РАСШИРЕННЫЙ ОТЧЕТ ЗА 2009 ГОД ПО ПРОЕКТУ РФФИ 08-07-00078-а

Форма 501. КРАТКИЙ НАУЧНЫЙ ОТЧЕТ

1.1. Номер проекта

08-07-00078

1.2. Руководитель проекта

Золотарев Валерий Владимирович

1.3. Название проекта

Разработка алгоритмов многопорогового декодирования для цифровых систем передачи, обработки и хранения данных для работы вблизи пропускной способности канала

1.4. Вид конкурса

а - Инициативные проекты

1.5. Год представления отчета

2010

1.6. Вид отчета

этап 2009 года

1.7. Аннотация

Во время очередного годичного этапа выполнялись работы по повышению эффективности многопороговых декодеров (МПД). Созданы и протестированы новые программные средства для генерации помехоустойчивых кодов с особо низким уровнем группирования ошибок на выходе декодеров. Это позволило ещё более снизить допустимое отношение сигнал/шум при использовании МПД в каналах космической и спутниковой связи. Выбрано дальнейшее направление для построения кодов, ещё более эффективных при большом шуме в случае их декодирования алгоритмами МПД. В результате характеристики МПД в области обеспечения низких вероятностей ошибки сопоставимы с характеристиками конкурирующих с ним алгоритмов. При этом сложность декодеров МПД (количество выполняемых простых математических операций) оказывается примерно в 60...130 раз меньшей, что чрезвычайно важно в реальных системах помехоустойчивого кодирования и является главной целью разработки новых методов декодирования.

Завершен важный этап развития каскадных методов кодирования символьной информации. По результатам этой работы защищена и уже утверждена в ВАК кандидатская диссертация по этим кодам, в которой найдены и исследованы новые каскадные методы декодирования такой информации для больших баз данных. Эти методы позволяют повысить достоверность хранения цифровых данных ещё на 2..4 порядка при усложнении алгоритма коррекции ошибок по сравнению с исходным всего на 10..30%.

Продолжены исследования сверхвысокоскоростных декодеров для каналов связи и систем дистанционного зондирования земли на 1 Гб/с и выше на созданном в ИКИ РАН аппаратно-программном комплексе. Данный комплекс включает МПД сверточного кода, реализованный на ПЛИС Altera, позволяющий выполнять декодирование информационного потока на скорости до 1,6 Гбит/с. По результатам этих работ получен патент на изобретение в области методов помехоустойчивого кодирования. Его применение позволяет ускоренно развивать методы и средства помехоустойчивого кодирования для спутниковых и космических линий в области ещё больших скоростей коррекции ошибок при

большом уровне шума.

В разработанных программных средствах реализована новая методика для защиты файлов от искажений при их долговременном хранении. Данная методика основана на последних достижениях в области разработки недвоичных многопороговых декодеров. Показано что применение предложенной методики позволяет в десятки раз увеличить скорость кодирования и восстановления информации по сравнению с существующими аналогами.

В течение всего периода выполнения проекта развивался специализированный веб-сайт ИКИ РАН www.mtdbest.iki.rssi.ru, на котором представляются основные результаты разработок МПД алгоритмов. Также началась разработка дополнительного веб-сайта www.mtdbest.ru, на котором также будет представлена информация о последних достижениях в области разработки многопороговых декодеров и других методов помехоустойчивого кодирования.

1.8. Полное название организации, где выполняется проект

Учреждение Российской академии наук Институт космических исследований РАН

"Исполнители проекта согласны с опубликованием (в печатной и электронной формах) научных отчетов и перечня публикаций по проекту"

Подпись руководителя проекта

Форма 502. КРАТКИЙ НАУЧНЫЙ ОТЧЕТ НА АНГЛИЙСКОМ ЯЗЫКЕ

2.1. Номер проекта
08-07-00078

2.2. Руководитель проекта
Zolotarev Valery Vladimirovich

2.3. Название проекта
Development of multithreshold decoders for digital systems of data transmition, processing and storage and storage for work near channel capacity

2.4. Год представления отчета
2010

2.5. Вид отчета
этап 2009 года

2.6. Аннотация

During this year works were performed on increase of efficiency of multithreshold decoders (MTD). New software for construction of error-correcting codes with especially low level of error propagation was created and tested. It has allowed to lower even more the admissible signal to noise ratio at use MTD over space and satellite communication channels. The further direction for construction of more effective codes for MTD was submitted. As a result of the performance of MTD in the field of low bit error ratio are comparable to the performance of existing algorithms. Thus complexity of MTD decoders (quantity of arithmetical operations) appears approximately in 60... 130 times smaller than complexity of other algorithms. It is extremely important in real systems and is an overall objective of working out of new methods of decoding.

The important stage of development of concatenated coding of the symbolical information is finished. By results of this work new methods of decoding of such information for the big databases were found and investigated. These methods allow to raise reliability of storage in 2..4 decimal order at complication of decoding algorithm on 10..30 % in comparison with initial MTD.

Researches of superhigh-speed decoders for communication channels and systems of remote sounding of the earth on 1 Gbps and above on created in Space Research Institute of the RAS hardware-software complex were continued. The given complex includes MTD for convolutional code, realised on FPGA Altera. It allows to carry out decoding information streams for the speed to 1,6 Gbps. By results of these works the patent for the invention in the field of methods of error-correcting coding is received. Its application allows to develop methods and means of error-correcting coding for satellite and space communication in area even the high speeds of correction at the large noise.

In the developed software the new technique for protection of files against distortions is realised at their long-term storage. The given technique is based on the last inventions in the field of working out of non-binary multithreshold decoders. It is shown that application of the offered technique allows to increase in tens times speed of coding and information restoration in comparison with existing analogues.

During all period of performance of the project specialised web-site Space Research Institute of the RAS www.mtdbest.iki.rssi.ru was developed. The basic results of workings out of MTD are represented on it. Working out of an

additional web site www.mtdbest.ru has begun.

