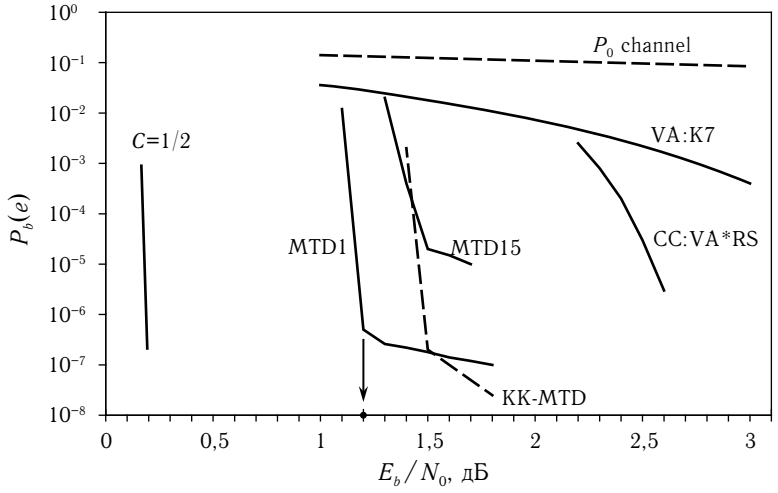

Рис. 3.6. Характеристики МПД алгоритма с использованием синергетического взаимодействия дивергенции и каскадирования с кодами контроля по чётности

Полезно также отметить, что представленные в [7, 9] характеристики МПД декодеров для символьных кодов, успешно работающих при вероятности независимых ошибок в канале $p_0 \lesssim 0{,}3$, а также декодеры для исправления стираний используют такие же, как и в двоичном случае, вложенные структуры дивергенции, что и позволяет им обеспечивать абсолютно уникальные характеристики помехоустойчивости на основе простейших по своей сути МПД декодеров.

Приведённые примеры применения дивергенции обеспечили значительное ускорение решения проблемы Шеннона в каналах с независимыми искажениями.

Рассмотрев кратко важность и эффективность базовых (некаскадных) дивергентных кодовых структур, проанализируем теперь возможности их взаимодействия с традиционными последовательными каскадными схемами. Как и обычные методы декодирования, дивергентные методы можно успешно применять совместно с каскадными схемами в непосредственной близости от границы Шеннона для любых кодовых скоростей и моделей каналов с независимыми ошибками. Оказалось, что синергетический эффект их взаимоподдержки действительно многократно повышает итоговую эффективность применения кодирования.

Однако для таких систем, которые следует использовать вблизи пропускной способности каналов, т. е. при $R \lesssim C$, существует очень важное ограничение на коды, входящие в состав создаваемой каскадной схемы. Оно состоит просто в том, что внешний второй код каскадной схемы должен иметь чрезвычайно малую избыточность, т. е. кодовую скорость $R_2 \lesssim 1$, т. к. иначе внутренний код со скоростью R_1 будет неработоспособным уже просто потому, что может оказаться, что $C < R_1$. Таким образом, становится очевидным, что наиболее подходящими внешними кодами для каскадной последовательной схемы становятся именно коды контроля по чётности, имеющие минимальную избыточность, но увеличивающие кодовое расстояние d каскадной схемы вдвое, т. к. у них это расстояние $d_2 = 2$. В этом случае возможно значительно, почти на 3 дБ поднять энергетический выигрыш кодирования. Для области $R \approx C$ будет, конечно, очень хорошим результатом, даже если ЭВК увеличится на меньшую величину, например, на ~ 2 дБ. Такой подход тем более важен, что ККЧ действительно очень просто взаимодействуют со многими типами внутренних кодов [4–6].

Однако другим весьма важным моментом при создании КК является то, что их длина N является произведением длин двух составляющих их кодов: $N_{\text{КК2}} = n_1 n_2$. А поскольку выше было указано, что избыточность второго внешнего кода ККЧ должна быть очень малень-

кой, то, очевидно, обязательно должно выполняться условие $n_2 \gg 1$. Но тогда длина N всего каскадного кода должна неизбежно вырасти в сотни раз. При выборе же меньших значений n_2 характеристики кодирования/декодирования будут обязательно удаляться от границы Шеннона просто из-за потерь от уменьшения кодовой скорости R_2.

Ниже предлагается простая схема каскадирования, удобная в реализации и удовлетворяющая всем перечисленным компромиссным требованиям. Для этого рассмотрим сначала классическую двумерную схему каскадирования на основе ККЧ и кодов с мажоритарным декодированием [3–6]. Если реализовать декодирование внутреннего кода на основе МПД и считать, что решение МПД для некоторого уровня шума в АБГШ канале практически совпадает с оптимальным, а вероятность его ошибки на бит равна $P_b(e)$, то вероятность ошибки полной каскадной схемы, как это хорошо известно [1, 4, 6], будет достаточно точно оцениваться выражением

$$P_{\text{КК}} \approx 2\big(P_b(e)\big)^2 n_2. \qquad (3.1)$$

Но самым существенным для создаваемой нами каскадной схемы является то, что двумерность каскадных кодовых структур была когда-то совершенно обязательной только из-за внутренних алгебраических кодов, при неправильном декодировании которых доля ошибок внутри кодового блока была весьма значительной. Однако ошибки при использовании МПД чаще всего происходят поодиночке, что определяется структурой используемых кодов для мажоритарного декодирования и высоким качеством декодирования на базе МПД, практически совпадающим с оптимальным. Но тогда оказывается возможным применить только простейшую одномерную схему кодирования малоизбыточным кодом, а затем этот же информационный поток с редкими вставками битов контроля по чётности кодировать внутренним кодом, который в приёмнике сумеет успешно декодировать МПД. И далее, поскольку оказывается, что ошибки МПД не просто одиночные, но и почти независимые, то можно ожидать что представленная выше оценка РКК будет достаточно точной оценкой и для нового КК гораздо меньшей длины $N_{\text{КК2}} \sim (n_1 + n_2)$.

Однако, если внутренние коды для МПД, декодирующего каскадный код, не слишком длинные, то возможно, что внутри кода ККЧ найдётся много пар информационных символов таких, что они одновременно являются и слагаемыми в некоторых проверочных символах. А для самоортогональных внутренних кодов с расстоянием d_1 это приводит к тому, что платой за «короткий» каскадный код оказывается то, что расстояние каскадного кода будет равно $d_{\text{КК}} = 2d_1 - 2$, а не $2d_1$. Это обстоятельство иногда дополнительно повышает вероятность ошибки декодера каскадного кода до 3–5 раз. Но поскольку

абсолютная величина ошибки декодирования всего каскадного кода, как было показано выше, достаточно мала, то такая плата за снижение длины КК на 2 десятичных порядка по сравнению с двумерной конструкцией является совершенно понятной и вполне допустимой.

С учётом изложенных особенностей каскадирования была разработана каскадная схема, показавшая свою высокую эффективность вблизи границы Шеннона. Внутренним кодом был выбран СОК с $R = 1/2$ и $d = 15$, который декодировался фактически оптимально при $E_b/N_0 \geqslant 1{,}5$ дБ, как это представлено на рис. 3.6 графиком MTD15. Количество итераций декодирования равно 80, а общая задержка решения составляет менее миллиона информационных символов, что для столь тяжёлых условий работы МПД является также очень хорошим результатом и по этим параметрам. Объём собранной статистики для трёх правых точек на графике превышал $5 \cdot 10^7$ битов и все ошибки декодирования были оптимальными, т. е. неисправимыми и при полном переборе каким-либо ОД, создать который для такого длинного кода, конечно, невозможно.

Каскадный код с использованием ККЧ с $(n_2, k_2, d_2) = (192, 191, 2)$ был построен по описанным выше правилам формирования «коротких» кодов, он имеет кодовое расстояние $d_{\text{kk}} = 2 \cdot 15 - 2 = 28$. Согласно [1, 3, 4], первоначально в каскадном коде работает МПД алгоритм по обычной схеме и доводит вероятности ошибки, как и в обычном случае, до оптимального уровня. В каскадном коде, по сравнению с исходным внутренним декодером МПД, добавлены 5 дополнительных итераций декодирования. Задержка декодирования осталась менее 1 млн. символов. Последние 20 итераций декодирования организованы с учётом наличия ККЧ. При этом после завершения приёма очередных 192 символов внешнего кода при успешной проверке по чётности внутренний декодер переходил к следующим символам, а при невыполнении проверки он изменял наименее надёжный символ внешнего кода, если он оказывался единственным. График эффективности каскадного кода представлен кривой КК–MTD. Объём статистики при $P_b(e) < 10^{-6}$ более $2 \cdot 10^8$ битов и все ошибки декодера соответствовали оптимальному декодированию. Как и должно следовать из описания созданной нами каскадной схемы, а также в согласии с [3–5], абсолютное большинство ошибок в КК были сдвоенными, находящимися на расстоянии менее n_2, и лишь совсем небольшая доля ошибок оказалась одиночными. Наличие только ошибок двух таких типов свидетельствует о том, что и КК декодируется с помощью МПД практически оптимально, но уже для всего каскадного кода в целом. Потери в скорости из-за наличия внешнего ККЧ составляют $\sim 0{,}02$ дБ. Это позволяет говорить о правильной организации

эффективного декодирования каскадного кода вблизи границы Шеннона, вероятность ошибки для которого с учётом всех сделанных для построенного каскадного кода комментариев совпала с оценкой (3.1).

Далее отметим, что успешность решения задачи каскадирования при очень высоком уровне шума на представленном выше весьма трудном примере позволяет оценить возможность каскадирования на основе МПД и для алгоритма, отмеченного на рис. 3.6 как MTD1, который эффективно работает при $E_b/N_0 = 1{,}2$ дБ, что является вообще недоступным для каких-либо других известных реализуемых алгоритмов. Поскольку для кода, представленного на рис. 3.6 кривой MTD15, экспериментальные данные хорошо совпали с давно уже известными оценками для КК с МПД декодированием, для близкого по типу к MTD15 кода MTD1 были выполнены такие же численные оценки согласно (3.1). Вертикальная стрелка ниже кривой MTD1 и точка на оси ординат указывают на то, что достаточно реальная оценка $P_b(e)$ для этого примера лежит существенно ниже уровня $P_{b\text{КК}}(e) \ll 10^{-9}$. Более точную оценку для этого кода можно было бы получить при использовании аппаратного макета, который, как следует из [7, 8], легко создать на основе уже имеющегося опыта успешного проектирования, создания и испытаний МПД с использованием ПЛИС Altera на скорость 1 Гбит/с. Вполне возможно, что реальный эксперимент на аппаратном макете дал бы вероятность ошибки $P_b(e) \sim 10^{-11}$.

Наконец, укажем, что методы каскадирования символьных кодов и для коррекции стираний, как и в случае двоичных кодов, реализуются на базе МПД столь же легко [5, 6]. Они повышают простейшими средствами достоверность декодирования на много десятичных порядков. Тем самым представленные результаты ещё более расширяют ту сферу применения Оптимизационной Теории, в которой характеристики декодирования МПД и ряда других методов столь эффективны, что и в этой стремительно расширяющейся сфере параметров каналов и систем кодирования проблема Шеннона — простое эффективное декодирование при $R \lesssim C$ — может считаться полностью успешно решённой, в том числе и на технологически доступном уровне.

Список литературы

1. *Золотарёв В.В., Овечкин Г.В.* Помехоустойчивое кодирование. Методы и алгоритмы. Справочник. — М.: Горячая линия — Телеком, 2004. — 126 с.
2. *Самойленко С.И., Давыдов А.А., Золотарёв В.В., Третьякова Е.Л.* Вычислительные сети. — М.: Наука, 1981. — 278 с.
3. *Золотарёв В.В.* Теория и алгоритмы многопорогового декодирования. — М.: Радио и связь, Горячая линия — Телеком, 2006;

второе издание — 2014.

4. *Zolotarev V.V., Zubarev Y.B., Ovechkin G.V.* Optimization Coding Theory and Multithreshold Algorithms. — Geneva, ITU, 2015. — 159 p.
5. *Золотарёв В.В., Зубарев Ю.Б., Овечкин Г.В.* Многопороговые декодеры и оптимизационная теория кодирования / Под ред. академика РАН В.К. Левина. — М.: Горячая линия — Телеком, 2012. — 238 с.
6. *Овечкин Г.В.* Теория каскадного декодирования линейных кодов для цифровых радиоканалов на основе многопороговых алгоритмов: дис. ... д-ра тех. наук. — Рязань: РГРТУ, 2011. — 301 с.
7. *Золотарёв В.В.* О новом этапе развития оптимизационной теории кодирования // Цифровая обработка сигналов. — 2017. — № 1. — С.33–41.
8. *Золотарёв В.В., Овечкин Г.В.* Эффективные многопороговые методы декодирования самоортогональных кодов // Вестник РГРТУ. — 2017. — № 60. — С.113–122.
9. *Зубарев Ю.Б., Золотарёв В.В., Овечкин Г.В., Овечкин П.В.* Итоги 25-летнего развития оптимизационной теории кодирования // Наукоёмкие технологии. — 2016. — Т.17. — С.26–32.
10. *Золотарёв В.В.* Способ декодирования помехоустойчивого кода: патент на изобретение № 2377722 с приоритетом от 21.06.2007. БИ № 36, 2009.

3.4. Расширение возможностей применения блоковых версий алгоритма Витерби

3.4.1. История вопроса

В [1–4] были представлены характеристики весьма простой модификации алгоритма декодирования квазициклических блоковых кодов, которые строятся на основе более коротких свёрточных кодов. При этом декодирование осуществляется обычным алгоритмом Витерби (АВ), не учитывающим блоковую структуру кода, а как бы декодирующим часть бесконечной последовательности свёрточного кода, несколько более длинной, чем размер конкретного декодируемого блокового кода n. После декодирования $m = 3...5$ последовательно расположенных кодовых блоков длины n, которые декодер АВ воспринимает просто как отрезок свёрточного кода длины $m \times n$, информационная последовательность, соответствующая средней части этого отрезка, содержащая минимум ошибок АВ, передаётся получателю.

По самому смыслу запатентованного школой ОТ нового блоково-

го алгоритма Витерби (БАВ) его сложность N остаётся пропорциональной $N \sim 2^K$, где K — это степень кодового полинома свёрточного кода, на основе которого строился кусочно-циклический код длины n [1–3]. Это существенно меньше, чем оценка сложности $N \sim 2^{2K}$ алгоритмов оптимального декодирования блоковых кодов, которые настойчиво предлагается изучать даже студентам в [5]. Напомним, что, как отмечалось в [3], подобно примеру созданного в NASA АВ с $K = 15$, в случае реализации его блокового варианта наша версия БАВ имела бы сложность N, в $\sim 16\,000$ раз меньшую, чем у схем, описанных в [5].

Ниже рассмотрены подходы к реализации БАВ, существенно расширяющие его возможности.

3.4.2. Гибкость методов реализации БАВ

Важной особенностью БАВ оказывается наличие у него двух основных параметров: длины K полинома свёрточного кода и собственно длины блокового кода n. Эта новая ситуация для алгоритма Витерби создаёт особые возможности для настроек систем кодирования и их адаптации к условиям применения. При достаточно больших значениях n вероятности ошибки на бит $P_b(e)$ у БАВ будут такими же, как и у обычного АВ с аналогичным полиномом длины K. На это было кратко указано в [1, 3].

Рассмотрим более детально особенности БАВ. На рис. 3.7 представлены для различных кодов графики вероятности ошибки на бит BER и на блок WER как зависимости от относительной энергетики гауссовского канала E_b/N_0. Пунктиры S1024 и H1024 соответствуют границе Хемминга (сферической упаковке) для вероятностей WER кодов с кодовой скоростью $R = 1/2$ и длиной $n = 1000$, которые являются удобным ориентиром эффективности кодирования для относительно коротких кодов.

В качестве опорного варианта БАВ возьмём блоковый код длины $n = 256$ с порождающим полиномом свёрточного кода длины $K = 15$. WER для него отмечена на рис. 3.7 как 15S. Он уже рассматривался в [1, 3, 8]. При его реализации на компьютере с процессором Core-i7 и с тактовой частотой ~ 3 ГГц скорость декодирования программной модели БАВ в гауссовском канале, написанной на языке C++, близка к 1000 битам в секунду. При переходе к другим параметрам кодов скорость работы изменяется примерно вдвое при увеличении или уменьшении значения K на единицу. Например, для $K = 18$ скорость декодирования составит немного более 100 бит/сек. График WER для БАВ в двоичном симметричном канале (ДСК) с $K = 15$ и $n = 256$ отмечен как 15H. Разумеется, в ДСК у этого БАВ такая же скорость

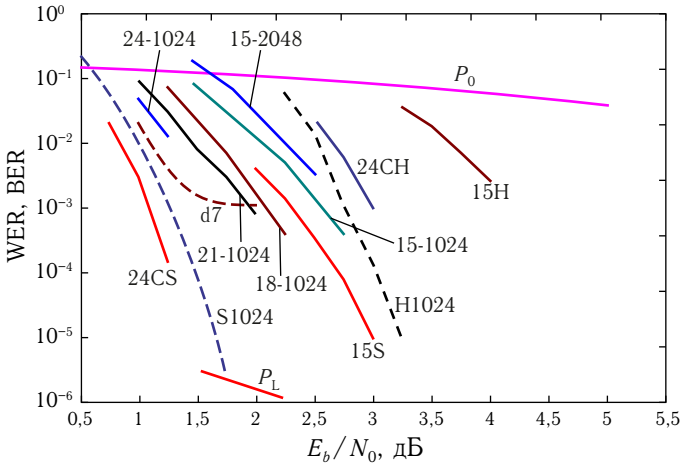

Рис. 3.7. Spheres and BVA performance for AWGN $R = 1/2$

работы ~ 1000 бит/с. Остальные графики вида $K - n$ соответствуют длине свёрточного полинома K и длине блокового кода n.

Новые возможности настройки БАВ иллюстрируются представленными тремя графиками WER для гауссовского канала с возрастающей длиной n от 256 до 2048 при фиксированном $K = 15$: S15 (15-256), 15-1024 и 15-2048. Эта настройка и создаёт условия для адаптации кода с БАВ к условиям применения. Вероятности WER растут у БАВ примерно пропорционально с ростом n, а BER при достаточно больших n совпадают с вероятностями для свёрточного АВ с тем же полиномом длины K.

Рассмотрим более сложные соотношения возможностей БАВ при изменении K. Для $K = 18$ и длины блока $n = 1024$ приведён WER график 18-1024. Заметим, что АВ с $K = 15$ был реализован в прошлом тысячелетии. Поэтому сейчас, через 25 лет, и значения $K \sim 24$ уже также следует отнести к реально актуальным устройствам, по меньшей мере, при аппаратной реализации. Экспериментальные графики 21-1024 и 24-1024 показывают всё большую близость WER к границе S1024 с ростом длины полинома K. Разумеется, из-за малой скорости моделирования две последние кривые даны по результатам ограниченного эксперимента, который в случае актуализации задачи на техническом уровне можно будет продолжить на другой экспериментальной базе.

Наконец, для сопоставления возможностей БАВ и свёрточного АВ график 24CH показывает BER в ДСК для свёрточного АВ с $K = 24$. Сравнение этого графика и кривой 15H с графиками для гауссовского канала показывает, что БАВ в ДСК всегда ведут себя аб-

солютно одинаково, но со сдвигом на 2 дБ, также сохраняя широкие возможности по адаптации на основе вариации параметров K и n.

3.4.3. Технологии реализации БАВ для длинных кодов

Использование БАВ позволяет, как и при использовании многопороговых декодеров (МПД) для квазициклических кодов, успешно декодировать блоковые коды без потери в кодовой скорости R, что и является предметом изобретения, обладающего ещё и хорошей адаптивностью к параметрам канала и системы связи. Однако необходимая для такого декодера память по порядку величины составляет около $\sim 2^{K-1} \times n \times R$ битов. А в целом ряде случаев объём такой памяти может составлять многие гигабайты.

Однако оказалось возможным существенно уменьшить реально необходимые размеры памяти блоковых АВ. Выяснилось, что всегда можно реализовать БАВ таким образом, что сначала близкие к принятым блокам сообщения более короткие части полных путей, запоминаемые декодером, хранятся в его памяти относительно небольшого размера. А в зависимости от выбранного кода, уровня шума и степени группирования ошибок на выходе БАВ можно провести некоторые дополнительные вычисления и вместо хранения всего экспоненциально большого числа вариантов полных путей запоминать только эти начальные текущие гипотезы-решения, создаваемые на достаточном небольшом удалении от места приёма декодером очередного блокового кода. А вместо экспоненциально большого числа более удалённых частей решений можно хранить в АВ декодере только единственный вариант вычисленного некоторым образом почти правильного пути. Таким образом, ситуация становится похожей на то, что происходит при декодировании свёрточного кода обычным АВ, когда пользователю поступает значение символа, вычисленного некоторым образом на основе значений крайних символов-решений всех хранимых путей ограниченной длины, даже если передаваемое сообщение имеет очень большую длину.

Реализация такого варианта БАВ действительно выявила возможность реализации БАВ совершенно произвольно большой длины n при весьма ограниченных размерах памяти такой его модификации. Это новое свойство алгоритма ещё более расширяет сферу применения БАВ, причём теперь уже без всяких дополнительных исследований, так как вероятность BER БАВ-декодера длинного кода просто совпадает с такой же вероятностью обычного классического АВ, что уже было понятно из свойств БАВ с самого начала рассмотрения его возможностей в работах [1, 8]. В результате этого теперь уже совершенно исключаются из рассмотрения абсолютно все прежние

методы как бы оптимального декодирования блоковых кодов, например, Чейза и других авторов, эффективность и польза которых очень невелики, а сложность и нетехнологичность просто не сопоставимы с практически идеальными АВ и БАВ. Увеличение объёма необходимых дополнительных вычислений в новом БАВ составляет до 1,3...2 раз, что никак не сокращает сколько-нибудь существенно сферу его применения.

На метод сокращения размеров памяти декодера и увеличения длины используемых кодов подана заявка на патент на изобретение.

Укажем справочно соотношение между возможностями двух главных методов, развиваемых в Оптимизационной Теории (ОТ) кодирования: различных МПД и АВ, в том числе БАВ. Как следует из [3, 7–10], для реализации оптимального декодирования (ОД) с минимальными вычислительными затратами вблизи пропускной способности канала следует применять МПД декодеры. Но для этого следует использовать весьма длинные коды. А при необходимости реализовать декодирование с малой задержкой следует применять различные модификации АВ. Однако в этом случае потребуются более высокие вычислительные затраты, что можно сделать как в программном варианте, так и при аппаратной реализации. И эти два подхода полностью закрывают всё пространство желаемых реальных параметров кодов и декодеров. Оба алгоритма фактически оптимальны и решают все задачи применения кодов для всех двоичных и стирающих каналов. А условий для применения прочих методов вместо технологий ОТ сейчас уже реально нельзя указать вообще. Так что появление методов АВ-декодирования блоковых кодов произвольной длины очень важно, так как окончательно снимает проблему выбора алгоритмов декодирования и блоковых, и свёрточных кодов за пределами ОТ. Таких методов с характеристиками, сопоставимыми с алгоритмами, создаваемыми в рамках ОТ, нет.

3.4.4. О методах каскадирования при использовании технологий ОТ

Приведённые в предыдущем разделе соотношения между алгоритмами по сложности полностью соответствуют всем актуальным реальностям проектирования кодеков. Но указанные соотношения справедливы именно для базовых методов декодирования. В [3, 4, 9] детально представлены различные методы каскадирования МПД декодеров. Они для всех алгоритмов позволяют достичь более высокой эффективности при несколько меньших вычислительных затратах по сравнению с исходными способами кодирования. Для АВ алгоритмов каскадирование тоже является вполне эффективным подходом к реализации методов декодирования. Наиболее известным таким ме-

тодом более 40 лет является вариант последовательного каскадирования свёрточного кода с алгоритмом Витерби при $K=7$ и кода Рида — Соломона (РС) [10]. Напомним, что эта весьма полезная схема обеспечивает РЕВ$\sim 10^{-5}$ при $E_b/N_0=2{,}5$ дБ. Правда, при этом не следует забывать, что данная каскадная конструкция из-за внешнего кода РС теряет в кодовой скорости порядка 0,6 дБ по сравнению со скоростью $R=1/2$ алгоритма Витерби, за счёт чего собственно и достигается неплохой уровень энергетики.

Рассмотрим возможности каскадирования для алгоритмов, графики которых представлены рис. 3.7. Начнём с анализа последовательных схем каскадирования. Внешний свёрточный двоичный код, который будет снижать итоговую кодовую скорость R не более, чем на 0,25 дБ, должен иметь кодовую скорость $R=17/18$. В ОТ создано много типов программных платформ, позволяющих за несколько минут оценить характеристики абсолютно любой схемы АВ или МПД. Оказалось, что такой малоизбыточный код выходит на уровни вероятностей ошибки РЕВ$\lesssim 10^{-6}$ с не более $I=25$ итерациями коррекции при вероятности ошибки на входе декодера $p_0\sim 0{,}002$. Обращаясь к рис. 3.7 и свёрточному коду с $K=24$ (график 24CS), получаем, что крайне малые вероятности на выходе каскадной схемы АВ с $K=24$ и МПД с $R=17/18$ будут при энергетике $E_b/N_0=1{,}5$ дБ, но, разумеется, только при аккуратной реализации перемежения символов на выходе АВ. Это улучшение энергетики на целый 1 дБ непосредственно вблизи границы Шеннона, да ещё с заметно меньшей потерей в скорости по сравнению с упоминавшейся выше традиционной уже схемой с АВ, $K=7$ и кодом РС, конечно, надо считать отличным результатом ОТ на базе АВ и МПД. Ещё раз напомним, что именно такой результат даст и достаточно длинный БАВ с $K=24$.

Если применить гораздо более лёгкую в реализации схему АВ с $K=18$, то оценки по этой же методике дают энергетику последовательного каскадирования и высокодостоверного декодирования порядка $E_b/N_0\sim 1{,}75$ дБ, что также является очень хорошим результатом, поскольку итоговые длины каскадных кодов в обоих случаях относительно невелики. А такие схемы изначально не предназначены для работы вблизи пропускной способности канала C, которая для $R=1/2$ и гауссовского канала равна $C=1/2$ при $E_b/N_0\sim 0{,}2$ дБ и квантовании двоичного сигнала на 16 уровней (4 бита).

Рассмотрим также один простой, но важный пример параллельного каскадирования — метода, открытого школой ОТ и сыгравшего большую роль в повышении эффективности многих алгоритмов, созданных с применением МПД и других подходов, которые развивает наша школа [3, 8–10]. На рис. 3.7 пунктиром d7 обозначен гра-

фик BER для длинного БАВ, который декодировал самоортогональный систематический код (СОК) с порождающим полиномом длины $K = 18$, $R = 1/2$ и $d = 7$ [10]. Он относится к типичному коду, который хорошо и просто декодируется с помощью МПД и при этом легко выходит на уровень оптимального декодирования (ОД). Анализ структуры ошибок БАВ показал, как и следовало ожидать для СОК, практически полную независимость ошибок декодирования БАВ в области входного шума АБГШ $E_b/N_0 > 1{,}25$ дБ. А это позволяет при использовании опять примерно такого же кода с $R \sim 0{,}95$ во внешнем слое параллельной каскадной схемы декодировать уже каскадный код в целом с потерей не более 0,25 дБ по энергетике из-за небольшого снижения кодовой скорости R и обеспечивать РЕВ$\sim 10^{-6}$ или даже более хорошие уровни достоверности, как показано на рис. 3.7 кривой P_L. Более точное согласование параметров такой параллельной каскадной схемы с использованием мощных средств оптимизации всех элементов кодовой конструкции обязательно позволит ещё значительно улучшить характеристики такого каскадного декодера с использованием БАВ и МПД.

Возможно, что ещё более впечатляющие результаты, как предлагалось в [3], будут получены в случае взаимодействия этих алгоритмов по дивергентному принципу, который тоже сохраняет общее число операций декодирования относительно небольшим, но существенно повышает итоговую эффективность кодирования вообще без потерь в кодовой скорости R.

Отдельного рассмотрения заслуживают также схемы каскадирования, на внешних ступенях которых применяются символьные (недвоичные) коды [3, 4, 6–10]. Они хорошо заменяют коды РС во внешних ступенях каскадных схем любого типа просто из-за их способности работать при уровне входного шума, в несколько раз превышающем допустимые вероятности ошибки на входе декодеров для кодов РС.

Заметим снова, что ещё одним ценным результатом обеих каскадных схем с АВ является заметное снижение задержек декодирования за счёт несколько большей вычислительной работы, которую выполняют различные версии АВ во внутренних каскадах рассмотренных выше схем.

3.4.5. Заключение

Дальнейшая модификация БАВ выявила новые возможности для создания схем декодирования блоковых кодов в гауссовских и ДСК каналах, а также в каскадных схемах, которые во всех случаях демонстрируют высокие энергетические характеристики предлагаемых

методов. Применение БАВ в каскадных схемах естественно уменьшает необходимые задержки принятия решений всеми алгоритмами, что также становится важным фактором при выборе тех или иных схем кодирования.

Сравнение с технологиями ОТ каких-либо других алгоритмов из тех, которые публикуются в настоящее время, показывает, что турбо, низкоплотностные (LDPC) и полярные коды и их алгоритмы декодирования не могут конкурировать с декодерами с прямым контролем метрики (ДПКМ) [3, 11, 17]. Многие характеристики АВ, БАВ и различных МПД просто недоступны для любых других способов декодирования как при рассмотрении вопросов приближения области их работы к границе Шеннона, так и для коротких кодов [11].

Однако, к огромному сожалению сторонников научной школы ОТ, все эти правильные в целом оценки заключения данной статьи на самом деле не имеют особого смысла по неожиданной, но очень веской причине. За многие последние десятилетия никто, кроме школы ОТ, ни разу не предъявил полных данных о «созданных» теми или иными авторами декодерах, достоверно проверяемых по триединому критерию «помехоустойчивость — достоверность — сложность». В абсолютном же большинстве публикуемых материалов школы ОТ указываются как результаты моделирования, показывающие возможности декодеров ОТ по первым двум компонентам этого обязательного критерия, так и скорости работы всех своих алгоритмов при их полном компьютерном моделировании на языке C++, что очень естественно и удобно для сравнения.

Дополнительные средства сопоставления сложности любых декодеров давно предложены школой ОТ и помещены на наши сетевые порталы [14].

Сложившаяся ситуация определяется тем, что ни для одного параметра указанного выше жёсткого, но абсолютно обязательного критерия сравнения, при большом уровне шума нельзя сейчас и не возможно в будущем найти их точные аналитические выражения, что и показало медленное угасание прежней теории кодирования с 1970-х годов и по 1990 г., когда фактически была полностью завершена вся ОТ [15]. Этот глобальный кризис взаимоотношений теории и эксперимента давно ощущала мировая наука, что признавалось и во многих статьях, например, опубликованных на портале РАН [13].

Некоторые вопросы конкретного сопоставления возможностей ОТ и прежней, уже неклассической теории кодирования рассмотрены в [11, 12, 16–18]. Из них непосредственно следует, что теория кодирования — это вовсе не математическая задача, а особая проблема теории оптимизации со специфическими параметрами поиска гло-

бального экстремума в дискретных пространствах, организованных с учётом структурных свойств кодов. Нам представляется, что для прежней российской теории кодирования давно настало время переосмыслить основные парадигмы нашей главной науки в области теории информации и принять на себя ответственность за разработку и решение новых проблем в сфере прикладной теории кодирования с использованием уже имеющихся серьёзных теоретических научных достижений ОТ и весьма изощрённых наукоёмких инновационных компьютерных технологий.

Автор благодарит сторонников научной школы ОТ за подготовленные для этой работы материалы и помощь в подготовки статьи.

