Обзор проблем полярных кодов с позиции технологий Оптимизационной Теории помехоустойчивого кодирования

Н. А. Кузнецов [1], В. В. Золотарёв [2], Г. В. Овечкин [3], Р. Р. Назиров [2], Д. Ж. Сатыбалдина [4], Е. Д. Омирбаев [4]

[1] *Институт радиотехники и электроники им. В. А. Котельникова РАН*
Москва, 125009, Россия
E-mail: kuznetsov@cplire.ru

[2] *Институт космических исследований РАН, Москва, 117997, Россия*
E-mail: zolotasd@yandex.ru

[3] *Рязанский государственный радиотехнический университет им. В. Ф. Уткина*
Рязань, 390005, Россия
E-mail: g_ovechkin@mail.ru

[4] *Евразийский национальный университет им. Л. Н. Гумилева*
Казахстан, 010008, Астана
E-mail: satybaldina_dzh@enu.kz

Рассмотрена общая ситуация в прикладных вопросах теории кодирования. Изложены основные проблемы, возникающие в области декодирования помехоустойчивых кодов. Особое внимание наряду с корректирующей способностью уделяется вычислительной сложности данных алгоритмов. Представлены последние результаты в области алгоритмов декодирования для полярных кодов (ПК), изложены основные проблемы их развития. Выполнено сопоставление прикладных результатов Оптимизационной Теории (ОТ) и имеющихся крайне ограниченных материалов для ПК. Кратко упомянуты результаты для низкоплотностных кодов. Представлены результаты сравнительного анализа характеристик ПК и блоковой версии алгоритма Витерби для коротких кодов. Также выполнено сравнение возможностей ПК и многопороговых декодеров алгоритмов, в том числе и при использовании каскадирования. Даны основные направления развития и улучшения характеристик алгоритмов ОТ. По итогам сравнения сделан вывод о безусловном лидерстве ОТ и об отсутствии необходимости применения ПК и ряда других кодов где-либо вообще в силу неизбежно слабых возможностей и большого списка недостатков декодеров этих направлений и методов их разработок в исследованиях для новых проектов спутниковой и космической связи, а также для систем дистанционного зондирования Земли.

Ключевые слова: граница Шеннона, пропускная способность канала, сложность алгоритмов, полярные коды, списочное декодирование, оптимальное декодирование, Оптимизационная Теория, блоковый алгоритм Витерби, коды Рида – Соломона, низкоплотностные и турбо-коды, многопороговые декодеры, параллельное каскадирование, дивергентный принцип, декодеры с прямым контролем метрики

Одобрена к печати: 29.06.2020
DOI: 10.21046/2070-7401-2020-17-4-9-26

Общая ситуация в прикладных вопросах теории кодирования

Как известно, турбо-коды, как и декодеры для кодов с низкой плотностью проверок (*англ.* Low-density parity-check code — LDPC), появившиеся в последнем десятилетии прошлого века, так и не стали локомотивами развития каких-либо новых направлений в теории кодирования двоичных потоков данных, на что мы неоднократно указывали в наших основных монографиях и ключевых публикациях (Золотарёв, 2006, 2018; Золотарёв, Овечкин, 2014; Золотарёв и др., 2012; Zolotarev, 2018; Zolotarev et al., 2015), в обзорах (Золотарёв, Овечкин, 2010; Золотарёв и др., 2015, 2018; Кузнецов и др., 2010; Zolotarev et al., 2017), справочнике (Золотарёв, Овечкин, 2004) и на наших сетевых порталах www.mtdbest.ru и www.mtdbest.iki.rssi.ru. Для этого было много причин.

Даже при рассмотрении только двоичных кодов этих классов эффективные алгоритмы их декодирования не укладываются в рамки операций с фиксированной точкой, т. е. такие декодеры вынуждены использовать арифметику действительных чисел, что сразу перевело их в разряд не самых простых методов. Кроме того, сложность декодирования этих кодов или существенно больше, чем линейная, или требует вычисления весьма неудобных функций, что дополнительно заметно замедляет их работу. Более того, и сами оценки сложности N для этих кодов на самом деле очень таинственны, так как за единицу такой сложности там обычно принимаются не простейшие операции типа сложений и сравнений, а циклы процедур (Милославская, 2015), особенности аппаратной реализации (Афанасьев и др., 2016), размеры списков решений и другие странные параметры (Афанасьев и др., 2016; Зяблов, Рыбин, 2012; Зяблов и др., 2009; Трифонов, 2018; Tal, Vardy, 2015).

Дополнительные трудности возникают у этих методов при их применении к свёрточным кодам. Можно отметить структурные проблемы кодов данного класса (Назаров, Щеглов, 2017). В течение длительного времени специалисты по декодерам турбо- и LDPC-кодов предпочитали не замечать и того противоречия, что, хотя целью этих алгоритмов было положено успешное декодирование вблизи пропускной способности каналов, например с аддитивным белым гауссовским шумом (АБГШ), каких-либо значимых результатов, например о том, что, последовательность решений этих итеративных методов вблизи границы Шеннона приближается к решению оптимального декодера, не было получено. Данные алгоритмы не измеряют расстояния своих решений до принятого сообщения, как декодеры с прямым контролем метрики (ДПКМ) (Золотарёв, 2018; Зубарев и др., 2019; Кузнецов и др., 2020; Zolotarev, 2018), что во многих случаях затрудняет достижение ими наилучших возможных результатов при достаточно высоких уровнях шума, даже если допустить дальнейшее значительное усложнение подобных декодеров. Но ожидать от алгоритма, который не измеряет расстояния своих решений до принятого, что он вообще «увидит» достижение требуемого результата, не приходится.

Возникает и ещё одна неожиданная сложность при сопоставлении этих проблемных алгоритмов, которая связана с тем, что в некоторых работах по данным направлениям допускаются отказы от декодирования. Как относиться к результатам такого декодирования, когда получается, что блоки могут просто «исчезать»? Допускать наличие переспроса? Но это уже принципиально другая постановка задачи. В значительной мере наличие этой и других подобных проблем с отказами в «старой» теории кодирования, проявившихся ещё в алгоритмах последовательного декодирования, и заставляет адептов «классики» придумывать всяческие откровенные «фокусы» для оправдания существования своих «методов», результаты работы которых даже непонятно как интерпретировать. Приходится не забывать, что и декодирование списками (из-за крайне низкой эффективности исходных алгоритмов) в рамках и «старых», и «новых» методов также полностью разрушает исходную постановку задачи декодирования, так как непонятно, что должна делать система связи, получившая 10 или 1000 сообщений на выбор, если она настроена на единственность используемого в дальнейшем сообщения, в котором всё же допустимы очень редкие ошибки. Все рассмотренные выше крайне неопределённые для реальных систем связи ситуации наглядно иллюстрируют общесистемный кризис «классической» теории кодирования, которая изначально не могла решать всех реальных задач высокодостоверной передачи цифровых данных и многих системных проблем сетей связи, особенно при больших уровнях шума.

Заметим, что в теоретических и прикладных исследованиях в рамках Оптимизационной Теории (ОТ) вообще не допускаются указанные выше кризисные ситуаций в алгоритмах. В ОТ существуют только правильные и ошибочные решения декодеров в каких-то символах. Разумеется, в ОТ всегда есть возможность уточнить постановку задачи и в случае малой надёжности тех или иных символов решения декодера их изредка можно объявить стёртыми, что значительно увеличит достоверность оставшихся битов данных. Но для системы связи это намного более естественная ситуация, чем использование списков. И в этом случае не происходит потери больших фрагментов передаваемой информации. Однако при анализе и публикации характеристик многопороговых декодеров (МПД) и различных версий алгоритма

Витерби (АВ) в ОТ практически никогда не пользуются даже этой допустимостью редких стираний наименее надёжных символов, показывая естественные возможности наших декодеров именно в традиционном первоначальном формате.

Но ситуация в теории кодирования второй половины прошлого века на самом деле ещё более драматична. Дело в том, что задачи декодирования недвоичных кодов уже в течение 60 лет находятся в кризисном состоянии, так как более технологичных алгоритмов их декодирования, чем для случая кодов Рида – Соломона (РС), так и не появилось. Турбо- и LDPC-коды тоже не продемонстрировали особо значимых успехов в результатах декодирования (см. (Кузнецов и др., 2010) и цитируемую литературу).

Отметим пока только кратко, что и полярные коды (ПК) потерпели абсолютное фиаско в реализации процедуры декодирования недвоичных кодов. Об этом свидетельствуют известные результаты, где алгоритмы декодирования ПК, основанных на кодах РС, имеют сложность порядка $N \approx n^2$, а в некоторых случаях и $N \approx Ln^3\log(n)$, где n — длина кода, причём операции проводятся в поле действительных чисел, а размер списка решений L при достаточно эффективном декодирования должен расти экспоненциально (Милославская, 2015). И это при том, что с 1984 г. известно о простейших, с линейной сложностью (т. е. с $N \approx n$), символьных (недвоичных) МПД-декодерах (Золотарёв, 1984, 2018; Золотарёв, Овечкин, 2004, 2010; Кузнецов и др., 2010, 2020), реализующих к тому же и фактически наилучшее оптимальное декодирование (ОД), эквивалентное переборному, при весьма высоких уровнях шума.