2.7. Полное название организации, где выполняется проект
Space Research Institute of the RAS

Подпись руководителя проекта

Форма 503. РАЗВЕРНУТЫЙ НАУЧНЫЙ ОТЧЕТ

3.1. Номер проекта

08-07-00078

3.2. Название проекта

Разработка алгоритмов многопорогового декодирования для цифровых систем передачи, обработки и хранения данных для работы вблизи пропускной способности канала

3.3. Коды классификатора, соответствующие содержанию фактически проделанной работы

07-660 07-820

3.4. Объявленные ранее (в исходной заявке) цели проекта на 2009 год

Целью очередного годичного этапа является разработка методов, методик и алгоритмов дальнейшего повышения эффективности многопороговых декодеров (МПД) и каскадных схем на его основе, причем основное внимание будет уделено повышению эффективности работы недвоичных многопороговых декодеров.

При этом будут решены следующие основные задачи:

1. Развитие методики совместного поиска кодов и параметров МПД, обеспечивающих лучшую корректирующую способность при большом уровне шума в канале.

2. Поиск и исследование условий, а также выбор параметров каскадных схем коррекции ошибок, основанных на МПД, которые позволят им эффективно работать вблизи пропускной способности канала.

3. Разработка методики применения МПД для передачи и хранения сверхбольших объемов цифровых данных.

4. Программная реализация недвоичных версий МПД, предназначенных для организации систем хранения сверхбольших объемов данных.

5. Проработка вопросов аппаратной реализации на ПЛИС МПД, использующего наиболее эффективные технические решения.

Отметим, что найденные за первый год выполнения проекта нашим коллективом технические решения по обеспечению роста скорости декодирования будут реализованы в макете декодера МПД в следующем году. Это позволит гарантированно поднять уже сейчас чрезвычайно высокие достигнутые информационные скорости декодирования в несколько раз и довести в 2009 году эту скорость до уровня, превышающего 1 Гбит/с при сохранении высокой энергетической эффективности кодирования. Для получения этого важного результата коллектив исследователей по проекту будет в 2009 г. увеличен с 3 до 5 человек.

Также в 2009 г. коллективом авторов запланировано участие в одной зарубежной конференции по проблемам передачи данных, а также публикация статей в зарубежных журналах. По тематике проекта планируется защита одной кандидатской диссертации.

3.5. Степень выполнения поставленных в проекте задач

За второй год работы над проектом в полном объеме решены следующие задачи:

1. Предложена методика совместного поиска кодов и параметров МПД, обеспечивающих лучшую корректирующую способность при большом уровне шума в канале. Использование предложенной методики позволило найти новые

самоортоональные коды, обеспечивающие несколько лучшие результаты при многопороговом декодировании, чем ранее известные.

2. Завершилась разработка каскадных схем коррекции ошибок в символьных данных, основанных на многопороговом декодере, и обеспечивающих лучшие, чем ранее полученные результаты.

3. Завершилась разработка методики применения недвоичных МПД для передачи и хранения сверхбольших объемов цифровых данных. Показано, что применение недвоичных МПД позволяет на много порядков уменьшить вероятность ошибки в символьных данных по сравнению с использованием кодов Рида-Соломона.

4. Предложенная методика реализована в программных средствах для защиты больших файлов от ошибок. Данные программные средства обеспечивают высокий уровень защиты данных от ошибок при существенно более высоком быстродействии по сравнению с аналогами.

5. Результаты исследований в области разработки недвоичных многопороговых декодеров легли в основу защищенной в 2009 году кандидатской диссертации.

6. Разработанный МПД сверточного самоортогонального кода реализован в ИКИ РАН на ПЛИС Altera. Созданное устройство коррекции ошибок на скоростях более 1 Гбит/с в дальнейшем позволит решить все проблемы связи и на произвольно высоких скоростях передачи данных вплоть до 30 Гбит/с. В основу данной разработки положены запатентованные в текущем году технические решения, которые позволили обеспечить столь выдающиеся характеристики декодера.

7. Результаты работ опубликованы в ряде ведущих российских журналах, а также материалах зарубежных конференций.

Таким образом, поставленные в проекте задачи полностью решены.

3.6. Полученные за отчетный период важнейшие результаты

1. Завершилась разработка методики совместного поиска кодов и параметров МПД, обеспечивающих лучшую корректирующую способность при большом уровне шума в канале, которая позволяет за счет оптимизации веса информационных и проверочных ветвей получать коды с существенно меньшим проявлением эффекта размножения ошибок, и, соответственно, обеспечивать их близкое к оптимальному декодирование при более высоком уровне шума в канале связи.

В процессе ранее проведенных работ по исследованию и повышению эффективности МПД были предложены так называемые самоортогональные коды (СОК) с параллельным каскадированием, которые обеспечивают большую эффективность декодирования по сравнению с обычными СОК. В основе построения схем параллельного кодирования лежит выделение в самоортогональном коде C_0 с кодовым расстоянием d_0 и кодовой скоростью $R_0=k/(k+m)$ ($m>1$) некоторого составляющего кода C_1 с кодовой скоростью $R_1>R_0$, тоже являющегося самоортогональным кодом (СОК). Кодовое расстояние d_1 выделенного кода выбирается значительно меньшим d_0, и, следовательно, область его эффективной работы будет ближе к границе Шеннона. При декодировании параллельного кода сначала выполняются несколько итераций декодирования составляющего кода C_1, позволяющие примерно на порядок снизить вероятность ошибки в принятой из канала информационной последовательности, после чего в

процесс декодирования включается оставшаяся часть кода C_0. Отличительной особенностью данной схемы кодирования является то, что здесь внешний код работает с кодовой скоростью R_0, в то время как в обычных каскадных кодах кодовая скорость внешнего кода близка к единице. Данное свойство обеспечивает существенное преимущество параллельному кодированию перед другими каскадными конструкциями.

Пример структуры кода с кодовой скоростью R_0=8/16 и кодовым расстоянием d_0=17 для схемы параллельного кодирования приведен на рис. 1. Здесь строки таблицы соответствуют проверочным ветвям, столбцы – информационным ветвям, а в каждой ячейке с индексами *i* и *j* таблицы указано количество элементов информационной ветви *j*, которое участвует в формировании каждого символа проверочной ветви *i*. В данном коде используется 8 информационных и 8 проверочных ветвей. В процессе декодирования этого кода на первых итерациях используется только код C_1 с кодовой скоростью R_1=8/15 и кодовым расстоянием d_1=8, содержащий первые 7 проверочных ветвей. Проверки в данных ветвях имеют малую размерность, и поэтому декодер такого "уменьшенного" кода хорошо работает при больших вероятностях ошибки в канале. Когда вероятность ошибки декодирования в информационных ветвях станет невысокой (порядка 10^{-3}), включается и последняя проверочная ветвь с большой размерностью проверок. С помощью этой ветви исправляются оставшиеся ошибки в информационных ветвях, и вероятность ошибки на выходе декодера снижается еще на несколько порядков.