Список литературы

1. *Золотарёв В.В., Овечкин Г.В., Овечкин П.В.* Характеристики блоковых реализаций алгоритма Витерби // Вестник РГРТУ. — 2017. — № 59. — С.30–35.
2. *Золотарёв В.В., Овечкин П.В.* Способ кодирования и декодирования блокового кода с использованием алгоритма Витерби. — Патент на изобретение № 2608872.
3. *Золотарёв В.В.* Теория кодирования как задача поиска глобального экстремума / Под научной ред. академика РАН Н.А. Кузнецова. — М.: Горячая линия — Телеком, 2018. — 220 с.
4. *Zolotarev V.V.* Coding Theory as a Simple Optimal Decoding near Shannon's Bound (Optimization Theory of error-correcting coding — is a new «quantum mechanics» of information theory). — M.: Hot Line — Telecom, 2018. — 333 p.
https://mtdbest.ru/articles/mtd_book_2019.pdf
5. *Кудряшов Б.Д.* Основы теории кодирования: Учебное пособие. — СПб.: БХВ-Петербург, 2016. — 393 с.
6. *Zolotarev V.V., Nazirov R.R., Ovechkin G.V., Ovechkin P.V.* Optimizing Theory: Taking Over the Leadership Baton From Classic Coding Theory // Information Technologies in Remote Sensing of the Earth — RORSE 2018. — P.198–206.
https://doi.org/10.21046/rorse2018.198
7. *Золотарёв В.В., Овечкин Г.В., Назиров Р.Р.* О передаче Оптимизационной Теории лидерства от прикладной классической теории помехоустойчивого кодирования // Некоторые аспекты современных проблем механики и информатики: сб. науч. ст. — М.: ИКИ РАН, 2018. — С.82–90. DOI: 10.21046/aspects-2018-82-90.
https://mtdbest.ru/articles/zolotarev_leadership.pdf

8. *Золотарёв В.В.* О новом этапе развития оптимизационной теории // Цифровая обработка сигналов. — 2017. — № 1. — С.33–41. https://mtdbest.ru/articles/Zolotarev_DSPA_2017.pdf
9. *Зубарев Ю.Б., Золотарёв В.В., Овечкин Г.В.* Развитие теории каскадных алгоритмов многопорогового декодирования // В сб.: Цифровая обработка сигналов и ее применение. — М., 2011. — Т. 1. — С.9–12. https://mtdbest.ru/articles/Zolotarev_dspa_2011.pdf
10. *Золотарёв В.В., Овечкин Г.В.* Помехоустойчивое кодирование. Методы и алгоритмы. Справочник. — М.: Горячая линия — Телеком, 2004. — 126 с. https://mtdbest.ru/articles/mtd_handbook.pdf
11. *Кузнецов Н.А., Золотарёв В.В., Овечкин Г.В., Назиров Р.Р., Сатыбалдина Д.Ж., Омирбаев Е.Д.* Обзор проблем полярных кодов с позиции технологий Оптимизационной Теории помехоустойчивого кодирования // Современные проблемы дистанционного зондирования Земли из космоса. — 2020. — Т. 17, № 4. — С.9–26.
12. *Зубарев Ю.Б., Золотарёв В.В., Овечкин Г.В.* Новые технологии и парадигмы помехоустойчивого кодирования: после решения проблемы Шеннона // Электросвязь. — 2019. — № 7. — С.56–61.
13. *Магаршак Ю.* Число, возведенное в абсолют // Независимая газета. 09.09.2009 г.
14. Ресурсы www.mtdbest.ru, www.mtdbest.iki.rssi.ru.
15. *Золотарёв В.В.* Субоптимальные алгоритмы многопорогового декодирования: дис. ... д-ра тех. наук. — М., 1990.
16. *Золотарёв В.В., Зубарев Ю.Б., Смагин М.С.* Преодоление системного кризиса в теории информации // Вестник связи. — 2020. — № 8. — С.25–35.
17. *Кузнецов Н.А., Золотарёв В.В., Зубарев Ю.Б., Овечкин Г.В., Назиров Р.Р., Аверин С.В.* Проблемы и открытия Оптимизационной Теории помехоустойчивого кодирования (ОТ в иллюстациях). — М.: Горячая линия — Телеком, 2020. — 36 с. http://www.mtdbest.ru/articles/comics.pdf
18. *Kuznetsov N.A., Zolotarev V.V., Zubarev Yu.B., Ovechkin G.V., Nazirov R.R., Averin S.V.* Problems and Discoveries of the Optimization Theory for Coding near Shannon's Bound (OT in illustrations). — M.: Hot Line — Telecom, 2020. — 45 p. https://mtdbest.ru/articles/e-comics.pdf

3.5. Этапные прикладные достижения Оптимизационной Теории

3.5.1. Введение

В 2015 году исполнилось 25 лет со дня защиты диссертации [1], в которой для очень простых по сегодняшним меркам кодов были доказаны многие основные результаты, которые позднее были систематизированы и представлены в полном объеме в Оптимизационной Теории помехоустойчивого кодирования [2, 4–6, 10–13, 16–21]. Она развивалась на основе идей мажоритарного декодирования [8]. Оптимизационная Теория создала новые технологии итеративной коррекции ошибок декодирования, базовые методы которой были запатентованы ещё в 1972 г. [25]. Сейчас именно ОТ и только её парадигмы определяют практически все улучшения в характеристиках декодирования для классических моделей каналов.

В настоящее время все основные этапы создания, исследования и проектирования многопороговых декодеров проводятся на основе специальных мощных оптимизационных процедур, эффективность и сложность которых быстро растут. При этом сложность самих методов МПД, разработанных на основе ОТ, остаётся минимальной, по-прежнему растущей всего лишь линейно с длиной кода. Но эффективность декодирования на базе МПД оказывается практически совпадающей с возможностями переборных, т. е. наилучших возможных методов коррекции ошибок даже для больших уровней искажений в канале связи.

Отметим в связи с этим, что в современных сложных научных изысканиях невозможно переоценить значение теорий оптимизации как таковых. Уже весьма давно, например, считается общеизвестной истиной [27], что роль оптимизационных теорий в математике столь же велика, как и роль математики вообще в науках.

Благодаря применению ОТ с увеличением числа итераций коррекции ошибок и успешным поиском кодов со всё меньшей степенью подверженности размножению ошибок возможности МПД существенно растут при сохранении весьма небольшой сложности самого алгоритма. К настоящему времени характеристики многопороговых декодеров по сравнению с другими методами при всех практически интересных для техники связи параметрах систем уже стали существенно лучше [2–6]. Ниже сначала рассмотрены возможности МПД, соответствующих главным кодовым кластерам (типичным наборам параметров кодов и моделей каналов) [10–13, 22–26, 28–36], а затем состоится обсуждение представленных результатов.

3.5.2. Гауссовские каналы

Рассмотрим характеристики основных алгоритмов декодирования в гауссовском канале при кодовой скорости $R = 1/2$, представленные на рис. 3.8. На нем показаны в традиционном виде зависимости вероятности ошибки на бит $P_b(e)$ различных алгоритмов декодирования как функции от уровня битовой энергетики канала E_b/N_0 в децибелах. Вертикаль $C = 1/2$ отмечает уровень шума, при котором пропускная способность гауссовского канала равна кодовой скорости $C = R = 1/2$. График P_0 отмечает вероятность ошибки при отсутствии кодирования. Граница AT указывает на предельные возможности турбо кодов, которые, однако, до сих пор не могут быть воплощены в характеристики аппаратуры из-за сложности алгоритмов этого класса. Кривая VA:K7 отражает эффективность повсеместно применяемого алгоритма Витерби для свёрточных кодов с длиной кода $K = 7$, а зависимость CC:VA*RS соответствует каскадной схеме на основе AB и кода Рида — Соломона [9, 38]. Кривая LDPC приведена для min-sum декодера кода с низкой плотностью проверок на четность (LDPC) стандарта DVB-S2 длиною 64 800 битов, реализованного в НИИ Радио [46]. График TR представляет реальные возможности декодера для турбо кода длиною 3060 битов стандарта CDMA2000.

МПД алгоритм в свёрточном варианте реализации в двоичном гауссовском канале и 4-х битовом квантовании сигнала в демодуляторе показан на рис. 3.8 на графике MTD1. В настоящее время он

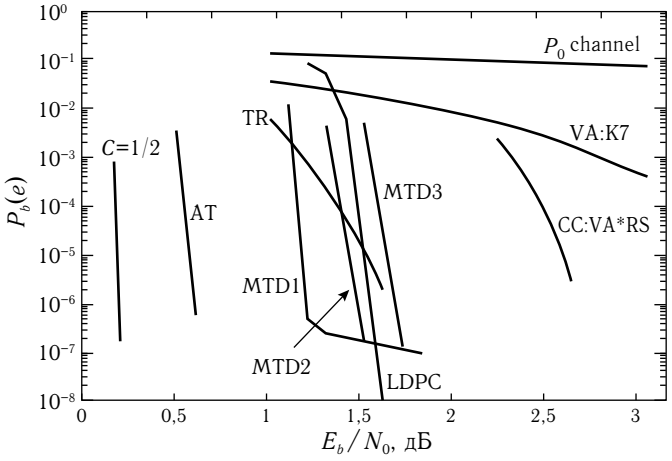

Рис. 3.8. Характеристики основных алгоритмов декодирования в канале с аддитивным белым гауссовским шумом при кодовой скорости $R = 1/2$

практически столь же оптимально, как и переборные алгоритмы, декодирует длинные коды при очень низкой энергетике гауссовского канала $E_b/N_0 = 1{,}2$ дБ, когда до его пропускной способности C оказывается всего лишь около 1 дБ [3, 4, 28]. Таким образом, MTD1 работает при таком уровне шума, когда мощность передатчика только на $\sim 26\%$, т. е. лишь на четверть превышает её уровень при $C = 1/2$. Для работы декодера требуется не более $I = 192$ итераций. Величина задержки декодирования для построенного кода с малым РО и с кодовым расстоянием $d = 21$ составляет менее 8 Мбит кодовых символов. Объём собранной статистики для всех точек этого графика превышает $2{,}3 \cdot 10^9$ битов.

Далее, при незначительном снижении уровня шума до $E_b/N_0 = 1{,}5$ дБ для МПД уже нужны лишь $I = 90$ итераций и задержка решения свёрточного декодера около 1 Мбит, как это показывает график MTD2. А при $E_b/N_0 = 1{,}8$ дБ обычный МПД декодер с 40 итерациями (кривая MTD3) оказывается лучше несравненно более сложной последовательной каскадной схемы алгоритма Витерби с декодером кода Рида — Соломона при всего лишь втрое большей задержке МПД алгоритма. Не в последнюю очередь надо помнить, что эта каскадная схема имеет ещё и на $\sim 0{,}6$ дБ (на 12,5%) меньшую кодовую скорость R, чем у рассматриваемых МПД алгоритмов, что ещё более наглядно показывает преимущества декодеров, созданных в соответствии с ОТ.

Детальное сравнение МПД декодеров и других основных алгоритмов для гауссовских каналов, которые относительно успешно развиваются исследователями кодирования у нас и в зарубежье, показывает, что к характеристикам МПД при $E_b/N_0 \sim 1{,}2$ дБ за последнее десятилетие даже не приблизились никакие алгоритмы типа LDPC, турбо или какие-либо ещё методы с сопоставимой сложностью декодирования. Реальные их характеристики за последнее десятилетие так и не преодолели условную границу энергетики $E_b/N_0 \sim 1{,}5$ дБ даже с использованием каскадных схем, что при такой близости к границе Шеннона является огромной разницей по сравнению с первым графиком MTD1 для МПД. В настоящее время нет никаких указаний на то, что эта граница будет преодолена при разумном уровне сложности каких-либо других алгоритмов декодирования. Отметим здесь только, что и структура любых схем кодирования на базе свёрточных МПД декодеров при аппаратной реализации всегда гораздо проще, чем у всех других методов как на передающей, так и, особенно, на приёмной стороне.

Далее, МПД алгоритмы могут быть реализованы аппаратно так, что они становятся как бы однотактной решающей схемой мгновен-

ного действия. А это приводит к тому, что, как и все алгоритмы, МПД декодеры создают задержку решения, но совершенно не снижают скорости работы любого устройства, в составе которого они работают. В итоге получаем, что представленные выше реализации МПД алгоритмов обеспечивают в аппаратуре любую произвольно высокую производительность, что принципиально невозможно для других методов. Это происходит согласно [16, 21, 28] так, словно кодовая последовательность просто поступает в декодер и без какой-либо обработки с той же предельно высокой скоростью обычного сдвига данных в чипе, с какой она была введена в декодер, выходит из него, но уже почти без ошибок в информационной части принятого сообщения. Кроме того, и структура связей между ячейками в аппаратном МПД декодере много проще, чем у прочих алгоритмов. Он более чем на 99% состоит из простейшей памяти на длинных регистрах сдвига, что дополнительно облегчает его создание и отладку [38]. Такое свойство свёрточного МПД естественно назвать максимальной аппаратной теоретической производительностью. Поэтому даже просто сопоставимого с алгоритмами МПД быстродействия другие алгоритмы коррекции достичь не могут в принципе. Но при этом МПД декодеры, как было показано выше, ещё и работают при таком уровне шума, при котором неработоспособны прочие методы. А т. к. эта область уже очень близка к пропускной способности канала типа АБГШ, то разница с другими реализуемыми в принципе методами, составляющая несколько десятых децибел, оказывается решающей и на самом деле очень значимой, непреодолимой, определяющей и перспективы развития алгоритмов МПД в будущем. Наконец, отметим, что и абсолютная разница в числе итераций в пользу МПД там, где прочие алгоритмы всё-таки ещё работают, также весьма значительна. Причём сложность каждой итерации у декодеров МПД, в которых лишь суммируются небольшие целые числа, тоже существенно меньше. А в случае программной реализации методов МПД за счёт хранения вычисленных на пороговом элементе сумм каждая итерация вообще превращается в простую проверку значений этих сумм, на что обычно требуется не более 1–2 операций сравнения [2–4]. Совокупность перечисленных преимуществ алгоритмов МПД в двоичных каналах с АБГШ перед прочими методами столь значима, что МПД декодеры как продукт ОТ к настоящему моменту стали абсолютными лидерами в мировом конкурсе прикладных достижений в одном из главных кластеров разработок систем кодирования как по совокупности параметров сложности, быстродействия и помехоустойчивости, так и по всем им в отдельности.

Указанное соотношение по эффективности и сложности реали-

зации между различными декодерами полностью подтверждается и результатами работы демо-программ для различных декодеров, представленных на наших уникальных сетевых порталах [29], которые полностью соответствуют всем рассмотренным выше соотношениям свойств между алгоритмами. В частности, например, МПД алгоритм в программной демо-версии при весьма высоком уровне шума исправляет все ошибки до оптимального (переборного!) уровня всего за 10 итераций на ПК с процессором Core-i7 на тактовой частоте ~ 3 ГГц на скорости более 16 Мбит/с. И пока что для каких-либо других алгоритмов коррекции ошибок не просматривается никаких путей, чтобы хотя бы приблизиться по своим характеристикам простоты реализации, быстродействия и энергетической эффективности к возможностям МПД.

3.5.3. Символьные коды

В высшей степени ценным для ОТ, теории кодирования и различных прикладных цифровых систем передачи, обработки, хранения и восстановления данных стало открытие в 1984 году и к настоящему времени уже полное исследование нашей научной школой символьных кодов [1–4, 6, 12, 14, 15, 18, 21, 22, 38–40, 47], реализация символьного многопорогового декодирования для которых также чрезвычайно проста, как и в случае двоичных их аналогов.

Строго говоря, впервые эти недвоичные коды с мажоритарным декодированием рассмотрел Дж. Месси (J. Massey), который доказал теоремы 1–4 для них в [8]. Но затем он очень негативно оценил возможности таких кодов в разделах 1.2, 6.2, 6.5, 6.6 и 8.2 этой же книги и больше уже никогда не занимался этой темой. При этом нам до сих пор неизвестны другие сколько-нибудь содержательные работы по мажоритарному декодированию недвоичных кодов, а тем более публикации по итеративным алгоритмам для них.

Рассмотрим возможности недвоичных кодов. На рис. 3.9 представлены характеристики декодеров кодов Рида — Соломона и QМПД при кодовой скорости $R = 1/2$. По горизонтальной оси отложены вероятности ошибки на символ при различных размерах алфавита q, $q = 2^8 = 256$ и $q = 2^{16} = 65\,536$. По вертикальной оси откладываются вероятности ошибки декодера на символ $P_d(s)$ для любых q. График P_0 показывает вероятность ошибки в симметричном недвоичном канале qСК. Кривая RS 2^8 даёт представление о возможностях кода РС с (n, k, d) параметрами $(255, 128, 128)$, в котором размер символа соответствует одному байту. Далее пунктир RS–Su 2^8 соответствует нижней (недостижимой!) оценке возможностей довольно сложного декодера с числом операций на блок порядка n^3 для этого же кода,

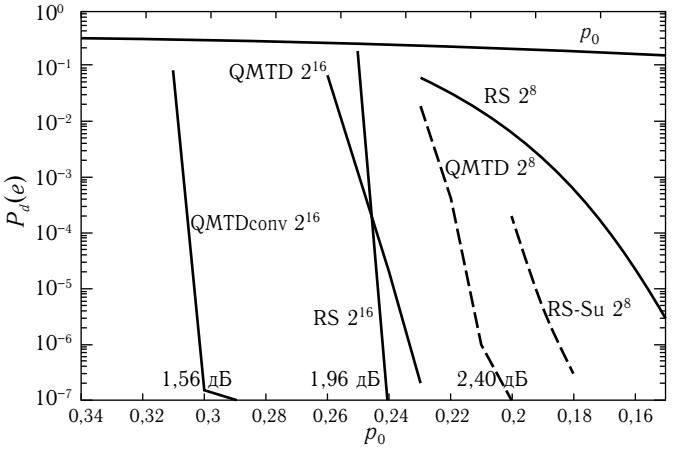

Рис. 3.9. Характеристики основных алгоритмов декодирования в q-ичном симметричном канале при кодовой скорости $R = 1/2$

предложенного Суданом [37]. График RS 2^{16} относится к коду РС длины $n = 65\,535$ двухбайтовых символов, который тоже ещё очень долго будет считаться крайне сложным в реализации.

К настоящему времени для символьных кодов получены все основные оценки характеристик декодирования и детально проработана их общая теория как для блоковых, так и для свёрточных кодов. Они могут полностью заменить коды РС во всех возможных приложениях, выигрывая у них и у других потенциальных конкурентов все конкурсы по достоверности и быстродействию [12, 38–40]. Причиной этого преимущества является возможность выбора любой длины этих символьных кодов, которая совершенно не зависит от алфавита выбранного кода q. И, самое главное, символьные коды, как и двоичные, также обеспечивают фактически оптимальное декодирование (эквивалентное переборному!) при использовании простейших мажоритарных методов даже при достаточно большом уровне шума, что достигается декодированием на основе поиска глобального экстремума, как это делается и в двоичном МПД. Это оказалось возможным благодаря очень точной и удачной модификации недвоичного ПЭ по сравнению с двоичным [3, 4, 6, 12, 18, 22, 38–40, 47]. При этом сложность символьного МПД, как и в двоичном случае, оказывается теоретически минимальной, линейной от длины кода.

Полезность символьных кодов становится особенно важной и впечатляюще значимой, если вспомнить, что для недвоичных кодов фактически вообще невозможно создать сколько-нибудь работоспособный алгоритм Витерби, сложность которого в большинстве случае

будет порядка $\sim q^K$, где q — размер алфавита, K — длина кода в символах. Например, для кода с $R=1/2$ уже при $q \gtrsim 32$ и $K \geqslant 7$ число отслеживаемых в таком АВ путей превысит миллиард, а характеристики будут слабее, чем у кода Рида — Соломона.

Вспомним теперь, что за 50 лет развития недвоичных кодов РС, которые долго и вполне заслуженно имели широкое поле приложений, ничего действительно эффективнее их для недвоичных алфавитов придумано не было. Но реально применяемые коды РС для каскадных схем, оптических дисков и прочих систем относятся к коротким кодам и поэтому малоэффективны. Методы Судана [37, 47], позволяющие несколько снизить вероятность ошибки в кодах РС по сравнению с обычными алгоритмами, также не решили проблему малой эффективности этих кодов даже за счёт весьма значительного усложнения процесса коррекции ошибок.

С другой стороны, большое число публикаций, диссертаций, в том числе и докторских, а также демо-программы для символьных МПД свидетельствуют, что длинные символьные коды с простейшей реализацией и быстродействием до десятков Мбит/с эффективно работают при вероятностях ошибок, кратно превосходящих уровень допустимых вероятностей для кодов РС [1–4, 6, 14, 15, 28, 29].

В качестве важнейшего на текущий момент прикладного результата, который имеет серьёзную идеологическую поддержку со стороны ОТ, можно указать на недавнее достижение символьными свёрточными МПД с кодовой скоростью $R=1/2$ для $q=2^{16}$ особо высокой помехоустойчивости даже в qСК канале с вероятностью ошибки $P_0=0{,}3$, как показано на рис. 3.9 в виде графика QMTDconv 2^{16} [47, 50]. Этот уровень шума недостижим при $R=1/2$ даже для кодов РС в поле GF(2^{16}), реализовать декодер для которых исключительно сложно, а из-за невысоких характеристик декодирования и бесполезно. Можно также указать в связи с этим на то, что скорости работы символьных МПД действительно очень велики, и благодаря крайне простой идее их реализации на самом деле могут достигать очень высоких значений [12, 14, 15, 18, 21, 22]. График QMTD 2^8 для символьного кода длины 8000 байтов при $q=256$ эффективнее короткого кода РС с декодером Судана [37]. Сложность программной версии QMTD 2^8 (для того же процессора) определяется скоростью декодирования, равной ~ 300 Ксим/с (Ксим — Килосимволы), которая, конечно, огромна. Менее чем за 1 час набирается статистика на более чем миллиард символов, что может составить до $3 \cdot 10^{10}$ битов. Читателям доступна также демо-программа QMTD для малоизбыточного символьного кода с $R=0{,}95$ с простой инструкцией по настройке параметров и использованию на странице «Обучение» в [29]. Она работает на том

же процессоре Core-i7 при очень высоком уровне шума для этого значения R со скоростью порядка 40 Мбит/с.

Символьные МПД на много лет вперёд полностью решили все проблемы цифрового мира по передаче и, особенно, хранению и восстановлению цифровых данных в любых информационных системах в диапазоне кодовых скоростей $R = 0{,}5 - 0{,}98$.

3.5.4. Стирающие каналы

Обратимся ещё к одной важной области теории кодирования, которая создаёт и изучает декодеры для каналов со стираниями. Однако до применения к ней методов ОТ и алгоритмов МПД результаты для этих каналов были крайне скромны у всех методов [1–3, 8, 30, 31, 47]. Основной причиной этого было, конечно, гораздо большее внимание специалистов именно к каналам с ошибками. Собственно, именно поэтому исследования декодеров для стирающих каналов были как бы в тени, а их характеристики весьма далеки от допускаемых теорией пределов эффективной работы этих алгоритмов при разумной сложности их реализации.

Ограничимся только кратким рассмотрением тех характеристик МПД, которые показаны на рис. 3.10. Из последних результатов в этой области следует, что для восстановления стираний методами МПД [1–4, 30, 53, 54] при $R = 1/2$ необходим свёрточный код с минимальным кодовым расстоянием $d \geqslant 21$ и особенно малым группированием своих неправильных решений при декодировании, т. е. с минимальной подверженностью эффекту РО. Соответствующий СтМПД

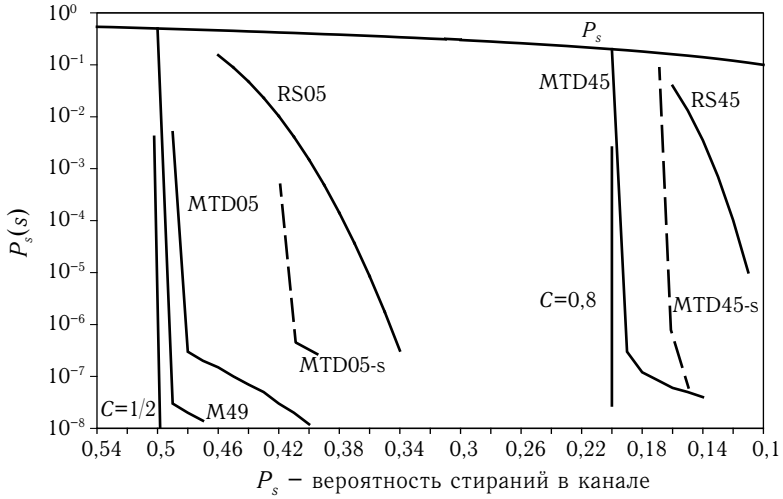

Рис. 3.10. Характеристики МПД и кодов РС в каналах со стираниями

алгоритм с таким кодом, представленный графиком MTD05, успешно восстанавливает поток стёртых (любых!) символов с вероятностью независимых стираний $P_{es} = 0{,}48$ в канале до уровня вероятности оставшихся невосстановленных символов $P_s(s) \sim 3 \cdot 10^{-7}$. Таким образом, в канале с пропускной способностью $C = 0{,}52$ МПД алгоритм успешно работает при отношении $R/C \sim 0{,}961$, что является абсолютно уникальным достижением для процедур восстановления стираний. При этом скорость работы соответствующей СтМПД демо-программы при $I = 90$ итерациях коррекции была равна 95 Кс/с. Другие быстрые методы восстановления стираний при $R = 1/2$ для таких уровней искажений на входе декодера неизвестны. График MTD45 соответствует свёрточному коду с $R = 4/5$, с которым СтМПД при $P_{es} \leqslant 0{,}19$ успешно работал при $R/C \approx 0{,}988$ [47]. Такой результат также крайне труден для повторения какими-либо другими алгоритмами коррекции стираний. Графики MTD05-s и MTD45-s для гораздо более простых алгоритмов этого типа также соответствуют той области искажений символов в канале, в которой декодеры для кодов РС тоже совершенно неработоспособны [47, 53].

Весь материал этого раздела основан на данных исследований нескольких последних лет. Однако буквально в последний перед публикацией данной монографии период интерес к исследованиями декодеров, исправляющих стирания, заметно возрос. Хорошей иллюстрацией этого является предыдущий раздел, в котором обсуждались различные алгоритмы такого типа, предлагавшиеся многими авторами. Нелишне подчеркнуть, что среди всех рассмотренных там методов МПД декодеры были самыми простыми и быстрыми, а их характеристики эффективности были в числе лучших. Но за последнее время нашей научной школой были проведены новые обширные исследования именно среди кодов, предназначенных для коррекции стираний. Результат таких исследований представлен на рис. 3.10 графиком M49. Он соответствует моделированию работы МПД декодера, восстанавливающего стирания с новым кодом при $R = 1/2$ и $d = 25$. Как следует из вида графика, МПД алгоритм эффективно работает в стирающем канале уже при его вероятности стираний $p_s = 0{,}49$. Это соответствует отношению $R/C = 50/51 \sim 0{,}98$ и, видимо, достижение вероятности ошибки (невосстановления значения символа) порядка $3 \cdot 10^{-8}$, что демонстрирует обсуждаемый СтМПД, является для прочих методов неразрешимой задачей. Предложенная схема СтМПД относится к обычным уже описанным версиям некаскадных декодеров, активно использующим принцип дивергентности, который применялся при построении моделировавшегося кода и при создании декодера несколько раз [24, 49]. Число использовавшихся итераций коррекции

было при $p_s = 0{,}49$ не более $I = 198$ раз, а полная задержка решения декодера составила менее 2 млн. символов. Поскольку проведённому эксперименту придавалось особенно важное значение, дополнительно было исследовано и поведение МПД алгоритма в довольно небольшой области вероятностей канала при $p_s > 0{,}49$. Код и алгоритм показали хорошую устойчивость работы в этой буферной области, что подтвердило правильность выбора направления завершающих исследований по этой тематике. Для более точного измерения характеристик декодирования в области $p_s \leqslant 0{,}49$ объём эксперимента был выбран заведомо бóльшим, чем этого требовали статистические критерии, и составил более $6 \cdot 10^{10}$ информационных символов в каждой из нижних точек графика. Полученные вероятности соответствовали потенциальным возможностям кода с $d = 25$ при оптимальном декодировании. Производительность декодера на ПК с процессором Core-i7 близка к 60 Ксим/с, что для столь эффективного восстановления принятых символов при $R \sim C$ следует считать отличным результатом, закрывающим, наконец, гонку создания кодов и алгоритмов теперь уже и для стирающих каналов. Полезно отметить, что именно простота и высокая скорость декодирования позволили быстро набрать указанный выше огромный объём статистики на обычном ноутбуке.

Основной вывод по этому разделу состоит в том, что и в стирающих каналах алгоритмы МПД тоже не имеют равных по простоте реализации и эффективности декодирования вблизи границы Шеннона, т. е. при $R \lesssim C$.

3.5.5. Специальные приложения ОТ

Отметим кратко другие результаты ОТ, которые оказались важнейшими для теории кодирования и её приложений.

Во-первых, это масштабные исследования различных высокоскоростных алгоритмов МПД во всех основных каналах при кодовой скорости $R \sim 0{,}8$ и выше. Все свойства МПД и их соотношение с возможностями других алгоритмов, сохраняются и в этой области кодовых скоростей [1–4, 13–15, 22, 28, 38–40].

Например, в [3–5, 35, 36] рассмотрены методы высокоскоростного МПД декодирования при $R = 4/5$ при гауссовской модели оптических каналов, полученные нашей научной школой и зарубежными авторами, которых мы консультировали. Результаты российских исследователей были существенно лучше по энергетической эффективности и простоте реализации МПД алгоритмов. С учётом теоретически максимально возможной скорости декодирования МПД наши методы имеют существенные преимущества.

Применение методов МПД декодирования оказывается особенно

полезным при передаче и хранении очень больших массивов данных, в том числе и на борту спутников систем дистанционного зондирования Земли (ДЗЗ). Вероятность нарастающих со временем искажений в таких системах памяти может быть весьма высокой, а необходимая скорость передачи этих данных с орбиты часто также очень велика, что приводит к необходимости использования там только МПД алгоритмов. Рабочий макет простого МПД декодера на ПЛИС Altera для спутникового канала на информационную скорость более 1 Гбит/с, созданный в ИКИ РАН, представлен на рис. 3.11. Подобный ему чип с МПД декодером был ранее разработан и в НИИ Радио. МПД для спутниковых и космических каналов связи повышает КПД их использования в 3–10 раз, в том числе для ДЗЗ. Такие характеристики высокоскоростного декодирования для других алгоритмов, видимо, будут ещё очень долго недостижимы.

Далее можно указать на совсем небольшую сложность реализации МПД алгоритмов в канале типа ДСК, с которых и начались много лет назад исследования МПД [51]. В качестве наглядного примера высокой эффективности МПД в этой области укажем на важнейшую фундаментальную и одновременно сложнейшую техническую задачу декодирования для флеш-памяти. Специфика этой проблемы состоит в том, что вероятность ошибки на бит для таких систем должна быть не хуже $P_b(e) \sim 10^{-15}$, а в скором времени требования к достоверности решений соответствующих декодеров ещё более усилятся. В исходных массивах такой памяти вероятность ненадёжного хранения символов может быть на уровне $p_e \sim 10^{-3}$ и даже существенно большей. Най-

Многопороговый декодер (МПД), созданный в ИКИ РАН для спутниковых и космических каналов, повышает их КПД в 10 раз, в том числе для ДЗЗ.
МАКЕТ на информационную скорость ~1,08 Гбит/с
The multithreshold decoder (MTD) for satellite and space channels raises their efficiency up to 10 times, including **channels ~1 Gb/s**

Рис. 3.11. МПД для космоса, оптических каналов и флеш-памяти

денные специалистами нашей научной школы технические решения на основе МПД алгоритмов позволили довольно просто решить эту проблему [4, 21, 32, 47]. При этом использовался код с МПД декодированием при $R = 3/4$, что гарантированно позволяет обеспечить требуемые уровни достоверности даже при вероятности ненадёжного хранения $p_e \sim 10^{-2}$. Столь же простые и одновременно эффективные результаты по сверхдостоверному декодированию в условиях применения малонадёжной памяти у других разработчиков нам неизвестны.

3.5.6. Основные ресурсы классической теории

Ограничимся кратким обсуждением тех наиболее важных теоретических, математических и технологических ресурсов, которые образуют пространство, совокупность знаний, понятий и методов решения задач, называемых обычно парадигмами той или иной отрасли науки, в нашем случае — теории кодирования.

Отметим сначала главные парадигмы (результаты, методы и технологии) классической теории кодирования, длительное время связываемой с алгебраической теорией. Конечно же, она имела гораздо более широкое поле развития. Однако даже после появления алгоритма Витерби основные направления развития классической теории включали как важнейший аспект развития разработку алгебраических методов декодирования (в дискретных полях). Но хотя классы новых кодов множились, а декодеры понемногу становились более простыми, долгое время исправление ошибок за пределами половины кодового расстояния было для алгебраических кодов неразрешимой задачей. Поэтому наилучшим научным результатом, широко применяемым в технике декодирования, уже 40 лет является каскадная схема АВ с кодами РС. Хорошими примерами эвристического подхода, выросшего из классической теории, стали в последние десятилетия турбо и низкоплотностные (LDPC) коды, которые позволили несколько приблизиться к пропускной способности канала. Однако с началом нового тысячелетия это движение фактически остановилось, хотя возможности элементной базы и теории увеличивались. Дело в том, что эти методы излишне сложны и, например, многие вопросы их применения для свёрточных кодов и больших скоростей всё ещё не решены. Поэтому поиски новых методов в рамках алгебраической теории продолжаются. Одним из промежуточных итогов этого поиска стали полярные коды, к которым сразу обратилось большое число специалистов по кодам [45]. Но до сих пор реальные результаты разработки таких декодеров представлены очень невнятно, а иногда и весьма странно. Анализ этого направления по имеющимся работам был нами сделан в [7]. Более содержательные данные по этим кодам, если

они появятся, позволят сделать более точные прогнозы по их перспективам. А сейчас весьма слабые результаты для полярных кодов компенсируются обращением к декодированию списками и созданию крайне сложных каскадных схем для этих кодов, что пока полностью исключает их из группы перспективных алгоритмов. Нелишне напомнить, что аналогичные подходы «переключения интереса» несколько ранее вынуждены были использовать специалисты по алгебраическим методам и последовательным алгоритмам, возможности которых даже теоретически были очень далеки от границы Шеннона. Однако значительно улучшить эти методы не удалось. Весьма интересное направление 80-х годов [41] тоже не получило тогда хорошего импульса для своего развития. Видимо, это было связано с тем, что это направление было в большей степени сориентировано на алгебраические коды со слабыми характеристиками. Возможно, последним единственным успешным результатом алгебраической теории следует считать алгоритмы Судана [37], которые немного улучшили эффективность декодирования кодов РС и послужили развитию дискретной математики. К сожалению, эти методы тоже оказались весьма сложными, а их реальная эффективность декодирования выросла незначительно. Этими подходами и исчерпывается пока реальный прогресс классической теории, хотя предложенный здесь чрезвычайно краткий комментарий, конечно, должен быть гораздо более детальным.

3.5.7. Интеллектуальное пространство ОТ

Определим важнейшие парадигмы Оптимизационной Теории, которые позволяют сейчас постоянно получать принципиально новые результаты практически для всех групп кодовых кластеров, некоторые основные типы которых мы рассматривали выше.