Жаль, но, как и в двоичном случае, авторы немногих новых методов для кодов РС не предъявили никаких действительно полных данных об эффективности и сложности их способов декодирования. Все опубликованные теоретические монографии по быстрому декодированию кодов РС и некоторых других структур, затем оформленные как докторские «достижения», остались, как и десятки лет назад, на уровнях сложности порядка $N \approx n^2$ или в лучшем случае $N \approx n{\cdot}\log(n)^2$) (Трифонов, 2018; Федоренко, 2008), что практически вообще ничего не меняет по существу вопроса. Иначе говоря, новых результатов в сфере недвоичных кодов уже 60 лет нет, а линейная сложность алгоритмов ОТ даже при большом уровне шума канала почти 40 лет вообще «не замечается».

И здесь снова полезно напомнить, что наша научная школа ОТ уже много лет настаивает на том, что полноценная публикация по прикладным вопросам кодирования должна обязательно содержать и полную проверяемую программу моделирования нового алгоритма. Но за последние десятилетия ни одна научная группа не представила реального эффективного алгоритма с детальным описанием и полноценной программой моделирования, который можно было бы полностью проверить по стандартному комплексному критерию «достоверность — помехоустойчивость — сложность», хотя некоторые авторы декларируют использование языка программирования С++ при моделировании, не сообщая никаких сведений о быстродействии реализованных алгоритмов (см., например, работу (Милославская, 2015)).

В связи с этим мы вынуждены снова отметить, что в ОТ все, в том числе и недвоичные (символьные) коды с МПД-декодированием обрабатываются с теоретически минимально возможной сложностью $N \approx n$. При этом декодеры МПД всех типов работают только в арифметике с фиксированной точкой (т. е. с целыми числами) и достигают решений ОД при уровнях шума, весьма близких к границе Шеннона (Золотарёв, 2006, 2018; Золотарёв, Овечкин, 2004, 2014; Золотарёв и др., 2012; Zolotarev, 2018; Zolotarev et al., 2015).

Подчеркнём, что упорное игнорирование всеми российскими «теоретиками» результатов ОТ на самом деле лишь обнуляет их собственные «научные» измышления за последние 30 лет. Отметим, что этот реальный трагический кризис сложился по той простейшей методологической причине, что вероятности ошибки никаких алгоритмов декодирования нигде и никогда не могут быть получены аналитически для областей шума каналов вблизи их пропускной способности. Но у нас в течение десятилетий очень многие «служители науки» никак не могут осознать этот непреложный факт. Ещё более сложные подходы к моделированию, в частности к аппаратному макетированию (чем мы тоже активно и очень успешно занимаемся (Золотарёв, 2018; Кузнецов и др., 2020; Zolotarev, 2018; Zolotarev et al., 2015)), мы далее рассматривать не будем.

Проблема соотношения теории и эксперимента возникла в науке около 40 лет назад, и она настолько остра и драматична, что некоторые публикации по этой теме были представлены даже на портале Российской академии наук (Магаршак, 2009). Строгая и всесторонняя оценка этой давно застоявшейся чрезвычайно конфликтной системно-организационной ситуации в отрасли теории кодирования последних 40 лет также лежит за рамками данной статьи.

Проблемы полярных кодов как крайнее проявление кризиса «старой» теории

Полярные коды (Arikan, 2009), десятилетие появления которых прошло почти незамеченным, явились печальной иллюстрацией продолжения глубокого кризиса классической теории кодирования, который длится уже более 30 лет. Именно поэтому при крайнем дефиците позитивных идей для развития теории кодирования и, видимо, отсутствии вообще каких-либо знаний о простом блоковом алгоритме Витерби (БАВ) (Золотарёв, 2018; Золотарёв, Овечкин, 2017; Зубарев и др., 2019; Кузнецов и др., 2020; Zolotarev, 2018), а также при полном непонимании глубины идей ОТ, согласно которым каждое изменение декодируемого символа во всех типах МПД-декодеров соответствует переходу к строго более правдоподобному решению, мировое сообщество специалистов по кодам начало активно анализировать и развивать именно ПК. «Теоретикам» в который уже раз снова показалось, что вот эти-то коды можно анализировать и развивать аналитически, без проведения каких-либо масштабных экспериментальных работ по компьютерному моделированию. А это ещё более углубило кризис теории кодирования.

Однако про ПК стало быстро ясно, что и они никак не способствуют прогрессу прикладной теории кодирования, т. е. разработке простых и, главное (!), технологичных декодеров вблизи границы Шеннона. Алгоритмы для ПК сразу должны были работать в области действительных чисел, а гарантированная вероятность ошибки декодирования уменьшалась с длиной кодов n крайне медленно, лишь как $\sim n^{-0,25}$ (Arikan, 2009), о чём адепты этого метода предпочитали вообще не распространяться. А ведь это, например, значит, что даже для типичной небольшой вероятности ошибки $P_w(e) \approx 10^{-5}$ в блоке для канала типа ДСК (двоичный симметричный канал) размер блока ПК должен быть $n \approx 10^{20}$! Безусловно, это никак не воодушевляет. И очевидно, что даже только по этой причине данная идея была уже изначально чрезвычайно сомнительной. От такой безысходности апологеты этого направления указывали, как мы цитировали в работе (Золотарёв, Овечкин, 2016), на весьма ограниченные возможности ПК, особенно при малых длинах кодов n. Приходится добавить, что очень проблемным вопросом ПК навсегда, видимо, останется и точность квантования действительных чисел (Трифонов, 2018; Seidl, Huber, 2013). С этим, как часто указывают, связана и проблема недостаточности обычной арифметики с плавающей запятой для точного учёта динамического диапазона используемых данных. Да и вообще, как признали, например, авторы (Giard et al., 2014), кроме алгоритмов декодирования и сами ПК могли бы быть получше. В частности, в работе (Ozgur, 2009) было показано, что полярные коды существенно уступают турбокодам по энергетическому выигрышу для всех возможных кодовых скоростей и типов каналов при одинаковых длинах. Полярные коды конечной длины уступают по эффективности и LDPC-кодам (Ammar, 2018; Tal, Vardy, 2015).

Как следствие, изначально слабые процедуры декодирования ПК стали преобразовывать в списочные декодеры (Sarkis et al., 2016; Tal, Vardy, 2015), применять к ним методы каскадирования и другие меры, что уже как-то и не очень было связано, а точнее абсолютно оказалось не связанным с исходными идеями ПК, хотя характеристики декодирования при этом по сравнению с заявленными в работе (Arikan, 2009) алгоритмом несколько улучшались (Золотарёв, Овечкин, 2016), как это и должно быть согласно основам теории кодирования и возможностям каскадирования.

Наконец, вновь укажем, что мы ни в одной из просмотренных нами публикаций не нашли каких-либо данных о реальной сложности декодеров ПК. Мы имеем в виду, что, как это уже неоднократно отмечалось в публикациях (Золотарёв, 2018; Кузнецов и др., 2020; Zolotarev, 2018), единственным на текущий момент реально полезным способом определения сложности конкретных алгоритмов декодирования, в минимальной степени подверженным ошибкам, искажениям и прямому обману, является предъявление редакциям журналов, рецензентам и оппонентам по диссертациям работающей проверяемой программы моделирования в гауссовском или ином канале с указанием типа процессора, его тактовой частоты и, главное, числа декодируемых символов в секунду при реализации алгоритмов, например на языке С++. Напоминаем, что для облегчения задачи правильного сравнения алгоритмов декодирования мы на порталах www.mtdbest.ru и www.mtdbest.iki.rssi.ru предложили средства сравнения скоростей декодеров, выделив для этого программы калибровки скоростей декодирования, также на С++, для случая использования различных компьютеров. Методы просты и общедоступны.

Исходя из описанной ситуации укажем только, что сторонникам методов ПК не следует продолжать испытывать терпение специалистов по алгоритмам декодирования ещё и следующие 10 лет, поскольку, видимо, период неумеренного увлечения декодерами ПК уже проходит. Ведь никаких конкретных и, главное, достоверных данных о реальном объёме вычислений хотя бы для одного декодера ПК нигде по-прежнему нет.

Соотношение возможностей ОТ и ПК

В настоящее время, как указано в работах (Золотарёв, 2018; Золотарёв, Овечкин, 2004; Золотарёв и др., 2012; Zolotarev, 2018; Zolotarev et al., 2015), на основе Оптимизационной теории помехоустойчивого кодирования для всех классических каналов с независимыми искажениями создан целый ряд новых декодеров класса МПД и новых модификаций АВ, в том числе и БАВ (Золотарёв, 2018; Золотарёв, Овечкин, 2017; Зубарев и др., 2019; Zolotarev, 2018). Они вместе с наилучшими уже известными подходами на основе свёрточных АВ, каскадных или дивергентных схем и других методов обеспечивают успешное декодирование с линейной от длины кодов сложностью МПД-декодеров в непосредственной близости от пропускной способности этих каналов. Полученные результаты позволяют утверждать, что ОТ создала алгоритмы и конкретные технологии разработки декодеров, соответствующих решению великой проблемы Шеннона, сформулированной им более 70 лет назад (Золотарёв, 2018; Золотарёв и др., 2018; Зубарев и др., 2019; Кузнецов и др., 2010; Zolotarev, 2018; Zolotarev et al., 2015, 2017). Тем самым новая ОТ для всех классических каналов превратилась в обширный набор технологий и парадигм, в рамках которых теперь можно создавать очень различные максимально простые в реализации декодеры, работающие вблизи пропускной способности каналов связи и обеспечивающие при правильном выборе кодов достижение решений ОД.