1	1	1	1	1	1	1	1	8
1	1	1	1	1	1	1	1	8
1	1	1	1	1	1	1	1	8
1	1	1	1	1	1	1	1	8
1	1	1	1	1	1	1	1	8
1	1	1	1	1	1	1	1	8
1	1	1	1	1	1	1	1	8
9	9	9	9	9	9	9	9	72
16	16	16	16	16	16	16	16	

Рис. 1. Структура параллельного кода

Сложность *q*МПД при параллельном кодировании (в смысле количества выполняемых операций) оказывается даже меньше сложности обычного *q*МПД, поскольку в данном случае на первых итерациях декодирования некоторые элементы синдромного регистра просто не участвуют в процессе вычисления суммы на пороговом элементе.

Заметим, что интуитивный выбор размерностей проверок для каждой информационной и проверочной ветви при построении СОК для схем параллельного кодирования является чрезвычайно трудоемкой задачей.

Для того чтобы автоматизировать процесс построения СОК, можно перебирать все возможные варианты кодов с различными размерностями проверок и выбирать тот, декодер которого оставляет после себя наименьший процент ошибок. Вычислительная сложность такого алгоритма для недвоичного многопорогового декодера равна $m^{nk \cdot nr} \cdot C_{q\text{МПД}}$ операций, где *nk* и *nr* – число информационных и проверочных ветвей, *m* – количество возможных вариантов числа проверок каждой пары информационная–проверочная ветвь, $C_{q\text{МПД}}$ –

вычислительная сложность qМПД. Данный алгоритм чрезвычайно эффективен при построении недвоичных СОК с небольшим количеством информационных и проверочных ветвей, так как осуществляется полный перебор возможных вариантов кодов. Однако при построении кодов с большим количеством информационных и проверочных ветвей применение алгоритма полного перебора из-за большой вычислительной сложности оказывается невозможным. Поэтому для построения недвоичных СОК целесообразно использовать немного менее эффективный алгоритм, основанный на известном алгоритме релаксаций для поиска в многомерном пространстве. Предложенный алгоритм обладает вычислительной сложностью $m \cdot nk \cdot nr \cdot N \cdot C_{q\text{МПД}}$ операций и, как показывают представленные далее результаты экспериментальных исследований, достаточно хорошей эффективностью. А дополнительная оптимизация параметров многопорогового декодирования полученных кодов позволяет еще дополнительно улучшить результаты.

Применение предложенного алгоритма, разработка которого началась еще в прошлом году, позволила получить ряд двоичных и недвоичных самоортогональных кодов, обладающих лучшей помехоустойчивостью по сравнению с известными кодами. Для примера на рис. 2 приведены результаты моделирования декодера для найденного с помощью предложенного алгоритма недвоичного СОК в q-ичном симметричном канале (кривая *6*). Кодовая скорость этого недвоичного СОК R=1/2, длина кода n=60000, минимальное кодовое расстояние d=17. При использовании данного кода достигаются гораздо лучшие результаты декодирования, чем ранее полученные. Вероятность ошибки на выходе декодера такого СОК составляет 10^{-7} при вероятности ошибки в канале P_0=0.267. При этом область эффективной работы найденного кода оказывается на 13% ближе к пропускной способности канала, равной для q=256 P_c=0.38, по сравнению с известным недвоичным СОК.

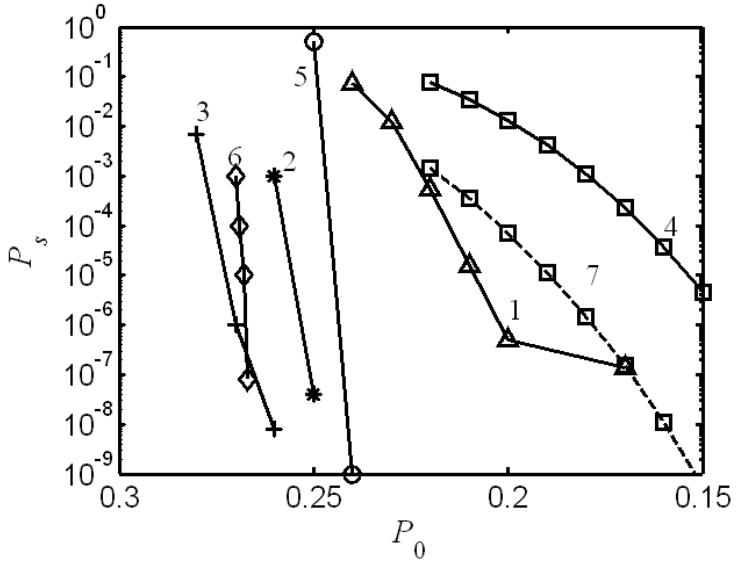

Рис. 2. Характеристики недвоичных кодов с R=1/2 в qСК

Еще более значительным получается улучшение характеристик qМПД для малоизбыточных кодов. На рис. 3 приведены результаты моделирования декодера найденного с помощью программы недвоичного СОК с кодовой скоростью R=7/8, минимальным кодовым расстоянием d=7 и длиной блока n=100000 в q-ичном симметричном канале (кривая *5*). Вероятность ошибки на выходе декодера такого СОК составляет 10^{-7} при вероятности ошибки в канале P_0=0.043. При этом область

эффективной работы найденного кода оказывается примерно на 20% ближе к пропускной способности канала P_c=0.076 по сравнению с известным недвоичным СОК с R=7/8 (кривая *1* на рис. 3).