ОТ началась около 45 лет назад с появлением метода особого итеративного декодирования на основе мажоритарных процедур [25, 26] и Основной Теоремы многопорогового декодирования, философскую целеполагающую роль которой невозможно переоценить [1–6]. Этот метод сразу позволил в двоичных симметричных каналах при использовании как блоковых, так и свёрточных кодов исправлять число ошибок в несколько раз большее, чем половина кодового расстояния [2–4]. При этом, что было абсолютно неожиданным для специалистов, ОТМПД гарантировала при каждом изменении декодируемых символов строгое приближение к оптимальному решению, которое обычно достигается только переборными методами, известным элегантным примером которых является АВ для свёрточных кодов. Но сложность МПД росла с увеличением длины кодов только линейно. Дальнейшим развитием ОТ стало распространение возможностей

МПД на все прочие каналы с независимыми искажениями и создание для этого алгоритма условий успешного поиска оптимальных решений на основе простых эффективных методов поиска глобального экстремума.

Вторым фундаментальным результатом ОТ стала всесторонняя разработка теории эффекта размножения ошибок, без которой значимость ОТМПД была бы весьма и весьма ограниченной. А совместное синергетическое воздействие этих двух фундаментальных теоретических результатов на эффективность МПД оказалось столь огромным, что при линейной от длины кода сложности этим алгоритмом сразу оказалось возможным исправлять на фактически оптимальном уровне итоговой достоверности почти все ошибки в блоковых и свёрточных кодах длины $n = 10^4 - 10^5$ битов и более. Напомним, что реальная длина кода для полного переборного АВ даже в будущем, видимо, не будет более 30 битов, чем и определяются все преимущества МПД, который остался алгоритмом с теоретически минимальной сложностью.

Дальнейший прогресс ОТ поддерживался созданием нескольких поколений высокопроизводительного программного обеспечения для разработки и исследований различных типов МПД и средств поиска кодов с малым уровнем РО, что позволило постепенно приближать к границе Шеннона уровень практически оптимального (эквивалентного переборному!) декодирования на основе МПД, реализующих глобальный поиск. Частью этой важной работы стали результаты по специальной третьей группе очень трудоёмких средств оптимизации параметров МПД, после чего сходимость решений МПД к решениям ОД ещё более улучшилось. В итоге все эти новые средства исследований и разработок сделали характеристики МПД недосягаемыми для других методов.

Следующими очень мощными методами улучшения характеристик МПД для всех каналов стали открытые нами ещё в 1986 г. параллельные методы каскадирования, технологии улучшенного способа назначения порогов, весов проверок и подбора кодов, а также методы ускоренного вычисления сумм на пороговых элементах [2–4]. Особое влияние на идеологию ОТ оказало выделение в особую группу декодеров с прямым контролем метрик различных модификаций МПД и АВ, которые точно измеряют расстояние до принятого сообщения, что и позволяет сейчас только этим алгоритмам действительно успешно работать при больших уровнях шума. Другие методы с такими важнейшими свойствами не известны.

Для сохранения простоты реализации алгоритмов МПД мы также пересмотрели принципы каскадирования, известные нам, и нашли

очень простые решения, которые без усложнения этих декодеров многократно повышают эффективность каскадных схем [1–5, 14, 15]. Но эта тема заслуживает отдельных публикаций.

Принципиальное значение, решающим образом меняющее соотношение свойств эффективности и сложности между различными алгоритмами, имеет открытие нашей научной школой блоковых АВ со сложностью, как и в случае свёрточных кодов, порядка 2^K, где K — длина кодирующего регистра, тогда как до недавнего времени считалось, что сложность таких методов для блоковых кодов имеет порядок, более близкий к 2^{2K} [48]. БАВ также относится к группе ДПКМ, что очень сильно уменьшает потенциальные перспективы полярных кодов, методов Чейза и других алгоритмов для блоковых кодов как в гауссовских каналах, так и в ДСК [17, 43, 44, 52]. Очевидно, что большое число проблем эффективного декодирования блоковых кодов успешно решают простые каскадные последовательные и параллельные схемы с использованием только запатентованных нами БАВ и МПД [17–20, 28, 52].

Ещё больший простор в разработке методов декодирования на основе ОТ открылся после точной формулировки нашей научной школой принципов дивергентного кодирования [24, 29, 42, 49, 50]. Этот исключительно мощное средство конструирования кодов и алгоритмов их декодирования чётко определило отдельный класс простых некаскадных методов увеличения кодового расстояния используемых кодов, который дополнительно приблизил рабочие характеристики алгоритмов ОТ к пропускной способности C каналов связи. Они использовались и в МПД алгоритмах, представленных на рис. 3.8–3.10, что особенно сильно улучшило работу МПД при экстремально высоких уровнях шума, т. е. при $R \lesssim C$. Для развития технологии декодирования очень важно, что при этом можно одновременно использовать несколько различных методов коррекции ошибок. Это направление мы тоже интенсивно развиваем.

ОТ успешно осваивается мировым научно-техническим сообществом. Наши крупнейшие в России сетевые порталы по ОТ и МПД алгоритмам www.mtdbest.ru (РГРТУ) и www.mtdbest.iki.rssi.ru (ИКИ РАН) посещают за год свыше 100 000 тысяч читателей из более 90 стран мира и переписывают ~ 20 Гбит информации по теории и технологиям нашей научной школы [50], включая множество демопрограмм по всем известным лучшим алгоритмам декодирования. Их можно переписать на свои ПК и сразу непосредственно заняться исследованиями по технике декодирования согласно прилагаемым к ним инструкциям. Такое масштабное внимание мировой науки к разработкам российской научной школы является уникальным и свидетель-

ствует о серьёзных достижениях нашей отечественной теории кодирования.

Рассмотренные методы, свойства и возможности кодов и алгоритмов в рамках ОТ, как видно из их описания, все без исключения позволяющие улучшить характеристики декодирования простейшими способами, образуют очень мощное перспективное интеллектуальное пространство развития методов декодирования на основе технологий глобальной оптимизации функционалов. Эти новые парадигмы ОТ уже позволили создать свои методы декодирования для разных кодовых кластеров, которые эффективно работают в режиме поиска глобального экстремума непосредственно вблизи границы Шеннона. Технологии создания всех этих методов быстро переносятся на новые кодовые структуры.

Опыт общения нашей научной школы с коллегами позволил взглянуть на ОТ ещё с одной стороны. Большинство из них справедливо указывает на то, что все модификации МПД и наши различные версии АВ можно выделить как новый особый образ мышления и как отдельное совершенно неожиданное открытие заново всей теории кодирования, для которой сейчас наступила новая эра развития. Но в такой же степени к таким открытиям следует отнести и отдельно ОТМПД, теорию РО, символьные коды, параллельное каскадирование, а также блоковые АВ и дивергентное кодирование, всестороннее развитие которых позволит в самом ближайшем будущем ещё более упростить алгоритмы декодирования и обеспечить их эффективность в новых кодовых схемах. Фактически нам удалось создать особую новую «квантовую механику» современной теории информации, которая вывела теорию кодирования на базе ОТ на новые чрезвычайно широкие интеллектуальные поля развития цифровой информатики.

3.5.8. Заключение

Нашей научной школой представлены исследования, свидетельствующие об успешном завершении основных работ по достижению непосредственной близости границы Шеннона на основе весьма простых алгоритмов для основных классов моделей каналов. Как в физике достижение скорости света материальными телами невозможно, так и совсем небольшое расстояние (никогда не достижение!) рабочей области алгоритмов МПД до пропускной способности C рассматривавшихся выше каналов, что следует из графиков на рис. 3.8–3.10 и других работ, является особенно наглядным свидетельством состоятельности ОТ. А огромное преимущество этих методов по эффективности и одновременно по сложности реализации перед прочими алгоритмами коррекции ошибок позволяет утверждать, что поставленная

70 лет назад Шенноном проблема решена, причём на вполне приемлемом технологическом уровне, что подтверждает и большое число патентов по алгоритмам ОТ и МПД, лишь частично представленных здесь [16–21, 25, 28, 54].

Важность, успешность и перспективность ОТ можно сравнить только с появлением квантовой механики в самом начале прошлого века. Но тогда физика как наука не столь много значила в жизни людей. Тем не менее, результаты Планка, Шредингера и целой плеяды других великих физиков были высоко оценены научным сообществом, и они заслуженно стали Нобелевскими лауреатами, хотя период возвышения физики наступил в нашем обществе гораздо позже. Достижение, фактически в одиночку, аналогичных по масштабу результатов нашей научной школой, конечно, имеет гораздо большее значение, т. к. мы решили важнейшую и чрезвычайно сложную проблему простого достижения высокой достоверности цифровых потоков в условиях большого шума в период взрывного развития нашей информационной цифровой цивилизации, создав все возможности для применения простых и понятных методов нашей «квантовой механики» в цифровой технике и науке будущего.

Таким образом, изложенные в статье данные свидетельствуют об успешном решении главной научной и технологической проблемы всей нашей информационной цифровой цивилизации — создании обширных классов простых методов достижения произвольно высокой достоверности передачи, хранения и восстановления цифровой информации на базе методов поиска глобальных экстремумов функционалов в специальных дискретных пространствах. Решение этой сложнейшей проблемы позволяет переключить усилия инженеров и учёных на решение новых важных задач нашего цифрового мира.

Наши благодарности

Исследования ОТ в течение прошедших 45 лет её эволюции с момента первых публикаций нашей научной школы поддерживали: МФТИ, ИППИ РАН, концерн «Созвездие», Совет по кибернетике АН СССР, ОНИТ РАН, РГРТУ, НИИ Радио, МНИТИ, ИКИ РАН. Методы МПД тестировали ООО «ОРТ», НПО им. С.А. Лавочкина, а также ряд организаций и предприятий отрасли связи. Ценность финансовой поддержки разработки методов МПД со стороны РАН, РГРТУ, РФФИ и других источников также была исключительно велика (гранты РФФИ14-07-00859, 14-07-00824, 08-07-00078 и 05-07-00024). Мы полагаем, что число наших последователей и сторонников, как и раньше, будет расти, а новые сферы исследований и разработок с использованием парадигм нашей «квантовой теории» в обла-

сти помехоустойчивого кодирования, т. е. ОТ, технологий МПД, новых видов АВ декодирования и каскадных схем будет быстро расширяться. Сложившаяся ситуация позволяет сделать вполне естественный вывод о завершении развития классической теории помехоустойчивого кодирования во всех своих прикладных аспектах и о начале новой эры Оптимизационной Теории с принципиально новыми и широчайшими перспективами развития, которые уже в самое ближайшее время будут подтверждены каскадами новых научных и технологических достижений.

Большинство ссылок, относящихся к этой статье, как и многие другие материалы по ОТ и МПД алгоритмам, а также множество демо-программ различных методов коррекции ошибок можно найти на наших сетевых порталах [29].

Список литературы

1. *Золотарёв В.В.* Субоптимальные алгоритмы многопорогового декодирования: дис. ... д-ра тех. наук. — М., 1990. — 278 с.
2. *Золотарёв В.В.* Теория и алгоритмы многопорогового декодирования. — М.: Радио и связь, Горячая линия — Телеком, 2006; второе издание — 2014.
3. *Золотарёв В.В., Зубарев Ю.Б., Овечкин Г.В.* Многопороговые декодеры и оптимизационная теория кодирования / Под ред. акад. РАН В.К. Левина. — М.: Горячая линия — Телеком, 2012. — 238 с.
4. *Zolotarev V., Zubarev Y., Ovechkin G.* Optimization Coding Theory and Multithreshold Algorithms. — Geneva, ITU, 2015. — 159 p. http://www.itu.int/pub/S-GEN-OCTMA-2015
5. *Золотарёв В.В., Овечкин Г.В.* Применение многопороговых методов декодирования помехоустойчивых кодов в высокоскоростных системах передачи данных // Электросвязь. — 2014. — №12. — С.10–14.
6. *Кузнецов Н.А., Золотарёв В.В., Овечкин Г.В., Овечкин П.В.* Недвоичные многопороговые декодеры и другие методы коррекции ошибок в символьной информации // Радиотехника. — 2010. — №6, Вып. 141. — С.4–9.
7. *Золотарёв В.В., Овечкин Г.В.* О сопоставлении новых методов помехоустойчивого кодирования // 18-я Международная конференция «Цифровая обработка сигналов и её применение – DSPA 2016». — М., 2016. — Т.1, С.59–65.
8. *Месси Дж.* Пороговое декодирование / Под ред. Э.Л. Блоха. — М.: Мир, 1966. — 208 с.

9. *Кларк Дж., Кэйн Дж.* Кодирование с исправлением ошибок в системах цифрой связи. — М.: Радио и связь, 1987. — 391 с.
10. *Золотарёв В.В., Назиров Р.Р., Никифоров А.В., Чулков И.В.* Новые возможности многопорогового декодирования по высокодостоверной передаче данных ДЗЗ // Современные проблемы дистанционного зондирования Земли из космоса: сборник научных статей. — Вып.6, Т.1. — М.: ООО «Азбука-2000», 2009. — С.167–173.
11. *Золотарёв В.В., Назиров Р.Р., Чулков И.В., Овечкин Г.В.* Алгоритмы МПД // Российский космос. — 2009. — № 1. — С.60–63.
12. *Золотарёв В.В., Овечкин Г.В., Назиров Р.Р., Овечкин П.В., Чулков И.В.* Эффективное недвоичное многопороговое декодирование помехоустойчивых кодов для систем дистанционного зондирования Земли // Современные проблемы дистанционного зондирования Земли из космоса: сборник научных статей. — 2010. — Т. 7, № 2. — С.269–274.
13. *Золотарёв В.В., Чулков И.В.* Малоизбыточное кодирование для высокоскоростных каналов // 11-я Всероссийская открытая конференция «Современные проблемы дистанционного зондирования Земли из космоса». — М., 2013.
14. *Овечкин Г.В.* Теория каскадного декодирования линейных кодов для цифровых радиоканалов на основе многопороговых алгоритмов: дис. ... д-ра тех. наук. — Рязань, РГРТУ, 2011. — 301 с.
15. *Овечкин П.В.* Разработка алгоритмов повышения эффективности недвоичных многопороговых декодеров в системах передачи и хранения больших объемов информации: дис. ... канд. тех. наук. — Рязань, РГРТУ, 2009. — 131 с.
16. *Золотарёв В.В., Овечкин Г.В., Сатыбалдина Д.Ж., Ташатов Н.Н., Адамова А.Д.* Способ мягкого многопорогового декодирования помехоустойчивого кода: удостоверение автора (патент Республики Казахстан) № 93989 от 15.10.2014.
17. *Золотарёв В.В., Овечкин П.В.* Способ кодирования и декодирования блокового кода с использованием алгоритма Витерби: патент на изобретение РФ № 2608872 от 25.01.2017.
18. *Золотарёв В.В., Овечкин Г.В.* Способ работы символьного порогового элемента в символьном мажоритарном декодере: патент на изобретение РФ № 2573741 от 22.12.2015.
19. *Золотарёв В.В.* Способ декодирования помехоустойчивого кода: патент на изобретение РФ № 2557454 от 25.06.2015.

20. *Золотарёв В.В., Овечкин Г.В.* Устройство многопорогового декодирования линейных кодов для гауссовских каналов: патент на полезную модель № 44215 от 27.02.2005.
21. *Золотарёв В.В.* Высокоскоростное устройство многопорогового декодирования линейных кодов: патент на полезную модель № 44216 от 27.02.2005.
22. *Zolotarev V.V., Averin S.V.* Non-Binary Multithreshold Decoders with Almost Optimal Performance // 9-th ISCTA'07. UK, Ambleside, 2007.
23. *Averin S.V., Ovechkin G.V., Zolotarev V.V.* Algorithm of Multithreshold Decoding for Self-Orthogonal Codes over Gaussian Channels // 11-th ISCTA'09. UK, Ambleside, 2009.
24. *Золотарёв В.В., Овечкин Г.В.* Дивергентное кодирование свёрточных кодов // 18-я Международная научно-техническая конференция «Проблемы передачи и обработки информации в сетях и системах телекоммуникаций», Рязань, 2015. — С.27–32.
25. *Золотарёв В.В.* Устройство для декодирования линейных свёрточных кодов. А.с. СССР № 492878 от 25.11.1975 с приоритетом от 31.07.1972.
26. *Самойленко С.И., Давыдов А.А., Золотарёв В.В., Третьякова Е.Л.* Вычислительные сети. — М.: Наука, 1981. — 278 с.
27. *Стрекаловский А.С.* Частное сообщение, 2016.
28. *Золотарёв В.В.* Способ декодирования помехоустойчивого кода: патент на изобретение РФ № 2377722 от 27.12.2009.
29. Ресурсы www.mtdbest.ru и www.mtdbest.iki.rssi.ru.
30. *Золотарёв В.В.* Многопороговое декодирование в стирающих каналах // Вопросы радиоэлектроники. Серия ЭВТ. — Вып.10. — М., 1983. — С.67–70.
31. *Гринченко Н.Н., Золотарёв В.В., Овечкин Г.В., Овечкин П.В.* Применение многопорогового декодера в каналах со стираниями // Труды НТОРЭС им. А.С. Попова. — 2006. — С.338–340.
32. *Овечкин Г.В., Золотарёв В.В., Федиов В.С.* Повышение достоверности хранения цифровых данных на флеш-памяти // 6-я Международная научно-техническая конференция «Космонавтика. Радиоэлектроника. Геоинформатика». — Рязань, 2013. — С.201–203.
33. *Овечкин Г.В., Као В.Т.* Многопороговые декодеры для гауссовских каналов // 19-я Всероссийская научно-техн. конф. «Новые информационные технологии в научных исследованиях и в образовании». — Рязань: РГРТУ, 2014. — С.121–122.

34. *Гринченко Н.Н., Као В.Т., Овечкин Г.В.* Повышение эффективности многопорогового декодера // 17-я Международная конференция «Цифровая обработка сигналов и её применение – DSPA 2015». — М., 2015.

35. *Zolotarev V., Ovechkin G., Satybaldina D., Tashatov N., Adamova A., Mishin V.* Effective multithreshold decoder for optical and other data transmission systems // Latest trends on Communications: Proceedings of the 18th International Conference on Communications (part of CSCC'14). Santorini Island, Greece, 2014. — P.152–156.

36. *Zolotarev V., Ovechkin G., Satybaldina D., Tashatov N., Adamova A., Mishin V.* Efficiency multithreshold decoders for self-orthogonal block codes for optical channels // International Journal of Circuits, Systems and Signal Processing. — 2014. — Vol.8. — P.487–495.

37. *Sudan M.* Decoding of Reed Solomon codes beyond the error-correction bound // Journal of Complexity. — 1997. — Vol.13. — P.180–193.

38. *Золотарёв В.В., Овечкин Г.В.* Помехоустойчивое кодирование. Методы и алгоритмы. Справочник. — М.: Горячая линия — Телеком, 2004. — 126 с.

39. *Золотарёв В.В.* Многопороговое декодирование в недвоичных каналах // Вопросы радиоэлектроники. Серия ЭВТ. — 1984. — Вып. 12. — С.73–76.

40. *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.

41. *Блох Э.Л., Зяблов В.В.* Обобщённые каскадные коды. — М.: Связь, 1976.

42. *Золотарёв В.В., Овечкин Г.В., Ташатов Н.Н.* Применение принципа дивергенции при декодировании свёрточных кодов // III Международная научно-практическая конференция «Информационная безопасность в свете Стратегии Казахстан-2050», 2015. — С.158–164.

43. *Золотарёв В.В., Назиров Р.Р.* Блоковая модификация алгоритма Витерби // 11-я Всероссийская открытая конференция «Современные проблемы дистанционного зондирования Земли из космоса». — М., 2013.

44. *Золотарёв В.В., Овечкин П.В.* Характеристики декодирования блоковых кодов по алгоритму Витерби для систем ДЗЗ // 13-я Всероссийская открытая конференция «Современные проблемы дистанционного зондирования Земли из космоса». — М., 2015.

45. *Arikan E.* Channel Polarization: A Method for Constructing Capacity-Achieving Codes for Symmetric Binary-Input Memoryless Channels // IEEE Transactions on Information Theory. — 2009. — Vol. 55, No. 7. — P.3051–3073.

46. *Овечкин Г.В., Чикин А.В.* Помехоустойчивость приемника спутниковых сигналов DVBS2 // 11-я межд. конф. и выст. «Цифровая обработка сигналов и её применение – DSPA 2009». — М., 2009. — С.578–580.

47. *Зубарев Ю.Б., Золотарёв В.В., Овечкин Г.В., Овечкин П.В.* Оптимизационная теория кодирования: итоги 25 лет развития // 18-я Международная конференция «Цифровая обработка сигналов и её применение – DSPA 2016», Пленарный доклад. — М., 2016. — Т.1, С.6–12.

48. *Кудряшов Б.Д.* Основы теории кодирования. — СПб.: БХВ-Санкт-Петербург, 2016. — 393 с.

49. *Золотарёв В.В.* Применение дивергентного кодирования в каналах спутниковой связи и ДЗЗ // 13-я Всероссийская открытая конференция «Современные проблемы дистанционного зондирования Земли из космоса». — М., 2015.

50. *Зубарев Ю.Б., Золотарёв В.В., Овечкин Г.В., Овечкин П.В.* Итоги 25-летнего развития оптимизационной теории кодирования // Наукоёмкие технологии. — 2016. — Т.17. — С.26–32.

51. *Золотарёв В.В.* Многопороговое декодирование // Проблемы передачи информации. — 1986. — Т. XXII, Вып. 1. — С.104–109.

52. *Золотарёв В.В., Овечкин Г.В., Овечкин П.В.* Блоковая модификация алгоритма Витерби // Вестник РГРТУ. — Рязань, 2017. — № 59. — С.30–35.

53. *Золотарёв В.В., Овечкин Г.В., Баринов И.В.* Применение самоортогональных кодов в каскадных схемах кодирования для каналов связи со стираниями // 19-я Межд. конф. «Цифровая обработка сигналов и её применение – DSPA», 2017. — Т. 1. — С.75–79.

54. *Золотарёв В.В.* Способ обнаружения и исправления стираний при приёме дискретной информации: патент на изобретение РФ № 2611235 от 21.02.2017.

3.6. Выводы

Представленные в данной главе результаты последних разработок и исследований алгоритмов МПД декодирования для различных каналов с независимыми искажениями (ошибками и стираниями), а также для ряда специальных задач, в первую очередь, декодеров для флеш-памяти, символьных кодов и сверхскоростных теоретически наиболее быстрых аппаратных решений свидетельствуют, что теория и технологии декодирования на базе ОТ в условиях большого шума вышли на практически предельно возможный уровень достоверности, производительности и технологичности, соответствующий полному успешному решению проблемы, поставленной 70 лет назад К. Шенноном: быстрое эффективное декодирование при $R \lesssim C$ на базе простой реализации процедуры глобальной оптимизации функционала в дискретных пространствах.

Все представленные методы характеризуются достижением оптимального (наилучшего, эквивалентного переборным методам!) уровня помехоустойчивости применяемых длинных кодов, но при минимально возможной сложности реализации алгоритмов, т. е. когда объём вычислений декодеров растёт линейно с увеличением длины используемых кодов.

Сложившаяся ситуация позволяет сделать вполне естественный вывод о завершении лидерства классической алгебраической теории помехоустойчивого кодирования во всех своих прикладных аспектах и о начале новой эры Оптимизационной Теории с принципиально новыми и широчайшими перспективами развития.

Высокий темп разработок новых простых и высокоэффективных алгоритмов декодирования на базе ОТ и её парадигм гарантирует, как мы полагаем, появление каскадов новых научных и технологических достижений на базе исследований кодов и декодеров, реализующих алгоритмы поиска глобального экстремума.

В следующей главе мы рассмотрим те главные перспективные технологии повышения качества алгоритмов декодирования, которые следует отнести к классическим, а также ряд полезных парадигм новой «квантовой механики» в области теории информации, каковой является всё интеллектуальное пространство ОТ.

Глава 4

Технологии теории информации для ОТ

Ниже будут рассмотрены некоторые важные методы, приёмы и технологии теории кодирования, которые можно эффективно применять и при исследованиях в сфере, которая теперь относится к Оптимизационной Теории помехоустойчивого кодирования, как к проблеме поиска глобального экстремума функционала (ПГЭФ).

Нам представляется весьма удивительным, что в течение многих десятилетий во многих аспектах развития прикладной теории по мере совершенствования микроэлементной базы, сетевых технологий и цифровых услуг, уже созданные ранее методы обработки, в том числе декодеры для разных кодов, фактически не менялись и не развивались вместе с новыми условиями исследований и применения, а уступали своё место совершенно новым разработкам. В связи с этим мы напомним о современных возможностях тех методов теории кодирования, которые хорошо известны. Затем мы обсудим их особенности в новых условиях развития алгоритмов на основе ОТ. Наверное, читатели по всем рассматриваемым далее вопросам могут найти достаточное число статей и книг, которые могут подтвердить или опровергнуть нашу точку зрения по тем или иным вопросам, обсуждаемым далее. Поэтому небольшое число ссылок на текущие и прошлые публикации при дальнейшем изложении нашего понимания ситуации в теории кодирования не следует расценивать как недостаток информированности специалистов нашей школы.

4.1. Использование МПД в классических каскадных схемах

Появление каскадных кодов открыло в своё время новую главу в развитии техники кодирования [26]. Эти коды способствовали ускорению внедрения результатов теории кодирования в технику связи и обеспечили широкий простор для новых исследований [3–5, 19, 27, 38, 40, 52]. Напоминаем, что после третьей «автономной» по ссылкам главы мы вернулись к общему списку литературы в конце книги.

Опишем 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. 4.1.

Произведем замену кода C_0 на некоторый код C_1 того же класса с параметрами (n_1, k_1, d_1), кодовой скоростью $R_1 > R_0$ и алгоритмом D_1. Далее добавим другой код C_2 со скоростью R_2 и параметрами (n_2, k_2, d_2), так что $R_1 R_2 = R_0$. Иначе говоря, заменим одношаговую процедуру кодирования двумя независимыми последовательными процедурами, причём суммарная кодовая скорость R_0 останется неизменной.

Процедура кодирования двумя кодами C_1 и C_2 начинается с обычного кодирования информации внешним кодом C_2, что приводит к увеличению общего результирующего числа символов в $1/R_2$ раз по сравнению с исходными данными. Далее весь новый поток данных направляется в качестве информационной последовательности не в канал, а во внутренний кодер кода C_1, что приводит к ещё большей избыточности сообщения по сравнению с первым этапом кодирования. Только после выполнения этой процедуры сообщение направляется в канал. На приемном конце последовательно работают декодеры внутреннего кода C_1, а затем внешнего кода C_2. Такова схема последовательного каскадирования. В настоящее время специалистами предлагается и анализируется много различных типов подобных кодовых конструкций.

К коду C_1, который при правильном проектировании системы можно взять существенно более коротким, применяется процедура декодирования D_1 того же класса, что и D_0, при её условной сложности $N_1 < N_0$. Тогда результирующая вероятность ошибки $P_b(e)$ в силу

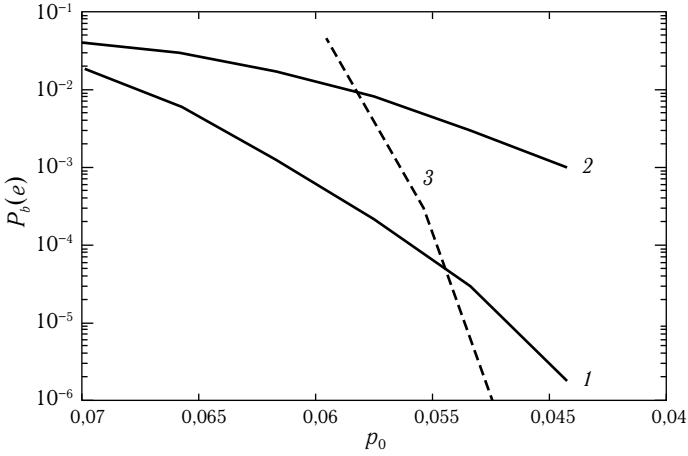

Рис. 4.1. Иллюстрация преимуществ каскадных схем перед обычными алгоритмами:
1 — R_0; *2* — $R_1 > R_0$; *3* — $R_0 = R_1 R_2$

условия $R_1 > R_0$ и выбора более простого кода будет соответствовать кривой *2* на рис. 4.1. 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*. При некотором шуме данная кривая будет ниже кривой *1* и, что важно, общая сложность декодирования $N_1 + N_2$ при этом оказывается значительно меньше, чем N_0. Таким образом, каскадные схемы действительно обеспечивают лучшее декодирование при меньших затратах.

Следует иметь в виду, что существует некоторая узкая область входных значений вероятности p_0 ДСК при большом шуме канала, где, как видно на рис. 4.1, исходный код C_0 может быть несколько эффективнее каскадного. Но это может иметь место при больших вероятностях ошибки в канале, 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 $d_0 = d_1 d_2$. Но термин каскадирования нередко применяется и для описания итеративных схем.

Заметим далее, что внутренний код C_1 должен удовлетворять более простым требованиям по вероятности ошибки декодирования, чем это требовалось от кода C_0. Разница между требуемыми корректирующими способностями кодов может составлять несколько порядков. Так, декодер D_2 кода C_2 обычно успешно декодирует сообщения с вероятностями ошибки, например, около $10^{-3} \ldots 3 \cdot 10^{-3}$, тогда как декодер кода C_0 должен был ошибаться с вероятностью не большей чем $\approx 10^{-5}$ при одном и том же уровне шума на входе, например, при $p_0 \approx 0{,}05$ для $R = 1/2$. Разница по уровню шума на входе для одной и той же вероятности $P_b(e)$, показанная на рис. 4.1 для кривых *1* и *3*, и демонстрирует преимущества каскадирования.

В [2—5, 53] и других работах нашей научной школы рассматривалось большое число эффективных каскадных схем. Многие результаты по этой тематике представлены на наших сетевых порталах.

4.2. Каскадирование с кодами контроля по четности

Целесообразно рассмотреть такие системы кодирования, в которых 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 [1, 3—5, 53].

Пусть задан блоковый двоичный код с нечетным d и $R = 1/2$.

Допустим также, что при некоторой вероятности p_0 результат декодирования сколь угодно мало отличается от результата оптимального декодера. Выберем некоторый достаточно длинный (n, k, d) код с проверкой на четность с параметрами $(k_2+1, k_2, 2)$, $k_2 \leqslant 400$. 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 этого блока являются поразрядной суммой по модулю 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 $P_b^{\text{МПД}}(e) \ll 1$. Считаем также, что для реализации возможностей каскадного кодирования после последней итерации $I \approx 10-50$ МПД запомнил все суммы проверок относительно всех декодированных символов. Допустим, что код с контролем четности использует предоставленную ему внутренним декодером информацию о проверках. Для всех k_2+1 символов блока ККЧ вычисляется надежность решения $\Delta_i = |m_i - d/2|$, где m_i — сумма проверок. Если контроль по четности обнаруживает ошибку в блоке, то изменяется тот символ, надежность Δ_i которого минимальна. Если же таких символов несколько, то никакого изменения символов не производится.

Оценим вероятность ошибки такой схемы декодирования. Во-первых, ошибка декодирования в ККЧ возможна при наличии двух ошибок во внешнем кодовом блоке. Вероятность такого события не превышает

$$P_{2e}(e) = \frac{1}{2}(k_2+1)k_2\left[P_b^{\text{МПД}}(e)\right]^2. \tag{4.1}$$

Во-вторых, неправильное решение декодера каскадного кода возможно, если произошла ошибка декодирования одного символа внешнего блока с надежностью Δ_i, а все другие символы декодированы верно, но среди них есть один или несколько символов с той же или ещё меньшей надежностью. В любом из этих случаев происходит ошибка декодирования каскадного кода, поскольку число ошибок в блоке внешнего кода, по меньшей мере, не уменьшается. Вероятность этой группы событий оценивается сверху как

$$P_{1e}(e) = k_2(k_2+1)\sum_{i=(d+1)/2}^{d} C_d^i p_0^i \sum_{j=d-i}^{(d-1)/2} C_d^j p_0^j.$$

Полагаем, что в той области шумов, где решения МПД и ОД практически не отличаются, вероятности остальных сочетаний оши-

бок канала, приводящих к ошибкам выбранной процедуры декодирования каскадного кода, малы и ими при оценках характеристик можно пренебречь. В этом случае вероятность $P_b(e)$ всей каскадной схемы оценивается с учётом (4.1) как

$$P_b(e) = \frac{2[P_{2e}(e) + P_{1e}(e)]}{k_2}. \qquad (4.2)$$

Заметим, что если внутренний код имеет кодовое расстояние d, то предложенный алгоритм исправляет любые сочетания из $d-2$ ошибок, а также значительное число ошибок большего веса.

На рис. 4.2 кривыми *1* и *3* представлены графики оценки вероятности $P_b(e)$ для двух каскадных кодов, состоящих из внутренних 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 внутренних СОК.

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 группирования ошибок характеристики этого, гораздо более короткого каскадного кода, несколько ухудшатся. Однако в области малых

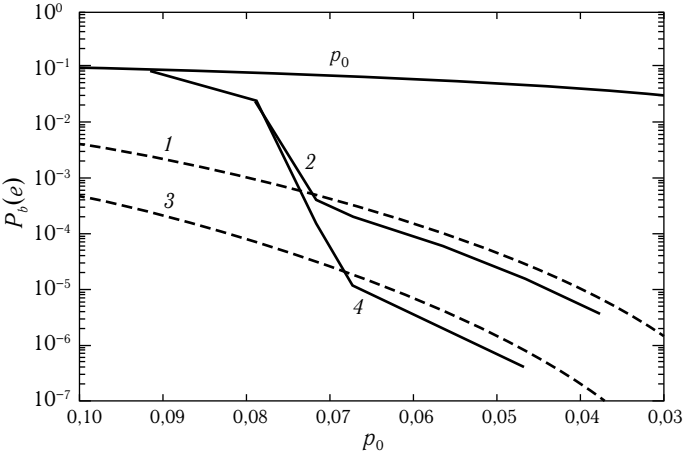

Рис. 4.2. Характеристики каскадных кодов с кодами контроля четности в ДСК без памяти:
1 — ОД ($d = 7$) + ККЧ; *2* — МПД ($d = 7$) + ККЧ;
3 — ОД ($d = 9$) + ККЧ; *4* — МПД ($d = 9$) + ККЧ

шумов результат работы МПД будет незначительно отличаться от оптимального.