Возможности ПК соответствуют принципиально другой постановке задачи помехоустойчивого кодирования. В связи со слабыми возможностями ПК и их алгоритмов декодирования, а также с неэффективностью длинных кодов специалисты сосредоточили наибольшее внимание на ПК для относительно коротких кодов, что сразу исключило обсуждение близости области их работы к пропускной способности каналов. Постоянные ссылки адептов ПК на то, что эти коды «добрались» до границы Шеннона, свидетельствуют только о непонимании такими авторами абсолютной бесперспективности всей этой затеи. Мы уже отмечали это выше. Кроме того, как это часто происходит последнее время в научном сообществе, «теоретики» ПК отказались вообще обсуждать сложность таких алгоритмов и опять (снова ошибочно!) решили, что для ПК можно практически всё рассчитать, а значит, как и раньше, совсем не заниматься полноценным моделированием алгоритмов. Как и с попытками решения задач с турбо- и LDPC-кодами, за 10 лет «раскрутки» ПК это не привело к правильному реалистичному отношению к данным кодам. Разумеется, никаких действительно полезных для технологий соотношений между возможностями ОД и ПК теоретики тоже не получили. ОТ с её более чем 40-летней историей давно заслуживает внимания к своим методам, и сторонники ПК совершенно зря ими не воспользовались. Насколько мы понимаем, с ПК на качественном уровне произошло то же самое, что и полвека назад с алгебраическими кодами, когда в цифровых пространствах не удалось создать такие обширные пространства дискретных полей, чтобы они полностью покрывали все допустимые шумовые конфигурации (что и ограничило сразу возможности алгебраических кодов). Но у ПК это случилось в результате сложностей точных вычислений с действительными числами и по другим указанным выше причинам, что уже само по себе привело и к множеству различных проблем ПК. Таким образом, исследования в области ПК не содержат важных результатов, хотя бы отчасти близких к уровню ОТ, как, например, Основная Теорема многопорогового декодирования (ОТМПД). И опять же, сложность МПД-декодеров линейна по n. А сложность ПК — это всё же $N \approx n\ln(n)$, причём это в основном операции с действительными числами в больших циклах вычислений (Милославская, 2015). И это всё, конечно, довольно непросто в плане реализации и крайне неопределённо для каких-либо вообще разумных оценок сложности.

Далее, с учётом вышесказанного, рассмотрим возможности ОТ и ПК для небольших длин кодов, т. е. в области, к работе в которой методы ОТ совершенно никем не адаптировались специально. Из этого класса алгоритмов мы выбирали только обычные схемы и коды с уже известными неплохими характеристиками. Подчеркнём также, что ОТ содержит в качестве основных алгоритмов все модификации МПД-декодеров и различные версии АВ, включая запатентованные нашей школой БАВ (Золотарёв, 2018; Золотарёв, Овечкин, 2017; Зубарев и др., 2019). Разумеется, при появлении хотя бы предварительных конкретных и понятных данных по реальной эффективности и сложности ПК мы получим возможность публикации и более точных результатов сопоставления методов ОТ и ПК.

Сравнительные характеристики ПК и АВ для коротких кодов

Поскольку данных о реальной сложности ПК (увы, повторим это) нет, рассмотрим немногие доступные сведения о достоверности алгоритмов ПК и уже известные или обновлённые результаты для методов ОТ. Начнём с сопоставления ПК и БАВ. Будем рассматривать самые простые схемы БАВ, причём пока без какой-либо связи с методами ПК и без адаптации к ним.

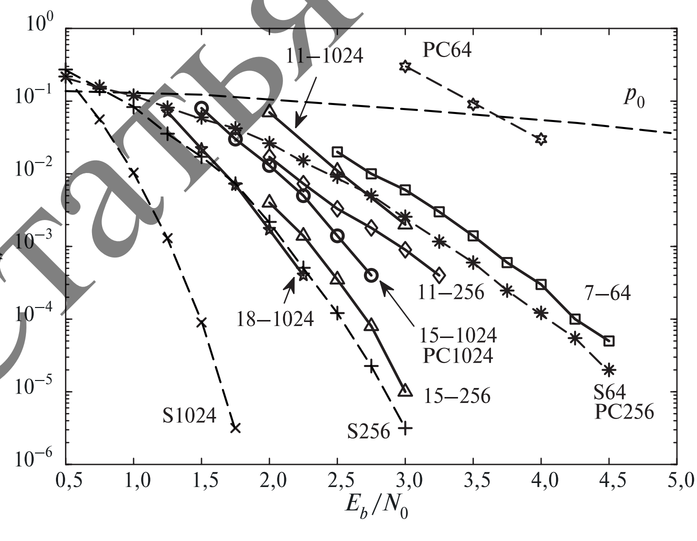

Рис. 1. Границы сферической упаковки и характеристики БАВ для кодов с $R = 1/2$ в канале с АБГШ

На *рис. 1* представлены границы сферической упаковки (пунктирные линии) для блоковых кодов в гауссовском канале с квантованием на 4 бита при кодовой скорости $R = 1/2$ в формате Sn, где n — длина блока. Остальные сплошные графики вида K-n соответствуют вероятностям ошибки декодирования блока $P_w(e)$ квазициклического блокового кода с использованием

БАВ для порождающего кодового полинома свёрточного кода длины K и длины блокового кода n. Короткая линия PC64 показывает для полярных кодов длины $n = 64$ нижние оценки в работах (Милославская, 2015; Трифонов, 2018) для декодеров нескольких ПК при обычном декодировании, т. е. когда размер списка решений L равен 1. Остальные результаты (около 10) на тех же рисунках из этих диссертаций соответствуют различным размерам списка решений вплоть до $L = 256$. Все они близки к графику (7-64) для БАВ или существенно выше него, так как граница S64, как известно, недостижима. Вынужденно повторим, что никаких данных о реальной сложности таких декодеров ПК, например о числе операций или скорости декодирования, нет.

А теперь уточним данные графика 7-64. Программа для БАВ на языке С++ на процессоре 3 ГГц работает на скорости ~95 Кбит/с. Блоковый АВ имеет практически ту же сложность, что и свёрточный, который для $K = 7$ был разработан ещё 50 лет назад (Золотарёв, Овечкин, 2004, 2016, 2017; Золотарёв и др., 2015). Даже если программа для ПК хотя бы при $n = 64$ будет написана, то с учётом всех нерешённых проблем этих кодов при очень успешной работе БАВ всё равно будет нельзя считать, что это направление ПК — новый шаг в теории и технике кодирования.

Рассмотрим коды длины $n = 256$. На этом же *рис. 1* представлены результаты для кодов с БАВ-декодированием при $K = 11$ и $K = 15$. А нижняя оценка $P_w(e)$ для целого ряда декодеров ПК разных типов, в том числе каскадных, представленных в статье (Seidl, Huber, 2013), совпала с границей S64, отмеченной поэтому и подписью РС256. Как видно из сравнения кодов длины $n = 256$, даже у БАВ с порождающим свёрточным полиномом длины $K = 11$ характеристики лучше, чем у ПК. А с БАВ при $K = 15$ сравниться уже вообще никому из ПК нельзя: крайне слабые результаты.

Почему же для сравнения был взят БАВ с $K = 15$? Тут можно вспомнить, что элементная база электроники последние десятилетия становится всё более быстрой, как и собственно сами технологии. И тогда уже совсем неудивительно, что ещё в прошлом тысячелетии НАСА (Национальное управление по аэронавтике и исследованию космического пространства, *англ.* NASA — National Aeronautics and Space Administration) реализовала АВ с $K = 15$ и запустила его на космическом корабле проекта «Кассини» (*англ.* Cassini) к Сатурну. Проект триумфально завершился в 2017 г. И коды не подвели! Это значит, что $K = 15$ — абсолютно реальный параметр. Скорость работы БАВ с $K = 15$ при тех же условиях близка к 1000 бит/с. Кстати, для ОТ разработаны разные простые версии АВ до длин $K \approx 24$. Таким образом, нам есть что обсуждать при необходимости и в других случаях.

Нелишне обратить взимание читателей на тот важнейший момент, что далее многие характеристики БАВ будут с $K = 15$. Он в 16000 раз проще в реализации, чем ОД на основе АВ в публикациях (Кудряшов, 2016; Кузнецов и др., 2010), т. е. в том числе в издании, которое предлагается использовать для обучения студентов. Также в этом пособии выделяется обсуждение особенностей методов, которые даже для не очень длинных кодов дают сложность декодирования $N > 10^{200}$, что превышает количество атомов во Вселенной. Согласитесь, что это тоже очень впечатляет.