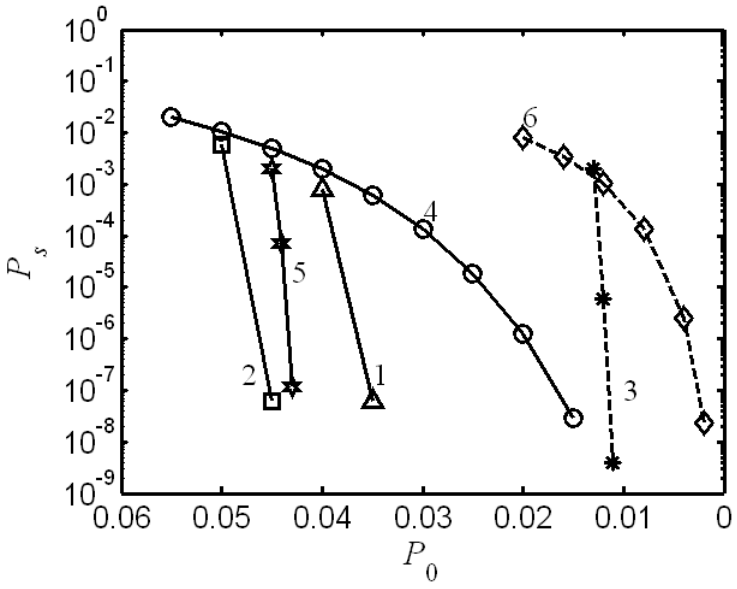

Рис. 3. Характеристики малоизбыточных недвоичных кодов

2. На основе последних достижений в области недвоичного многопорогового декодирования разработана методика для защиты файлов от искажений. Применение данной методики позволяет в десятки раз увеличить скорость кодирования и восстановления информации по сравнению с существующими аналогами.

Ни одно современное устройство для хранения информации не может работать без использования схем коррекции ошибок. Среди таких устройств винчестеры, оперативная память, CD, DVD, Blu-ray, HD-DVD и т.д. В большинстве своем данные устройства для защиты информации используют коды Рида-Соломона в том или ином сочетании. Иногда возможностей встроенных в устройства хранения схем коррекций ошибок бывает недостаточно (например, если на оптическом диске хранится особо важная информация). В этом случае приходят на помощь специальные программы, основанные на кодах Рида-Соломона и кодировании/декодировании с использованием матриц Вандермонда, которые для файла или набора файлов создают дополнительный файл, используя который, можно восстановить исходную информацию, даже если она была искажена.

Главными недостатками существующих программ для защиты файлов от искажений в процессе хранения или при передаче по каналам связи являются:

– низкая скорость восстановления информации при разбиении файлов на большое количество блоков;

– неспособность бороться даже с малым процентом независимых ошибок.

Альтернативным методом коррекции ошибок, который предлагается применять для защиты файлов от искажений, является недвоичный многопороговый декодер (qМПД). qМПД является простейшим декодером с линейной от длины кода сложностью реализации. Он эффективно работает не только в каналах с независимыми ошибками, но и в каналах с пакетирующимися ошибками. Поэтому, для того чтобы решить проблемы существующих программных средств для защиты файлов, необходимо разработать методику

использования qМПД для защиты файлов от искажений при длительном хранении.

Процесс создания файла с избыточной информацией для защищаемого файла будет следующим. Исходный файл представляется как совокупность символов одинакового размера. Причем, так как вычислительная сложность декодирования для qМПД не зависит от размера символа, то можно использовать символы большой размерности, например, восьмибайтовые символы, что позволит существенно увеличить скорость кодирования и декодирования информации. Последовательность символов исходного файла кодируется кодером недвоичного самоортогонального кода, а полученная в процессе кодирования избыточная информация записывается в проверочный файл. При повреждении исходного файла при длительном хранении или передаче по каналам связи, файл может быть восстановлен при использовании qМПД и избыточной информации из проверочного файла даже в случае его искажения. Программу, которая использует для восстановления искаженных файлов алгоритм недвоичного многопорогового декодирования, назовем MTDProtect.

Особую сложность при работе такого вида программ представляет обработка файлов большой размерности, порядка нескольких гигабайт. Если использовать кодирование одним блоком, то не хватает памяти даже на мощнейших компьютерах с несколькими гигабайтами оперативной памяти. При использовании небольших блоков существует большая вероятность того, что при пакетирующихся ошибках искаженным окажется весь блок и восстановление будет невозможно. Поэтому нужно работать с блоками как можно большей размерности при использовании перемежения, но с учетом размеров оперативной памяти ЭВМ. Для предложенной методики используется следующий алгоритм перемежения. Исходный файл разбивается на t блоков, каждый из которых разбивается еще на n подблоков. По схеме, показанной на рис. 4, из подблоков составляются кодовые информационные последовательности, которые поступаются на вход кодера. Первый кодовый блок будет состоять из подблоков a_{11}, a_{21}, a_{31},…, a_{t1}.

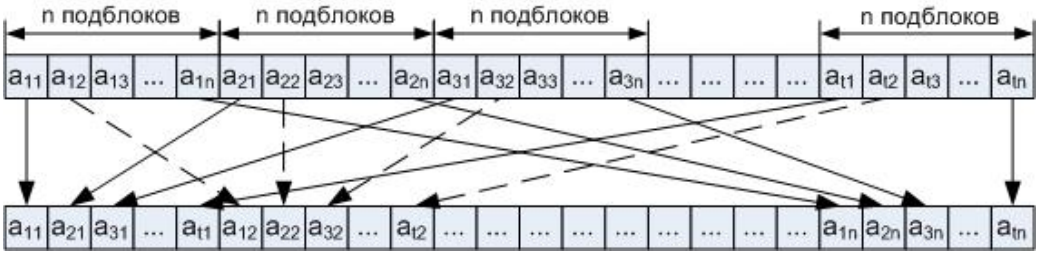

Рис. 4. Схема перемежения

Полученная в процессе кодирования избыточная информация также перемежается по указанной схеме и записывается в проверочный файл. В процессе декодирования производится обратная операция к блоковому перемежению – деперемежение. Использование данной схемы перемежения/деперемежения позволит qМПД исправлять пакеты ошибок большой длины.

Рассчитаем вычислительную сложность кодирования и восстановления информации на блок с помощью qМПД. В процессе кодирования информации необходимо выполнить $n \cdot (d-1)$ операций сложения целых чисел по модулю q (параметр d обычно выбирается небольшим, например d=9). В процессе восстановления информации необходимо выполнить $n \cdot (d-1)$ операций сложения целых чисел по модулю q для вычисления синдрома, $n \cdot N_{q\text{ПЭ}} \cdot i$ операций сравнения и

сложения целых чисел и в случае нахождения ошибки d операций сложения целых чисел. Здесь i – количество итераций декодирования (для данного алгоритма достаточно 5 итераций), $N_{q\text{ПЭ}}$ – количество операций, выполняемых пороговым элементом, $N_{q\text{ПЭ}} \approx 10 \div 50$.