Аналогичные характеристики можно получить для свёрточных кодов, каскадируемых с ККЧ. Эти вопросы рассмотрены в [1, 3–5]. Подчеркнем ещё раз, что использование ККЧ связано с тем, что эти коды почти не вносят потерь в кодовую скорость из-за добавляемой ими избыточности. И, кроме того, они очень хорошо соответствуют рассматриваемым в этой книге вариантам кодовых систем, в которых внутренний код декодируется практически оптимально. Ясно, что он обеспечивает в этом случае очень небольшую вероятность ошибки, соответствующую возможностям ОД. А это приводит, в свою очередь, согласно (4.2) к высокой эффективности и всего каскадного кода в целом.

Отметим, что в [5] рассмотрены и другие несложные методы каскадирования с хорошей эффективностью: для символьных кодов, в том числе с кодами Хемминга, а также для символьных СОК во внешних каскадах. Все они просто реализуются и обладают высокими характеристиками.

Напомним также, что каскадные коды для гауссовского канала и ККЧ рассматривались в параграфе 3.3, где они показали высокие характеристики вблизи границы Шеннона. Это оказалось возможным благодаря очень высоким характеристикам оптимального декодирования внутренних кодов на основе МПД и хорошему взаимодействию внутренних и внешних декодеров, которые успешно решали задачу поиска оптимального решения для всего каскадного кода в целом.

4.3. Применение МПД в схемах параллельного каскадирования

Как уже отмечалось в этой главе, возможности применения многих простых методов коррекции ошибок, в том числе и МПД, ограничены кодами с не очень большой корректирующей способностью. Конкретные проявления этих ограничений оказываются для разных алгоритмов также весьма специфическими. Например, в АВ очень жёсткие ограничения на эффективность возникают из-за сложности реализации, т. е. объема вычислений и памяти. В МПД же ограничение на рост ЭВК с увеличением минимального кодового расстояния d проявляется в виде быстрого ухудшения эффективности использования проверок. Это объясняется тем, что при увеличении размерности проверок вероятность ошибочности этих проверок при достаточно большом шуме быстро приближается к 0,5, обесценивая их использование в мажоритарных схемах. Такое объяснение ограничений и свойств мажоритарных схем со стороны признанных авторите-

тов [8, 10] на длительный период исключило мажоритарные методы из списка перспективных направлений развития теории и техники кодирования. Хотя развитие исследований по тематике ОД и МПД раздвинуло границы эффективности мажоритарных методов, с ростом d снова, как и в обычном мажоритарном декодере, но уже при существенно большей вероятности p_0 в ДСК ухудшение эффективности проверок проявляется и в МПД.

Одним из наиболее традиционных способов компенсации этого ограничения, как было показано выше, является использование МПД в каскадных схемах кодирования. Вместе с тем применение последовательных схем каскадных кодов усложняет решение задачи синхронизации. Но ещё более существенно, что необходимость компенсации потери ЭВК из-за скорости $R_2 < 1$ внешнего кода, которая может составлять почти 1 дБ при общем ЭВК около $7-9$ дБ, приводит к уменьшению эффективности этих схем.

Рассмотрим схему кодирования и декодирования, в несколько большей степени свободную от этих особенностей базового алгоритма МПД и отмеченных недостатков последовательных каскадных схем. Назовем её *системой параллельного каскадирования* [4, 5, 52]. Возможно, это вообще первая известная схема каскадирования такого типа. Пусть некоторый СОК с кратными скоростями (или, что то же самое, 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 два из каждой информационной ветви, которые и определяют размерность используемых проверок.

Преобразуем теперь код, выделив четыре первых проверочных ветви кода под декодер первого этапа с меньшим числом проверок, например, по 6 от каждой информационной ветви. Остальные проверочные соотношения, по 4 для каждой информационной ветви, отнесем к пятой проверочной ветви кода. Она будет теперь уже иметь размерность проверок, равную 20. Разумеется, все порождающие полиномы должны быть для пятой проверочной ветви пересчитаны соответствующими методами так, что весь код с порождающими полиномами теперь уже очень различного веса остался в классе самоортогональных кодов и имел то же значение кодового расстояния $d = 11$. Кроме того, нужно обеспечить и ещё достаточно малый уровень РО при использовании такого кода в МПД. Для этого придётся провести несколько тестовых экспериментов с МПД и кодами-кандидатами. Положим далее, что проверки пятой проверочной ветви вместе с первыми четырьмя ветвями с проверками меньшей размерности будут использоваться на втором этапе декодирования также на основе процедур типа МПД.

А на первом этапе работы такого МПД пусть он принимает решения только по проверкам первых четырёх ветвей.

Проанализируем полученную схему этого параллельного каскадирования. Отметим сначала, что при таком подходе к схемам кодирования на самом деле получаются два кода: первый (внутренний) код C_1 с $R_1 = 5/9$ и $d_1 = 7$ и внешний код C_2 с $R_2 = 5/6$ и $d_2 = 5$. При этом оба кода относятся к классу СОК, и, что существенно, их совокупность также остается СОК в силу принципа своего построения. Создание на основе одной и той же информационной последовательности двух кодов с различными скоростями передачи и позволяет назвать данный метод *параллельным каскадированием*.

Декодирование внутренним кодом с $R_1 = 5/9$ не имеет никаких новых принципиальных отличий по сравнению с обычными последовательными каскадными схемами. Оно осуществляется более или менее эффективно благодаря малому увеличению R_1 по сравнению с $R_0 = 1/2$, а также, что является главным моментом, 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 какой-либо другой эффективный алгоритм) существенно уменьшит с помощью кода C_1 вероятность ошибки $P_b(e)$ в принятом сообщении, происходит переход к главному этапу работы декодера — декодированию полного кода с $R_0 = 1/2$. Но если при этом из-за использования кода с меньшим кодовым расстоянием первый декодер будет работать при более высоком уровне шума, — а этого довольно часто можно добиться, — то и весь такой каскадный код будет более эффективным при меньшей энергетике канала, чем его прототип с полиномами одинакового веса. В нем и заключаются все преимущества и своеобразие параллельного каскадирования. Если в последовательных каскадных схемах на втором этапе декодирования на основе внешнего кода $R_2 \lesssim 1$, то при параллельном каскадировании скорость декодируемого кода второго этапа равна R_0, т. е. в рассматриваемом примере $R_0 = 1/2$. Именно существенное увеличение избыточности кода на втором этапе декодирования и определяет преимущество работы алгоритма параллельного каскадирования. Обычно в каскадном коде при $R_2 \sim 4/5$ 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}. В случае же параллельной схемы с использованием МПД второй каскад будет работоспособен при вероятности ошибки на входе этой второй ступени $p_0' = 10^{-2}$ или даже несколько выше. Эта разница

в граничной работоспособности схемы с МПД декодером при меньшей скорости и, главное, меньшем кодовом расстоянии первого кода и определяет преимущества параллельного каскадирования, если параметры первого кода C_1 были выбраны правильно и МПД для этого кода сумел эффективно его декодировать. Это преимущество появляется у декодера МПД из-за того, что проверки первых четырёх проверочных ветвей малой размерности используются и на следующем втором этапе декодирования при общей низкой кодовой скорости схемы $R_0 = 1/2$.

Обратим внимание на то, почему невозможно использовать все присутствующие в СОК проверки сразу без выполнения первого этапа декодирования, например, в ДСК. Для рассмотренного кода проверки пятой ветви имеют очень большую размерность и в ходе первого этапа коррекции ошибок при $p_0 = 0{,}05...0{,}07$ 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 $\sim 2 \cdot 10^{-2}$ или менее оказывается, что вероятность истинности для проверки из пятой проверочной ветви составляет уже $\sim 0{,}7$ или более, т. е. эти проверки гораздо более полезны. Именно это и демонстрирует МПД на втором этапе коррекции.

На рис. 4.3 представлены графики вероятности ошибки декодирования для кода типа СОК с $R = 1/2$, $d = 13$, которая достигается при использовании ПК на основе МПД. Кривые *2* и *3* соответствуют предельным значениям $P_b(e)$ для кодов с $d = 7$ и $d = 13$ в ДСК без памяти. Пунктирная кривая *1* отображает график вероятности ошибки декодирования с внутренним кодом с $R_1 = 5/9$ и $d_1 = 7$ при $I_1 = 6$ итерациях первого и $I_2 = 4$ итерациях второго этапов декодирования для полного кода с $R_0 = 5/10$ и $d = 13$.

На рис. 4.4 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 ещё на величину порядка 1 дБ.

Итак, параллельное каскадирование увеличивает ЭВК при фиксированной вероятности ошибки $P_b(e) = 10^{-5}$ в области уже достаточно высокой исходной эффективности МПД в ДСК без памяти и в канале гауссовского типа. Это подтверждает полезность и перспективность применения этого метода декодирования в реальных системах связи.

Важно отметить, что этот наш исключительно важный и в общем-то новый метод каскадирования уже много лет успешно при-

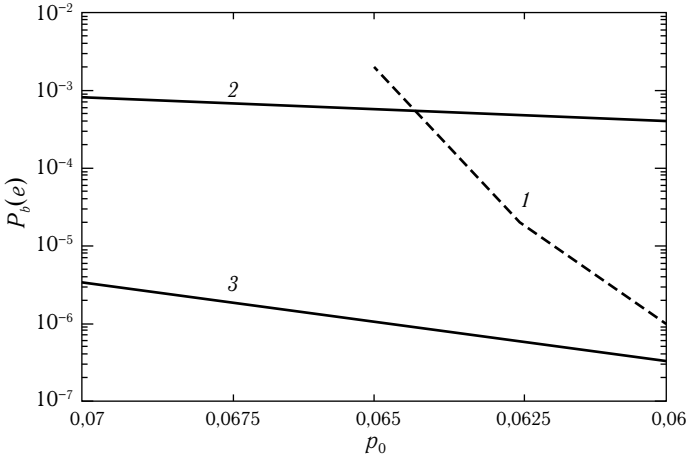

Рис. 4.3. Характеристики МПД декодера в режиме параллельного каскадирования для ДСК:
1 — ПК, $d = 13$; *2* — ОД, $d = 7$; *3* — ОД, $d = 13$

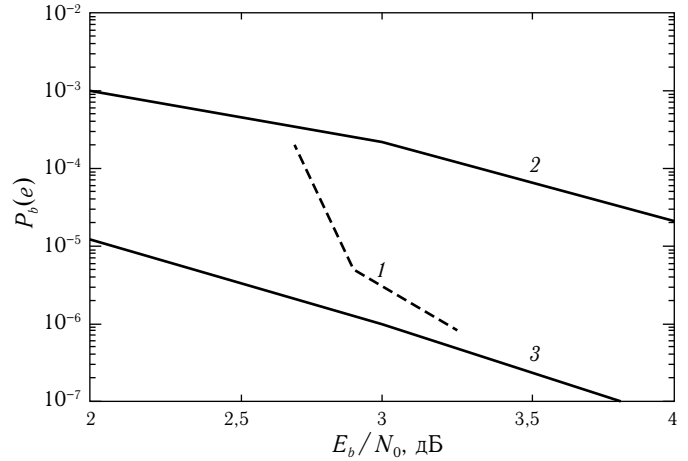

Рис. 4.4. Характеристики МПД декодера в режиме параллельного каскадирования для гауссовского канала:
1 — ПК, $d = 13$; *2* — ОД, $d = 7$; *3* — ОД, $d = 13$

меняется нами на практике. Фактически все без исключения МПД алгоритмы, представленные в главе 3, в той или иной степени использовали параллельное каскадирование по крайней мере в тех схемах, которые демонстрировали успешную работу в окрестностях границы Шеннона. Полезно также отметить, что метод параллельного каскадирования относится к дивергентным принципам кодирования, поскольку

ку МПД алгоритм переходит от декодирования кода с $d = 7$ к коду с $d = 13$. Несомненно, трёхкаскадные параллельные схемы кодирования также достойны изучения.

Наконец, укажем на то, что описанная здесь параллельная каскадная конструкция является отправной точкой для ещё более тонкой настройки весов полиномов в алгоритмах МПД. Обширный набор таких приёмов для улучшения работы наших алгоритмов вблизи пропускной способности канала мы объединили под общим названием кодов с выделенными ветвями, которые тоже смогли улучшить эффективность работы МПД декодеров при большом уровне шума. Они детально описаны в [3—5] и также успешно применялись в кодах, описанных в главе 3. В частности, символьный декодер, работающий в QCK канале с вероятностью ошибки $p_0 \leqslant 0{,}30$, был создан с учётом возможностей кодов с выделенными ветвями, что заметно расширило область эффективной работы этого алгоритма. Эти коды используются и во многих схемах ОТ, работающих в режиме ПГЭФ.

4.4. Кодирование для систем многопозиционной модуляции

В [3—5] рассматривались характеристики декодеров типа МПД при их согласовании с системами сигналов ФМN и АФМN. Многие схемы такого типа были проанализированы в [53]. Опыт разработки и анализа схем кодирования для сложных систем сигналов однозначно показал, что, как и для других кодовых систем, те алгоритмы, которые хорошо себя зарекомендовали в ДСК и АБГШ канале, также всегда успешно работают и с различными АФМ и ФМN сигналами. Это позволяет уверенно рекомендовать МПД алгоритмы различных типов для всех сложных систем сигналов. Необходимость помнить при этом о правильном согласовании кодовых и сигнальных систем столь же очевидна.

4.5. Использование МПД для кодов с неравной защитой символов

Внимание многих исследователей, работающих в области кодирования, привлекают коды с неравной защитой символов (КНЗС). Эти коды характеризуются тем, что разные группы символов, например, в блоковом систематическом коде, входят в различное число проверочных символов в качестве слагаемых. В результате информационные символы в таких кодах даже при оптимальном декодировании будут декодироваться ошибочно с различной вероятностью. Эта вероятность определяется кодовым расстоянием между кодовыми словами, отличающимися только символами, входящими в одну из подгрупп.

Применение МПД для декодирования кодов с $R = k_0/n_0$,

$k_0 = 2, 3, ...$, попутно решает и вопросы декодирования таких КНЗС. Например, при построении обычного СОК с $d = 7-11$ и $R = k_0/(k_0+1)$ необходимо иметь k_0 полиномов, определяющих вид (k_0+1)-й проверочной ветви кода по первым k_0 информационным. Переход к КНЗС может быть осуществлен путем использования таких полиномов для блоковых и свёрточных СОК, которые имели бы, например, вместо 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. К этим кодам применимы все технологии проектирования и развития, созданные в ОТ для успешной реализации ПГЭФ при большом шуме канала.

На рис. 4.5 представлены характеристики МПД для двоичного кода с $R = 3/4$ и $d = 7$ в ДСК (кривая *4*), а также предельные для малого шума вероятности ошибки кодов с $d = 5$, 7 и 9 (кривые *1–3*). Графики *5–7* 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 видим, предельные по $P_b(e)$ характеристики получаются при несколько большей вероятности ошибки канала p_0, чем $p_0 \approx 0{,}017$ для исходного кода с $d = 7$. Использование предложенного КНЗС кода для передачи (в данном случае) трёхразрядных чисел может существенно снизить среднеквадратичную ошибку.

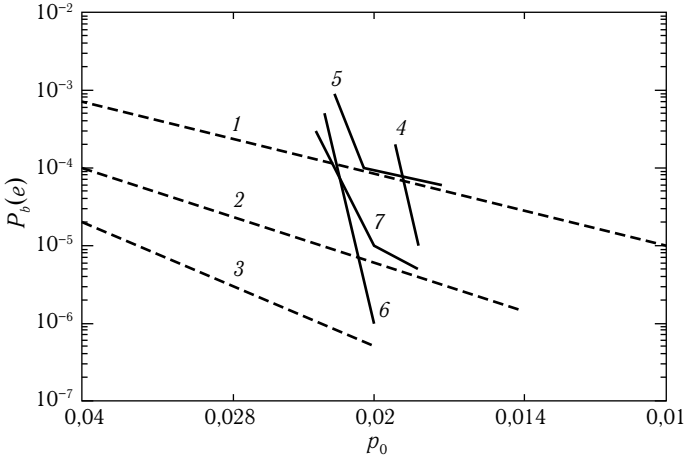

Рис. 4.5. Характеристики кодов с неравной защитой символов:
1 — ОД, $d = 5$; *2* — ОД, $d = 7$; *3* — ОД, $d = 9$; *4* — МПД, $d = 7$;
5 — КНЗС, $d = 5$; *6* — КНЗС, $d = 7$; *7* — КНЗС, $d = 9$

4.6. ОТ: приём эстафеты от алгебраической теории кодирования

Рассмотрим с более общих позиций возможности алгоритмов, созданных для реализации методов достижения решений ОД как задачи ПГЭФ и классических методов, которые созданы в рамках алгебраической теории кодирования.

В третьей главе мы уже анализировали символьные коды и методы восстановления стираний и выяснили, что ОТ и алгоритмы МПД обладают несравненными преимуществами перед всеми прочими способами коррекции ошибок в этих прикладных областях. Поэтому в этом параграфе мы рассмотрим двоичные ДСК и АБГШ каналы, которые в течение многих десятилетий считаются главным полигоном, на котором проводится сравнение лучших методов декодирования.

Одной из самых впечатляющих революций в технике декодирования для каналов с аддитивным белым гауссовским шумом в 70-х годах прошлого века, на начальном этапе развития теории кодирования, стал алгоритм Витерби [1, 15, 18–20]. В этот период специалисты начали понемногу понимать, что никакие алгебраические методы, например, коды БЧХ, Рида — Соломона не смогут решить проблему эффективного простого декодирования при $R \lesssim C$. Это было время первого большого разочарования, когда выбранное интересное и важное сначала направление работ по созданию эффективных алгоритмов декодирования оказалось тупиковым. В тот момент и возникла надежда, что именно АВ и связанные с ним методы выведут исследователей на правильное направление поиска. Рассмотрим, каким образом за 50 лет разработок изменились возможности АВ и что вообще сейчас может предложить классическая теория кодирования.

На рис. 4.6 представлены вероятности ошибки на бит $P_b(e)$ различных алгоритмов декодирования в двоичном гауссовском и двоичном симметричном каналах, которые практически всегда являются одним и тем же физическим каналом. По горизонтальной оси на рисунке отложены отношения битовой энергетики канала к спектральной плотности мощности шума E_b/N_0, выраженные в дБ. Линия «P_0 channel» указывает для выбранной кодовой скорости $R = 1/2$ вероятности ошибки на символ в канале при разных значениях E_b/N_0. Если в демодуляторе применяется, например, жёсткий модем, определяющий только знак принятых двоичных символов, то в декодер поступают значения «0» и «1» демодулированных битов, пришедших в этом случае из ДСК канала. А если в модеме приёмника перед декодером стоит аналого-цифровой преобразователь (АЦП), то в этот декодер будет поступать, возможно, решение мягкого модема об очередном переданном бите, квантованное, например, на 16 уровней (4 бита).

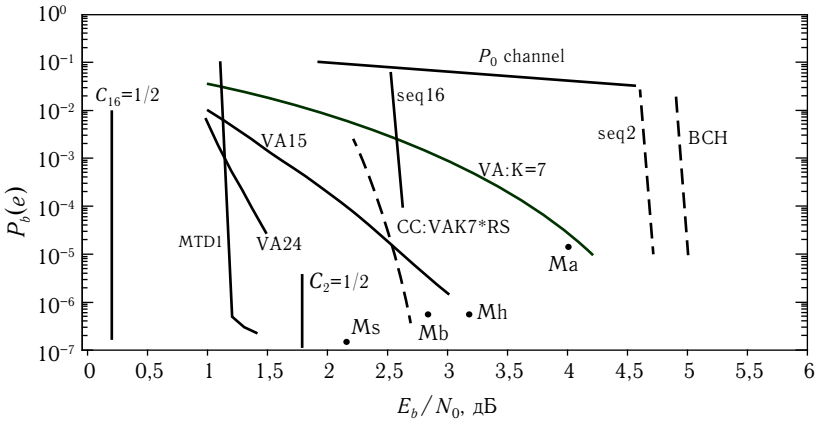

Рис. 4.6. Характеристики МПД, АВ и других классических алгоритмов декодирования в ДСК и гауссовском канале при $R = 1/2$

Это и будет двоичный АБГШ канал, над проблемой эффективного декодирования в котором уже 25 лет особенно напряжённо работают специалисты всего мира с тех пор, как были открыты турбо коды [30]. Авторы турбо декодеров дали нам тогда уже вполне обоснованную надежду на то, что приемлемые по сложности декодеры для уровня шума канала, соответствующего непосредственной близости к границе Шеннона, т. е. когда $R \lesssim C$, создать всё-таки можно. Однако они оказались неоправданно сложными и нетехнологичными.

Кроме того, на рис. 4.6 представлены вертикальные границы, отмечающие для ДСК и гауссовского канала с 16 уровнями квантования уровни энергетики, при которых пропускная способность каналов равна $C = 1/2$, помеченные как C_2 и C_{16} соответственно. Крутой график «MTD1» показывает наилучшие пока на данный момент реальные возможности МПД алгоритма, построенного на основе ОТ при использовании ПГЭФ, который при задержке решения не более 10 Мбитов и менее $I = 200$ итераций декодирования может быть спроектирован и создан в виде, который обязательно может иметь теоретически максимально возможное быстродействие при аппаратной реализации [58, 59]. Способы достижения столь большой производительности МПД декодера были запатентованы [28, 54—57]. Этот конкретный декодер работает, как и другие примеры декодеров на данном рисунке, при $R = 1/2$. А совсем простой МПД с 45 итерациями, отмеченный точкой Ms, лучше и границы для последовательного декодера в АБГШ канале и каскадной схемы АВ-РС при всего лишь впятеро большей задержке решения по сравнению с последней схемой. Развитие мягких МПД, их приближение к границе Шеннона и работа по

снижению размеров задержки их решений будут продолжены. Отметим, что каскадная схема АВ*РС фактически является единственным прикладным достижением классической алгебраической теории, да и то лишь в каскадной схеме со свёрточным кодом. Можно ещё раз упомянуть методы Судана для кодов РС, реально послужившие развитию теории, но и они не имели практического значения.

Далее на рис. 4.6 приведены графики для свёрточных кодов длины $K = 7, 15$ и 24, где K — длина кодирующего регистра, для которых при их декодировании использовался алгоритм Витерби. Как следует из вида этих графиков, самый первый из декодеров АВ с $K = 7$, созданный около 50 лет назад, гораздо слабее последующих. Но и АВ для $K = 15$ также был впервые сделан ещё в прошлом тысячелетии для проекта НАСА «Кассини», причём для небольшой кодовой скорости. Таким образом, АВ для $K = 15$ тоже является вполне реальным устройством. Разумеется, АВ для $K = 24$ пока недоступен для реализации просто из-за экспоненциально растущей с K сложностью декодера. Здесь же показаны характеристики главной каскадной схемы АВ с $K = 7$ и кодом РС [1, 19]. Это основные успешные и немногие реальные сейчас методы кодирования для гауссовских каналов. Посмотреть характеристики конкретных низкоплотностных (LDPC) и турбо декодеров, которые сейчас относятся к реализуемым системам, можно в разделе 3.5 предыдущей главы. Там же перечислены их основные недостатки. Самым главным свойством этих алгоритмов, которое ограничивает их возможности, является то, что эти методы не измеряют расстояние своих решений до принятого из канала связи вектора. Таким образом, хотя эти декодеры весьма высокой степени сложности и относятся к итеративным процедурам, они не являются оптимизационными процедурами, а это не позволяет отнести их к перспективным методам кодирования. Этот их главный недостаток оказалось возможным точно сформулировать только сейчас. Но и остальные ограничения, которые им свойственны, не позволяют сделать серьёзные ставки на их успешное развитие. И поэтому их реальные возможности уже значительно отстали от достижений МПД алгоритмов, особенно при большом уровне шума. На рис. 4.6 указаны также границы эффективности seq2 и seq16 для последовательных алгоритмов, которые так и не смогли преодолеть уровня вычислительных скоростей R_1 гауссовского и ДСК каналов, которые более чем на 2 дБ выше уровня энергетики канала при $R \sim C$. Таким образом, последовательные алгоритмы также уже очень давно не участвуют в конкурсе эффективных процедур декодирования для большого уровня шума канала.

Подчеркнём далее в связи с этим, что сейчас только все моди-

фикации МПД, а также свёрточные и блоковые АВ точно измеряют расстояние своих решений до принятого сообщения. Мы объединяем все эти алгоритмы в группу декодеров прямого контроля метрики. Скорее всего, только на них и надо ориентироваться при разработке методов, которые позволят быстрее других достичь ещё более близких к границе Шеннона рабочих значений уровня шума при декодировании, чем это уже достигнуто сейчас. Разумеется, движение рабочей области алгоритмов МПД к этой границе будет продолжено, как это и было всё последнее время. А пока для гауссовских каналов, ДСК, символьных кодов и стирающих каналов наиболее высокие характеристики при очень умеренном уровне сложности обеспечивают только алгоритмы на базе ОТ и МПД, дивергентных принципов, простых приёмов каскадирования и реализации ПГЭФ.

Как ещё одно полезное направление развития укажем также на то, что каскадирование АВ при $K \sim 15$ с символьными кодами, как видно из графика для АВ, возможно, могло бы обеспечить для этой схемы хорошие характеристики при $E_b/N_0 \sim 1$ дБ. Этот вопрос стоит детального рассмотрения, чтобы ещё раз оценить возможности, предоставленные теорией и современной элементной базой. Использование с этим АВ двоичных кодов тоже нужно изучать.

Рассмотрим возможности других алгоритмов в канале ДСК. Неконкурентность последовательных процедур, сыгравших в своё время определенную положительную роль в теории кодирования, мы уже отметили выше и увидели по граничным кривым для них на рис. 4.6. А возможности кодов БЧХ оказались крайне слабыми из-за того, что при росте длины кодов отношение кодового расстояния к длине кода d/n для этих кодовых структур быстро падает. И кроме того, в отличие от кодов с мажоритарным декодированием, декодеры БЧХ всегда ошибаются, если число ошибок в принятом блоке превышает $d/2$. Эти два серьёзнейших недостатка вместе со сложностью их декодирования, не доведённой до линейной от длины кода, приводят к тому, что граница для кодов БЧХ по энергетике лежит на рис. 4.6 даже дальше, чем для последовательных алгоритмов для ДСК. На это давно известное свойство кодов БЧХ указывалось в [1].

Далее точкой Ма на рис. 4.6 помечен результат 30-летней давности для крайне простого МПД декодирования при $E_b/N_0 = 4$ дБ для свёрточного кода с $d = 11$ и $I = 14$ итерациями декодирования [29]. Тем самым наглядно видно, что уже в те годы были полностью перекрыты все возможные достижения для кодов БЧХ и всех прочих методов алгебраической теории. Это однозначно определялось достижением МПД алгоритмом и в этом случае уровня оптимального декодирования при всего лишь $I = 14$ итерациях декодирования для до-

вольно хорошего в плане РО кода. При снижении энергетики ДСК при $R = 1/2$ до ~ 3 дБ достижение высокого уровня достоверности декодирования тоже не составляет проблемы, если значительный рост задержки решения в блоковом или свёрточном вариантах декодирования до 1 Мбита признаётся допустимым. Эта достижимая для многих видов МПД декодеров и кодов точка отмечена рис. 4.6 как Mh. При отличии рабочей энергетики МПД от шенноновского уровня для $R = 1/2$ в ДСК на ~ 1 дБ сложность и задержка МПД будут, как следует из стандартных оценок, примерно в 1,5 раза меньше, чем у довольно не простого уже MTD1, что вполне естественно для столь большого уровня шума. Значит, и в ДСК у ОТ, МПД и методов ПГЭФ конкурентов вообще нет.

Таким образом, из комплексного обзора сведений об алгоритмах декодирования получается, что в гауссовских каналах пока что нет реально других перспективных алгоритмов, кроме МПД и АВ. Мы уже немного обсудили, почему турбо и LDPC коды выпали из конкурса перспективных алгоритмов. История последних 25 лет изучения декодеров этого типа, когда рост их эффективности прекратился, однозначно подтверждает наш вывод о слабых характеристиках алгоритмов, не относящихся к группе ДПКМ. В самом деле, достаточно сложно ожидать от алгоритма, который не измеряет расстояние своих решений до принятого вектора, успешного хоть в какой-то мере декодирования, тем более при максимально допустимом теорией уровне шума.

А пока сделаем завершающие жёсткие выводы по каналам типа ДСК и QCK.

В предыдущих разделах мы уже неоднократно отмечали, что символьные коды навели, наконец, в случайных недвоичных каналах полный порядок после 50-летнего застоя, случившегося после важнейшего для теории кодирования 60-х годов открытия кодов Рида — Соломона. Но коды РС реальны только в своих коротких версиях. Использовать длинные коды РС нельзя, да и не надо, т. к. они тоже малоэффективны, а их декодеры очень сложны. Ну, а больше ничего и нет.

Напомним, что символьные коды могут быть любой длины и даже при большом уровне шума декодируются оптимально, как это сделал бы недвоичный АВ, создать который для каких-либо не очень коротких недвоичных кодов, скорее всего, совершенно нереально. Уровень шума, при котором QМПД декодирует символьный код оптимально, в разы больше по вероятности ошибки канала, чем это могут позволить себе декодеры для кодов РС. Обширный экспериментальный материал об этом широко опубликован уже очень давно [40]. Та-

ким образом, уже созданные системы с кодами РС должны работать, пока они нужны, а все новые задачи для недвоичных каналов следует решать с использованием символьных кодов, т. к. конкурентов у них просто нет.

В качестве примера высокой эффективности символьного МПД при очень малой избыточности, когда $R = 19/20$, читатели могут переписать на свой компьютер демо-программу для МПД (QМПД) блокового символьного кода по гиперссылке [69] со страницы «Обучение» на сайте **www.mtdbest.ru**. Эта демо-программа, как и все другие программные средства на наших порталах, сопровождается инструкцией, которая позволяет настроить ряд параметров декодера. Очень важно, что на самых обычных ПК производительность QМПД, как и алгоритмов для двоичных кодов достигает десятков Мбит/с, что отлично иллюстрирует преимущество методов, созданных на базе ОТ, над другими методами декодирования.

Напомним ещё раз, что причина высокой скорости работы декодеров этого типа одна: единственный активный блок МПД — пороговый элемент, простейшее устройство. В случае аппаратной реализации в соответствии с теми же уже запатентованными решениями для ДСК и АБГШ каналов [28, 54–57] символьный декодер также может обеспечить теоретически максимально возможную производительность для любой элементной базы, которая будет просто совпадать со скоростью продвижения данных по регистрам сдвига микросхемы.

Таким образом, при наличии до недавнего времени работоспособной системы кодирования на базе только недвоичных коротких кодов РС (а в силу этого и малоэффективных!) алгоритмы QМПД оказываются сейчас единственными реальными высокопроизводительными декодерами для недвоичных случайных каналов. Они характеризуются высочайшей производительностью и способностью находить решения ОД даже в условиях очень большого уровня шума. Это означает, что ОТ полностью решила вопросы простого и высокодостоверного декодирования в недвоичных каналах и на сегодняшний день, и на перспективу.

Наконец, подчеркнём, что в стирающих каналах запатентованные алгоритмы, идеологически похожие на МПД, на больших скоростях декодируют данные при $R = 1/2$ и при вероятности приёма из канала стёртых символов $\sim 0{,}49$ снижают долю невосстановленных алгоритмом символов до уровня менее 10^{-6} [60]. А недавно запатентованный нами АВ [61] для блоковых кодов со сложностью $\sim 2^K$, а не 2^{2K}, как умели буквально до недавнего времени наши теоретики, полностью исключает из конкурсов для гауссовских каналов вообще все алгебраические алгоритмы.

Таким образом, представленные результаты для всех основных типов каналов чётко свидетельствуют о безусловном и очень большом по всем параметрам эффективности и сложности преимуществе технологий и идеологии ОТ при решении задач теории кодирования, относящихся к исправлению, восстановлению, контролю и хранению цифровых данных в современных цифровых системах. ОТ успешно приняла эстафету во всех прикладных вопросах от классической алгебраической теории кодирования и выходит в новое бескрайнее интеллектуальное пространство оптимизационных алгоритмов, с линейной от длины кодов сложностью решающих все проблемы достижения оптимальной по максимуму правдоподобия достоверности цифрового контента нашей информационной цивилизации.

Глава 5

Технологические средства поиска глобального экстремума

5.1. Программное обеспечение для исследований в области ОТ

Для реализации методов МПД декодирования необходимо использовать обширный ассортимент методов построения кодов, сбора статистики и настройки параметров алгоритмов декодирования совершенно особого вида, которых не было в средствах, созданных алгебраической теорией. При разработке методов и технологий ОТ было создано более двух десятков различных оптимизирующих программ, которые можно условно разбить на три большие группы.