Наконец, обратимся к кодам длины $n = 1024$. Здесь представлены в явном виде два БАВ с $K = 15$ и $K = 18$. Добавим к этому, что для большей полноты оценок полезно оценить и возможности кода с $K = 11$. Он представлен линией (11-1024). Рассмотрим данные о ПК длины $n = 1024$. Нижняя оценка для группы таких кодов из статьи (Seidl, Huber, 2013), использующих разные «улучшения», в том числе и каскадирование, помеченная как РС1024, практически совпадает с кривой (15-1024). А тогда из графиков для кодов с $n = 1024$ следует, что БАВ при $K = 11$ немного слабее, чем ПК; при $K = 15$ достоверности близки, но при $K = 18$ БАВ гораздо лучше. Сложен ли такой БАВ? Он всего лишь в ~8 раз более медленный, чем при $K = 15$, и декодирует цифровой поток на тех же программных средствах со скоростью чуть более 100 бит/с. Но напомним, что АВ с $K = 15$ был создан в прошлом тысячелетии. Так что отвергать код с $K = 18$ не следует. Кроме того, аппаратная реализация АВ давно легко полностью распараллеливается и вообще АВ очень технологичен. Так что и тут трудно увидеть хотя бы какие-то преимущества ПК, особенно если учесть все как перечисленные, так и не упомянутые здесь проблемы этих кодов. А в программной реализации очень удобно использовать ещё и разные специализированные процессоры (Zolotarev et al., 2016). Здесь АВ, работающие только с целыми числами, имеют ещё бóльшие преимущества перед ПК, которые являются заложниками неустойчивых вычислений с действительными числами и массы других проблем.

В конце обсуждения графиков на *рис. 1* можно также указать, что возможности ПК длины $n = 1024$ даже при $L = 16$ достигают уровня не лучшего, чем тот, который показывает кривая 15-1024, а нижняя оценка для ПК с $n = 2048$ в работе (Giard et al., 2014) фактически соответствует кривой S256. Это означает, что ПК вообще не начинают приобретать каких-либо особых достоинств с увеличением длины кодов n или даже при учёте возможностей декодирования списком, что наша школа ОТ (подчеркнём этот принципиальнейший момент снова) полностью отвергает как неправомерное сравнение результатов при совершенно другой постановке задачи декодирования. И здесь никаких конкретных данных по реальной доказуемой сложности декодирования конкретных ПК найти не удалось.

Заметим, что на *рис. 1* были представлены характеристики и границы в том числе и каскадных вариантов ПК. А вся совокупность методов БАВ была представлена только своими простейшими базовыми версиями. Очевидно, что привлечение каскадных структур для АВ к сопоставлению декодеров, как это всегда и происходит при правильном проектировании и анализе каскадных схем, обязательно многократно улучшит эффективность и одновременно снизит сложность декодеров, созданных согласно технологическим парадигмам ОТ.

Оставляем возможность подтверждения изложенных здесь простых и абсолютно гарантированных результатов всем нашим коллегам, которые в этом случае будут обеспечены нашей самой разнообразной технологической и идеологической поддержкой. Успешное завершение такой важной работы по глубокому технологическому обновлению прикладной теории кодирования другими научными коллективами вполне может создать для них новую высокотехнологичную платформу для развёртывания широкой исследовательской деятельности во всех новых перспективных сферах ОТ.

Сравнение возможностей ПК и МПД-алгоритмов

Сравним кратко характеристики ПК и алгоритмов МПД, основных в теории ОТ, при условии выбора небольших длин применяемых кодов. Далее рассмотрены коды и МПД-алгоритмы также без какой-либо адаптации к условиям их сравнения с ПК. На *рис. 2* (см. с. 17) в том же формате представлены вероятности ошибки на кодовое слово $P_w(e)$ для кодов ПК в тех же гауссовских каналах. Кривая Arik2048 соответствует по данным (Морозов, 2013) оригинальному методу Арикана (Arikan, 2009) для ПК длины $n = 2048$. MS256 оценивает снизу возможности нескольких ПК длины $n = 256$, часть из которых имеет каскадную структуру (Seidl, Huber, 2013); MS1024 — нижняя оценка для значительного числа ПК, включая списочные алгоритмы их декодирования (Милославская, 2015; Seidl, Huber, 2013), которые, что мы всё время подчёркиваем, не должны сравниваться с традиционными методами, в том числе с алгоритмами ОТ. Но мы учли даже их! И наконец, для группы ПК длины $n = 2048$ представлены графики нижних оценок G2048 из работы (Giard et al., 2014) и DS2048 (Морозов, 2013) со ссылкой на статью (Dumer, Shabunov, 2006).

Сопоставим с ПК алгоритмы МПД для коротких кодов в тех же обозначениях OT256, OT1024 и OT2048. Во всех этих случаях применялись коды с $R = 1/2$ без использования каскадирования или других мер повышения эффективности. Число итераций декодирования у всех МПД — не более $I = 80$. Поскольку эти алгоритмы исключительно простые, то даже у МПД для кода длины $n = 2048$ скорость декодирования на тех же программных средствах превышает 140 Кбит/с. Достоверность результатов МПД или совпадает с возможностями ПК, или близка к ним. А это очень важно, так как для сравнения были взяты простейшие схемы МПД, в то время как декодеры ПК допускают использование списков, а сложность самих декодеров для ПК совершенно неопределённа, хотя в работе (Милославская, 2015) отмечается экспоненциальный рост размеров списков ($L >> 1000$), необходимость вычислений с действительными числами и в некоторых случаях — большое число итераций ($I > 10^4$). Но результаты для МПД очень близки даже к возможностям ПК в списочных вариантах. Отсюда следует, что применение ОТ и предлагаемых ею декодеров с прямым контролем метрики, среди которых МПД и различные АВ, решают вообще все проблемы декодирования и при ограничениях на длины кодов, причём на базе хорошо и давно изученных методов, которые предлагает ОТ. Существенно и то, что результаты получены без какой-либо адаптации к новым условиям сопоставления для небольших длин кодов, что, конечно, ещё многократно добавило бы эффективности методам ОТ. Также крайне важно, что все решения МПД-декодеров, взятых для сопоставления, как и в случае выбора длинных кодов, сходятся к оптимальным решениям при любой небольшой длине. Этим и обусловлено их преимущество перед всеми другими алгоритмами.

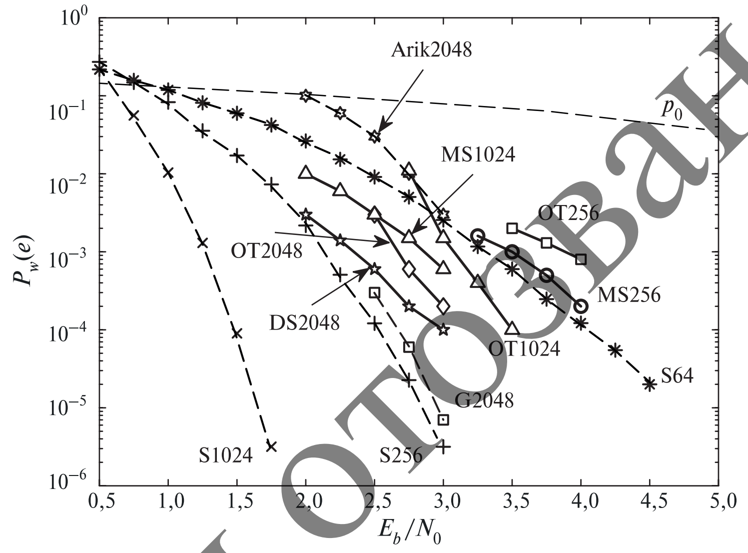

Рис. 2. Характеристики МПД и ПК для кодов $R = 1/2$ в канале с АБГШ

Более эффективные алгоритмы класса ОТ, например каскадные**,** можно будет проанализировать, если среди ПК будут выявлены коды и алгоритмы с конкретной предъявленной и убедительно доказанной сложностью декодирования. Однако этой ситуации можно и не дождаться, поскольку адепты ПК за последние 10 лет не удосужились предъявить ни одного такого декодера, а эффективность методов ОТ постоянно растёт, причём часто даже при некотором упрощении алгоритмов.

О методах улучшения характеристик алгоритмов ОТ

Как было показано выше, технология декодирования ПК очень мало связана с базовыми идеями помехоустойчивого кодирования и тем более — с оптимальным декодированием (ОД) или мощными методами ОТ, которые обеспечивают быструю, линейную от длины блока сходимость к ОД. Именно поэтому идею ПК не спасают даже всегда мощные каскадные схемы и абсолютно противоречащие исходной постановке задачи помехоустойчивого кодирования списочные методы с большим размером таких списков L. Как мы увидели, основные, простейшие по своей сути МПД и модификации АВ в ОТ вообще без какой-либо специальной дополнительной адаптации показали, безусловно, очень достойные высокие характеристики.

Тем не менее для читателей, которые готовы согласиться с тем, что ПК — тоже тупиковая ветвь в прикладных исследованиях теории кодирования, укажем некоторые варианты развития исследований в сфере ОТ, которые позволят, в чём мы абсолютно уверены, дополнительно существенно улучшить характеристики ОТ и при декодировании коротких кодов. Причём, как следует из уже представленных выше данных, реально нужно адаптировать методы ОТ для кодов длины $n = 1024...2048$, так как для более коротких кодов задача уже успешно решена. И тут сразу надо чётко указать, что в данной постановке задачи проблема сравнения ОТ с ПК даже не ставится. Никаких результатов у ПК, как мы увидели, вообще нет, а значит, и повод для такого обсуждения просто отсутствует. Иначе говоря, ниже предложены методы повышения эффективности ОТ, АВ и МПД безотносительно к каким-либо другим методам просто потому, что в настоящее время сопоставимых с ОТ технологий вообще не существует.