Теперь сравним возможности разработанной программы MTDProtect и возможности наиболее часто используемых программ для защиты файлов: ICE ECC (российская разработка, которая появилась сравнительно недавно, по мнению большинства пользователей является лучшей на данный момент программой для защиты файлов), QuickPar (иностранная разработка, которая является самой популярной в мире программой для защиты файлов). Для сравнения возможностей программ был выбран файл размером порядка 700 мегабайт. Допустим, что этот файл очень ценен, и его необходимо сильно защитить, поэтому выбираем избыточность 100%, то есть создается проверочный файл равный по размерам защищаемому файлу. В таблице 1 содержатся результаты проведенных экспериментов.

Табл. 1 Результаты сравнения скорости обработки информации для программ ICE ECC, QuickPar, MTDProtect и ErasureMTDProtect.

	ICE ECC	QuickPar	MTDProtect	Erasure MTDProtect
Время кодирования	1 час	1.5 часа	1 мин.	1 мин.
Время восстановления файла с однобитовой ошибкой	3 мин.	3 мин.	3 мин.	1.5 мин.
Время восстановления файла, с поврежденным блоком размером 50% от размера файла	50 мин.	1 час	12 мин. (файл не восстановлен)	2.5 мин.
Время восстановления файла, с поврежденным блоком размером 25% от размера файла	40 мин.	50 мин.	10 мин.	2 мин.
Время восстановления файла с независимыми ошибками, которые возникают с вероятностью P_0=0.1	невозможно	невозможно	7 мин.	невозможно

При проведении экспериментов для лучшей помехоустойчивости исходный файл разбивался на 2048 блоков для программы ICE ECC, а для программы QuickPar на 1902 блока (максимальное значение для QuickPar). Результаты тестирования возможностей программ ICE ECC и QuickPar для защиты файлов показали, что кодирование файлов размером 700 мегабайт занимает не менее одного часа на компьютере со средними характеристиками. Восстановление незначительно искаженных файлов производится сравнительно быстро (несколько минут), однако для восстановления искаженного наполовину файла потребуется порядка одного часа. В свою очередь программа MTDProtect справляется с данными операциями за несколько минут, работая быстрее в десятки раз.

Сравнение программ по эффективности исправления ошибок показало, что ICE ECC и QuickPar исправляют пакет ошибок намного большей длины, чем это может сделать программа MTDProtect. Например, при избыточности 100%, даже если потеряно 100% защищаемых данных, то программы ICE ECC и QuickPar восстановят исходные данные, MTDProtect же может восстановить данные не более чем при 25% потерь. Но в свою очередь для *q*MTD абсолютно не важен характер повреждения файла, так как применяется алгоритм декодирования с перемежением, эффективно исправляющий и пакеты ошибок, и независимые ошибки. Программы ICE ECC и QuickPar из-за больших размеров блока не способны бороться даже с 0.01% независимых ошибок.

Сравнивая обычный недвоичный многопороговый декодер и недвоичный многопороговый декодер, способный исправлять стирания, можно заметить, что *q*МПДст для стираний исправляет намного больше стираний, чем *q*МПД исправляет ошибок. Поэтому для защиты информации от искажений предлагается использовать *q*МПДст.

Так как основную сложность *q*МПД составляет пороговый элемент, то применение методики восстановления файлов с использованием стираний позволит существенно сократить время исправления ошибок в файле за счет того, что заметно снизится сложность работы порогового элемента. Также при декодировании нужно просматривать не все символы исходного файла, а только те, которые отмечены признаком стирания. При этом вычислительная сложность декодирования будет пропорциональна количеству возникающих в исходном файле ошибок.

Для того чтобы можно было использовать *q*МПДст для защиты файлов от искажений при длительном хранении, разработан алгоритм, позволяющий преобразовать файл с ошибками в файл со стираниями. Основная идея алгоритма заключается в том, что исходный файл и проверочный файл, полученные с помощью кодера недвоичного самоортогонального кода, разбиваются на блоки длиной n символов. Для каждого блока подсчитывается контрольная сумма по модулю q его q-ичных элементов и добавляется в проверочный файл, например, как показано на рис. 5.

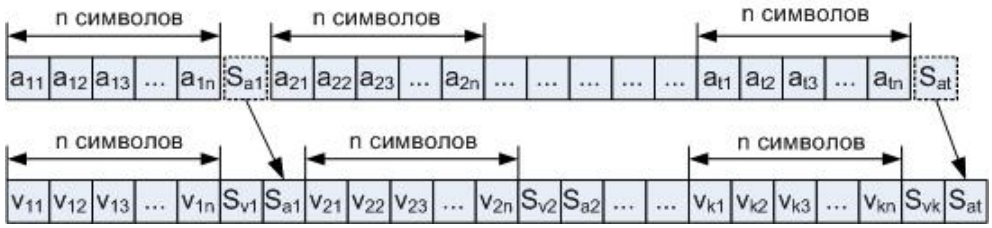

Рис. 5 Структура исходного и проверочного файлов

Здесь a_{ij} – q-ичный элемент исходного файла, который находится на j-й позиции в i-м блоке; v_{ij} – q-ичный элемент проверочного файла, который находится на j-й позиции в i-м блоке; S_{ai} – контрольная сумма элементов для i-го информационного блока; S_{vi} – контрольная сумма элементов для i-го проверочного блока.

При декодировании последовательно просматриваются все блоки из n символов файла; для каждого блока заново рассчитывается контрольная сумма по модулю q его элементов, и эта величина сравнивается с символом S_{ai} или S_{vi} для соответствующего блока. При этом каждому символу блока, где контрольные

суммы не совпадают, присваивается признак стирания. После этого полученная последовательность декодируется с помощью qМПД, который может исправлять стирания.

Для того чтобы выявить как можно больший процент ошибочных блоков, следует использовать символы и контрольные суммы достаточно большой размерности, например восемь байт (всего $q=2^{64}=18446744073709551616$ различных вариантов одного символа). Работа с символами такой большой размерности возможна только при использовании qМПД, так как при этом вычислительная сложность декодирования не зависит от размера символа. При этом вероятность не обнаружения ошибочного блока будет равна $P_{skip} = \frac{1}{q}$.