К *первой группе* относится программное обеспечение (ПО) для построения кодов с малым уровнем РО, которые имели настроечные параметры, позволявшие регулировать уровень РО при не очень быстром росте длины кодов, которые при отсутствии такого контроля становились исключительно длинными. При поиске хороших кодов было необходимо удовлетворять компромиссным требованиям между качеством кодов и временем их поиска, длиной и задержкой принятия решений, что потребовало создания линейки программ оптимизации для поиска хороших кодов с различной сложностью такого поиска. При отказе от контроля за длиной кодов задача построения лучшего по критерию РО кодов превращается в проблему поиска глобального экстремума по одному или нескольким критериям минимизации РО. Из различных вариантов таких программ с ориентировочной сложностью вычислений от $\sim d^3$ до $\sim d^5$ наиболее подходящими для разработки методов ОТ оказались те оптимизирующие программы, которые имели порядок сложности, более близкий к $k_0 n_0 d^4$. Здесь k_0 и n_0 — параметры, определяющие кодовые скорости проектируемых кодов $R = k_0/n_0$, и оба могут варьироваться в пределах от 1 от 100. Реальная проектируемая величина кодового расстояния обычно не превышала значения $d \sim 35$ и была вполне достаточной для всех реальных исследований и приложений ОТ. Типичное время поиска кодов по выбранным простым или комплексным критериям составляло от нескольких секунд до десятков часов, что позволило решить все задачи построения кодов по заданным требованиям к ним.

Вторая группа программ предназначена для решения главной задачи определения параметров эффективности тех или иных алгоритмов декодирования — основной проблемы прикладной теории кодиро-

вания. Программы этого типа для задачи поиска (по возможности, конечно!) глобального экстремума, согласно теореме ОТМПД, написаны особенно экономно для более быстрого набора статистики, что во многих случаях очень важно, поскольку требования к кодам и алгоритмам декодирования по вероятности ошибки декодирования непрерывно растут, и уже для нескольких вариантов создания быстрых и эффективных алгоритмов декодирования оказывается необходимым снизить вероятность ошибки на бит до уровня $P_b(e) < 10^{-12}...10^{-15}$. А это требует весьма значительного объёма статистики, которую надо собрать при моделировании декодера. При этом часто оказывается полезным рассмотреть структуру ошибок декодера в процессе сбора статистики, активность различных пороговых элементов декодера, а также взаимодействие различных алгоритмов декодирования в каскадных и иных схемах. В большинстве случаев при использовании МПД алгоритмов основные затраты на декодирование приходятся на моделирование работы множества пороговых элементов. При необходимости оценить быстродействие работы МПД алгоритмов можно использовать демо-программу сверхскоростного МПД декодера на странице «Обучение» с сайта **www.mtdbest.ru**. Она, как и другие демо-программы, имеет инструкцию по использованию. Перепишите по гиперссылке [70] модуль демо-программы и по гиперссылке [71] простые правила работы с программой. После распаковки вы можете оценить быстродействие алгоритма МПД в гауссовском канале при большом шуме. На обычных ПК с ОС Windows свёрточный МПД, который имитируется этой демо-программой, при достаточно большом уровне шума декодирует со скоростью $6-18$ Мбит/с, если в декодере каждый информационный символ проходит через 10 пороговых элементов. Это, наряду с другими данными по быстродействию, представленными в книге, характеризует действительно высокие скорости работы алгоритмов на базе МПД.

Наконец, *третью*, особенно сложную группу программ, также реализующую алгоритмы поиска глобального экстремума, образуют методы настройки различных параметров МПД алгоритмов, которые используются для значительного повышения скорости сходимости решений МПД и других связанных с ним алгоритмов к оптимальному решению, т. е. к абсолютному минимуму расстояния решений МПД до принятого сообщения. Реализация этих методов требует сотен и тысяч прогонов достаточно длинных зашумлённых кодовых последовательностей. Это один из важнейших этапов проектирования алгоритмов типа МПД, в результате которого возможно дополнительное сокращение задержки декодирования или улучшение характеристик декодирования при больших уровнях шума. Настраиваемыми элемен-

тами декодера могут быть значения порогов на ПЭ, веса тех или иных проверок, разностные отношения между полиномами и внутри них, веса полиномов и расстояния между ПЭ и другие параметры алгоритмов МПД.

Схемы перебора тех или иных параметров МПД составляют отдельный класс задач, решаемых при проектировании этих алгоритмов. Разумеется, возможны различные способы последовательного перебора параметров, когда эти параметры меняются в различном порядке, учитывающем поставленные при поиске цели. Постановка проблемы реализации ПГЭФ уже сама по себе предполагает наличие большого числа режимов поиска, что создаёт огромный простор для творческого воображения при создании новых кодов и типов МПД алгоритмов.

Использование на различных этапах проектирования МПД оптимизационных процедур позволяет относительно простыми по своей идее методами достичь существенного повышения эффективности алгоритмов МПД и связанных с ними других процедур, например, каскадных декодеров без какого-либо увеличения числа операций, выполняемых такими улучшенными МПД с оптимизированными параметрами.

Разумеется, создание средств разработки и исследований алгоритмов в рамках ОТ не ограничивается только оптимизационными программами. Важнейшее значение имеет правильная постоянно контролируемая работа нескольких классов датчиков случайных чисел (ДСЧ), от качества которых в решающей степени зависят качество создаваемых декодеров и достоверность получаемых экспериментальных результатов. Датчики нужны при имитации многих типов шумящих каналов разного качества, формирования информационных потоков и решения задач синхронизации. Необходимо контролировать статистические свойства ДСЧ, их периодичность, если они не случайные, а также их взаимодействие, если генерация потоков шума и данных формируется на основе нескольких взаимодействующих процессов. Очень полезно иметь контрольные тестовые ситуации, которые все ДСЧ должны регулярно проходить.

Очень важно также иметь развитые средства контроля за работой моделируемых алгоритмов. Наличие тестовых потоков, на которые алгоритм декодирования должен реагировать абсолютно правильно, совершенно обязательно, причём таких тестов должно быть достаточно много. Абсолютно всегда нужно создавать возможность работы различных информационных потоков с одинаковыми шумовыми последовательностями для каждого изучаемого алгоритма. В случае получения на таких тестах различных результатов экспериментатор может узнать о своём ПО и проверяемом алгоритме много интересного.

Наконец, во многих случаях после выполнения всех изучаемых процессов с тем или иным алгоритмом декодирования часто оказывается полезной автоматическая разборка декодируемого блока или потока свёрточного кода на отдельные информационные, кодовые и шумовые потоки, которые после завершения моделирования процесса должны совпасть с исходным набором символов и ошибок канала, который сохраняется до конца эксперимента.

5.2. Особенности процедур набора статистики и оптимизации

При наборе статистики для алгоритмов декодирования на уровне вероятности ошибки на бит $P_b(e) \sim 10^{-7}$ и менее приходится дополнительно учитывать целый ряд специфических условий. Во-первых, при долгом сборе статистики происходят случайные отклонения от заданных в эксперименте вероятностей ошибки, и с увеличением объёма собираемой статистики таких совершенно естественных статистических отклонений, например, интенсивности шума канала, оказывается больше, а их амплитуда заметнее. Но алгоритм должен быть устойчивым к таким обязательным девиациям входного потока ошибок. Значит, корректирующая способность исследуемых методов декодирования с очень высокой итоговой достоверностью своих решений должна иметь небольшой запас «прочности». Это предъявляет к создаваемым декодерам дополнительные требования по их готовности успешно преодолевать короткие всплески шумового потока и требует высокого уровня способности корректировать ошибки в исследуемых алгоритмах.

Для оценки такого запаса помехоустойчивости можно при исследованиях декодера для какого-то уровня вероятности ошибок канала на входе анализировать его поведение ещё и при вероятностях ошибки на входе, на 0,5–2,0% бóльших уровня номинальных значений вероятностей. Успешная работа алгоритма при таких немного завышенных уровнях шума позволяет полагать, что при номинальной вероятности ошибки декодер будет работать вполне устойчиво. Разумеется, при этом необходимо делать правильные статистические оценки происходящих процессов.

Далее, возможно использование наборов статистики для последующей оценки возможностей декодеров на основе «перекошенных распределений». Для этого выполняется, например, сбор детальных статистик декодирования всех кодовых блоков некоторого кода с запоминанием количества таких блоков с различным числом ошибок на входе и количеством ошибок (или их отсутствием) на выходе декодера. После сбора достаточного числа данных о декодированных блоках можно пересчитать вероятности ошибки на бит для тех же блоков,

если эти блоки с таким же числом ошибок на входе появляются при меньшей вероятности ошибок в канале. Оказывается, что размеры эксперимента, который необходимо провести при более высокой вероятности ошибки на входе, оказываются существенно, на порядки меньшими, чем необходимые объёмы такой работы для обычного сбора статистики. В ряде случаев, как показали тестовые эксперименты, можно сэкономить на длительности эксперимента и сократить его таким образом в 100 раз и более. Но этот очень полезный подход следует реализовать только после соответствующих оценок точности и достоверности получаемых при пересчёте оценок. Ещё более актуальными являются ситуации, когда необходимо оценить вероятности ошибки, на 3–5 порядков меньшие, чем те, которые может дать обычный статистический эксперимент. Это технологическое направление исследований очень важно, т. к. требования к достоверности декодирования стремительно растут и технологии перерасчёта вероятностей ошибок декодирования вскоре будут очень востребованы.

Аналогичную задачу полезно решить на практике и в случае использования свёрточных кодов. Но при этом нужно будет аккуратно перенести этот метод с блоковых кодов на свёрточные.

Наконец, при реализации самой трудоёмкой процедуры — настройки параметров декодера, — когда нужно прогонять через декодер сотни и тысячи раз длинные входные последовательности, настраивающие огромное число параметров декодеров на более быструю сходимость к решению ОД, проблема правильного распределения вычислительных ресурсов становится особенно актуальной. Весьма частым случаем настройки параметров алгоритмов МПД оказывается вариант, при котором эти параметры настраиваются по группам, например, по 10 ПЭ. Тогда сначала настраиваются пороговые элементы декодера первой группы, затем следующие 10 ПЭ, затем третий блок и т. д. А тогда становится возможным не генерировать каждый раз полный поток данных и не заставлять многократно работать те части МПД декодера, которые уже были настроены ранее, а сгенерировать один раз тот поток входных символов, который поступает в новую группу настраиваемых ПЭ после завершения работы с предыдущей. Такой поток и надо запомнить один раз, а потом вводить его сразу во вторую группу ПЭ и т. д. Это может сократить до десяти-тридцати и более раз процесс последовательной настройки элементов МПД по группам, особенно в тех случаях, когда общее число настраиваемых элементов МПД может достигать многих сотен и даже тысяч. Не забудем снова напомнить, что, несмотря на такую сложную систему настроек, итоговый МПД будет выполнять такое же число операций, как и исходный алгоритм до выполнения требуемых настроек. А пре-

имущество такой адаптации декодера к каналу, в котором он должен работать, будет заключаться в том, что сходимость МПД к решениям ОД будет происходить при использовании ПГЭФ гораздо быстрее, что позволит уменьшить задержку декодирования, сократить объём декодера или ускорить его работу.

5.3. Краткий обзор руководящих парадигм ОТ

Теория информации переживает сейчас завершение перехода лидерских позиций в теории кодирования от классической алгебраической к Оптимизационной Теории помехоустойчивого кодирования на основе процедур поиска глобального экстремума функционалов в цифровых пространствах. Описанию этого перехода вместе с сопутствующими ему обстоятельствами и посвящена данная книга. Эта ситуация требует хотя бы краткого описания условий, в которых предстоит развиваться этому важнейшему для цифровой информационной цивилизации научному направлению. Подчеркнем, что зафиксированное нами событие является естественным результатом глубокого застоя старого направления, которое уже более 30 лет не может найти вектор устойчивого развития. Вклад нашей научной школы в приближение этого момента невозможно переоценить, поскольку небольшая российская группа специалистов решила все труднейшие прикладные задачи теории кодирования и создала оптимальные декодеры с теоретически минимально возможной сложностью реализации для всех основных моделей каналов передачи данных и систем памяти.

В связи с принципиальным разворотом всей теории информации в направлении оптимизации как глобального поиска в задачах декодирования цифровых потоков рассмотрим главные обстоятельства, в которых, видимо, будет развиваться теперь теория кодирования.

В первую очередь укажем на недавний российский патент для блокового алгоритма Витерби [61]. Поскольку выше уже было указано, что он возвращает блоковые коды на рельсы реальности по сложности декодирования, то эта версия АВ закрывает вообще все проблемы декодирования блоковых кодов на алгебраической основе в АБГШ каналах, т. к. какая-либо необходимость в них теперь отсутствует. Невообразимая идеальность АВ приводит к тому, что в небытие отправляются все попытки декодирования в гауссовских каналах блоковых кодов с использованием методов Чейза и других крайне странных алгоритмов. Мы уверены, что наш блоковый АВ будет активно использоваться повсеместно, как и его свёрточная исходная версия, самостоятельно или в простейших каскадных схемах, которые, как мы показали в наших работах, являются самыми полезными.

Конечно, на второй позиции по приоритетным важнейшим свой-

ствам стоит вовремя сделанное нами выделение из набора разных алгоритмов группы декодеров с прямым контролем метрики. Уникальнейший опыт изучения различных алгоритмов декодирования, которые мы запрограммировали и поместили как демо-программы на наши сетевые порталы, показал, что только АВ и МПД во всех своих модификациях контролируют расстояние своих решений до принятого из канала вектора. Очень похоже, что только декодерам из этой группы и будет позволено действительно ещё ближе подойти к уже совсем близкой для них границе Шеннона. Их разнообразные возможности для этого уже были представлены в этой монографии.

Далее, несомненно, следует назвать выделенный нами из огромного числа полезных приёмов улучшения алгоритмов декодирования принцип дивергенции. Его принципиальным главным свойством является некаскадное постепенное увеличение кодового расстояния используемых свёрточных кодов, которое мы применяем уже очень давно. Формализация и выделение этого принципа из общего потока идей значительно ускорило наше продвижение по пути поиска простых методов повышения эффективности ОТ и МПД алгоритмов. Этот принцип создаёт новые направления развития методов декодирования и позволяет улучшать уже известные алгоритмы. Огромные надежды мы возлагаем на этот принцип ещё и потому, что он позволяет использовать там, где эта возможность специально подготовлена, декодирование одновременно несколькими методами. Мы полагаем, что это направление работ может быть исключительно успешным.

Ещё одно важнейшее достижение нашей научной школы — параллельное каскадирования, которое, как мы полагаем, первой тоже открыла в 1986 г. наша школа. Его важнейшим свойством, которое всегда проявляет себя с самой лучшей стороны, является то, что декодирование на втором этапе коррекции ошибок в параллельном каскадном коде осуществляется на полной кодовой скорости всего кода, тогда как в последовательном каскадировании на втором этапе работает малоизбыточный код со слабой корректирующей способностью. К этому можно добавить, что при параллельном каскадировании, как ни в каких других кодовых структурах, оказывается легко и удобно оптимизировать по разным критериям кодовые расстояния и веса проверок составляющих кодов, что чрезвычайно расширяет возможности глубокой оптимизации параметров кодов и МПД алгоритмов. Наша школа активнейшим образом работает с параллельным каскадированием как с ключевым во многих случаях методом.

Целенаправленное выделение группы ДПКМ декодеров также позволяет правильно ориентироваться в выборе кодов и алгоритмов для проектов с декодированием вблизи границы Шеннона. Трудности

в развитии методов, которые не входят в эту группу, как мы уверены, не даст им остаться в конкурсе актуальных алгоритмов. Они не преодолимы. Однако из этого не следует, что не появятся другие алгоритмы, которые попадут в эту важную для прогресса техники декодирования группу. Несомненно, это откроет новые возможности для группы ДПКМ методов.

В очередной раз подчеркнём, что упомянутые выше ключевые парадигмы как средства достижения цели при всех сложных условиях, в которых они используются или закладываются в МПД алгоритмы, приводят только к тому, что МПД декодер остаётся простейшим мажоритарным декодером на всех своих итерациях. Единственным его отличием от простой обычной схемы в этом случае оказывается лишь разное число проверок, поступающее на тот или иной ПЭ, что иногда приводит даже к небольшому уменьшению числа операций по сравнению с максимальным использованием всех проверок на каждой итерации.

Наконец, в качестве последнего руководящего средства повышения эффективности декодирования мы укажем каскадирование с кодами контроля по чётности. На первый взгляд, эта парадигма не несёт той мощной идеологической нагрузки, как предыдущие. Однако она обретает особую силу именно вместе с решающим повышением эффективности внутренних декодеров каскадных кодов (КК) вблизи пропускной способности канала, когда оказывается возможным их декодировать действительно с большой достоверностью и оптимально. Как раз в таком случае ККЧ дополнительно снижают вероятность ошибки в таком КК, причём также в максимальной степени. А это оказывается особенно важным при том большом уровне шума, который всегда присутствует вблизи границы Шеннона.

Ну, и напоследок укажем, что все ключевые парадигмы могут использоваться и учитываться при проектировании и исследованиях алгоритмов МПД и других методов в различных сочетаниях, что приумножает их совместный синергетический эффект.

5.4. Интеллектуальный космос развития методов кодирования

Неподготовленный читатель, которому сообщают о том, что создана новая величайшая теория, про которую главный теоретик объяснил, что в ней уже почти всё сделано, может испытывать весьма сложные чувства, связанные с необходимостью смены профессии, уходом на пенсию или в отшельничество. На самом деле поле теории, пространство разработок новых схем, идей и подходов благодаря переходу в мир оптимизационных задач, наоборот, расширяется при

этом воистину тысячекратно и даже требует привлечения как новых генераторов оригинальных научных идей, так и активных высокопрофессиональных специалистов, создающих по новым сложным схемам и стандартам инновационное цифровое оборудование для глобальных сетей.

Рассмотрим представленную ниже табл. 5.1 кодов и алгоритмов различного класса, которая, конечно, не может быть полной и всеобщей. Тем не менее, постараемся указать те основные коды и алгоритмы, для которых все главные задачи, связанные с простым, но оптимальным декодированием, решены. Это позволит рассмотреть и тот фронт работ, который открывается в сфере разработки алгоритмов на основе ОТ и методов ПГЭФ.

Таблица 5.1. Объём покрытия ОТ — основные кодовые кластеры

2 — Коды блоковые — свёрточные
3 — Коды базовые — каскадные (класс. посл. + паралл.)
2 — Модемы жёсткие — мягкие
2 — Коды двоичные — символьные
2 — Коды для стираний — для ошибок
2 — Кодовые скорости средние — высокие
2 — Декодеры обычные — сверхбыстрые
2 — Декодеры обычные — сверхдостоверные
2 — Декодеры обычные — альтернативные

Итого 768, реально готовы $\sim$100 типов. Дополнительные: АФМ, ФМ, пАФМ, ДПКМ, НЭК, дивергенция, конвергенция и т. д.; всего, видимо, $\sim$3000 кластеров.

Таблица 5.1 подготовлена исходя из простого принципа дихотомии кодов по различным существенным в теории кодирования параметрам. Только во второй строке указаны 3 варианта кодов, без чего тоже нельзя было обойтись. Если мы перечислим все возможные сочетания кодов во всех девяти строках признаков кодов, то и получим 768 их вариантов, указанных в таблице внизу. Но там же отмечены и другие условия применения кодов: многопозиционные системы сигналов, дивергенция и другие, к которым можно добавить на самом деле ещё многие десятки типов систем, использующих всеобщую доступность кодирования, что теперь может сделать любой высокопрофессиональный читатель. А обязательное появление новых, ещё неизвестных нам постановок задач, обусловленных возможностью простого и эффективного декодирования, сделает пространство поисков новых решений совершенно безграничным.

Опишем без особой детализации те сферы кодирования, которые мы хорошо проработали с помощью ОТ. Это, конечно, все основ-

ные классические каналы, рассматриваемые в теории, причём как для средних, так и для высоких кодовых скоростей, порядка $R = 3/4$ и выше. Надо получить и результаты из области низких скоростей, которые полезны для космической связи. Далее наши конкретные аппаратные и программные разработки совместно с патентами показали, что идеи ОТ работают при высоких физических скоростях декодирования, а также для двоичных и недвоичных (символьных) кодов и алгоритмов. Кроме того, у нас абсолютно лучшие результаты для каналов со стиранием символов, а не только в тех, где происходят только ошибки передачи. Наконец, мы разработали несколько сверхдостоверных по итоговой вероятности ошибки декодеров для флеш-памяти, а также получили очень высокие результаты в каскадных схемах различных типов. Это позволяет аккуратно пересчитать все конкретные достижения нашей школы по типам кодов и каналов, что и даст в общей сложности около ста действительно завершённых нами принципиальных инновационных результатов вблизи границы Шеннона. Это подтверждает наши пионерские приоритеты, но, самое главное, оставляет ещё для полной глубокой проработки многие сотни вариантов приложений только из верхних девяти строк таблицы. Но, учитывая быстрый рост требований к кодам, будущие разработки ждут исследователей, которые будут готовы погрузиться в новый стиль работ в области современной теории кодирования. К этому можно добавить воистину грандиозное количество методов модуляции, для которых нужны новые эффективные коды и алгоритмы. В процессе таких работ многие коллективы найдут совершенно новые пути развития в ОТ. Но тогда с неизбежностью возникнет и проблема большого числа специалистов, которых надо обучить новым технологиям ОТ и направить на разработки новых схем кодирования для современной цифровой техники. Так что давайте изучать МПД и ОТ, чтобы быть лидерами в этой важнейшей сфере знаний цифрового мира. Технологии теорий поиска глобального экстремума в теории кодирования, опубликованные нашей школой, уже создали все условия для быстрого и успешного освоения новых методов простого эффективного декодирования.

Глава 6

Рекомендации к дальнейшим исследованиям

Как и многие другие специалисты, ответственно относящиеся к возможности проведения дальнейших исследований по тематике их основных трудов, мы считаем необходимым тоже указать важнейшие, по нашему мнению, направления исследований, которые могут быть успешными и полезными для развития на новом оптимизационном уровне теории помехоустойчивого кодирования. Необходимость хотя бы небольшого раздела с рекомендациями в этой сфере становится очевидной ещё и в связи с тем, что, конечно, объявление об окончании затянувшегося на десятилетия кризиса многие работники научной сферы воспримут как большую неожиданность. Предлагаемые ниже направления исследований помогут многим из таких специалистов менее болезненно перейти к работе в сфере разработок по тематике кодирования. Это позволит им быстрее приобрести необходимый новый опыт, знания и уверенность в работе с декодерами как со средством поиска глобального экстремума функционала.

6.1. Алгоритмы Витерби

Появление нашей простой версии блокового АВ, несомненно, вернёт и даже усилит интерес исследователей и к свёрточной версии этого великого алгоритма. Учитывая, что АВ знаком всем специалистам, можно ожидать волну результатов, которые поднимут возможности этого метода на новый уровень, который и до этого был всегда достаточно высок.

Невозможно даже перечислить все новые темы, которые можно связать с АВ. Конечно, надо получить характеристики блокового АВ для всего спектра типичных скоростей, при которых используется свёрточный АВ. Далее было бы полезно подобрать или создать для БАВ некоторый набор кодов с «выкалыванием», которые позволят быстрее внедрить его в системы с высокоскоростным кодированием.

Огромный объём работ нужно выполнить для получения стандартного набора каскадных схем с БАВ. Важно здесь отдельно рассмотреть и каскадные коды, в которых внешние коды активно взаимодействуют с внутренним алгоритмом, как это успешно делается в КК с МПД и ККЧ.

Другое важнейшее направление для АВ обоих типов составляют методы неполного просмотра путей. Здесь есть несколько подходов,

которые все ещё весьма мало проработаны. Это трудная сфера исследований, т. к. тут надо аккуратно бороться с размножением ошибок, которое в случае АВ имеет иную природу, чем при использовании МПД. Однако успешное решение этой проблемы значительно упростит АВ и, возможно, снизит сложность вычислений на 1–3 порядка.

Представляется несомненным, что возврат к решению задач кодирования/декодирования при участии обоих типов АВ создаст условия и для решения других проблем кодирования, не упомянутых здесь, особенно систем каскадного кодирования, которыми уже очень долго не интересовались, хотя возможности микроэлектроники позволяют теперь решать все эти задачи с АВ на другом уровне.

Следует обратить внимание на то, что наши рекомендации по поводу возврата к исследованиям АВ основаны не на наших предпочтениях, а на принадлежности к декодерам группы с прямым контролем метрики обоих типов АВ и всех модификаций МПД. Все прочие методы, не включенные в эту группу, всегда решают проблемы эффективного декодирования за счёт гораздо более сложных вычислений, чем это необходимо в случае декодирования, ориентированного на оценку или, лучше, точное вычисление расстояния своих кодовых слов-решений до принятого сообщения. А так выполняют вычисления только декодеры из группы ДПКМ. Непринадлежность прочих алгоритмов к группе ДПКМ сильно ослабляет их возможности в области высоких шумов канала и переводит их в бесперспективное множество алгоритмов декодирования.

Совершенно особой задачей оказывается проблема построения некоторого аналога АВ для недвоичных кодов. Как мы уже многократно указывали на невозможность создания полного переборного АВ для больших алфавитов, сосредоточение усилий разработчиков на упрощённых его версиях будет очень полезным вариантом поиска эффективного недвоичного декодера. Особо полезным будет дивергентное соединение работы такого АВ и QMПД. Это сильно приблизит область оптимального декодирования символьных кодов к границе Шеннона.

6.2. Алгоритмы МПД

Достигнутые высокие характеристики эффективности МПД декодеров в областях, непосредственно близких к границе Шеннона, являются уникальными и всеобщими по быстродействию, что обеспечивается применением в этих алгоритмах процедур поиска глобального экстремума функционалов с линейной от длины кода сложностью.

При дальнейшем развитии этой тематики нужно искать способы ускорения сходимости к решению ОД. Он должен остаться поиском

глобального экстремума, а именно минимально возможного расстояния до принятого сообщения. Но нужно двигаться к нему быстрее, а не по одному символу, т. е. вместо обычного порогового элемента нужно найти не очень сложную другую решающую функцию перехода к более правдоподобному кодовому слову. Они существуют и число их, вообще говоря, велико. Из них нужно выбрать такую, у которой будет лучшая сходимость при минимальной её сложности по числу операций. Это дополнительно повысит допустимый уровень шума, при котором решения МПД достаточно быстро сходятся к решению ОД.

Подчеркнем, что эта единая задача стоит и для символьных МПД, причём ещё актуальнее, т. к. символьные МПД очень далеко обошли все прочие методы по эффективности при большом шуме, но расстояние до пропускной способности у них тоже пока большое, т. к. все специалисты пока что больше усилий тратили на двоичные коды в гауссовских каналах. Но для символьных кодов выбор других решающих функций вместо пороговых гораздо шире, чем у двоичных. При этом надо особо внимательно выбирать кандидатов на решающую функцию по вычислительной сложности, т. к. в недвоичных полях выполнять вычисления всё же несколько сложнее.

6.3. Принцип дивергенции — расширение приложений

Дивергенция, как средство роста эффективности МПД и других алгоритмов декодирования, должна была возникнуть гораздо раньше. В этом случае результаты её успешного применения были бы гораздо масштабнее. Сейчас надо расширить сферу её применения и провести ревизию для того, чтобы понять, где в алгоритмах МПД она уже применялась, но не была замечена.

Фактически дивергенция проявляется во многих конкретных алгоритмах повсеместно. Например, она всегда есть при параллельном каскадировании, т. к. декодер первого уровня всегда работает с подкодом большого кода и сначала использует не все проверки. Если параллельное каскадирование трёхслойно, т. е. размеры кода увеличиваются не один раз, а дважды, а то и трижды, то получается многократное применение этого подхода.

Даже в самом простом случае реализации свёрточного МПД можно не ставить одинаковые узлы порогового декодирования один за другим, а частично совместить их, сделать «внакладку». Тут тоже может оказаться, что первый пороговый элемент не полностью реализует кодовое расстояние, а ему помогает второй и аналогичные последующие узлы. Очень мощный синергетический эффект образуют параллельные методы каскадирования вместе с идеей дивергенции, когда одновременно 2-й и 3-й уровни дивергентности совмещаются и

большой скачок роста кодового расстояния при выполнении некоторых полезных условий сильно улучшает процесс декодирования.

Но особенно большой эффект от использования дивергенции может быть получен от того полезнейшего свойства кодов, которое состоит в том, что многие коды допускают применение различных алгоритмов декодирования, например АВ и МПД. Предварительные опыты уже показали перспективность такого подхода. Несомненно, он может существенно улучшить итоговую эффективность декодирования, возможно, даже при некотором упрощении декодера. Но эта тонкая работа требует большой предварительной подготовки.

Возможно, что через некоторое время работы, предлагаемые в предыдущем абзаце, выйдут на столь высокий уровень, что будут найдены способы достигать на группах различных пороговых узлов столь же высокой эффективности работы при большом уровне шума, которая обеспечивается с помощью АВ. Разумеется, подбор для этого особых пороговых элементов с разными настройками потребует определённого времени. Но если и эта работа будет успешной, создание высокоскоростных МПД даже у самой границы Шеннона будет успешно решённой проблемой.

6.4. Конвергенция решений

Если дивергенция для свёрточных кодов оказывается полезнейшим средством роста эффективности, то в квазициклических блоковых кодах гораздо проще и эффективнее применять различные методы конвергентного (сходящегося) типа.

Эта простая, но вполне заслуживающая внимания идея состоит просто в том, что блоковый код несколько раз декодируется, реализуя сходимость к некоторому промежуточному решению при большом шуме из совершенно различных исходных состояний настроек элементов МПД. При высокой производительности микроэлектроники и не очень большой скорости передачи по некоторым каналам многократные попытки декодирования блока будут естественным решением. Получившиеся решения весьма различного вида, не все совпадающие между собой во множестве позиций декодируемого блока, переоцениваются, например, мажоритарным образом посимвольно и отправляются снова на конечную обработку или на реализацию такой же следующей параллельной процедуры обработки, которая была на первом этапе. Учитывая, что МПД многократно проще других методов, обработка блока несколько раз может, таким образом, повысить эффективность декодирования, но оставить МПД в той же позиции самого быстрого алгоритма среди известных на данный момент. Предварительные эксперименты показали, что это очень полезный подход.

Он решает все те вопросы, которые не могут решить многие «новые» алгоритмы декодирования. Наверное, понятно, что аккуратность и изобретательность при такой постановке задачи декодирования тоже необходимы.

6.5. Комплексный подход

Большое число способов улучшения возможностей различных схем с АВ и МПД позволяет реализовать их в различных сочетаниях или почти все вместе. При этом и АВ, и процедуры МПД остаются столь же простыми и однородными, как их исходные версии.

Однако наибольший эффект от перемещения всех поисков лучших декодеров в область оптимизации на базе ПГЭФ расширяет пространство этих поисков просто безгранично. Сюда легко подключаются уже проверенные полезные методы вариации весов полиномов, расстояний между ПЭ, изменения параметров алгоритмов и просто их полной замены. Но несомненно, что будут реализованы и совершенно неизвестные пока эффективные методы. Здесь всегда актуальной будет задача сохранения при всех модификациях максимальной простоты и однородности АВ и МПД.

Мы уверены, что бескрайние просторы возможностей и ресурсов оптимизации, как показало последнее десятилетие развития ОТ и МПД, обеспечат создание многих новых и простых алгоритмов коррекции ошибок для космоса, сетей и всего цифрового мира.

Заключение

Совсем недавно состоялся юбилей воистину великой статьи К. Шеннона [14], которая была опубликована более 70 лет назад и дала начало масштабным исследованиям мирового научно-технического сообщества по созданию тех очень нужных нашей цифровой информационной цивилизации методов коррекции ошибок в дискретных данных, о существовании которых нам было точно и доступно сказано в этой работе. Наша научная школа Оптимизационной Теории (ОТ) тоже активно участвует в решении проблемы помехоустойчивого кодирования, о чём свидетельствуют сотни наших публикаций, новые работы и монографии [4, 5, 79, 90, 91, 94, 100]. Они продемонстрировали исключительно широкие возможности мажоритарных методов на основе ОТ во всём множестве классических каналов, изучаемых теорией. Результатам успешного завершения поисков этих и ряда других методов и посвящена данная монография научной школы ОТ, в которой, как полагают сторонники нашего научного направления, наконец убедительно решена действительно великая проблема, сформулированная в той юбилейной публикации.

В данной книге дано полное решение поставленной К. Шенноном задачи предельно простого и эффективного исправления ошибок в цифровых потоках для всех основных моделей цифровых каналов связи. Технологии ОТ успешно работают вплоть до областей шума, непосредственно близких к границе, известной как пропускная способность канала, которую чётко указал этот великий американский учёный. Данная граница недостижима, так как она абсолютно упруга, как и скорость света для материальных тел. Но к настоящему времени для всех главных в теории типов каналов в ОТ уже существуют технологии создания декодеров, успешно работающих непосредственно в ближайшей от этой границы области энергетики и/или вероятностей ошибок или стираний, чем и завершён принципиальный и сложнейший полувековой процесс поиска технологичного и простого решения проблемы Шеннона. То вполне небольшое оставшееся расстояние до границы, указанной им, можно пройти (конечно, только частично!) с помощью методов, которые уже разработаны или ещё будут созданы в процессе последующих исследований Оптимизационной Теории (ОТ) помехоустойчивого кодирования и других методов. Бесконечно высокая упругость пропускной способности канала будет и в дальнейшем очень неохотно допускать работу реальных алгоритмов декодирования при экстремально высоких уровнях шума. Так что полученный результат — это действительно очень хороший компромисс с природой, совсем небольшая плата ей за линейную сложность МПД ал-

горитмов вместо экспоненциальной, которая раньше требовалась для достижения решения оптимального декодера (ОД).