Рассмотрим для этого на *рис. 3* предварительные данные для кодов длины $n = 1024$ при $R = 1/2$ по вероятности ошибки на бит $P_b(e)$ для случая БАВ-декодирования. Кроме границы сферической упаковки S1024 в виде $P_w(e)$ и пунктира $P_b(e)$ для свёрточного кода с порождающим полиномом длины $K = 18$, все остальные графики $P_b(e)$ соответствуют порождающим полиномам длины $K = 15$, что, как мы обсудили выше, уже очень давно технологически вполне доступно. Основные графики вида S_k и N_k, где $k = 0$ и $k = 8$, соответствуют систематическим и несистематическим обычным кодам при $k = 0$ и перфорированным кодам при $k = 8$, т.е. с исключением каждого 8-го кодового символа второй кодовой ветви у исходного кода с $k = 0$.

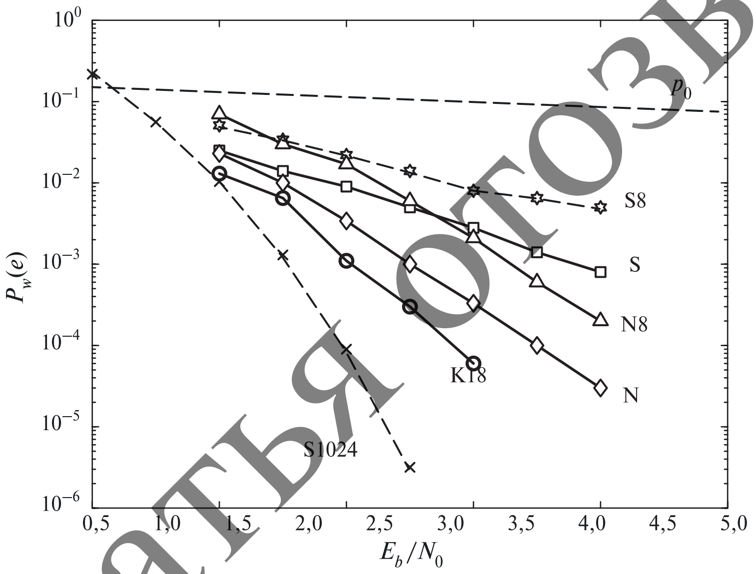

Рис. 3. Предварительные характеристики БАВ для кодов с $R = 1/2$ в канале с АБГШ

Как следует из *рис. 3*, достоверность перфорированных кодов весьма высока. Это гарантирует эффективность каскадирования с перфорированными кодами, которое должно быть успешным как в традиционных последовательных схемах, так и в параллельных, где у ОТ есть много полезных результатов. Советуем специалистам, действительно заинтересованным в развитии технологий декодирования, рассмотреть реальные возможности предлагаемых подходов, которые могут обеспечить значительное повышение эффективности алгоритмов коррекции ошибок. Школа ОТ гарантирует поддержку этим работам, консультирование и программное сопровождение.

Полезно обратить внимание и на код с $K = 18$. Мы полагаем, что внимательный анализ БАВ позволит сократить сложность его декодирования за счёт просмотра меньшего числа путей или на основе других методов, например использующих принцип дивергенции. Наконец, очевидно, что и без использования перфорированных кодов в БАВ можно рассматривать каскадирование кодов с $k = 0$ с внешними высокоскоростными кодами в обоих вариантах возможного каскадирования. Эти гарантированно положительные результаты, которые можно получить очень быстро, также будут очень полезны, хотя и при несколько меньшей, чем $R = 1/2$, итоговой скорости, но зато при существенно большей итоговой достоверности, что обычно и происходит при каскадировании такими методами.

Ещё раз подчеркнём необходимость чёткого понимания, что вероятности ошибки никаких алгоритмов декодирования при большом уровне шума никогда нельзя оценить аналитически. Теория кодирования, как это абсолютно безальтернативно доказала ОТ, — не математическая проблема (Золотарёв, 2018; Зубарев и др., 2018; Кузнецов и др., 2020). Все итоговые характеристики эффективности и сложности алгоритмов коррекции ошибок для большого уровня шума канала могут быть всегда очень быстро получены исключительно путём полномасштабного моделирования алгоритмов декодирования на основе различных оптимизационных методик (Золотарёв, 2018; Zolotarev, 2018; Zolotarev et al., 2015). Технологии ОТ и результаты их применения полностью и всесторонне подтверждают это важнейшее суровое обстоятельство, столь долго не признаваемое некоторой частью специалистов в области теории кодирования.

Замечания о «развитии» прочих алгоритмов

Отметим совсем кратко основные теоретические результаты текущего тысячелетия, которые публикуются некоторыми сторонниками LDPC-кодов, где виден крайне скромный уровень обсуждаемых методов, просто потому что и эти авторы избегают каких-либо работ по моделированию и разумных оценок сложности декодирования.

В статье (Зяблов и др., 2009) предложен метод «простого» декодирования LDPC-кода со странно определённой сложностью декодирования через ссылку на другую публикацию, тем не менее равной $N \approx n{\cdot}\ln(n)$. Но простые методы, как давно известно, имеют сложность $N \approx n$ (Золотарёв, 2006, 2018; Золотарёв, Овечкин, 2004; Золотарёв и др., 2012; Зубарев и др., 2019; Zolotarev, 2018; Zolotarev et al., 2015). Оценки $P_w(e)$ в статье (Зяблов и др., 2009) сделаны через использование более 50 сложных, совершенно непроверяемых соотношений с перекрёстными ссылками, что является типичным крайне проблемным случаем, описанным в сообщении (Магаршак, 2009). Итогом статьи является результат в стиле, который стал популярным в определённом сообществе, но совершенно непонятным с точки зрения исследований методов улучшения характеристик декодирования. Авторы публикации (Зяблов и др., 2009) определяли относительные доли успешно декодируемых символов блокового кода. В данной работе эта доля для кодовой скорости $R = 1/2$ равна ~0,0003. Но можно отметить, что ещё 60 лет назад очень слабые коды Боуза — Чоудхури — Хоквингема (БЧХ-коды), как это справочно указывается в книге (Питерсон, Уэлдон, 1976, с. 308, рис. 9.1), почти всегда исправляли долю ошибок порядка 0,03, что на два десятичных порядка лучше результата статьи. Более того, МПД ещё в 1981 г. экспериментально продемонстрировал возможность исправления почти всех ошибок при вероятности ошибки в канале (здесь — тоже эквивалент доли исправляемых ошибок) $p_0 \approx 0{,}05$, причём при линейной сложности алгоритма МПД, т. е. когда $N \approx n$ (Золотарёв, Овечкин, 2004; Золотарёв и др., 2018).

В недавней работе (Зяблов, Рыбин, 2012) на 27 страницах также предложены методы оценки доли исправляемых ошибок, проверить которые нереально. Величина такой доли при $R = 1/2$ — менее 0,002, что также много слабее, соответственно в 15 и 25 раз, чем обеспечивают БЧХ-коды и МПД-декодеры, известные уже 40 лет.

В работах (Афанасьев и др., 2016; Зигангиров, Зигангиров, 2006; Зяблов, Рыбин, 2009) рассмотрены аналитические оценки долей исправляемых стираний LDPC- и другими кодами. При этом авторы снова своеобразно трактуют вопросы сложности и даже предлагают не обращать на них внимание. Верхние оценки долей исправляемых стираний для этих методов при $R = 1/2$ везде составляют менее 0,1. Экспериментальных данных все эти авторы не предъявили. В то же время в публикациях (Золотарёв, 2006, 2018; Золотарёв и др., 2012; Кузнецов и др., 2020; Zolotarev, 2018; Zolotarev et al., 2015) доля простейшим образом исправляемых стираний существенно больше, чем 0,3, причём при линейной сложности.

Приходится снова напомнить, что в статьях (Золотарёв, 2006, 2018; Золотарёв и др., 2012; Zolotarev, 2018; Zolotarev et al., 2015) и в ряде других публикаций даны очень простые оценки ОД в стирающих каналах, определяющие нижние оценки для вероятности невосстановления стирания в некотором символе кода $P_{b,er}(s) \approx p_{er}{}^{d}$, где p_{er} — вероятность появления в канале стёртого символа; d — минимальное кодовое расстояние используемого кода. Вывод оценки занял полстраницы крайне простых рассуждений. В работах (Золотарёв, 2006, 2018; Золотарёв и др., 2012; Zolotarev, 2018; Zolotarev et al., 2015) также показано, что предложенная оценка (соответствующая ОД) достигается с применением упрощённых МПД с линейной сложностью даже вблизи пропускной способности стирающего канала. Так что все возможные выводы и по такому сравнению кодов и декодеров очевидны. В процессе данного декодирования на каждой итерации решается одно простейшее уравнение для трёх небольших целых чисел с неизвестным X: $A = B + X$. Неудивительно поэтому, что и для каналов со стираниями у ОТ вообще нет конкурентов, так как алгоритмы для МПД в таких каналах имеют минимально возможную сложность, наилучшую возможную достоверность и огромную скорость (Золотарёв, 2006, 2018; Золотарёв и др., 2012; Zolotarev, 2018; Zolotarev et al., 2015).