Например, при использовании символов размером 8 байт, т.е. при $q=2^{64}$, данная вероятность будет примерно равна $P_{skip} \approx 5.42 \cdot 10^{-20}$.

Пусть с использованием данной методики был защищен файл размером 100 мегабайт. Размер символа $q=2^{64}$, в каждом блоке $n=1000$ символов. Пусть исказился непрерывный фрагмент файла размером 10 мегабайт, то есть исказилось около $w=1250$ блоков. Вероятность того, что не будут выявлены искаженные блоки, равна $P = 1-(1-P_{skip})^{w} = 6.78 \cdot 10^{-17}$, то есть невыявленные блоки останутся только менее чем в одном 100 мегабайтовом файле из 10^{16} таких файлов.

Программу, которая использует для восстановления искаженных файлов алгоритм недвоичного многопорогового декодирования, способного исправлять стирания, назовем ErasureMTDProtect.

Рассчитаем вычислительную сложность кодирования и восстановления информации на блок с помощью qМПД, который может бороться со стираниями.

В процессе кодирования информации необходимо выполнить $n \cdot (d-1)$ операций сложения целых чисел по модулю q. В процессе восстановления информации необходимо выполнить $n \cdot (d-1)$ операций сложения целых чисел по модулю q для вычисления синдрома, $n_{er} \cdot (d-1) \cdot i$ операций сравнения целых чисел и в случае нахождения ошибки d операций сложения целых чисел. Здесь i – количество итераций декодирования, n_{er} – количество стертых символов информационной последовательности. Причем после выполнения каждой итерации n_{er} становится все меньше и меньше и на последних итерациях ее значение обычно не превышает 10.

Результаты сравнения возможностей наиболее часто используемых программ для защиты файлов ICE ECC, QuickPar и ErasureMTDProtect представлены в таблице 1.

По результатам, представленным в таблице, видно, что ErasureMTDProtect работает в десятки раз быстрее, чем известные программы-аналоги, имея преимущество даже по сравнению с MTDProtect. Следует отметить, что основное время при работе программ ErasureMTDProtect и MTDProtect тратится на операции чтения и записи файлов, которые можно еще ускорить, применяя, например, проецирование файлов в память ЭВМ. Чистая же скорость кодирования и декодирования составляет десятки мегабайт в секунду, а при декодировании файлов с небольшим числом ошибок даже сотни мегабайт в секунду. В свою очередь скорость работ программ ICE ECC и QuickPar ограничена именно скоростью работы применяемого алгоритма коррекции ошибок. Причем при увеличении размеров файла скорость кодирования и декодирования ErasureMTDProtect и

MTDProtect возрастает линейно.

С точки зрения эффективности исправления ошибок ErasureMTDProtect заметно превосходит возможности программы MTDProtect и может при избыточности 100% восстановить данные при 75% потерь защищенного файла, но немного проигрывает программам ICE ECC и QuickPar, которые при избыточности 100% могут восстановить 100% потерь защищенного файла. При этом ErasureMTDProtect оказывается в десятки раз быстрее ICE ECC и QuickPar, что очень важно при защите файлов большого объема.

Отметим, что и *q*МПД и *q*МПДст используются для декодирования одного и того же самоортогонального кода. Поэтому, если характер повреждений носит случайный характер (большой процент контрольных сумм ошибочен), то при восстановлении информации программой ErasureMTDProtect можно воспользоваться возможностями программы MTDProtect, которая эффективно борется с независимыми ошибками.

Результаты исследования показывают, что использование *q*МПД для защиты файлов позволяет повысить скорость кодирования/восстановления информации примерно **в десятки раз** по сравнению с известными аналогами. Также следует особо отметить, что *q*МПД способен исправлять как независимые ошибки в данных, так и группирующиеся ошибки. Этого нельзя сказать о методах коррекции ошибок, используемых для защиты файлов в существующих на рынке ПО программах, которые эффективно исправляют пакеты ошибок, но не справляются даже с малым процентом независимых ошибок. В частности программы ICE ECC и QuickPar из-за больших размеров блока не способны бороться даже с 0.01% независимых ошибок, а разработанное ПО, использующее алгоритмы МПД, позволяет исправлять до 25% независимых ошибок.

3. В текущем году завершилась разработка каскадных схем коррекции ошибок, основанных на многопороговом декодере, обеспечивающих лучшие, чем ранее полученные результаты.

В результате выполненных исследований были предложены каскадные схемы коррекции ошибок, состоящие из недвоичного МПД и модифицированных обычных или расширенных недвоичных кодов Хэмминга. Отличительной особенностью последних является то, что при кодировании и декодировании используется работа с целыми числами, а не элементами из полей Галуа. В результате данные коды можно использовать практически для любого размера символа. Также в отличие от известных недвоичных кодов Хэмминга с помощью предложенных модифицированных недвоичных кодов Хэмминга в большинстве случаев может исправлять две ошибки в блоке.

Результаты предварительного анализа и проведенного исследования разработанных каскадных схем кодирования показывают, что с их помощью обеспечивается уменьшение вероятности ошибки декодирования в области эффективной работы недвоичных многопороговых декодеров на 2..4 и ряде случаев даже более порядков.

4. Разработанный МПД сверточного самоортогонального кода реализован в ИКИ РАН на ПЛИС Altera. Созданное устройство коррекции ошибок на

скоростях более 1 Гбит/с в дальнейшем позволит решить все проблемы связи и на произвольно высоких скоростях передачи данных вплоть до 30 Гбит/с.

Одна из последних реализаций МПД была разработана в ИКИ РАН на ПЛИС Altera Stratix EP1S20 (рис. 6). Этот МПД является следующим этапом развития (с 1972 г.) этих декодеров сверточных кодов на базе МПД и может считаться представителем их шестого поколения.

Рис. 6. МПД, разработанный в ИКИ РАН на ПЛИС Altera Stratix EP1S20

В данной ПЛИС реализован кодер, модуль генератора гауссовского шума и декодер, состоящий из 9-ти итераций коррекции ошибок (рис. 7). Разрядность шины данных 8 бит, частота следования данных 40 МГц (общая информационная скорость до 320 Мбит/сек). Длина каждой итерации декодера составляет 256 бит.