Все полученные к настоящему времени результаты по энергетике и вероятностным характеристикам наших декодеров ориентировочно для ста наиболее значимых существенно различных кодовых кластеров (типичных наборов параметров кодов, декодеров и каналов) теперь уже ясно демонстрируют, что проблема простого и эффективного декодирования в каналах с независимым искажениями полностью решена. Для этого созданы и уже давно активно применяются понятная специалистам тонкая теория вместе с мощным набором разнообразных технологий и программных средств проектирования, исследования и настройки кодеков (кодеров и декодеров), практически всегда позволяющие разрабатывать необходимые системы кодирования приемлемой сложности, эффективности и достоверности для работы вблизи пропускной способности канала связи.

Мы полагаем, что алгебраическая теория была хорошей учебной стартовой площадкой на начальных этапах исследований алгоритмов коррекции ошибок. В первые десятилетия своего развития она позволила приобщить к теории кодирования высокопрофессиональные кадры научного сообщества. А теперь уже полностью состоялась передача эстафеты лидерства от прежней алгебраической к Оптимизационной Теории (ОТ) помехоустойчивого кодирования во всех прикладных аспектах. На этом новом этапе своего развития ОТ, как и раньше, будет расширять сферу своих исследований.

В монографии были представлены мощные технологии разработки алгоритмов МПД декодирования для четырёх главных классических каналов теории помехоустойчивого кодирования с минимальной теоретически возможной линейной от длины кодов сложностью и одновременно (!) с эффективностью, практически совпадающей с оптимальным декодированием (ОД) вплоть до ближайших окрестностей границы Шеннона, для которого ранее практически всегда требовалось осуществление полного, экспоненциального от длины кода перебора всех возможных решений. При этом ширина недоступной пока для работы МПД декодеров области вблизи границы Шеннона уже достаточно мала. Возможно, размер этой зоны можно будет ещё несколько уменьшить в будущем. Но это уже чисто технологический вопрос.

Эффективность и быстродействие наших методов подтверждается интерактивным взаимодействием монографии с нашими крупнейшими в мире порталами по Оптимизационной Теории (ОТ) кодирования www.mtdbest.iki.rssi.ru и www.mtdbest.ru. Десятки представленных на них демонстрационных модулей и новейшие программные платформы

для декодеров различного типа, в том числе и не относящихся к алгоритмам ОТ (!), особенно наглядно демонстрируют высокую достоверность, помехоустойчивость и уникальное быстродействие наших методов, большинство из которых (около 40) запатентовано в России, за рубежом и даже ещё в СССР.

Все основные характеристики наших алгоритмов, судя по текущей ситуации в прикладных результатах теории кодирования, стали уже недоступны никаким другим методам коррекции ошибок с сопоставимой сложностью, причём разница между ними, насколько нам известно, очень велика. Это следует из того, что по триединому комплексному критерию «помехоустойчивость — достоверность — сложность» методы ОТ имеют абсолютно наилучшие возможные значения и по каждому из параметров критерия в отдельности. А все без исключения алгоритмы, развиваемые вне парадигм ОТ, не удовлетворяют этому критерию ни по одному параметру. Более того, их отставание от технологий ОТ очень значительно, что подтверждают наши новые обзоры по прикладным вопросам теории кодирования, которые можно найти в основных журналах по телекоммуникациям, в наших докладах на конференциях, а также просмотреть по ссылкам на наши новые публикации с номерами [73] и далее в конце данной монографии.

Вновь подчеркнем, что ни один параметр триединого критерия вообще не может быть вычислен для какого-либо алгоритма декодирования вблизи границы Шеннона сколько-нибудь точно. Иначе говоря, прежняя прикладная теория кодирования не научилась за 60 лет своего как бы «активного» существования даже просто определять эти самые главные параметры для хотя бы каких-либо эффективных алгоритмов вблизи пропускной способности каналов, т. е. она так и не умеет вообще ничего. Но этого никто, да и, видимо, никогда и не сможет! А масштабные интеллектуальные программные средства ОТ, активно помогающие в течение 50 лет теории ОТ ускоренно решать все проблемы в сфере кодирования, определяют все указанные выше параметры этого критерия практически мгновенно. И такого ПО до сих пор, видимо, нет ни у одного занимающегося кодами научного коллектива в мире. А тем самым и завершён глобальный конкурс алгоритмов в теории кодирования. У нашей ОТ конкурентов просто не оказалось! Но они нужны! С ними интереснее. Ну, будем искать.

Но есть ещё важнейшее обстоятельство при обсуждении конкурса алгоритмов и их параметров триединого критерия для большого уровня шума. Невозможность аналитической оценки главных свойств декодеров не позволяет кому-либо из специалистов, оставшихся в рамках «прежней» теории, создавать реальные эффективные

алгоритмы, поскольку оценить их характеристики в больших шумах, что нужно для успешного решения проблемы Шеннона, чисто теоретически совершенно невозможно. И, наверное, так будет всегда! Именно эта причина обеспечивает абсолютное лидерство ОТ в решении проблемы Шеннона, т. к. созданное школой ОТ за полвека многоцелевое интеллектуальное инновационное программное обеспечение (ПО) наряду с решением множества различных сложнейших проблем развития позволяет — и это самое главное! — практически мгновенно определять все эти три параметра критерия. Такое уникальное для мира теории кодирования ПО школы ОТ как раз и позволяет быстро создавать, корректировать и ускоренно развивать алгоритмы ОТ так, чтобы они в очень хорошем темпе приобретали наилучшие возможные характеристики. Это — главная причина исключения алгоритмов декодирования за пределами ОТ из всех конкурсов проектируемых и исследуемых декодеров. И снова укажем, что алгоритмы ОТ уже давно являются теоретически наилучшими по всем параметрам комплексного критерия: минимально возможная сложность, наивысшая оптимальная достоверность и максимальная близость области работы к пропускной способности цифровых каналов.

К сожалению, приведённые выше суждения при более строгом к ним отношении оказываются довольно беспредметными по одной довольно веской и грубой причине. Дело в том, что нам неизвестны никакие научные группы, которые за последние 30 лет предъявили вообще хотя бы один алгоритм, который можно было бы внимательно проанализировать по триединому критерию, просмотреть программу его реализации, например, хотя бы на языке C++ и «вживую» замерить её производительность. Таких предъявленных для сравнения алгоритмов просто вообще ни у кого нет! А это значит, что и обсуждать проблемы теории кодирования на содержательном уровне нам пока просто вообще не с кем. В связи с этим укажем тут ещё раз, что в наших книгах и на сетевых порталах школы ОТ приведены десятки демо-программ и представлено множество программных платформ, которые всегда непосредственно готовы показать специалистам все параметры упоминавшегося выше критерия для тысяч кодов, для которых можно именно «вживую» запустить МПД декодеры разных типов на этих платформах и мгновенно оценить все необходимые свойства кодов и алгоритмов. Т. е. у нас всё создано, работает и готово к использованию в разработках и исследованиях.

Но более того, мы выполнили за кого-то и совсем чужую работу: на наших порталах есть написанные нами демо-программы и для алгоритмов, не относящихся к ОТ. Посмотрите их тоже!

Важность сбалансированного развития теоретических и экспе-

риментальных исследований стала осознаваться во многих отраслях мировой науки ориентировочно с 80-х годов XX века и к концу тысячелетия уже активно и всесторонне учитывалась при различных исследованиях. Теория сама по себе всегда слаба и очень ограничена, а эксперимент, поставленный без теоретической поддержки, почти всегда неточен или даже просто ошибочен. Наша научная школа осознала эту взаимосвязь в науке где-то в 70-х годах. Некоторые важнейшие статьи по этой болезненной для теоретиков тематике можно было найти даже на портале РАН [96]. Приведём ряд выдержек из такой публикации: «Противостояние компьютерного моделирования и теории, основанной на математических методах, — болезнь века... Теоретик, работающий в любой научной области, знает, что далеко не все задачи можно решить аналитически: для подавляющего большинства проблем получить точные и даже приближенные решения не удается... Комбинирование возможностей теории и моделирования — особая профессия, требующая сочетания навыков и талантов, необходимых теоретикам прошлого века и специалистам по компьютерному моделированию современности».

В наших исследованиях в рамках ОТ как раз правильная балансировка идей, методик, парадигм и теорем тонкой оригинальной теории с изощрённым оптимизационным моделированием обеспечила грандиозное синергетическое ускорение наших работ, позволивших в итоге решить великую проблему Шеннона тогда, когда весь мир отстал от нас, возможно, на 20–30 лет. Но и многие наши важнейшие результаты даже 35-летней давности до сих пор не повторил пока никто. Но это понятно почему: ни у кого нет вообще никакого программного обеспечения для работы с кодами, которое может создать только специалист, активно и глубоко занятый проблемами теории кодирования и хорошо понимающий ценность и возможности вычислительной техники с правильно выбранным ПО. Значит, таких пока и нет. Но следует заметить, что выбрать ПО для работ по кодированию и затем как-то заполучить его просто в принципе невозможно. ПО создаётся только самими специалистами по кодированию, и для этого требуются очень долгие годы! И тут ещё надо очень хорошо понимать, какой должна быть создаваемая экспериментальная база и что же именно должно уметь делать такое ПО. А это тоже требует немалого числа лет очень глубоких раздумий и разностороннего опыта.

В связи с этим мы полагаем также крайне важным и просто жёстко настаиваем на том, что исключительно для избавления научного сообщества от обмана и фальсификации научных результатов в теории кодирования, которые поразили вообще всю прикладную часть

нашей отрасли науки, в ближайшие годы следует допускать к публикации и защите диссертаций только реальные полезные научные работы. В них должны быть точно и строго описаны и проанализированы предлагаемые их авторами алгоритмы коррекции ошибок. Но при этом также обязательны к предъявлению и сами работающие алгоритмы. Они должны быть реализованы на языке C++, который позволяет писать программы с малыми накладными расходами сверх собственно операций декодера, а также допускает их полную проверку экспертами по прикладным вопросам теории кодирования и методам моделирования этих алгоритмов при большом уровне шума. Школа ОТ для калибровки сложности декодеров, т. е. скорости предлагаемых авторами новых алгоритмов, уже давно подготовила простую демо-программу на портале **www.mtdbest.ru** (см. гиперссылку [70] и краткое описание методов её использования [71]). Она общедоступна, готова для использования, понятна и абсолютно необходима для правильной оценки разработок всех новых алгоритмов декодирования, создаваемых специалистами.

Малые накладные вычислительные расходы языка C++, его свойства и некоторые элементы языка высокого уровня, а также другие его достоинства определяют совсем умеренные в этом случае требования к способностям авторов новых алгоритмов создавать их программные реализации. Такой подход к оценке новых результатов в прикладной теории кодирования с калибровкой параметров эффективности и производительности позволит, в основном, достаточно правильно оценивать реальные уровни сложности, достоверности и помехоустойчивости предлагаемых новых декодеров. Столь естественный уровень контроля правильности оценки основных свойств методов декодирования сразу наведёт порядок в прикладном научном уровне разработок всех типов декодеров. Только такое отношение к созданию алгоритмов декодирования, ни в какой мере не являющееся жёстким, позволит сразу избавиться от безбрежного потока фантазий, ошибок и просто откровенного обмана в исследованиях прикладных вопросов в сфере корректирующих кодов.

Мы не можем не выразить здесь и наше глубочайшее сожаление о том, что лозунг конца того тысячелетия: «Программирование — вторая грамотность!» — уже давно и прочно забыт. Его последствия для науки, как мы видим, тоже весьма трагичны. Без способностей к моделированию в науке делать вообще нечего (вспомните ссылку [96])! Ну, конечно, если при этом и теоретические разработки также ведутся на действительно высоком уровне.

Сторонники нашей школы всегда доступны для консультаций и с удовольствием будут всесторонне помогать авторам всех новых ал-

горитмов, которые будут иметь высокие реальные характеристики декодирования при малых отношениях сигнал/шум цифрового канала.

Нет сомнения, что активно развиваемая уже почти пять десятилетий ОТ и далее будет обязательно находить новые методы разработки декодеров и для таких проектов, когда имеющихся технологий создания эффективных кодеков вблизи границы Шеннона окажется в отдельных случаях всё же недостаточно. При этом нужно чётко понимать, что трудный процесс проектирования систем помехоустойчивого кодирования в дальнейшем будет развиваться только вместе с прогрессом широкомасштабных программных систем оптимизации и мощных комплексов поиска глобальных экстремумов функционалов всё более сложной природы, которые активно и теперь уже фактически повсеместно применяются в ОТ. Таким образом, дальнейший прогресс в создании технологий декодирования вблизи границы Шеннона будет ещё более жёстко связан с развитием компьютерной техники и со специальным программным обеспечением, чем ранее. Это вполне естественный ход развития реальных, а не кабинетных наукоёмких инновационных технологий. И, наверное, сейчас это единственный конструктивный путь. Наша научная школа ОТ и далее будет напряжённо работать, чтобы оставаться в лидерах теоретических научных исследований и разработок, а также поддерживать новых российских «Ньютонов», которые придут в обновлённую теорию кодирования.

Ключевым моментом полного успешного разрешения сложнейшей проблемы цифрового мира стало глубокое понимание теперь уже многими специалистами того важнейшего обстоятельства, что достижение, казалось бы, несбыточной мечты специалистов цифровой связи обеспечили именно методы теорий поиска глобального экстремума функционалов (ПГЭФ) в специфических условиях работы на массивах со свойствами корректирующих структур. Никаких оснований считать, что здесь конкурентоспособными будут и какие-либо другие методы, пока нет и, скорее всего, никогда не будет. Лучшего даже в теоретическом смысле уровня по достоверности и сложности, чем у ОТ, достичь уже в принципе невозможно. При этом и в плане близости к границе Шеннона сотни уже созданных версий МПД декодеров также оказались существенно лучше прочих известных подходов к коррекции ошибок. Это значит, что никаких вариантов появления других теорий столь же технологичного и особенно простого типа просто не предвидится. Пока лишь теории ПГЭФ и позволяют рассматривать только методы поиска оптимальных решений декодеров типа МПД со сложностью, пропорциональной длине кода. Другие методы с такой сложностью неизвестны.

Однако этот подход к проблеме декодирования оказывается рабо-

тоспособным только тогда, когда одновременно с разработками различных версий МПД декодеров правильно и абсолютно точно решается и задача выбора кода с низкими уровнями подверженности воздействию размножения ошибок (РО). А проблему малого РО правильно оценила и создала её отдельную полную содержательную теорию опять же только единственная в мире школа ОТ. Никакие иные группы специалистов за последние 50 лет не смогли даже просто правильно сформулировать для себя такую проблему. Действительно, без понимания философской глубины идей мажоритарных алгоритмов даже только правильно поставить задачу борьбы с группированием ошибок в МПД декодерах не получится.

Мы также с удовлетворением отмечаем запатентованный нами алгоритм Витерби для блоковых кодов (БАВ) со сложностью аналогичных ему АВ декодеров для свёрточных кодов. Это соответствует уменьшенной вдвое экспоненте сложности блокового ОД, полученной в рамках прежних методов «теоретически». К сожалению, этот исключительно грандиозный по числу операций ОД с удвоенной экспонентой по сравнению со свёрточным идеальным алгоритмом Витерби уже много лет крайне агрессивно предлагается для изучения в ВУЗах [116], что абсолютно недопустимо. Как известно, NASA создала АВ декодер для кода длины $K = 15$. Наш БАВ был бы для аналогичного блокового кода в 16 000 раз проще, чем предлагает «та» теория.

Наш БАВ полностью исключил из любых конкурсов для блоковых кодов методы, наработанные алгебраической теорией, в частности Чейза, Велдона и проч. Новые патенты на наши БАВ в школе ОТ уже также начали оформляться. И мы испытываем вполне понятное глубокое заслуженное удовлетворение от того, что именно классические великие алгоритмы мажоритарного типа и оптимальные АВ декодеры снова абсолютно обоснованно заняли главные позиции на Олимпе лучших алгоритмов коррекции ошибок для цифровых каналов.

Объединение всех типов АВ и различных модификаций МПД в группу ДПКМ декодеров, особых алгоритмов, единственных точно измеряющих расстояние своих решений до принятого сообщения, также абсолютно однозначно указало множество методов, которые, видимо, и далее будут решать все проблемы создания хороших во всех указанных выше смыслах декодеров. Скорее всего, все новые алгоритмы последнего тридцатилетия, никак не связанные с теориями поиска глобального экстремума и обязательным точным измерением указанных расстояний даже в предположении возможности дальнейшего роста их сложности, не имеют ни перспектив движения к границе Шеннона, ни, тем более, других вариантов для развития. В

самом деле, для алгоритма, который не измеряет расстояний от своих решений до принятого сообщения, велика вероятность, что он «не увидит» и уже достигнутого решения ОД, вследствие чего он пройдёт мимо него. Понятно, что в нашей теории ОТ такая ситуация просто невозможна.

Не стоит даже останавливаться на истории рекламы и краха полярных кодов, которые стали, как мы думаем, ещё одной показательной катастрофой «прежней» теории, иллюстрирующей необходимость всегда решать научные проблемы только точно подобранными адекватными средствами. Несколько последних статей школы ОТ по кодам, где упоминались и полярные коды, можно посмотреть на наших порталах [40] и в обзорах [74, 90, 92, 93, 98, 103, 108]. Мы не намерены в дальнейшем возвращаться к этой проблеме, так как нас ожидают более актуальные и конструктивные задачи следующего этапа развития ОТ. И мы крайне сожалеем, что мы оказались сейчас единственным в стране (а возможно, что и в мире!) научным коллективом, который имеет право и даже просто обязан во спасение прикладной теории кодирования регулярно писать обзоры по этой теме. Однако более поручить эту сложнейшую многофакторную работу просто абсолютно некому. Но мы очень хотели бы найти таких мудрых коллег, с которыми можно было бы обсуждать все сложнейшие и интереснейшие проблемы развития нашей тематики, важнейшей для всего цифрового мира.

Разумеется, конкретные реальности уже ближайшего времени строго проверят правомерность нашего весьма жёсткого мнения по всем затронутым выше вопросам.

Таким образом, ОТ приняла во всём объёме эстафету развития прикладных методов от прежней теории. Это неудивительно, так как алгебраическая теория за многие годы своего очень условного лидерства не решила никаких основных проблем своего развития: не нашла простых способов коррекции ошибок выше уровня половины кодового расстояния, не преодолела сложностей декодирования блоковых кодов в гауссовских каналах, а также не вышла на линейный от длины кодов уровень сложности декодирования.

Необходимо, как мы полагаем, особенно отметить, что технологии микроэлектроники позволяли создавать АВ декодеры даже для кодов с длиной $K \sim 15$ ещё в том тысячелетии. Так что возрождение внимания к АВ и его новым модификациям, которыми мы тоже занимаемся, будет, несомненно, весьма масштабным. ОТ уже вносит свой вклад и в это прикладное направление, изучает характеристики блоковых АВ и патентует новые лучшие схемы такого класса. Возврат глубокого внимания к АВ обусловлен именно тем, что АВ —

простейший по логике идеальный оптимальный декодер (ОД), очень технологичный и понятный для инженеров. Именно поэтому он теперь снова будет развиваться и применяться. Однако забывшие и о нём теоретики просто не могли смоделировать даже его крайне простую схему, которая много лучше всех вариантов полярных и очень многих других «новых» кодов. Но это — проблемы «теоретиков».

Таким образом, поставленная Шенноном проблема решена в ОТ путем использования на различных шагах создания систем декодирования мощных оптимизационных процедур, в том числе на основе поиска глобального экстремума функционалов (ПГЭФ). Конечно, по мере приближения рабочей области систем кодирования к пропускной способности канала количество необходимых декодеру операций будет несколько расти, что вполне понятно. Неизбежный при этом значительный рост задержки принятия решений тоже очевиден и при большом шуме просто обязателен, так как работать вблизи пропускной способности канала могут всегда только весьма длинные коды.

Перечислим основные оптимизационные процедуры проектирования алгоритмов ОТ. В первую очередь, конечно, это собственно МПД алгоритм, настраиваемый на приближение при каждом изменении контролируемых символов к оптимальному переборному (!) решению при собственной минимальной линейной сложности. Это типичная задача поиска глобального минимума функционала в дискретных пространствах с явно выраженной корректирующей структурой.

Вторым мощным оптимизационным средством, используемым при создании эффективных МПД или ДПКМ алгоритмов, стали методы поиска кодов, в наибольшей степени соответствующих критериям минимума размножения ошибок (РО) при декодировании. Для этого была создана абсолютно уникальная теория РО, совершенно не похожая на попытки 50-летней давности крайне примитивно описать этот сложнейший процесс для мажоритарных схем. Оптимизация кодов сразу по нескольким критериям РО многократно улучшила сходимость МПД методов к оптимальным решениям.

Наконец, третьим и, безусловно, самым сложным образцом успешного использования процедур глобальной оптимизации оказался целый класс методов комплексной настройки различных элементов МПД декодеров. Эта гигантская по трудоёмкости проблема, превышающая в сотни раз затраты сил и времени на обе первые методики, потребовала и разработки эффективных способов ускорения процессов такой настройки, что также было сделано в кратчайшие сроки. Результаты создания мощных систем настройки сотен и тысяч элементов МПД при большом разнообразии целевых функций такой настройки декодеров дополнительно многократно повысили темпы схо-

димости решений МПД к оптимальным.

Совокупность этих трёх базовых подходов и стала ядром тех методов, которые в синергетическом взаимодействии довели эффективность МПД по сложности, помехоустойчивости и достоверности до уровня, который уже давно в принципе не доступен никаким другим методам «прежней» теории кодирования. И все эти результаты стали возможными только благодаря совместному развитию теории ОТ и специального интеллектуального оптимизационного ПО.

Нелишне в этой связи ещё раз напомнить уже давно сформировавшееся мнение математиков о том, что роль теорий оптимизации в математике столь же велика, как и роль математики вообще в науке.

Таким образом, затянувшийся на многие десятилетия из-за обычного в науке человеческого фактора с 80-х годов прошлого века очень болезненный переход к созданию эффективных декодеров именно на базе теорий глобальной оптимизации сложных функционалов завершен. С появлением в 1990 году нашей ОТ эта полная прикладная теория кодирования вышла из слишком длительного подготовительного как бы «классического» алгебраического этапа и перешла к широкому применению мощных и быстрых оптимизационных методов декодирования для всех технических систем, обеспечивающих простыми средствами высокую достоверность при экстремально большом шуме.

Так что теперь и нам, и очень многим специалистам ясно, что теория кодирования — вовсе не математическая проблема. Она не решила никаких поставленных перед ней прикладных задач. Вынужденно повторим, что неразрешённые противоречия прежней прикладной теории, до сих пор вообще абсолютно не признаваемые её адептами, кратко описаны в [96].

Важно также указать, что значительный вклад в развитие ОТ и её технологий вносят такие новые руководящие парадигмы, которых вообще не было до появления нашей теории: символьные коды и декодеры, дивергенция, каскадирование параллельное и с кодами контроля по чётности (ККЧ), БАВ, быстрые алгоритмы восстановления стираний и правило ДПКМ, чётко рекомендующие к реализации те или иные методы из всего большого набора мощных технологий ОТ. Наиболее важную роль здесь, по нашему мнению, играет принцип дивергенции, а также параллельное каскадирование, которое впервые предложила тоже именно наша научная школа [52].

Упрощённые 3D-системы каскадирования тоже заслуживают внимательного изучения.

Широкий спектр потенциальных возможностей новых направлений разработок алгоритмов декодирования, кратко описанный в по-

следних разделах нашей книги, также свидетельствует о совершенно безграничных перспективах ОТ — новой «квантовой механики» теории информации.

Мы полагаем, что читатели этой монографии будут абсолютно согласны с нами в том, что мы не затрагивали в ней (как и других наших книгах) особенности организации ускоренного технического развития в корпорациях, производящих аппаратуру помехоустойчивого кодирования. Они функционируют по совершенно особым своим законам. А мы обсуждали здесь только вопросы развития научного знания, которые и без того чрезвычайно сложны.

Просмотрев немалое количество публикаций большого числа авторов, пишущих статьи «про коды», что делалось в поисках коллег, с которыми можно было бы наладить сотрудничество по новым направлениям ОТ, мы испытали ещё одно огромное разочарование. Уже в нашем тысячелетии продолжаются «исследования» и докторские защиты по «интереснейшим» темам, которые мы полагаем насмешкой над наукой. Например, в нашем веке, как ещё и в самом конце прошлого, очень популярны темы снижения экспоненты сложности декодирования в 2–3–5 раз по сравнению с полным перебором. Причём нередко эти «результаты» оказываются практически единственными, которые в их диссертационных работах вообще можно как-то обсуждать. Но это значит, что даже для относительно коротких кодов длины $n \sim 10^4$ соответствующие «декодеры» должны выполнить порядка $N \sim 10^{200}$ операций, что на много порядков превышает число атомов во Вселенной. И авторы таких «работ» как-то «не заметили», что простейшие оптимальные декодеры с линейной, т. е. минимально возможной сложностью есть уже даже в нашем справочнике 2004 года [1], а также были опубликованы в 1981 г. в [37], в [2] в издательстве «Наука», в 1981 г., в диссертации 1978 г. [38], а также в 1990 г. в другой диссертации [36]. Про абсолютно неприемлемый по сложности блоковый аналог декодера Витерби уже был комментарий на предыдущих страницах.

Кроме того, огромный поток статей «о быстром декодировании» кодов Рида — Соломона и многих прочих чудесах «прежней» теории, везде со сложностью, как и раньше, порядка $N \sim n^2$, а то и более, также не демонстрирует знаний таких «учёных» о наших символьных кодах также с линейной сложностью и оптимальным декодированием, т. е. при $N \sim n$, которые уже давно даже помещены в справочник [1]! И ведь это всё тоже было опубликовано нами в изданиях Научного совета по комплексной проблеме «Кибернетика» АН СССР ещё в 1985 г. [39] (!), как и в десятках других статей и докладов тоже в том тысячелетии. Большое множество подобных непостижимых при

нормальном развитии науки ситуаций, как и раньше, сопровождают развитие воистину актуальнейшей из информационных наук при формировании цифрового мира в течение всех 50 лет существования ОТ.

Таким образом, у той «теории» и её адептов нам найти ничего конструктивного не удалось.

Желающие могут ещё посмотреть также работы известнейших специалистов немногих «цитаделей» нашей отрасли науки на портале **www.mathnet.ru**. Там очень легко найти декодеры, которые работают при уровне входного шума, на 2 порядка (!) меньшем, чем это могли делать ещё 60 лет назад очень слабые уже тогда коды БЧХ. Зато всё это удалось посчитать?! Увы, это всё «научные труды» тех жертв науки, которые не поспевают за её развитием, т. е. на самом деле в принципе не желают поспевать. И таких «чудес» у подобных разных как бы «математиков» непозволительно много. А наша крайняя непочтительность к этим публикациям определяется как экстремально слабыми их результатами, которые просто нельзя было публиковать даже 50 лет назад, так и абсолютной невозможностью проверки правильности публикуемых ими данных вообще. В связи с этим мы вынуждены снова обратиться к нашему буклету [90] и к статье [96], мнение автора которой является выстраданным результатом проверки очень многих теоретических «шедевров». Этот печальный огромный список катастроф научных биографий, спровоцирован самими создателями подобных «достижений». Они уже более 40 лет прекрасно существуют вне реальной науки и не замечают, что она уже ушла на десятилетия далеко вперёд и даже скрылась где-то там за горизонтом. Столь невероятная трагическая ситуация безответственного игнорирования развития науки и затаптывания чужих идей ещё ждёт своих строгих аналитиков. Нашу отрасль науки давно пора лечить.

Так что наша самая современная и обогнавшая всех ОТ давно поняла, что она должна только сама создавать условия для воспитания новых молодых образованных кадров, на которые только и остаётся надеяться в ближайшие годы. Именно эту работу и проводят одиннадцать наших книг, сотни статей, справочник, обзоры и наши самые большие в мире учебно-методические порталы по современным методам помехоустойчивого кодирования с описанием технологий, парадигм, методик, демо-программ и специальных удобных программных платформ для реальной научной, учебно-педагогической и просветительской работы.

Мы полагаем, что объявить о полной смене лидирующей идеологии в прикладной теории кодирования можно было ориентировочно 15–20 лет назад, когда уже давно была создана теория ОТ, решены все принципиальные вопросы эффективности по всем алгоритмам, в

том числе для символьных кодов, для стирающих и для ДСК каналов. Напомним, что полная теория ОТ была завершена во всех аспектах ещё раньше, к 1990 году [36]. В это же время для гауссовских каналов МПД алгоритмы успешно работали при энергетике, превышавшей уровень границы Шеннона примерно на ~ 2 дБ. Однако уровень развития и быстродействие доступной вычислительной техники и созданного нами ПО ещё не позволяли нам в те годы найти коды и такие методы оптимизации, которые приблизили бы рабочую область МПД алгоритмов к пропускной способности гауссовского канала хотя бы до уровня полутора децибелов. Поэтому мы ответственно приняли тогда единственно правильное решение сначала дополнительно улучшить достигнутые к тому времени характеристики МПД декодеров в гауссовских каналах и только после этого объявить о нашем полном решении поставленной К. Шенноном задачи.

Сейчас вполне реализуемые МПД алгоритмы, например, в гауссовских двоичных каналах работают при относительной энергетике, которая по мощности лишь на 26 %, т. е. только на 1 дБ, превышает уровень абсолютно упругой и в принципе вообще недостижимой границы Шеннона. Такие характеристики уже недоступны никаким другим алгоритмам декодирования. Получены и проверяются уже и ещё более впечатляющие результаты. Это и позволяет нам заявить именно теперь о полном переходе лидерства во всех прикладных вопросах в теории кодирования к новой «квантовой механике» теории информации, названной нами Оптимизационной Теорией помехоустойчивого кодирования. Мы с удовлетворением отмечаем, что весь мир быстро разбирается в реальных проблемах кодирования и неплохо понимает нашу ОТ.

Представленная на рис. 1 (слайд из [90]) структура ОТ показывает её основные компоненты. Темы 1, 2 и 3, как видно на рисунке, мы

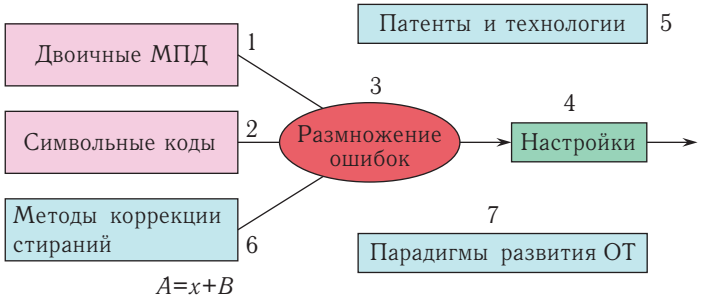

Рис. 1. Открытия Оптимизационной Теории:
1, 2, 3 — нобелевские достижения (после 60 лет застоя!);
4, 5, 6, 7 — важнейшие открытия теории кодирования.

и некоторые наши коллеги уже давно относим к нашим безусловно нобелевским достижениям, а темы 4–7 содержат много принципиально важных открытий в теории кодирования. Это неудивительно, т. к. уровень текущего состояния ОТ опережает результаты всего мира примерно на 30 лет (или более?!), а для каждого из многих десятков патентов всегда есть, конечно, ещё 3–5 уточняющих его «ноу-хау». Но чтобы только просто приблизиться к нашему уровню, эти патенты и их детали надо сначала хотя бы прочесть и, конечно, понять! Мы никого не видим близкими к нам даже на горизонте.

На рис. 2 (слайд из [90]) представлен граф популярности ОТ в мире.

Rank	Country	Visitors	
1	United States	13988	45.79%
2	Not determined	10280	33.65%
3	Germany	2178	07.13%
4	Russian Federation	1607	05.26%
5	Ukraine	859	02.81%
6	China	619	02.03%
7	United Kingdom	228	00.75%
8	Kazakhstan	103	00.34%
9	Belarus	80	00.26%
10	Italy	52	00.17%

Рис. 2. Показатели популярности ОТ

Мы видим, что технологически развитые страны активно интересуются реальными достижениями научного мира, в том числе и нашими.

И, наконец, чуть детальнее рассмотрим слайд из [90] о сути оптимизационных технологий.

На этом заключительном слайде по горизонтальной оси условно отложены реалистичные цифры для обычного двоичного симметричного канала (ДСК), т. е. некоторые правдоподобные условия передачи по шумящему каналу связи.

А по вертикальной оси — также типичные вероятности ошибки на бит некоторого МПД алгоритма, потенциальные возможности которого при оптимальном декодировании изображены графиком $P_{\text{opt}}(e)$. График p_0 соответствует уровню шума в ДСК канале. Ниспадающие линии $I = 10$, $I = 20$ и $I = 30$ — примерные графики для вероятности ошибки реального МПД алгоритма с разным числом итераций декодирования. Конкретно рассчитать точное местоположение этих

графиков на слайде в ОТ тоже нельзя. Ориентировочная оценка количества необходимых для этого операций имеет абсолютно неприемлемую сложность, близкую к экспоненте от произведения кодового расстояния d на число итераций декодирования I. И ещё нужно придумать, как вывести эту формулу, если это вообще будет возможно. Но в ОТ эта ситуация типична и давно понятна. Моделирование в течение минут решает все такие вопросы абсолютно однозначно.

Отсюда ясна и вполне разумная простая технология проектирования МПД по некоторому техническому заданию (ТЗ), пример которого есть в Приложении 1 к этой монографии. Пусть для некоторого непротиворечивого ТЗ МПД должен достигнуть уровня оптимального декодирования при определённой вероятности ошибки канала (в данном примере — ДСК), которая находится в области между вычислительной скоростью канала и границей Шеннона, т. е. пропускной способностью канала для выбранной кодовой скорости. Если вероятность ошибки канала, заложенная в ТЗ, меньше этой вычислительной скорости, то для хорошего кода с малым уровнем РО никаких проблем нет и вообще без каких-либо усилий выбор нужного числа итераций решает задачу достижения оптимальной кривой на слайде. Но даже и в этом случае нужна хотя бы простейшая программа моделирования работы МПД в ДСК (для этого примера).