Наконец, отметим, что получить разумные оценки сложности для всех методов декодирования недвоичных кодов, кроме МПД, очень трудно, о чём говорилось в статье (Кузнецов и др., 2010). Там же есть и ряд ссылок на алгоритмы для недвоичных кодов, не относящиеся к ОТ. В абсолютном большинстве случаев, где приближённое сопоставление сложности МПД и прочих методов было вообще как-то возможно, преимущество МПД по скорости декодирования составляло тысячи и более раз по простой причине оптимального декодирования с линейной от длины кода сложностью.

Таким образом, теория ОТ существенно опережает результаты, полученные для абсолютно всех других известных классов алгоритмов декодирования, благодаря правильному соотношению теоретических и экспериментальных методов исследований. Целый ряд результатов ОТ, вполне возможно, надолго останется недостижимым для прочих алгоритмов декодирования.

О совершенстве ОТ

Наконец, рассмотрим итоговый *рис. 4* (см. с. 21), иллюстрирующий главные возможности ОТ. Как видно из этого рисунка, ОТ для кодов, выбранных в соответствии с каким-либо типичным техническим заданием, легко строит вероятность первоначальной стартовой ошибки декодера, обычно называемую вероятностью ошибки в первом символе $P_1(e)$ (Золотарёв, 2006, 2018; Золотарёв, Овечкин, 2004), и столь же простые формулы для предельно возможных вероятностей ошибки МПД-декодирования на уровне оптимального решения $P_{opt}(e)$ в абсолютно всех каналах, рассматриваемых в теории кодирования. А все остальные заботы специалиста в области ОТ состоят просто в том, чтобы подобрать оптимизационными методами лучшие коды и технологии ОТ, которые могут обеспечить требуемый уровень $P_{opt}(e)$. При этом нужно не забыть, что всегда искомые характеристики следует искать при кодовой скорости проектируемого декодера R, находящейся между пропускной способностью канала C и вычислительной скоростью канала R_1. Главным варьируемым параметром в ОТ оказывается число итераций декодирования $I = 5...50$ или более. Именно поэтому вся теория ОТ чрезвычайно компактна и является фактически системно-философским трактатом о решении оптимизационных задач, ориентированных на проблемы коррекции цифровых данных. И всё это в значительной степени делается средствами высокоразвитого интеллектуального программного обеспечения. Можно считать, что ОТ меньше по содержательному объёму, чем «классика», примерно на три десятичных порядка, что особенно подчёркивает совершенство ОТ как полной прикладной теории, разрабатывающей алгоритмы декодирования, сопоставимых с которыми среди других методов «классики» или «новых» направлений пока просто вообще нет. И ожидать появления новых и более предпочтительных методов очень трудно, так как ОТ предлагает методы с характеристиками ОД при минимально возможной, линейной от длины кодов сложности, работоспособные даже в непосредственной близости от границы Шеннона. Иначе говоря, трудно придумать совсем другой метод, который будет лучше, чем алгоритмы ОТ, которые по всем главным параметрам «помехоустойчивость — достоверность — сложность» уже сейчас обеспечивают наилучшие возможные характеристики.

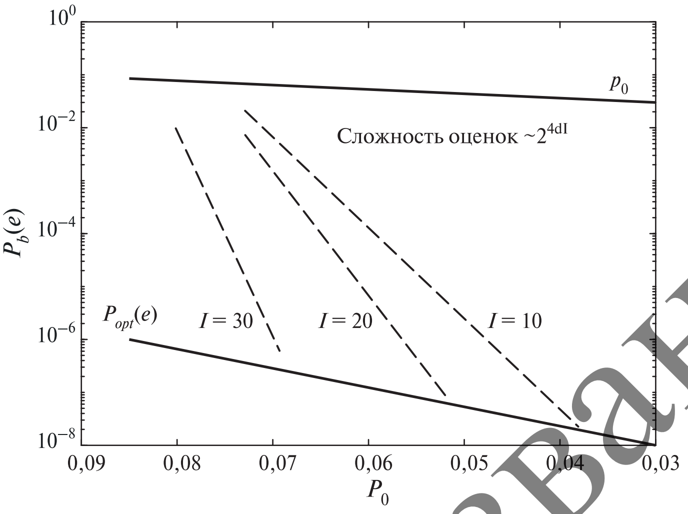

Рис. 4. Варианты стремлений МПД к решению оптимального декодера

Обращаясь к *рис. 4*, подчеркнём, что сложность аналитической оценки вероятности ошибки МПД, например на 9-й или 38-й итерации, как пока нам представляется и как показано в строчке «Сложность оценок», исключительно велика и экспоненциально зависит от указанных на слайде параметров декодера: произведения кодового расстояния и числа итераций. И значит, это, видимо, никогда не будет сделано. В то же время экспериментальные результаты для различного числа итераций декодирования могут быть получены на программных или аппаратных макетах в течение крайне ограниченного срока от нескольких секунд до десятков часов, так как сложность всех алгоритмов МПД исключительно мала, линейна от длины кода. Этим и решаются все вопросы технологий и разработок в ОТ на основе МПД. Очевидно, что и все модификации АВ, как мы показали в настоящем обзоре, моделируются столь же быстро и не менее убедительно.

Таким образом, текущее абсолютное предпочтение ОТ перед прочими подходами к проблемам прикладной теории кодирования, которые не дали за последние десятилетия никаких действительно новых результатов, всесторонне и, безусловно, обосновано.

Заключение

Разумно сбалансированное развитие ОТ как новой «квантовой механики» в теории информации совместно с проводимыми в течение многих десятилетий широкомасштабными программными разработками и оптимизацией систем проектирования кодеков МПД позволило решить великую проблему Шеннона и создать уникальные технологии для разработок методов помехоустойчивого кодирования, которые, по всей видимости, ещё в течение длительного времени никто не сможет даже частично повторить именно из-за отсутствия у специалистов каких-либо разумных представлений о правильном соотношении и взаимодействии между теоретическими и экспериментальными методами исследований (Кузнецов и др., 2020; Магаршак, 2009). ОТ является основой для разработок новых систем спутников связи и проектов дистанционного зондирования Земли с параметрами быстродействия и достоверности, принципиально недоступными для каких-либо иных методов кодирования.

Хотя данная статья формально была более сориентирована на обсуждение проблем полярных кодов, совершенно естественно получился самый общий обзор крайне драматического, если не сказать большего, абсолютно кризисного многолетнего состояния прикладной теории помехоустойчивого кодирования. Он показал реальные и очень существенные преимущества ОТ не только в плане достижения границы Шеннона (Золотарёв, 2018; Зубарев и др., 2019; Кузнецов и др., 2020; Zolotarev, 2018), но и в случае рассмотрения эффективности декодирования коротких кодов. Важно, что при этом не потребовалось какой-либо предварительной адаптации методов ОТ к сильно изменённой в данном варианте постановке задачи сравнения, к тому же не выдерживающей никакой критики по ряду аспектов сопоставления кодов и декодеров.

Научная школа ОТ предлагает всем специалистам в области цифровой обработки присоединиться к нашими усилиям по диверсификации технологий ОТ на все направления цифровой информатики, повышающих достоверность дискретных данных в наибольшей степени и простейшими средствами. Поддержка энтузиастам и специалистам, которые придут в новую отрасль теории кодирования, всеми нашими ресурсами и знаниями гарантируется.

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проект № 18-47-620001), Института космических исследований Российской академии наук (ИКИ РАН), Рязанского государственного радиотехнического университета (РГРТУ). Большой объём дополнительной информации о многопороговых декодерах можно найти на веб-сайтах ИКИ РАН (www.mtdbest.iki.rssi.ru) и РГРТУ (www.mtdbest.ru).

Литература

1. *Афанасьев В. Б.*, *Давыдов А. А.*, *Зигангиров Д. К.* Оценка доли стираний, исправляемых линейными кодами // Информац. процессы. 2016. Т. 16. № 4. С. 352–404.
2. *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.
3. *Золотарёв В. В.* Многопороговое декодирование в недвоичных каналах // Вопросы радиоэлектроники. Сер. ЭВТ. 1984. Вып. 12. С. 73–76.
4. *Золотарёв В. В.* Теория и алгоритмы многопорогового декодирования / под ред. Ю. Б. Зубарева. М.: Изд-во «Горячая линия – Телеком», 2006. 266 с. URL: https://mtdbest.ru/articles/теория и алгоритмы 2006.pdf.
5. *Золотарёв В. В.* Теория кодирования как задача поиска глобального экстремума (Оптимизационная Теория помехоустойчивого кодирования — новая «квантовая механика» теории информации) / под ред. Н. А. Кузнецова. М.: Изд-во «Горячая линия – Телеком», 2018. 222 с.
6. *Золотарёв В. В.*, *Овечкин Г. В.* Помехоустойчивое кодирование. Методы и алгоритмы: справ. М.: Изд-во «Горячая линия – Телеком», 2004. 126 с.
7. *Золотарёв В. В.*, *Овечкин Г. В.* Эффективное многопороговое декодирование недвоичных кодов // Радиотехника и электроника. 2010. Т. 55. № 3. С. 324–329.
8. *Золотарёв В. В.*, *Овечкин Г. В.* Применение многопороговых методов декодирования помехоустойчивых кодов в высокоскоростных системах передачи данных // Электросвязь. 2014. № 12. С. 10–14.
9. *Золотарёв В. В.*, *Овечкин Г. В.* О сопоставлении новых методов помехоустойчивого кодирования // Докл. 18-й Международ. конф. «Цифровая обработка сигналов и ее применение». М., 2016. Т. 1. С. 59–65.
10. *Золотарёв В. В.*, *Овечкин П. В.* Способ кодирования и декодирования блокового кода с использованием алгоритма Витерби. Патент РФ 2608872. Рег. 25.01.2017.
11. *Золотарёв В. В.*, *Зубарев Ю. Б.*, *Овечкин Г. В.* Многопороговые декодеры и оптимизационная теория кодирования / под ред. В. К. Левина. М.: Изд-во «Горячая линия — Телеком», 2012. 238 с.
12. *Золотарёв В. В.*, *Зубарев Ю. Б.*, *Овечкин Г. В.*, *Аверин С. В.*, *Овечкин П. В.* 25 лет оптимизационной теории кодирования: новые перспективы // Материалы 18-й Международ. научно-техн. конф. «Проблемы передачи и обработки информации в сетях и системах телекоммуникаций». М.: Изд-во «Горячая линия – Телеком», 2015. С. 10–17.
13. *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.