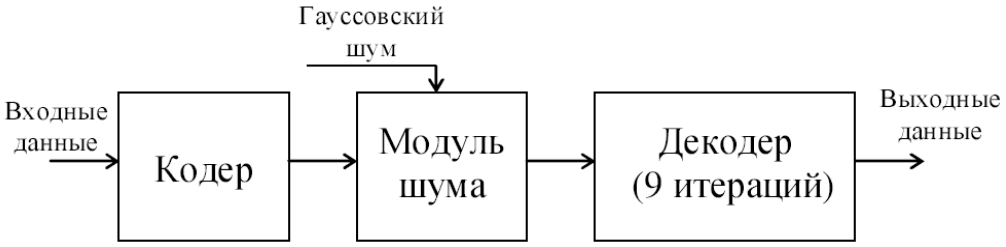

Рис. 7. Схема ПЛИС

В процессе разработки рассматриваемого МПД как составной части аппаратно-программного демонстрационно-измерительного стенда был создан комплекс программных средств (рис. 8), который обеспечивал:

– генерацию информационного потока;

– генерацию шума с настраиваемыми параметрами;

– имитацию аппаратной версии декодера;

– оценку скорости работы прибора (демонстрация производительности декодера в спутниковом канале ДЗЗ на скорости 320 Мбит/сек);

– измерение достоверности декодирования в зависимости от уровня шума канала.

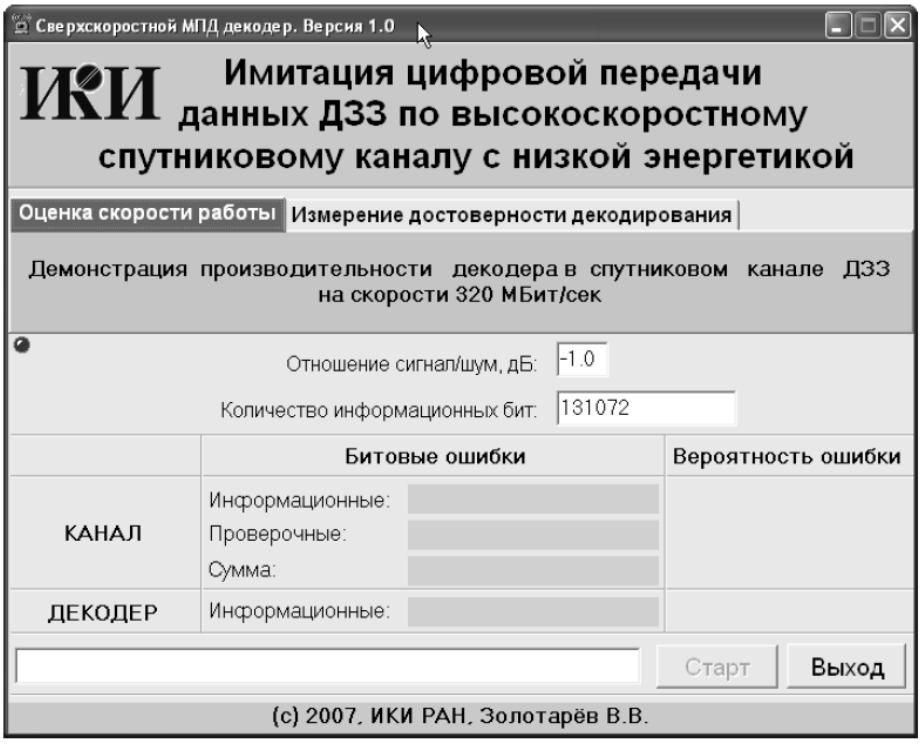

Рис. 8. Интерфейс программного комплекса МПД

При первом режиме работы программы демонстрируется скорость работы декодера. В кодер поступает информация, сгенерированная внутри ПЛИС, а на вход имитатора гауссовского шума подаются данные, находящиеся во внутренней памяти ПЛИС, которой достаточно для передачи 128 Кбит данных через декодер. При передаче большего количества данных шум из внутренней памяти повторяется. В этом режиме работы данные в кодере и декодере передаются на максимальной скорости (8-битовый поток с частотой 40 МГц), так как вся информация генерируется непосредственно в ПЛИС.

Для запуска программы нужно задать отношение сигнал/шум, а также количество передаваемых бит данных и нажать кнопку «Старт». Через декодер данные пройдут с максимальной скоростью, и программа покажет количество битовых ошибок на входе и выходе декодера, а также вероятность того, что декодер не исправит ошибку при данном соотношении сигнал/шум. В данном режиме работы показывается максимальная производительность работы декодера 640 Мбит/с в канале.

Во втором режиме работы измеряется эффективность декодирования в зависимости от уровня шума канала. Здесь также задается отношение сигнал/шум и количество передаваемых бит, но в этом случае информация на вход кодера и данные имитатора гауссовского шума поступают из компьютера. В этом режиме имеется возможность проверить работу декодера на большом количестве данных при постоянно изменяющемся уровне шума в канале.

Данный проект показал, что можно получить хорошие энергетические характеристики кодирования при высоком уровне шума на информационной скорости до 320 Мбит/с при очень малой аппаратной сложности, что чрезвычайно ценно для систем ДЗЗ.

В 2009 г. в ИКИ РАН завершились испытания декодера, работающего на информационной скорости более 1 Гбит/с. Этого удалось достичь за счет использования конвейера при реализации процедур вычислений на пороговом элементе декодера. При реализации этой сверхвысокоскоростной версии МПД

декодера удалось максимально эффективно использовать вычислительные ресурсы очень недорогой ПЛИС. Энергетическая эффективность и общие размеры наземной части комплекса (декодера) в общем случае определяются выбором конкретных типов ПЛИС приёмной части системы кодирования.

В таблице 2 представлены ПЛИС фирмы Altera, необходимые для реализации декодера с требуемым энергетическим выигрышем.

Таблица 2

ПЛИС Altera	**Используемая память, Кбит**	**Энергетический выигрыш**
Stratix EP1S20	489	8,2 дБ
Stratix EP1S80	2219	8,7 дБ
Stratix2 EP2S180	4074	9,1 дБ

5. В течение всего периода выполнения проекта развивался специализированный веб-сайт ИКИ РАН www.mtdbest.iki.rssi.ru, на котором представляются основные результаты разработок МПД алгоритмов.

На веб-сайте регулярно помещаются новые статьи, демонстрационные материалы и презентации последних результатов по МПД. Здесь же можно найти ответы на вопросы по кодированию и объявления о предстоящих или уже состоявшихся событиях в сфере разработок МПД алгоритмов.