Если уровень шума в ДСК очень близок к границе Шеннона, то это — предмет научных исследований и здесь надо хорошо потрудиться с использованием всех ресурсов ОТ.

А вот если уровень шума ДСК больше вычислительной скорости, но не предельно высок, то это тот самый случай, когда отработанные программные оптимизационные технологии, работающие в соответствии с основными руководящими парадигмами ОТ, всегда обеспечивают достижение уровня оптимального декодирования при достаточ-

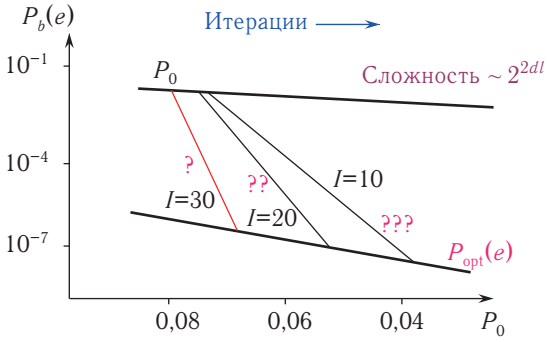

Рис. 3. Варианты стремления решений МПД к оптимальному

но высоком заданном уровне относительного шума. В этом случае в течение нескольких часов или дней создаётся один или даже несколько возможных вариантов вполне технологически реализуемого МПД алгоритма с такими параметрами триединого критерия, которые не могут теперь обеспечить вообще никакие другие методы коррекции ошибок. Тем самым и прорисовывается абсолютно точно одна из ниспадающих линий (реально, конечно, каких-то конкретных кривых) на слайде, т. е. реальных характеристик достоверности созданного МПД, которые в принципе невозможно найти аналитически. Результаты работы такой самонастраивающейся системы однозначно определяют и все параметры сложности созданного МПД.

Включение в состав проектируемых систем одной из модификаций АВ приводит к требуемому результату ещё быстрее, т. к. алгоритмы АВ всех типов по определению оптимальны и циклы настроек и оптимизации для них оказываются ещё короче.

Варианты совместного применения АВ и МПД также, видимо, будут вскоре публиковаться.

В процессе разработки алгоритмов АВ и МПД мы не смогли даже примерно указать хотя бы такое ограниченное пространство параметров систем кодирования, где бы было предпочтительнее применить другие классы методов коррекции ошибок. Пока мы полагаем, что дальнейшая разработка всех прочих известных типов декодеров, не соответствующих лучшим значениям параметров триединого критерия и свойствам алгоритмов группы ДПКМ, совершенно нецелесообразна.

* * *

Завершая столь напряжённую и трудную работу, позволим себе хорошо известный шутливый комментарий к выполненному проекту, который, как многие согласятся, относится к историческому периоду ускоренного динамичного прогресса в научно-техническом развитии.

Стадии закончившегося успешного проекта:

Шумиха,

неразбериха,

наказание невиновных,

награждение непричастных...

Если теперь вспомнить об эпиграфе американского философа перед авторским обращением к читателям, то можно проследить интересную связь его почти серьёзных слов с этим шутливым воспоминанием о реализации проектов в условиях научно-технического прогресса (НТП). В самом деле, кто, кроме нас, может сейчас «...утверждать, будто сам открыл ОТ»?

Сообразно с текущими реальностями нам кажется, что никто не

сможет объявить, что сделал всё это сам, а не мы. Ну, так не получится просто потому, что в такое (!) мало кто вообще поверит.

Т. е. великий проект завершён только нами! И — ВСЁ!

А тогда, обращаясь к приведённому выше комментарию, после окончания проекта возникает и вопрос о невиновных с непричастными. Тут опыт показывает, что конкретно и в нашем случае с непричастными во всех смыслах полный порядок. Действительно, их уже хорошо наградили, да и не один раз. Разумеется, без нас. Но мы не будем ничего конкретизировать. Тут всё хорошо. Здесь всё идёт по проторённым отлаженным схемам, т. е. как это и положено.

А вот как-то наказать — да, такое возможно. И даже кое-что уже было вполне успешно сделано. Нас недавно отлучили от РФФИ, написали забавные рецензии на некоторые наши работы, подчеркнув там много раз, что кроме кодов Рида — Соломона (РС) ничего лучшего в мире нет и быть не может, ну, и т. д. Правда, получилось это всё у них как-то очень вяло и уныло. Однако, это мелочи. Но всерьёз-то наказывать за что? Это весьма трудно. У нас всё-таки есть великие достижения нобелевского уровня по трём позициям. Маленькая научная школа ОТ обогнала весь мир на 30 (или более?!) лет. Часто ли такое бывает? Нет, ни разу не слышали. И всё-то мы делали сами, бесплатно, а не по договору, на чистом энтузиазме. Ну, а поскольку даже маленькой зацепки, никакого реального повода нет, то и серьёзного наказания, видимо, не будет.

Вот в итоге и получается, что у нас вообще-то всё в порядке.

Хорошо, что мы прожили эти годы по принципу всех пионеров: «Через тернии — к звёздам»!

Так что поздравляем всех с величайшим успехом нашей науки!

* * *

И в заключение подчеркнем, что огромное разнообразие всевозможных схем глобального поиска образует совершенно грандиозное интеллектуальное поле для создания самых неожиданных новых кодов, алгоритмов и технологий. На их основе, как мы уверены, новые талантливые исследователи, молодые российские «Ньютоны», проектировщики и инженеры впишут следующие страницы в ОТ и предложат нашей цивилизации самые лучшие технологичные и быстрые системы обеспечения высокого уровня достоверности при передаче, хранении, восстановлении и контроле целостности данных для современного цифрового информационного мира.

Приложение 1

Примерное 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 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 4×4) 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, мс.
   3.2. Задержка решения декодирования, мс.
   3.3. Виды и способы взаимодействия декодера с системами синхронизации (ветвевая, символьная, блоковая, кадровая, ...).
   3.4. Реализация (программная или 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.

Приложение 2

Таблицы

Таблица П-1. 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, «жёсткий» модем
1	*2*	*3*	*4*
−15,00	$4{,}01 \cdot 10^{-1}$	0,0365	0,0286
−14,50	$3{,}95 \cdot 10^{-1}$	0,0412	0,0321
−14,00	$3{,}89 \cdot 10^{-1}$	0,0466	0,0359
−13,50	$3{,}83 \cdot 10^{-1}$	0,0526	0,0402
−13,00	$3{,}76 \cdot 10^{-1}$	0,0594	0,0450
−12,50	$3{,}69 \cdot 10^{-1}$	0,0670	0,0504
−12,00	$3{,}61 \cdot 10^{-1}$	0,0755	0,0563
−11,50	$3{,}53 \cdot 10^{-1}$	0,0851	0,0630
−11,00	$3{,}45 \cdot 10^{-1}$	0,0958	0,0704
−10,50	$3{,}36 \cdot 10^{-1}$	0,1077	0,0786
−10,00	$3{,}27 \cdot 10^{-1}$	0,1209	0,0878
−9,50	$3{,}18 \cdot 10^{-1}$	0,1356	0,0980
−9,00	$3{,}08 \cdot 10^{-1}$	0,1518	0,1093
−8,50	$2{,}98 \cdot 10^{-1}$	0,1696	0,1217
−8,00	$2{,}87 \cdot 10^{-1}$	0,1892	0,1356
−7,50	$2{,}75 \cdot 10^{-1}$	0,2105	0,1508
−7,00	$2{,}64 \cdot 10^{-1}$	0,2337	0,1676
−6,50	$2{,}52 \cdot 10^{-1}$	0,2588	0,1860
−6,00	$2{,}39 \cdot 10^{-1}$	0,2857	0,2062
−5,50	$2{,}26 \cdot 10^{-1}$	0,3145	0,2283
−5,00	$2{,}13 \cdot 10^{-1}$	0,3452	0,2524
−4,50	$2{,}00 \cdot 10^{-1}$	0,3776	0,2785
−4,00	$1{,}86 \cdot 10^{-1}$	0,4116	0,3067
−3,50	$1{,}72 \cdot 10^{-1}$	0,4472	0,3371
−3,00	$1{,}58 \cdot 10^{-1}$	0,4841	0,3696
−2,50	$1{,}44 \cdot 10^{-1}$	0,5221	0,4042
−2,00	$1{,}31 \cdot 10^{-1}$	0,5610	0,4408
−1,50	$1{,}17 \cdot 10^{-1}$	0,6004	0,4792
−1,00	$1{,}04 \cdot 10^{-1}$	0,6400	0,5192
−0,50	$9{,}09 \cdot 10^{-2}$	0,6794	0,5605

1	*2*	*3*	*4*
0,00	$7{,}86 \cdot 10^{-2}$	0,7180	0,6026
0,50	$6{,}71 \cdot 10^{-2}$	0,7554	0,6451
1,00	$5{,}63 \cdot 10^{-2}$	0,7911	0,6875
1,50	$4{,}64 \cdot 10^{-2}$	0,8247	0,7291
2,00	$3{,}75 \cdot 10^{-2}$	0,8556	0,7693
2,50	$2{,}97 \cdot 10^{-2}$	0,8835	0,8073
3,00	$2{,}29 \cdot 10^{-2}$	0,9082	0,8427
3,50	$1{,}72 \cdot 10^{-2}$	0,9295	0,8747
4,00	$1{,}25 \cdot 10^{-2}$	0,9474	0,9031
4,50	$8{,}79 \cdot 10^{-3}$	0,9620	0,9273
5,00	$5{,}95 \cdot 10^{-3}$	0,9734	0,9474
5,50	$3{,}86 \cdot 10^{-3}$	0,9821	0,9635
6,00	$2{,}39 \cdot 10^{-3}$	0,9885	0,9758
6,50	$1{,}40 \cdot 10^{-3}$	0,9930	0,9847
7,00	$7{,}73 \cdot 10^{-4}$	0,9959	0,9909
7,50	$3{,}99 \cdot 10^{-4}$	0,9978	0,9949
8,00	$1{,}91 \cdot 10^{-4}$	0,9989	0,9974
8,50	$8{,}40 \cdot 10^{-5}$	0,9995	0,9987
9,00	$3{,}36 \cdot 10^{-5}$	0,9998	0,9995
9,50	$1{,}21 \cdot 10^{-5}$	0,9999	0,9998
10,00	$3{,}87 \cdot 10^{-6}$	1,0000	0,9999
10,50	$1{,}08 \cdot 10^{-6}$	1,0000	1,0000
11,00	$2{,}61 \cdot 10^{-7}$	1,0000	1,0000
11,50	$5{,}33 \cdot 10^{-8}$	1,0000	1,0000
12,00	$9{,}01 \cdot 10^{-9}$	1,0000	1,0000
12,50	$1{,}23 \cdot 10^{-9}$	1,0000	1,0000

Таблица П-2. Нижние оценки для $P_b(e)$ при оптимальном декодировании СОК в двоичном симметричном канале

E_s/N_0	p_0	$d=7$	$d=13$	$d=19$	$d=25$
−4,0	$1{,}86\cdot10^{-1}$	$2{,}60\cdot10^{-2}$	$4{,}61\cdot10^{-3}$	$8{,}80\cdot10^{-4}$	$1{,}74\cdot10^{-4}$
−3,0	$1{,}58\cdot10^{-1}$	$1{,}47\cdot10^{-2}$	$1{,}76\cdot10^{-3}$	$2{,}28\cdot10^{-4}$	$3{,}07\cdot10^{-5}$
−2,0	$1{,}31\cdot10^{-1}$	$7{,}33\cdot10^{-3}$	$5{,}40\cdot10^{-4}$	$4{,}31\cdot10^{-5}$	$3{,}58\cdot10^{-6}$
−1,0	$1{,}04\cdot10^{-1}$	$3{,}13\cdot10^{-3}$	$1{,}26\cdot10^{-4}$	$5{,}49\cdot10^{-6}$	$2{,}50\cdot10^{-7}$
0,0	$7{,}86\cdot10^{-2}$	$1{,}10\cdot10^{-3}$	$2{,}08\cdot10^{-5}$	$4{,}30\cdot10^{-7}$	$9{,}24\cdot10^{-9}$
1,0	$5{,}63\cdot10^{-2}$	$3{,}06\cdot10^{-4}$	$2{,}27\cdot10^{-6}$	$1{,}84\cdot10^{-8}$	$1{,}55\cdot10^{-10}$
2,0	$3{,}75\cdot10^{-2}$	$6{,}32\cdot10^{-5}$	$1{,}47\cdot10^{-7}$	$3{,}72\cdot10^{-10}$	$9{,}88\cdot10^{-13}$
3,0	$2{,}29\cdot10^{-2}$	$9{,}07\cdot10^{-6}$	$4{,}99\cdot10^{-9}$	$3{,}00\cdot10^{-12}$	$1{,}89\cdot10^{-15}$
4,0	$1{,}25\cdot10^{-2}$	$8{,}29\cdot10^{-7}$	$7{,}66\cdot10^{-11}$	$7{,}76\cdot10^{-15}$	$8{,}22\cdot10^{-19}$
5,0	$5{,}95\cdot10^{-3}$	$4{,}33\cdot10^{-8}$	$4{,}41\cdot10^{-13}$	$4{,}92\cdot10^{-18}$	$5{,}74\cdot10^{-23}$
6,0	$2{,}39\cdot10^{-3}$	$1{,}13\cdot10^{-9}$	$7{,}51\cdot10^{-16}$	$5{,}46\cdot10^{-22}$	
7,0	$7{,}73\cdot10^{-4}$	$1{,}24\cdot10^{-11}$	$2{,}81\cdot10^{-19}$		
8,0	$1{,}91\cdot10^{-4}$	$4{,}64\cdot10^{-14}$	$1{,}58\cdot10^{-23}$		

Таблица П-3. Нижние оценки для $P_b(e)$ при оптимальном декодировании СОК в АБГШ канале, 16 уровней квантования

E_s/N_0	p_0	$d=7$	$d=13$	$d=19$	$d=25$
−4,0	$1{,}86\cdot10^{-1}$	$9{,}82\cdot10^{-3}$	$7{,}50\cdot10^{-4}$	$6{,}26\cdot10^{-5}$	$5{,}45\cdot10^{-6}$
−3,0	$1{,}58\cdot10^{-1}$	$4{,}30\cdot10^{-3}$	$1{,}74\cdot10^{-4}$	$7{,}72\cdot10^{-6}$	$3{,}58\cdot10^{-7}$
−2,0	$1{,}31\cdot10^{-1}$	$1{,}56\cdot10^{-3}$	$2{,}86\cdot10^{-5}$	$5{,}78\cdot10^{-7}$	$1{,}22\cdot10^{-8}$
−1,0	$1{,}04\cdot10^{-1}$	$4{,}52\cdot10^{-4}$	$3{,}09\cdot10^{-6}$	$2{,}34\cdot10^{-8}$	$1{,}85\cdot10^{-10}$
0,0	$7{,}86\cdot10^{-2}$	$9{,}82\cdot10^{-5}$	$1{,}97\cdot10^{-7}$	$4{,}39\cdot10^{-10}$	$1{,}02\cdot10^{-12}$
1,0	$5{,}63\cdot10^{-2}$	$1{,}49\cdot10^{-5}$	$6{,}50\cdot10^{-9}$	$3{,}15\cdot10^{-12}$	$1{,}60\cdot10^{-15}$
2,0	$3{,}75\cdot10^{-2}$	$1{,}45\cdot10^{-6}$	$9{,}39\cdot10^{-11}$	$6{,}78\cdot10^{-15}$	$5{,}13\cdot10^{-19}$
3,0	$2{,}29\cdot10^{-2}$	$8{,}07\cdot10^{-8}$	$4{,}84\cdot10^{-13}$	$3{,}24\cdot10^{-18}$	$2{,}28\cdot10^{-23}$
4,0	$1{,}25\cdot10^{-2}$	$2{,}24\cdot10^{-9}$	$6{,}93\cdot10^{-16}$	$2{,}40\cdot10^{-22}$	$8{,}72\cdot10^{-29}$
5,0	$5{,}95\cdot10^{-3}$	$2{,}63\cdot10^{-11}$	$2{,}03\cdot10^{-19}$	$1{,}76\cdot10^{-27}$	
6,0	$2{,}39\cdot10^{-3}$	$1{,}07\cdot10^{-13}$	$8{,}44\cdot10^{-24}$		
7,0	$7{,}73\cdot10^{-4}$	$1{,}17\cdot10^{-16}$	$3{,}16\cdot10^{-29}$		
8,0	$1{,}91\cdot10^{-4}$	$2{,}59\cdot10^{-20}$			

Приложение 3

Об итогах конкурса двух теорий

Публикации нашей научной школы всегда содержат те или иные сопоставления новых результатов ОТ с другими наиболее интересными достижениями. Здесь мы рассмотрим итоговые соотношения возможностей ОТ и завершившей свой цикл прежней до предела математизированной теории. Вынужденно напоминаем вновь, что крайняя формализация прикладной (!) теории не помогла ей стать хоть в какой-то степени истинной, поскольку большинство её результатов не только крайне слабые, но и абсолютно непроверяемые [90, 96]. А итоговыми сравнениями мы их считаем просто потому, что более у нас вообще не осталось никаких причин обсуждать в дальнейшем что-либо из идей и фантазий того огромного сонма «сотрудников науки», которые ни разу не попробовали воссоздать в корректном проверяемом эксперименте хоть что-нибудь из тех «достижений», которыми они пытались осчастливить цифровой мир.

Существенно, как мы уже отмечали это ранее, что мы не касаемся здесь деятельности фирм, производящих аппаратуру кодирования. Это совершенно другой мир.

Наша научная школа Оптимизационной Теории (ОТ) в этой монографии декларирует свой полный успех в решении великой проблемы Шеннона. Она решена нами на уровне наилучших возможных теоретических и практических параметров алгоритмов декодирования для всех четырёх традиционных типов каналов, анализировавшихся в прежней теории. Эта же тематика будет в более широких аспектах разрабатываться в ОТ и далее. Сопоставимых с нашими алгоритмами по реальной сложности, достоверности и помехоустойчивости других методов сейчас нет даже на горизонте. И мы полагаем, что в ближайшее время их не будет по многим причинам. Одной из наиболее важных проблем, которую ещё долго не смогут преодолеть прочие научные группы, оказалось полное отсутствие в мире хоть какой-то экспериментальной базы для проверки, разработки и настройки параметров алгоритмов, исправляющих ошибки вблизи границы Шеннона. Такое программное обеспечение, а тем более аппаратные стенды, создаются десятилетиями. Но мы так и не обнаружили в XXI веке ни одной публикации, в которой были бы хотя бы намёки на существование или на процесс создания такой обязательной экспериментальной платформы. А это и привело к тому, что практически все работы большинства научных групп по алгоритмам декодирования с оценками их

достоверности являются слабыми, ненужными, ошибочными или даже просто фальсификациями на тему коррекции ошибок, особенно при описаниях их работы в условиях большого уровня шума.

Однако наиболее удобными способами маскировки параметров триединого критерия «помехоустойчивость — достоверность — сложность» оказались именно вопросы сложности, трактуемые почти всеми авторами с привлечением безудержной фантазии и выдумки. Но это не помогает никому из них решать реальные проблемы прикладной теории, поскольку ни один из параметров триединого критерия ушедшая с полей науки теория так и не научилась оценивать для большого уровня шума канала ни для одного из своих алгоритмов. А в ОТ все параметры этого критерия определяются в эксперименте фактически мгновенно. Всё необходимое ПО для этого давно создано, причём с большим функциональным запасом. Мы на наших порталах даже предлагаем всем коллегам демо-модели многих алгоритмов, совсем не относящихся к ОТ! Так что мы высказываем вовсе не субъективные негативные эмоции, а излагаем конкретный опыт проверки и других схем коррекции ошибок, выполняя абсолютно не нашу, а чью-то чужую, проигнорированную кем-то работу.

Указанными обстоятельствами и можно было бы завершить обсуждения проблемы сопоставления двух теорий, поскольку их полное корректное сравнение невозможно, т. к. прежняя теория вообще не может предъявить что-либо для этого сопоставления. Однако мы понимаем, что для вдумчивых специалистов цифрового мира, не занятых непосредственно в разработках новых декодеров, краткое описание нынешней трагической ситуации необходимо, хотя многие страницы других публикаций по ОТ всегда предоставляются для тех или иных сравнений. Постараемся выполнить наш очень краткий анализ достаточно чётко и понятно.

Укажем сначала наши новые работы и монографии [4, 5, 79, 90, 91, 94, 100]. В большинстве из них есть разделы по сравнению прикладных результатов ОТ и прочих алгоритмов. Они есть также на наших крупнейших в мире порталах [40] и в Справочнике [1]. Очень полезно просмотреть наши трудные для восприятия (из-за обилия важного цифрового материала), но вполне точные по существу обзоры последнего времени [59, 64, 73–76, 78, 82, 88, 89, 93–95, 98, 103, 108]. При первом прочтении больших обзоров, правильное понимание которых, конечно, является крайне тяжёлой работой, мы всегда предлагаем не погружаться сразу во все тонкости цифровых соответствий. Они могут быстро утомить любого человека, который не посвятил свою профессиональную деятельность кодам. Сначала следует уделять внимание различным локальным и качественным, а уже

потом конкретным и общим выводам, которые мы обычно делаем и для отдельных разделов таких обзоров. А потом, по мере выявления интереса к конкретным методам и соотношениям, можно более успешно воспринимать и собственно весь огромный цифровой контент. Как мы проверили опытным путём, наши коллеги в этом случае гораздо лучше и глубже воспринимают затем и все остальные результаты крупных статей обобщающего стиля, подготовленных научной школой ОТ.

Наши обзоры затрагивают различные особенности развития ОТ и прежней теории, включая возможности низкоплотностных (LDPC), турбо и полярных кодов (ПК). Большинство обзоров имеют собственный список ссылок. Для тех, кто нечасто до сегодняшнего дня встречался с проблемами кодирования, мы рекомендуем начать чтение с буклета-комикса [90], где на основе красочных слайдов большой коллектив авторов нашей научной школы просто и наглядно описывает текущее состояние ОТ и прежней теории. Отдельный глубокий анализ полярных кодов (ПК) [117], которые стали новой яркой и печальной иллюстрацией общего кризиса прежней теории кодирования, есть в весьма непростых (из-за многоплановости проблем ПК) обзорах [74, 92]. Эта же тема есть в обзорах [79, 90, 91, 93, 98].

Очень большое количество работ, упомянутых в монографии, можно совершенно свободно найти в сети. И особенно удобно то, что абсолютное большинство важнейших литературных ссылок этой монографии сопровождается и гиперссылками на наши книги, обзоры и статьи. Это сохранит огромные ресурсы так необходимого нам всем времени, т. к. позволит каждому специалисту при первой же необходимости мгновенно вывести на экраны своих компьютеров все эти необходимые публикации школы ОТ. Мы полагаем, что такая организация работы с нашей книгой увеличивает информационный объём монографии в несколько раз. Столь же легко переписать с наших порталов и все программные платформы, а также демо-программы (в том числе и не только наших алгоритмов!), о которых мы уже писали в нескольких разделах этой и других монографий. Несмотря на это краткое перечисление наиболее информативных работ, много полезных фактов и идей можно найти, проанализировав все те публикации из литературных ссылок монографии, которые имеют номера [73] и более, которые написаны сторонниками нашей школы. Это основные работы научной школы ОТ текущего тысячелетия.

Кратко прокомментируем ситуацию в теории кодирования.

Мы неоправданно редко пишем, что все методы декодирования за пределами ОТ используют действительные числа, что крайне усложняет их реализацию, особенно в аппаратном виде. Методы ОТ приме-

няют только арифметику с фиксированной точкой, т. е. наши декодеры оперируют лишь с небольшими целыми числами. Это преимущество ОТ также очень важно, хотя при использовании для моделирования алгоритмов стандартной компьютерной техники и программных средств, в том числе на языке C++, эта разница из-за очень мощных современных процессоров не столь сильно заметна.

Далее, прежняя теория кодирования обеспечивала очень слабые уровни достоверности при разумной сложности. Из-за этого там стали как бы «развивать» списочное декодирование. Однако это необоснованное полное разрушение исходной постановки проблемы декодирования в прикладной теории. Но, с другой стороны, правильно спроектированные алгоритмы в ОТ практически всегда достигают решений ОД, т. е. наилучших возможных по достоверности, вследствие чего качество наших методов всегда много выше, чем у списочных. Здесь ОТ также не имеет конкурентов, что способствует сохранению и дальнейшему только всегда корректному уточнению исходной и других возможных постановок задач декодирования [74, 92].

Наши блоковые АВ (БАВ) и МПД как для коротких, так и для длинных кодов безо всякой адаптации к сопоставлении с ПК обеспечивают гораздо более высокие характеристики помехоустойчивости, чем ПК [74, 92]. Многие из таких характеристик алгоритмов ОТ при небольших затратах почти достигают границ сферической упаковки и, тем самым, не могут быть никак ещё улучшены [92]. Среди других методов с приемлемой сложностью реализации таких алгоритмов нет.

Мы уже давно указываем в наших работах программную производительность наших методов на компьютерах, тогда как для ПК и LDPC кодов мы нигде не смогли увидеть ни одного полного описания характеристик хотя бы для одного декодера. При этом, однако, скорости всех наших декодеров значительны или даже просто огромны при всех сравнениях с декодерами ПК и LDPC, для которых их сложность всегда изобретательно прячется. Можно утверждать, что прочие технологии кодирования за 60 лет «активной» работы действительно не предъявили ни одного метода. Ни одного! Так что все наши рассуждения о сложности пока фактически беспредметны. Правда, при детальном анализе вполне доступных в сети авторефератов и диссертаций по ПК и другим вопросам теории кодирования [106, 107] оказывается, что сложность декодеров ПК и LDPC или очень значительна, или даже просто абсолютно грандиозна [90]. И ещё раз напоминаем, что все желающие также могут обратиться к нашим демо-программам для алгоритмов, вообще не относящихся к ОТ. Это поможет специалистам самим уточнить соотношения сложности различных методов. Но у авторов «тех» алгоритмов ничего такого найти нельзя. Там же

ничего нет. Ну, кстати, сама эта ситуация хорошо показывает, что там искать и вообще нечего.

Поскольку наш краткий анализ сопоставления сложности методов двух теорий оказался неудачным (не из-за нас!), рассмотрим достижения разных научных групп по достоверности. В работах [104, 112–115], а также в большом числе других статей на портале www.mathnet.ru можно найти совсем новые (это весьма важно!) результаты этого тысячелетия по достоверности алгоритмов декодирования для LDPC кодов. Такие оценки с непостижимым упорством аналитически выводятся на 10–25 страницах очень мелкого текста с использованием отсылок к другим «трудам», но не доводятся при этом до каких-то простых выражений в ДСК или в стирающих каналах. По этому поводу уместно напомнить серьёзные сомнения, которые были изложены в [96] и дополнительно прокомментированы в [90], в плане большой проблемности правильности многих подобных результатов. Но зато они получены аналитически, хотя и с абсолютным подчёркнутым игнорированием проблемы сложности. Однако по данным [97, стр. 308] часть этих методов на 2 порядка хуже весьма слабых кодов БЧХ по входной (!) вероятности, которые в свою очередь вдвое не дотягивают опять же по входной (!) вероятности ошибки до самого простейшего МПД декодера, опубликованного ещё в 1986 году в [102]! У других методов разница по этой же входной вероятности искажений по сравнению с алгоритмами МПД оказывается несколько меньшей. Они оказываются хуже только в 4–10 раз. Но это тоже абсолютно непозволительно слабо для публикаций в ведущих журналах нашей отрасли науки. Подчеркнём снова, что всё это происходит из-за принципиальной невозможности строить оценки каких-либо параметров всех декодеров при большом шуме канала. Но такие математические «развлечения» в «той» теории кодирования всё ещё процветают вот уже 40 лет. И это несмотря на то, что никаких шансов на получение корректных содержательных результатов при большом уровне входного шума в принципе нет и никогда не будет!

Приходится снова отвлекаться и напоминать, что для МПД алгоритмов оценки достоверности всегда очень просты и реально достижимы при правильной формулировке задачи декодирования и хорошем выборе параметров. Собственно вероятности ошибки в ДСК в этом случае определяются обычными биномиальными распределениями. Их даже не требуется выводить. Они очевидны и очень просто достижимы обычными МПД, что было уже 35 лет как понятно ещё и по результатам в [102]. В случае же использования МПД декодеров в стирающих каналах также достижимые на простых программных моделях оценки достоверности имеют для вероятности невосстанов-

ленных символов вид $P_s(e) \sim p_s^d$, где p_s — вероятность стирания в канале, d — минимальное кодовое расстояние. Ну, куда проще? И при этом они точные и проверяемые. Оценки для наших алгоритмов выводятся на половине страницы всех наших монографий и все они легко достижимы при весьма небольшой сложности конкретных декодеров.

Обещанные совсем недавно в [104, 106] «быстрые» алгоритмы декодирования попросту там отсутствуют. Они много сложнее, чем методы ОТ, что было сначала доказано ещё 1981 г. в [2] для некоторых и затем полностью для всех кодов в 1990 г. [36], а в 2004 г. все соответствующие сведения уже были помещены в Справочник [1]. Тем не менее, авторы всё же стали докторами наук. И это при том, что реальные очень простые декодеры символьных (недвоичных, как и у этих теперь докторов!) с линейной от длины кодов сложностью и оптимальным (!) решением опубликованы в 1985 г. [1, 6, 36, 39], о чём эти доктора не сочли возможным вспомнить и вскользь упомянуть хотя бы мельком даже через 30 лет после создания полной теории символьных кодов, давно решивших вообще все проблемы сохранения высочайшей достоверности байтовых (всяких недвоичных!) массивов.

В [101] предлагаются весьма трудные методы декодирования, объявленные на 1990 г. лучшими. Однако к этому времени вышло уже около 50 работ по методам, которые вскоре стали основой ОТ и была завершена разработка самой ОТ [36]. Авторы [101], предложившие на самом деле крайне слабые и сложные подходы к коррекции ошибок, ни тогда, ни позже в течение следующих 30 лет не сочли возможным «заметить» ОТ. Наши комментарии этой ситуации есть в [93], а также в [103, с. 22]. Эту ссылку полезно изучить ещё и из соображений оценки общего уровня нашего научного сообщества. Представляется крайне важным не оставлять выявленные в этом большом обзоре-комментарии обстоятельства существования научных сотрудников и преподавателей очень разной квалификации при текущем формате развития науки.

Очень популярными у нас и в зарубежье после 70 лет как бы «развития» теории кодирования оказались ещё и всяческие оценки, которые сводятся к тому, что вместо полного (экспоненциального!) перебора всех возможных решений, как это элегантно делает для коротких кодов алгоритм Витерби (АВ), объём соответствующих вычислений можно сократить, причём существенно. Огромное число успешных (!) докторских диссертаций, предъявивших различные решения этой задачи, уменьшили экспоненту сложности таких «полупереборных» алгоритмов в 2–5 раз [116 и другие ссылки там же]. Но в ре-

альности даже для кодов относительно небольшой длины $n \sim 10\,000$ это приводит к сложности декодирования $N \sim 10^{200}$ операций, что на сотни порядков превышает число атомов во Вселенной. Очень ценно, не так ли? В абсолютном большинстве таких «научных работ» прочих значимых достижений вообще нет. И ведь это докторские защиты недавних лет нынешнего столетия! Вынужденно кратко вновь указываем, что линейное, т. е. при сложности $N \sim n$, оптимальное декодирование, эквивалентное переборному, стало сначала доступной реальностью в 1978 г. [38], а затем было обосновано в ОТ для всех каналов в 1990 г. [36] и даже вошло в Справочник в 2004 г. [1].

Наконец, в [109, 110] представлен уникальный стиль «разработки» алгоритмов декодирования, детально прокомментированный нами в [93]. Он крайне прост и состоит из набора странных фраз, лишь некоторые из которых можно с трудом отнести к терминологии теории кодирования, например, опять же представленной в нашем Справочнике [1]. Без особой печали признаюсь, что в этих «талмудах» я понял лишь несколько таких неожиданных словосочетаний. Какие-либо результаты там вообще отсутствуют в принципе. Но автор защитил докторскую, растит, причём довольно быстро, себе смену (есть уже к.т.н.) и рассылает с докладами по различным конференциям аспирантов. Понять их я тоже не мог. Ученики, однако!

Трагический для науки вывод: формы выживания отдельных людей принимают крайне опасный оборот. Результат: более сотни человек, принявших участия в различных защитах «про коды» в Ульяновске, совершенно ничего не понимающие по существу в представленных «научных работах», искалеченные нравственно аспиранты и абсолютно необразованные в результате всего этого студенты и будущие инженеры — это ли не серьёзная катастрофа?! А причина — в абсолютной бесконтрольности, в падении уровня образования и науки, а также во всеобщем нежелании хоть как-то организовывать и поддерживать критические научно-технические обзоры и строгие выводы из них. Да и писать-то их просто некому. Кстати, сейчас это уже стало реально опасным. Совершенно обязательными тут смотрятся все мероприятия, самым жёстким образом отсекающие таких «сказителей» от науки и преподавания. Следует укреплять систему рецензирования, обеспечить контроль уровня исследований и корректность публикаций, организовать технологии отсева халтуры, а также многое другое. Однако это выходит за рамки вопросов наших публикаций.

И мы вынуждены согласиться с тем, что всё это, увы, совсем неудивительно, если в нескольких предыдущих абзацах было показано, что творится в наших «цитаделях» науки.