14. *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. URL: http://www.mtdbest.ru/articles/elsv2020.pdf.
15. *Зяблов В.В.*, *Рыбин П.С.* Исправление стираний кодами с малой плотностью проверок // Проблемы передачи информации. 2009. Т. 45. Вып. 3. С. 15–32.
16. *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.
17. *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.
18. *Кудряшов Б.Д.* Основы теории кодирования: учебное пособие для вузов. СПб.: БХВ-Санкт-Петербург, 2016. 393 с.
19. *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.
20. *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. М.: ИКИ РАН, 2020. 36 с. URL: http://www.mtdbest.ru/articles/comics.pdf.
21. *Магаршак Ю.* Число, возведенное в абсолют // Независимая газета. 09.09.2009. URL: https://www.ng.ru/science/2009-09-09/11_maths.html.
22. *Милославская В.Д.* Методы построения и декодирования полярных кодов: дис. … канд. техн. наук. СПб., 2015. 206 с.
23. *Морозов Р.А.* Декодирование полярных кодов с помощью алгоритма Думера–Шабунова // Список-2013: материалы всероссийской науч. конф. по проблемам информатики. 23–26 апр. 2013, Санкт-Петербург. СПб.: Изд-во ВВМ, 2013. С. 261–262. URL: spisok.math.spbu.ru/2013/txt/papers/s7_1.odt.
24. *Назаров Л.Е.*, *Щеглов М.А.* Характеристики полных и укороченных помехоустойчивых низкоплотностных кодов на основе конечных геометрий // Успехи современной радиоэлектроники. 2017. № 6. С. 38–48.
25. *Питерсон У.*, *Уэлдон Э.* Коды, исправляющие ошибки. М.: Мир, 1976. 594 с.
26. *Трифонов П.В.* Методы построения и декодирования многочленных кодов: дис. … д-ра техн. наук. СПб., 2018. 254 с.
27. *Федоренко С.В.* Методы быстрого декодирования линейных блоковых кодов. СПб., 2008. 198 с.
28. *Ammar H.* Optimisation and analysis of polar codes in communication systems: Doctoral Thesis. University of Manchester, 2018. 177 p.
29. *Arikan E.* Channel Polarization: A Method for Constructing Capacity-Achieving Codes for Symmetric Binary-Input Memoryless Channels // IEEE Trans. Information Theory. 2009. V. 55. No. 7. P. 3051–3073.
30. *Dumer I.*, *Shabunov K.* Soft-Decision Decoding of Reed-Muller Codes: Recursive Lists // IEEE Trans. Information Theory. 2006. V. 52. No. 3. P. 1260–1266.
31. *Giard P.*, *Sarkis G.*, *Thibeault C.*, *Gross W.J.* Fast Software Polar Decoders // Proc. IEEE Intern. Conf. Acoustics, Speech and Signal Processing (ICASSP). 2014. 5 p.
32. *Ozgur U.* A Performance Comparison of Polar Codes with Convolutional Turbo Codes: Doctoral Thesis. 2009. 166 p.
33. *Sarkis G.*, *Giard P.*, *Vardy A.*, *Thibeault G.*, *Gross W.J.* Fast list decoders for polar codes // IEEE J. Selected Areas in Communications. 2016. V. 34. No. 2. P. 318–328.
34. *Seidl M.*, *Huber J.B.* An Efficient Length- and Rate-Preserving Concatenation of Polar and Repetition Codes // Computer Science, Mathematics. 2013.
35. *Tal I.*, *Vardy A.* List decoding of polar codes // IEEE Trans. Information Theory. 2015. V. 61. P. 2213–2226.
36. *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. URL: https://mtdbest.ru/articles/mtd_book_2019.pdf.
37. *Zolotarev V.V.*, *Zubarev Yu.B.*, *Ovechkin G.V.* Optimization Coding Theory and Multithreshold Algorithms. Switzerland: ITU, 2015. 158 p. URL: https://mtdbest.ru/articles/Zolotarev_ITU.pdf.
38. *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.
39. *Zolotarev V.V.*, *Ovechkin G.V.*, *Chulkov I.V.*, *Ovechkin P.V.*, *Averin S.V.*, *Satybaldina D.Zh.*, *Kao V.T.* Review of Achievements in the Optimization Coding Theory for Satellite Channels and Earth Remote Sensing Systems: 25 Years of Evolution // Sovremennye problemy distantsionnogo zondirovaniya Zemli iz kosmosa. 2017. V. 14. No. 1. P. 9–24.

Overview of polar codes problems from Optimization Error Correction Coding Theory technologies points of view

N. A. Kuznetsov [1], V. V. Zolotarev [2], G. V. Ovechkin [3], R. R. Nazirov [2], D. Zh. Satibaldina [4], E. D. Omirbayev [4]

[1] *Kotelnikov Institute of Radioengineering and Electronics RAS*, *Moscow 125009*, *Russia*
E-mail: kuznetsov@cplire.ru

[2] *Space Research Institute RAS*, *Moscow 117997*, *Russia*
E-mail: zolotasd@yandex.ru

[3] *Utkin Ryazan State Radio Engineering University*, *Ryazan 390005*, *Russia*
E-mail: g_ovechkin@mail.ru

[4] *Gumilyov Eurasian National University*, *Astana 010008*, *Kazakhstan*
E-mail: satybaldina_dzh@enu.kz

The general situation in the applied issues of coding theory is considered. The main problems in the field of decoding of error-correction codes are stated. The main attention in addition to error-correcting performance is paid to decoding complexity. The latest results in the field of decoding algorithms for polar codes (PC) are presented, as well as the main problems of their development. The application results of Optimization Theory (OT) and extremely limited materials available for PC are compared. The results for low density parity check (LDPC) codes are briefly mentioned. The results of performance comparison for PC and block version of Viterbi decoder (BVA) for short codes are presented. Also comparison of possibilities for PC and MTD algorithms, including using concatenation, was fulfilled. The main directions for the development and improvement of characteristics of OT algorithms are suggested. Based on the results of comparison, it has been concluded that there is an unconditional leadership of OT and no need to use PC and a number of other codes anywhere at all due to inevitably weak capabilities and a large list of shortcomings of decoders of these directions and methods of their development in research for new satellite and space communication projects, including remote sensing of Earth systems.

Keywords: Shannon boundary, channel capacity, algorithm complexity, polar codes, list decoding, optimal decoding, Optimization Theory, block viterbi algorithm, Reed — Solomon codes, low density parity check and turbo codes, multithreshold decoders, parallel concatenation, divergent principle, direct control metric decoders

Accepted: 29.06.2020
DOI: 10.21046/2070-7401-2020-17-4-9-26

References

1. Afanas'ev V. B., Davydov A. A., Zigangirov D. K., Otsenka doli stiranii, ispravlyaemykh lineinymi kodami (Estimation for part of erasures recovered with linear codes), *Informatsionnye protsessy*, 2016, Vol. 16, No. 4, pp. 352–404.
2. Zigangirov D. K., Zigangirov K. Sh., Dekodirovanie nizkoplotnostnykh kodov s proverochnymi matritsami, sostavlennymi iz perestanovochnykh matrits, pri peredache po kanalu so stiraniyami (Decoding of low density codes with parity check matrixes consisting of permutation matrixes for erasure channels), *Problemy peredachi informatsii*, 2006, Vol. 42, pp. 44–52.
3. Zolotarev V. V., Mnogoporogovoe dekodirovanie v nedvoichnykh kanalakh (Multithreshold decoding over non-binary channels), *Voprosy radioelektroniki*, *Ser. EVT*, 1984, Vol. 12.
4. Zolotarev V. V., *Teoriya i algoritmy mnogoporogovogo dekodirovaniya* (Theory and algorithms for multithreshold decoding), Moscow: Goryachaya liniya — Telekom, 2006, 266 p.
5. Zolotarev V. V., *Teoriya kodirovaniya kak zadacha poiska global'nogo ekstremuma* (*Optimizatsionnaya Teoriya pomekhoustoichivogo kodirovaniya — novaya "kvantovaya mekhanika" teorii informatsii*) (Coding Theory as a Global Extremum Search Task (Optimization Theory of error-correcting coding — a new "quantum mechanics" of information theory)), Moscow: Goryachaya liniya — Telekom, 2018, 222 p.
6. Zolotarev V. V., Ovechkin G. V., *Pomekhoustoichivoe kodirovanie. Metody i algoritmy* (Error-correcting coding. Methods and algorithms), Moscow: Goryachaya liniya — Telekom, 2004, 126 p.

7. Zolotarev V. V., Ovechkin G. V., Effektivnoe mnogoporogovoe dekodirovanie nedvoichnykh kodov (Effective multithreshold decoding for non-binary codes), *Radiotekhnika i elektronika*, 2010, Vol. 55, No. 3, pp. 324–329.
8. Zolotarev V. V., Ovechkin G. V., Primenenie mnogoporogovykh metodov dekodirovaniya pomekhoustoichivykh kodov v vysokoskorostnykh sistemakh peredachi dannykh (Application of multuthreshold decoders for error-correcting codes in high-speed digital communications), *Elektrosvyaz'*, 2014, No. 12, pp. 10–14.
9. Zolotarev V. V., Ovechkin G. V., O sopostavlenii novykh metodov pomekhoustoichivogo kodirovaniya (About comparison of new error correction coding methods), *Tsifrovaya obrabotka signalov i ee primenenie*, *Proc. 18^{th} Intern. Conf.*, Moscow, 2016, Vol. 1, pp. 59–65.
10. Zolotarev V. V., Ovechkin P. V., *Sposob kodirovaniya i dekodirovaniya blokovogo koda s ispol'zovaniem algoritma Viterbi* (A method for encoding and decoding of block code with using of Viterbi algorithm), Patent RU 2608872, Reg. 25.01.2017.
11. Zolotarev V. V., Zubarev Yu. B., Ovechkin G. V., *Mnogoporogovye dekodery i optimizatsionnaya teoriya kodirovaniya* (Multithreshold decoders and optimization coding theory), Moscow: Goryachaya liniya — Telekom, 2012, 238 p.
12. Zolotarev V. V., Zubarev Yu. B., Ovechkin G. V., Averin S. V., Ovechkin P. V., 25 let optimizatsionnoi teorii kodirovaniya: novye perspektivy (25 years of optimization coding theory: new perspectives), *Problemy peredachi i obrabotki informatsii v setyakh i sistemakh telekommunikatsii*, *Proc. 18^{th} Intern. Scientific and Technological Conf.*, 2015, pp. 10–17.
13. Zolotarev V. V., Ovechkin G. V., Nazirov R. R., O peredache Optimizatsionnoi Teorii liderstva ot prikladnoi klassicheskoi teorii pomekhoustoichivogo kodirovaniya (Optimization Theory: the Reception of the Baton of Leadership from the Applied Classic Theory of Error-Correcting Coding), In: *Nekotorye aspekty sovremennykh problem mekhaniki i informatiki: sbornik nauchnykh statei*, Moscow: IKI RAN, 2018, pp. 82–90.
14. Zubarev Yu. B., Zolotarev V. V., Ovechkin G. V., Novye tekhnologii i paradigmy pomekhoustoichivogo kodirovaniya: posle resheniya problemy Shennona (New technologies and paradigms of error correction coding: after solving of Shannon problem), *Elektrosvyaz'*, 2019, No. 9, pp. 56–61, available at http://www.mtdbest.ru/articles/elsv2020.pdf.
15. Zyablov V. V., Rybin P. S., Ispravlenie stiranii kodami s maloi plotnost'yu proverok (Recovering erasures with low density codes), *Problemy peredachi informatsii*, 2009, Vol. 45, pp. 15–32.
16. Zyablov V. V., Rybin P. S., Analiz svyazi svoistv MPP-kodov i grafa Tannera (The analysis of connection between properties of LDPC codes and Tanner graph), *Problemy peredachi informatsii*, 2012, Vol. 48, pp. 3–29.
17. Zyablov V. V., Iokhannesson R., Lonchar M., Prosto dekodiruemye kody s maloi plotnost'yu proverok na osnove kodov Khemminga (Simple for decoding low density parity check codes based on Hamming codes), *Problemy peredachi informatsii*, 2009, Vol. 45, pp. 25–40.
18. Kudryashov B. D., *Osnovy teorii kodirovaniya* (Basics of error correction codes), Saint Petersburg: BKhV-Sankt-Peterburg, 2016, 393 p.
19. Kuznetsov N. A., Zolotarev V. V., Ovechkin G. V., Ovechkin P. V., Nedvoichnye mnogoporogovye dekodery i drugie metody korrektsii oshibok v simvol'noi informatsii (Non-binary multithreshold decoders and other methods for error correction in symbolical information), *Radiotekhnika*, 2010, No. 6, pp. 4–9.
20. Kuznetsov N. A., Zolotarev V. V., Zubarev Yu. B., Ovechkin G. V., Nazirov R. R., Averin S. V., *Problemy i otkrytiya Optimizatsionnoi Teorii pomekhoustoichivogo kodirovaniya* (Problems and discoveries of optimization error correction coding theory), Moscow: Goryachaya liniya — Telekom, 2020, 36 p., available at: http://www.mtdbest.ru/articles/comics.pdf.
21. Magarshak Yu., Chislo, vozvedennoe v absolyut (Elevating number to an absolute), *Nezavisimaya gazeta*, 09.09.2009, abailable at: https://www.ng.ru/science/2009-09-09/11_maths.html.
22. Miloslavskaya V. D., *Metody postroeniya i dekodirovaniya polyarnykh kodov: Diss. kand. tekhn. nauk* (Methods for construction and decoding of polar codes, Cand. techn. sci. thesis), Saint Petersburg, 2015, 206 p.
23. Morozov R. A., Dekodirovanie polyarnykh kodov s pomoshch'yu algoritma Dumera–Shabunova (Decoding polar codes using the Dumer–Shabunov algorithm), *Spisok-2013: materialy vserossiiskoi nauchnoi konferentsii po problemam informatiki*, Saint Petersburg: Izd. VVM, 2013, pp. 261–262, available at spisok.math.spbu.ru/2013/txt/papers/s7_1.odt.
24. Nazarov L. E., Sheglov M. A., Kharakteristiki polnykh i ukorochennykh pomekhoustoichivykh nizkoplotnostnykh kodov na osnove konechnykh geometrii (Characteristics of length-compatible low-density parity-check codes on finite geometries), *Uspekhi sovremennoi radioelektroniki*, 2017, No. 6, pp. 38–48.
25. Piterson U., Ueldon E., *Kody*, *ispravlyayushchie oshibki* (Codes correcting errors), Moscow: Mir, 1976, 594 p.
26. Trifonov P. V., *Metody postroeniya i dekodirovaniya mnogochlennykh kodov*: *Diss. dokt. tekhn. nauk* (Methods for construction and decoding of multi-partition codes, Dr. techn. sci. thesis), Saint Petersburg, 2018, 254 p.
27. Fedorenko S. V., *Metody bystrogo dekodirovaniya lineinykh blokovykh kodov* (Methods of fast decoding for linear block codes), Saint Petersburg, 2008, 198 p.

28. Ammar H., *Optimisation and analysis of polar codes in communication systems: Doctoral Thesis*, University of Manchester, 2018, 177 p.
29. Arikan E., Channel Polarization: A Method for Constructing Capacity-Achieving Codes for Symmetric Binary-Input Memoryless Channels, *IEEE Trans. Information Theory*, 2009, Vol. 55, No. 7, pp. 3051–3073.
30. Dumer I., Shabunov K., Soft-Decision Decoding of Reed-Muller Codes: Recursive Lists, *IEEE Trans. Information Theory*, 2006, Vol. 52, No. 3, pp. 1260–1266.
31. Giard P., Sarkis G., Thibeault C., Gross W. J., Fast Software Polar Decoders, *Proc. IEEE Intern. Conf. Acoustics*, *Speech and Signal Processing* (*ICASSP*), 2014, 5 p.
32. Ozgur U., *A Performance Comparison of Polar Codes with Convolutional Turbo Codes: Doctoral Thesis*, 2009, 166 p.
33. Sarkis G., Giard P., Vardy A., Thibeault G., Gross W. J., Fast list decoders for polar codes, *IEEE J. Selected Areas in Communications*, 2016, Vol. 34, No. 2, pp. 318–328.
34. Seidl M., Huber J. B., An Efficient Length- and Rate-Preserving Concatenation of Polar and Repetition Codes, *Computer Science*, *Mathematics*, 2013.
35. Tal I., Vardy A., List decoding of polar codes, *IEEE Trans. Information Theory*, 2015, Vol. 61, pp. 2213–2226.
36. 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*), Moscow: Hot Line — Telecom, 2018, 333 p., available at https://mtdbest.ru/articles/mtd_book_2019.pdf.
37. Zolotarev V. V., Zubarev Yu. B., Ovechkin G. V., *Optimization Coding Theory and Multithreshold Algorithms*, Switzerland: ITU, 2015, 158 p., available at https://mtdbest.ru/articles/Zolotarev_ITU.pdf.
38. 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*), 2016.
39. Zolotarev V. V., Ovechkin G. V., Chulkov I. V., Ovechkin P. V., Averin S. V., Satybaldina D. Zh., Kao V. T., Review of Achievements in the Optimization Coding Theory for Satellite Channels and Earth Remote Sensing Systems: 25 Years of Evolution, *Sovremennye problemy distantsionnogo zondirovaniya Zemli iz kosmosa*, 2017, Vol. 14, No. 1, pp. 9–24.