На этом фоне уже кажется и не особенно удивительным, что

абсолютно все переводные книги по прикладным вопросам теории кодирования, например [105], радостно рекомендуемые нашими «корифеями» для перевода и последующего обучения студентов, являются перепевами методов ещё 80–90-х годов. Но забавно, что в списках дополнительной литературы для этих скучнейших иноземных «бестселлеров», подготовленных в теперь уже немногих как бы «ведущих» центрах страны, занимающихся теорией кодирования, не указано ни одной из 600 публикаций научной школы ОТ. Жаль!

Да и вообще мы полагаем, что кроме замечательной книги [19] в конце того столетия о прикладных проблемах теории кодирования в мире более ничего и не появлялось. Но вся теория ОТ вместе со всей экспериментальной базой ПО была к этому времени у нас уже создана.

А как же всё-таки эти и многие подобные крайне прискорбные события и ситуации прокомментирует сама наука?

Подводя теперь итог, конечно, не обзору, а краткому комментарию наших обзоров (увы, мы единственные, кто их может писать!) и отдельных особых как бы «научных достижений», общее число которых уже давно недопустимо велико, наша научная школа считает, что она выдержала тяжелейший груз одиночества, игнорирования и беспрецедентного чиновного давления в нашем сложнейшем упорном поиске решения великой проблемы Шеннона. И однако же, мы всё это сделали!

Обращаясь к здоровым силам, заинтересованным в развитии настоящей передовой науки, мы предлагаем интенсивно осваивать самую передовую прикладную теорию кодирования на базе ОТ и быстро двигаться дальше, глубоко очищая хрупкие структуры науки, пока оставленные без всякого системного и организационного контроля, от наслоений зловредного мусора и создавая на этом обновлённом древе науки новые точки роста!

Научная школа ОТ всегда готова вам помочь. Дерзайте!

Список сокращений

АБГШ	аддитивный белый гауссовский шум
АВ	алгоритм декодирования Витерби
АФМ	амплитудно-фазовая модуляция
АЦП	аналого-цифровой преобразователь
БАВ	блоковая версия алгоритма Витерби
БЧХ	код Боуза — Чоудхури — Хоквингема
ДПКМ	декодер с прямым контролем метрики
ДСК	двоичный симметричный канал
ДСЧ	датчик случайных чисел
КК	каскадный код
ККЧ	код с контролем по четности
КНЗС	коды с неравной защитой символов
КСЗ	коэффициент совершенства Золотарёва
МПД	многопороговый декодер (алгоритм декодирования)
НЗ-коды	коды с неравной защитой символов
НЭК	каналы с неравномерной энергетикой
ОД	оптимальный декодер
ОТ	Оптимизационная Теория помехоустойчивого кодирования
ОТМПД	Основная Теорема многопорогового декодирования
ОТQМПД	Основная Теорема многопорогового декодирования недвоичных (символьных) кодов
ПГЭФ	поиск глобального экстремума функционалов
ПД	пороговый декодер
ПК	параллельный код, параллельное каскадирование
ПФВ	производящая функция вероятности
ПЭ	пороговый элемент
РО	размножение ошибок
РС	код Рида — Соломона
СОК	самоортогональный код
СтМПД	многошаговое декодирование в стирающих каналах
СтСК	симметричный стирающий канал
ФМ	фазовая модуляция
ЭВК	энергетический выигрыш кодирования
QМПД	q-ичный многопороговый декодер
QПД	символьный пороговый декодер
QСК	q-ичный симметричный канал

Список литературы

1. *Золотарёв В.В., Овечкин Г.В.* Помехоустойчивое кодирование. Методы и алгоритмы. Справочник. — М.: Горячая линия — Телеком, 2004. — 126 с.
2. *Самойленко С.И., Давыдов А.А., Золотарёв В.В., Третьякова Е.Л.* Вычислительные сети. — М.: Наука, 1981. — 278 с.
3. *Золотарёв В.В.* Теория и алгоритмы многопорогового декодирования. — М.: Радио и связь, Горячая линия — Телеком, 2006; второе издание — 2014.
4. *Золотарёв В.В., Зубарев Ю.Б., Овечкин Г.В.* Многопороговые декодеры и оптимизационная теория кодирования / Под ред. академика РАН В.К. Левина. — М.: Горячая линия — Телеком, 2012. — 238 с.
5. *Zolotarev V., Zubarev Y., Ovechkin G.* Optimization Coding Theory and Multithreshold Algorithms. — Geneva, ITU, 2015. — 159 p. http://www.itu.int/pub/s-gen-octma-2015
6. *Кузнецов Н.А., Золотарёв В.В., Овечкин Г.В., Овечкин П.В.* Недвоичные многопороговые декодеры и другие методы коррекции ошибок в символьной информации // Радиотехника. — 2010. — № 6, вып. 141. — С.4–9.
7. *Бородин Л.Ф.* Введение в теорию помехоустойчивого кодирования. — М.: Советское радио, 1968.
8. *Месси Дж.* Пороговое декодирование. — М.: Мир, 1966.
9. *Колесник В.Д., Мирончиков Е.Т.* Декодирование циклических кодов. — М.: Связь, 1968.
10. *Касами Т., Токура Н., Ивадари Е., Ипагаки Я.* Теория кодирования. — М.: Мир, 1978.
11. *Галлагер Р.* Теория информации и надежная связь. — М.: Советское радио, 1974.
12. *Блейхут Р.* Теория и практика кодов, контролирующих ошибки. — М.: Мир, 1986.
13. *Towsend R.L., Weldon E.J.* Self-Orthogonal Quasi-Cyclic Codes // IEEE Trans. On Inform. Theory. — 1967. — Vol. IT-13, No. 2.
14. *Shannon C.* A Mathematical Theory of Communication // Bell System Technical Journal. — Vol. 27 (July and October 1948). — P.379–423 and 623–656. (*Шеннон К.Э.* Математическая теория

связи // В сб.: Работы по теории информации и кибернетике. — М.: Иностранная литература, 1963)

15. *Forney G.D.* Convolutional codes. II. Maximum-likelyhood decoding // Information and control. — 1974. — Vol. 25, No. 3.
16. *Нейфах А.Э.* Свёрточные коды для передачи дискретной информации. — М.: Наука, 1979.
17. *Solomon G., van Tilborg C.A.* A connection between block and convolutional codes // SIAM Journal of Applied Mathematics. — 1979. — Vol. 37, No. 2.
18. *Heller J.A., Jacobs J.M.* Viterbi decoding for satellite and space communication // IEEE Trans. on Comm. Technology. Part II. — 1971. — Vol. COM-19, No. 5.
19. *Кларк Дж., Кейн Дж.* Кодирование с исправлением ошибок в системах цифровой связи. — М.: Радио и связь, 1987.
20. *Витерби А.Дж.* Границы ошибок для свёрточных кодов и асимптотически оптимальный алгоритм декодирования // В сб.: Некоторые вопросы теории кодирования. — М.: Мир, 1970.
21. *Котельников В.А.* Теория потенциальной помехоустойчивости. — М.-Л.: Госэнергоиздат, 1956.
22. *Зубарев Ю.Б., Золотарёв В.В., Овечкин Г.В., Овечкин П.В.* Итоги 25-летнего развития оптимизационной теории кодирования // Наукоёмкие технологии. — 2016 — Т. 17. — С.26–32.
23. *Bose R.C., Ray-Chaudhuri D.K.* On a class of error correcting binary group codes // Information and Control. — 1960. — № 3.
24. *Hocquenghem A.* Codes correcteures derreurs // Cheffres. — 1959. — Vol. 2.
25. *Massey J.* Threshold decoding. — M.I.T. Press, Cambridge, Massachusetts, 1963.
26. *Форни Д.* Каскадные коды. — М.: Мир, 1970.
27. *Хацкелевич Я.Д., Готлиб В.М.* Эффективность каскадного кода при декодировании с метками надежности // Труды НИИР. — 1981. — № 1.
28. *Золотарёв В.В.* Устройство для декодирования линейных свёрточных кодов: авторское свидетельство СССР № 492878.
29. *Золотарёв В.В.* Многопороговое декодирование // Проблемы передачи информации. — М.: 1986. — т. XXII, вып. 1. — С.104–109.

30. *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. — P.1064–1070.

31. *MacKay D.J.C., Neal R.M.* Near Shannon limit performance of low density parity check codes // IEEE Electronics Letters. — 1996. — Vol. 32, No. 18. — P.1645–1646.

32. *Richardson T., Shokrollahi M., Urbanke R.* Design of capacity-approaching irregular low-density parity-check codes // IEEE Trans. on Inform. Theory. — 2001. — Vol. 47. — P.638–656.

33. Press Release, AHA announces Turbo Product Code Forward Error Correction Technology. 1998, Nov. 2.

34. *Jin H., Khandekar A., McEliece R.* Irregular repeat-accumulate codes // Proc. 2nd Int. Symp. on Turbo Codes and Related Topics (Brest, France). — 2000. — P.1–8.

35. *Li J., Narayanan K.R., Georghiades C.N.* Product accumulate codes: A class of capacity-approaching, low-complexity codes // Submitted to IEEE Trans. on Inform. Theory, 2001.

36. *Золотарёв В.В.* Субоптимальные алгоритмы многопорогового декодирования: дис. ... д-ра тех. наук. — М., 1990.

37. *Золотарёв В.В.* Эффективные многопороговые алгоритмы декодирования // Научный совет по комплексной проблеме «Кибернетика» АН СССР. Препринт. — М.: 1981. — 76 с.

38. *Золотарёв В.В.* Исследование алгоритмов многопорогового декодирования свёрточных кодов: дис. ... канд. тех. наук. — М., 1978.

39. *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.

40. Сетевые ресурсы **www.mtdbest.iki.rssi.ru** и **www.mtdbest.ru**.

41. *Золотарёв В.В.* Использование многопорогового декодера вместо алгоритма Витерби // Вестник РГРТА. — 2002. — вып. 10. — С.117—119.

42. *Cain J.B., Clark G.G.* Some results on error propagation of convolutional feedback // IEEE Trans. on Inform. Theory. — 1972. — Vol. IT-18, No. 5.

43. *Bahl L., Jelinek P.* On the Structure of Rate $1/n$ Convolutional

Codes // IEEE Trans. on Inform. Theory. — 1972. — Vol. IT-18, No. 1. — P.192–196.

44. *Massey J.L., Bin R.W.* Application of Lyapunov's Direct Method to the Error-Propagation Effect in Convolutional Codes // IEEE Trans. on Inform. Theory. — 1964. — Vol. IT-10, No. 4. — P.248–250.
45. *Massey J.L., Sain M.K.* Inverses of Linear Sequential Circuits // Trans. Computers. — 1968. — Vol. C-17, No. 4. — P.330–337.
46. *Габидулин Э.М., Ларин А.Д.* Размножение ошибок при декодировании равномерных свёрточных кодов // Проблемы передачи информации. — 1969. — Т. V, вып. 3. — С.73–77.
47. *Ларин А.Д.* О максимальной длине размножения ошибок при пороговом декодировании равномерных свёрточных кодов // Известия вузов. Радиоэлектроника. — 1972. — т. XV, № 4. — С.507–510.
48. *Massey J.L.* Catastrophic error propagation in convolutional codes // Proc. 11th Midwest Circuit Theory Symp. University Notre Dame. Ind., May, 1968.
49. *Робинсон Дж.П.* Размножение ошибок и прямое декодирование свёрточных кодов // В сб.: Некоторые вопросы теории кодирования. — М.: Мир, 1970.
50. *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, No. 1.
51. *Блох Э.Л., Зяблов В.В.* Линейные каскадные коды. — М.: Наука, 1982. — 229 с.
52. *Золотарёв В.В.* Параллельное кодирование в каналах СПД // В сб.: Вопросы кибернетики. ВК-120. — М., 1986.
53. *Овечкин Г.В.* Теория каскадного декодирования линейных кодов для цифровых радиоканалов на основе многопороговых алгоритмов: дис. ... д-ра тех. наук. — Рязань: РГРТУ, 2011. — 301 с.
54. *Золотарёв В.В.* Способ декодирования помехоустойчивого кода: патент на изобретение РФ № 2557454 от 25.06.2015.
55. *Золотарёв В.В., Овечкин Г.В.* Устройство многопорогового декодирования линейных кодов для гауссовских каналов: патент на полезную модель № 44215 от 27.02.2005.
56. *Золотарёв В.В.* Высокоскоростное устройство многопорогового декодирования линейных кодов: патент на полезную модель № 44216 от 27.02.2005.

57. *Золотарёв В.В.* Способ декодирования помехоустойчивого кода: патент на изобретение РФ № 2377722 от 27.12.2009.

58. *Золотарёв В.В.* О новом этапе развития оптимизационной теории // Цифровая обработка сигналов. — 2017. — № 1. — С.33–41.

59. *Золотарёв В.В., Овечкин Г.В.* Эффективные многопороговые методы декодирования самоортогональных кодов // Вестник РГРТУ. — 2017. — № 60. — С.113–122.

60. *Золотарёв В.В.* Способ обнаружения и исправления стираний при приёме дискретной информации: патент на изобретение РФ № 2611235 от 21.02.2017.

61. *Золотарёв В.В., Овечкин П.В.* Способ кодирования и декодирования блокового кода с использованием алгоритма Витерби: патент на изобретение РФ № 2608872 от 25.01.2017.

62. *Финк Л.М.* Теория передачи дискретных сообщений. — М.: Советское радио, 1970.

63. *Золотарёв В.В., Зубарев Ю.Б., Овечкин Г.В.* Высокоскоростной многопороговый декодер для систем передачи больших объемов данных // Научно-технический сборник «Техника средств связи», серия «Техника телевидения», юбилейный выпуск. — МНИТИ, 2010. — С.41–43.

64. *Золотарёв В.В., Зубарев Ю.Б., Овечкин Г.В., Аверин С.В., Овечкин П.В.* 25 лет Оптимизационной Теории кодирования — новые перспективы. Пленарный доклад // Научно-техническая конференция РГРТУ, 2017.

65. *Золотарёв В.В., Овечкин Г.В.* Применение многопороговых методов декодирования помехоустойчивых кодов в высокоскоростных системах передачи данных // Электросвязь. — 2014. — № 12. — С.10–14.

66. *Золотарёв В.В., Овечкин Г.В.* Способ реализации символьного порогового элемента в символьном мажоритарном декодере: патент РФ № 2573741

67. http://www.mtdbest.ru/articles/demoop_apr4.pdf

68. http://www.mtdbest.ru/program/mtddemo.zip

69. http://www.mtdbest.ru/program/qmtd_demo_r.zip

70. http://www.mtdbest.ru/program/demo_quick.zip

71. http://www.mtdbest.ru/program/instrrusg_educ_r.pdf

72. http://www.mtdbest.iki.rssi.ru/labrus.zip

73. *Золотарёв В.В., Овечкин Г.В., Назиров Р.Р.* О передаче Оптимизационной Теории лидерства от прикладной классической теории помехоустойчивого кодирования // Некоторые аспекты современных проблем механики и информатики: сб. науч. ст. — М.: ИКИ РАН, 2018. — С.82–90. DOI:10.21046/aspects-2018-82-90.

74. *Золотарёв В.В., Овечкин Г.В., Овечкин П.В.* О сопоставлении новых методов помехоустойчивого кодирования // Доклады 18-й Международной конференции «Цифровая обработка сигналов и её применение». Том 1. — М., 2016. — С.59–64. https://mtdbest.ru/articles/Zolotarev_DSPA2016.pdf

75. *Кузнецов Н.А., Золотарёв В.В., Овечкин Г.В., Назиров Р.Р., Аверин С.В.* Многопороговые алгоритмы на базе оптимизационной теории вблизи границы Шеннона // Некоторые аспекты современных проблем механики и информатики: сб. науч. ст. — М.: ИКИ РАН, 2018. — С.99–120. DOI: 10.21046/aspects-2018-99-120. https://mtdbest.ru/articles/99-120.pdf

76. *Золотарёв В.В., Зубарев Ю.Б., Овечкин Г.В.* Теория кодирования как оптимизационная проблема декодирования вблизи границы Шеннона // Труды 21-й Международной конференции по цифровой обработке сигнала. Том 1. Пленарный доклад. — М., 2019. — С.11–15. https://mtdbest.ru/articles/DSPA_2019_пленарный.pdf

77. *Золотарёв В.В., Овечкин Г.В.* Каскадирование самоортогональных кодов для каналов со стираниями // Труды 21-й Международной конференции по цифровой обработке сигнала. Том 1. — М., 2019. — С.124–127.

78. *Зубарев Ю.Б., Золотарёв В.В., Овечкин Г.В.* Новые технологии и парадигмы помехоустойчивого кодирования: после решения проблемы Шеннона // Электросвязь. — 2019. — №9. — С.56–61. https://mtdbest.ru/articles/elsv2020.pdf

79. *Zolotarev V.V.* Coding Theory as a Simple Optimal Decoding near Shannon's Bound (Optimization Theory of error-correcting coding is a new quantum mechanics of information theory). — M.: Hot Line — Telecom, 2018. — 333 p. https://mtdbest.ru/articles/mtd_book_2019.pdf

80. *Zolotarev V., Grinchenko N., Ovechkin G., Ovechkin P.* The Performance of Multithreshold Decoders in Concatenated Schemes Over Erasure Channels // 8th Mediterranean Conference on Embedded Computing MECO2019 including ECYPS2019. — P.517–520.

81. *Zolotarev V., Ovechkin G., Satibaldina D., Tashatov N., Omirbaev E.* Performances of the Decoding Algorithms near Shannon Limit // 2nd International Conference on Informatics, Control and Automation (ICA2019). — P.428–432.

82. *Zolotarev V.V., Nazirov R.R., Ovechkin G.V., Ovechkin P.V.* Optimizing Theory: Taking Over the Leadership Baton From Classic Coding Theory // Information Technologies in Remote Sensing of the Earth — RORSE 2018. — P.198–206. https://doi.org/10.21046/rorse2018.198

83. *Золотарёв В.В., Овечкин Г.В., Омирбаев Е.Д., Сатыбалдина Д.Ж., Ташатов Н.Н.* Производительность алгоритмов декодирования свёрточных кодов вблизи границы Шеннона для работы в беспроводных сетях // Вестник Восточно-Казахстанского государственного технического университета им. Д. Серкибаева. — 2019. — № 2 (84). — С.116–121.

84. *Гринченко Н.Н., Золотарёв В.В., Овечкин Г.В.* Каскадирование самоортогональных кодов для каналов со стираниями // 21-я Международная конференция «Цифровая обработка сигналов и ее применение», 2019. — Вып. XXI-1. — С.67–72.

85. *Золотарёв В.В., Гринченко Н.Н., Овечкин Г.В.* Применение каскадных самоортогональных кодов в каналах связи со стираниями // Радиотехника. — 2019. — Т. 83, № 5. — С.175–182.

86. *Золотарёв В.В.* Оптимизационная Теория как базис для создания декодеров, работающих вблизи границы Шеннона // 17-я Открытая Всероссийская конференция «Современные проблемы дистанционного зондирования Земли из космоса». Тезисы докладов. — 2019. — С.49.

87. *Золотарёв В.В.* Способ ускоренного декодирования линейного кода: патент на изобретение РФ № 2699833 от 11.09.2019 г.

88. *Золотарёв В.В.* Российская теория кодирования // Знание — сила. — 2019. — № 7. — С.53–57.

89. *Золотарёв В.В.* Российский подарок Клоду Шеннону и всей теории кодирования. — М., 2019. https://mtdbest.ru/articles/PocR.pdf

90. *Кузнецов Н.А., Золотарёв В.В., Зубарев Ю.Б., Овечкин Г.В., Назиров Р.Р., Аверин С.В.* Проблемы и открытия Оптимизационной Теории помехоустойчивого кодирования (ОТ в иллюстрациях). — М.: Горячая линия — Телеком, 2020. — 36 с. http://www.mtdbest.ru/articles/comics.pdf

91. *Kuznetsov N.A., Zolotarev V.V., Zubarev Yu.B., Ovechkin G.V., Nazirov R.R., Averin S.V.* Problems and Discoveries of the Optimization Theory for Coding near Shannon's Bound (OT in illustrations) — Moscow: Hot Line — Telecom, 2020. — 45 p. https://mtdbest.ru/articles/e-comics.pdf

92. *Кузнецов Н.А., Золотарёв В.В., Овечкин Г.В., Назиров Р.Р., Сатыбалдина Д.Ж., Омирбаев Е.Д.* Обзор проблем полярных кодов с позиции технологий Оптимизационной Теории помехоустойчивого кодирования // Современные проблемы дистанционного зондирования Земли из космоса. — 2020. — Т. 17, № 4. — С.9–24. http://jr.rse.cosmos.ru/default.aspx?id=96

93. *Золотарёв В.В., Зубарев Ю.Б., Смагин М.С.* Преодоление системного кризиса в теории информации // Вестник связи. — 2020. — № 8. — С.25–35.

94. *Золотарёв В.В.* Теория кодирования как задача поиска глобального экстремума // Под научной редакцией академика РАН Н.А. Кузнецова. — М.: Горячая линия — Телеком, 2018. — 223 с.

95. *Золотарёв В.В.* О новом этапе развития Оптимизационной Теории кодирования // Цифровая обработка сигналов. — 2017. — № 1. — С.33–41. https://mtdbest.ru/articles/Zolotarev_DSPA_2017.pdf

96. *Магаршак Ю.* Число, возведенное в абсолют // Независимая газета, 09.09.2009. https://mtdbest.ru/articles/theory_modell.pdf

97. *Питерсон У., Уэлдон Э.* Коды, исправляющие ошибки. — М.: Мир, 1976.

98. *Золотарёв В.В., Овечкин Г.В.* Оптимизационная теория — технологический стиль проектов вблизи границы Шеннона // Материалы Международной конференции по цифровой обработке сигнала и её приложениям «ДСПА-2020»: электронный сборник статей. — М., 2020.

99. *Золотарёв В.В.* Способ декодирования помехоустойчивого кода: патент на изобретение РФ № 2721937 от 25.05.2020 г.

100. *Zolotarev V.V., Zubarev Y.B., Ovechkin G.V.* Optimization Coding Theory and Multithreshold Algorithms // Geneva, ITU, 2015. — 159 p. https://mtdbest.ru/articles/Zolotarev_ITU.pdf

101. *Зяблов В.В., Коробков Д.Л., Портной С.Л.* Высокоскоростная передача сообщений в реальных каналах связи. — М.: Радио и связь, 1991.

102. *Золотарёв В.В.* Многопороговое декодирование // Проблемы передачи информации. — 1986. — Т. 22, вып. 1. — С.104–109. http://mi.mathnet.ru/rus/ppi/v22/i1/p104

103. *Золотарёв В.В.* О реальностях теории кодирования: что там есть на самом деле. https://mtdbest.ru/articles/book2018_full_response.pdf

104. *Федоренко С.В.* Методы быстрого декодирования линейных блоковых кодов. — СПб., 2008. — 198 с.

105. *Морелос-Сарагоса Р.* Искусство помехоустойчивого кодирования. — М.: Техносфера, 2006. — 314 с.

106. *Трифонов П.В.* Методы построения и декодирования многочленных кодов: дис. ... д-ра тех. наук. — СПб., 2018.

107. *Милославская В.Д.* Методы построения и декодирования полярных кодов: дис. ... канд. тех. наук. — СПб., 2014.

108. *Кузнецов Н.А., Золотарёв В.В., Овечкин Г.В., Овечкин П.В.* Недвоичные многопороговые декодеры и другие методы коррекции ошибок в символьной информации для систем передачи и хранения данных // Радиотехника. — 2010. — №6. — С.4–9. https://mtdbest.ru/articles/Zolotarev_radiotechnik_2010.pdf

109. *Гладких А.А. и др.* Методы эффективного декодирования избыточных кодов и их современные приложения. — Ульяновск: УлГТУ, 2016. — 260 с.

110. *Гладких А.А.* Основы теории мягкого декодирования избыточных кодов в стирающем канале связи. — Ульяновск, 2010. — 380 с.

111. Программа моделирования работы многопорогового декодера. https://mtdbest.ru/program/mtd.zip

112. *Зигангиров Д.К., Зигангиров К.Ш.* Декодирование низкоплотностных кодов с проверочными матрицами, составленными из перестановочных матриц, при передаче по каналу со стираниями // Проблемы передачи информации. — 2006. — Т. 42, вып. 2. — С.44–52.

113. *Зяблов В.В., Рыбин П.С.* Исправление стираний кодами с малой плотностью проверок // Проблемы передачи информации. — 2009. — Т. 45, вып. 3. — С.15–32.

114. *Зяблов В.В., Рыбин П.С.* Анализ связи свойств МПП-кодов и графа Таннера // Проблемы передачи информации. — 2012. — Т. 48, вып. 4. — С.3–29.

115. *Зяблов В.В., Йоханнессон Р., Лончар М.* Просто декодируемые коды с малой плотностью проверок на основе кодов Хемминга // Проблемы передачи информации. — 2009. — Т. 45, вып. 2. — С.25–40.

116. *Кудряшов Б.Д.* Основы теории кодирования: учебное пособие для вузов. — СПб.: БХВ-Петербург, 2016. — 393 с.

117. *Arikan E.* Channel Polarization: A Method for Constructing Capacity-Achieving Codes for Symmetric Binary-Input Memoryless Channels // IEEE Trans. Inf. Th. — 2009. — Vol. 55, No. 7. — P.3051–3073.

118. *Zolotarev V., Ovechkin G., Ovechkin P., Satybaldina D., Tashatov N., Sankibayev D.* High Throughput Software Multithreshold Decoder on GPU // 3rd Intern. Conf. Mathematics and Computers in Sciences and in Industry (MCSI), Chania, Greece, Aug. 27–29, 2016.

Указатель терминов и определений

адаптация 210
алгоритм Витерби 5, 19, 71, 75, 134, 198, 215
    блоковый 11, 134, 135, 210, 215
    свёрточный 135
алгоритм Судана 168, 169, 175

вектор
    кодовый 37, 83
    разностный 77, 79, 101
    синдрома 41, 77–79, 83, 101

граница Шеннона 3, 7, 9, 13, 16, 17, 22, 25, 26, 32, 53, 128
граница сферической упаковки 58

декодер
    мажоритарный 33, 60, 67
    многопороговый 7, 16, 20, 84
    на ПЛИС Altera 148, 152, 173
    пороговый символьный 64, 167
    с «джинном» 110
    с прямым контролем метрики 11, 134, 143, 201
декодер Витерби 49
декодирование
    дивергентное 133, 147
    сверхдостоверное 174
демо-программы алгоритмов декодирования 129, 203, 206
дивергенция 149, 213, 217

зависимость
    вероятности ошибки 90, 133
    от размножения ошибок 91

канал
    гауссовский (с АБГШ) 44
    двоичный симметричный 44
    с экстремально большим шумом 8
    стирающий 46
каскадирование 62, 113, 150, 152, 186, 188
    параллельное 148, 191–193, 211, 217
    последовательное 187, 211
    с ККЧ 150, 188

код
  квазициклический 38
  переменный во времени 110
  полярный 33, 174
  с «выкалыванием» 215
  с кратными скоростями 110, 192
  с низкой плотностью проверок на чётность (LDPC) 164
  самоортогональный 41
  турбо 71, 174, 199
кодовый кластер 9, 48
конвергенция решений 218
коэффициент совершенства Золотарёва 54
КПД использования канала 53, 173

матрица
  порождающая 37–39, 92
  проверочная 37, 39, 40, 83
многопороговый декодер
  для восстановления стираний 170
модем
  жёсткий 44
  мягкий 44, 49, 88
модуляция
  многопозиционная 196
  фазовая 44

Оптимизационная Теория помехоустойчивого кодирования 7, 32, 78, 128
оптимизационные процедуры 163, 207
оптимизирующие программы 205
ортогональность 41
Основная Теорема многопорогового декодирования 8, 20, 84, 175
  для символьного (недвоичного) МПД 94

поиск глобального экстремума 75, 82, 86, 186, 205
поле Галуа 37
полином порождающий 40, 41, 60
принцип дивергенции 103, 145, 211, 217
проблема Шеннона 3, 9, 146, 152
производящая функция вероятности 62, 90, 105, 107
  многомерная 106, 107

размерность проверок 62, 63

размножение ошибок 21, 22, 104, 176
    верхняя оценка для пакета из двух ошибок 109
    нижняя оценка для одиночной ошибки 89, 109
разностный регистр 79, 80
расстояние 40, 76, 77
    Хемминга 37, 79, 92
    минимальное кодовое 37–39, 57, 65
    свободное 39, 57
решающая функция 65

синдром 102
синергетическое взаимодействие 145, 217
сложность
    АВ блокового 11, 177, 203
    АВ свёрточного 11
    МПД 53
    аппаратуры 49
    декодера 200
    декодирования 33, 188
    реализации 33, 191, 210
стремление к решению ОД 34, 72, 82, 86, 104

ускоренное вычисление сумм 176
устойчивость решений МПД 87, 88

функция правдоподобия 89

Чейза метод 177, 210

энергетический выигрыш кодирования 5, 51, 102, 149
    предельный 51
эффективность декодирования 48

Оглавление

От научного редактора 3
О новом формате прикладной теории кодирования 16
От автора 19
Введение 32
Глава 1. Основы теории кодирования и мажоритарных алгоритмов 37
1.1. Линейные коды 37
1.2. Единство блоковых и свёрточных кодов 42
1.3. Каналы связи 43
1.4. Алгоритмы декодирования корректирующих кодов 46
1.5. Эффективность декодирования 48
1.6. Длины используемых кодов 57
1.7. Пороговое декодирование и повторная коррекция 60
1.8. Вероятность первой ошибки порогового декодера самоортогонального кода 62
1.9. Пороговые процедуры для недвоичных кодов 64
1.10. «Мажоритарное» декодирование в стирающих каналах 68
Глава 2. Основные принципы многопорогового декодирования 71
2.1. Об «избыточной» корректирующей способности мажоритарных методов 73
2.2. Принцип глобальной оптимизации функционала 75
2.3. Алгоритм многопорогового декодирования 82
2.4. Гауссовский канал 88
2.5. Предельные возможности МПД алгоритмов в гауссовских каналах 89
2.6. Символьные (недвоичные) коды 91
2.7. Нижние границы эффективности символьных МПД 97
2.8. Итеративные «мажоритарные» процедуры в каналах со стираниями 98
2.9. Несистематические коды 101
2.10. Многопозиционные системы сигналов 102
2.11. Расширение области приложения принципов МПД 103
2.12. Размножение ошибок в мажоритарных схемах декодирования 104
2.13. Особенности контроля уровня размножения ошибок 113
2.14. Об особых свойствах МПД и ОТ 120
2.15. О компактности и совершенстве ОТ 124
2.16. Выводы 127

Глава 3. Основные достижения Оптимизационной Теории ... 128
3.1. Принципы дивергентного кодирования ... 129
Список литературы ... 135
3.2. Блоковая модификация алгоритма Витерби ... 135
Список литературы ... 144
3.3. О синергетическом взаимодействии дивергентности и каскадирования ... 145
Список литературы ... 152
3.4. Расширение возможностей применения блоковых версий алгоритма Витерби ... 153
3.4.1. История вопроса ... 153
3.4.2. Гибкость методов реализации БАВ ... 154
3.4.3. Технологии реализации БАВ для длинных кодов ... 156
3.4.4. О методах каскадирования при использовании технологий ОТ ... 157
3.4.5. Заключение ... 159
Список литературы ... 161
3.5. Этапные прикладные достижения Оптимизационной Теории ... 163
3.5.1. Введение ... 163
3.5.2. Гауссовские каналы ... 164
3.5.3. Символьные коды ... 167
3.5.4. Стирающие каналы ... 170
3.5.5. Специальные приложения ОТ ... 172
3.5.6. Основные ресурсы классической теории ... 174
3.5.7. Интеллектуальное пространство ОТ ... 175
3.5.8. Заключение ... 178
Список литературы ... 180
3.6. Выводы ... 185
Глава 4. Технологии теории информации для ОТ ... 186
4.1. Использование МПД в классических каскадных схемах ... 186
4.2. Каскадирование с кодами контроля по четности ... 188
4.3. Применение МПД в схемах параллельного каскадирования ... 191
4.4. Кодирование для систем многопозиционной модуляции ... 196
4.5. Использование МПД для кодов с неравной защитой символов ... 196
4.6. ОТ: приём эстафеты от алгебраической теории кодирования ... 198

Глава 5. Технологические средства поиска глобального экстремума 205
5.1. Программное обеспечение для исследований в области ОТ 205
5.2. Особенности процедур набора статистики и оптимизации . 208
5.3. Краткий обзор руководящих парадигм ОТ 210
5.4. Интеллектуальный космос развития методов кодирования . 212
Глава 6. Рекомендации к дальнейшим исследованиям 215
6.1. Алгоритмы Витерби 215
6.2. Алгоритмы МПД 216
6.3. Принцип дивергенции — расширение приложений..... 217
6.4. Конвергенция решений 218
6.5. Комплексный подход 219
Заключение 220
Приложение 1. Примерное ТЗ на разработку системы кодирования 238
Приложение 2. Таблицы 240
Приложение 3. Об итогах конкурса двух теорий..... 243
Список сокращений 251
Список литературы..... 252
Указатель терминов и определений 262

Адрес издательства в Интернет www.techbook.ru

Научное издание

Золотарёв Валерий Владимирович

Оптимальные алгоритмы декодирования Золотарёва
(Оптимизационная Теория – компактное
совершенное решение проблемы Шеннона)

Под научной редакцией
члена-корреспондента РАН Ю.Б. Зубарева

Редактор Г. В. Овечкин
Компьютерная верстка А. А. Терещенко
Обложка художника О. Г. Карповой

Подписано в печать 09.09.2021. Формат 60×88/16. Уч. изд. л. 16,88.
Печать цифровая. Изд. № 210919.
ООО «Научно-техническое издательство «Горячая линия – Телеком»