Веб-сайт ориентирован на научно-методическую и учебно-информационную деятельность. Он содержит более **300 (!!!)** позиций структурированных материалов: статьи, комментарии, демонстрационные материалы, презентации, переписку с читателями сайта, компьютерные фильмы по методам МПД и другую полезную информацию. Его объем существенно превышает размеры порталов всех известных нам крупнейших научных и коммуникационных организаций России, занимающихся аналогичными научно-технологическими проблемами.

В 2009 г. также началась разработка дополнительного веб-сайта www.mtdbest.ru, на котором будет представлена информация о последних достижениях в области разработки многопороговых декодеров и других методов помехоустойчивого кодирования.

3.7. Степень новизны полученных результатов

В рамках проекта РФФИ в 2009 году получены новые научные результаты по разработке методов совместного поиска структуры самоортогональных кодов и параметров их многопорогового декодирования, обеспечивающих наилучшую эффективность при близком к предельном уровне шума в канале связи.

Научной новизной также обладают разработанные каскадные схемы коррекции ошибок в символьных данных, применение которых позволяет уменьшить вероятность ошибки декодирования на 2..4 десятичных порядков и более даже по сравнению с уже изначально очень эффективным недвоичным МПД! В текущем году завершилось исследование и оптимизация параметров данных каскадных схем. Результаты этих исследовании легли в основу защищенной в 2009 г. кандидатской диссертации.

В текущем году был получен патент РФ №2377722 на способ декодирования помехоустойчивого кода, в котором предлагается конвейерный пороговый элемент, используемый при декодировании самоортогонального кода. Применение подобного порогового элемента позволяет существенно повысить скорость работы декодера при его реализации на ПЛИС.

3.8. Сопоставление полученных результатов с мировым уровнем

Основное внимание в текущем году было уделено развитию недвоичных многопороговых декодеров недвоичных самоортогональных кодов. Поэтому сравнение результатов с мировым уровнем выполним только для недвоичных кодов. Сравнение эффективности полученных результатов для двоичных кодов было выполнено в отчете по проекту за прошлый год.

На сегодняшний день в теории кодирования известен ряд недвоичных кодов, различающихся корректирующей способностью, вносимой избыточностью, сложностью декодирования и многими другими важными параметрами. Рассмотрим эффективность современных методов коррекции ошибок в символьных данных при различных параметрах кода и размерах символа. При сравнении характеристик будем использовать классическую модель q-ичного симметричного канала (qСК), которая хорошо подходит для оценивания возможностей данных методов. В таком канале каждый символ искажается независимо с вероятностью P_0, причем при искажении символ с равной вероятностью переходит в один из q–1 других символов. Подобная модель, например, соответствует каналу с пакетами ошибок при использовании перемежения/деперемежения на уровне символов.

Среди недвоичных кодов в настоящее время практическое применение нашли только коды Рида-Соломона (РС), обладающие рядом положительных свойств. Для коротких кодов РС существуют эффективные алгоритмы декодирования, в полной мере использующие корректирующие возможности кода. Сложность реализации наиболее простых из них пропорциональна $n\cdot\log^2 n$. Под сложностью реализации здесь и далее понимается число арифметических операций, требуемых для декодирования кодового блока.

Характеристики кодов РС с кодовой скоростью R=1/2 и длиной n=255 однобайтовых символов (размер алфавита q=256) в qСК представлены на рис. 9 кривой *1*. По оси абсцисс на рисунке отложена вероятность ошибки P_0 в qСК, а по оси ординат – оценка вероятности ошибки на символ после декодирования, полученная путем компьютерного моделирования. При этом теоретически в qСК для q=256 и R=1/2 можно работать при P_0=0.380. Видно, что показываемые кодами РС характеристики очень далеки от теоретически возможных.

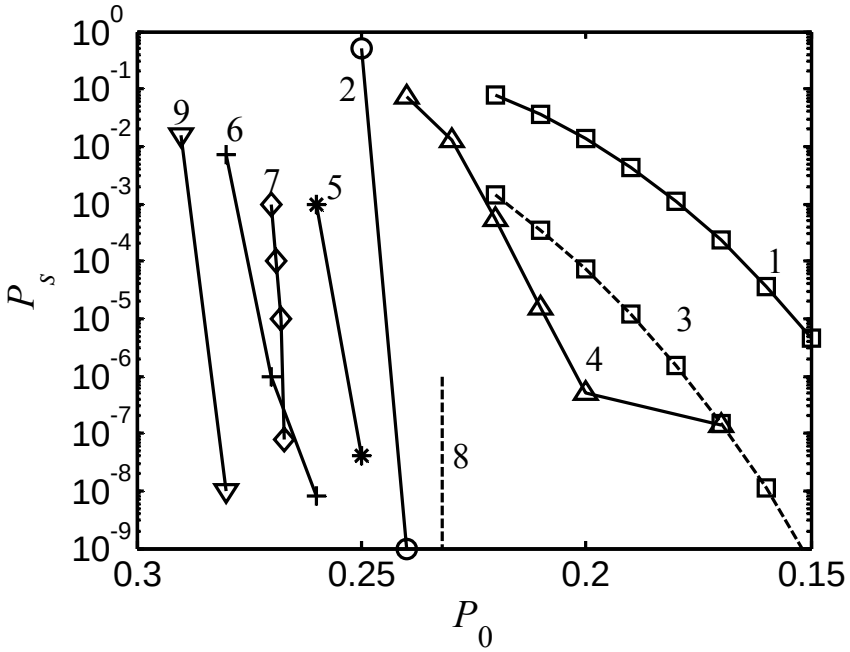

Рис. 9. Характеристики недвоичных кодов с R=1/2 в qСК

Потенциальные возможности более длинных кодов РС с кодовой скоростью R=1/2 и длиной n=65535 двухбайтовых символов (q=2^{16}) отражены на рис. 9 кривой *2*. И такие коды работают при вероятности ошибки в канале, значительно меньшей теоретически возможной, равной P_0=0.438 для данных условий.

Особый интерес для систем передачи и хранения данных часто представляют малоизбыточные помехоустойчивые коды. Для таких кодов РС характеристики представлены на рис. 10. Здесь кривая *1* отражает вероятность символьной ошибки декодера кода РС с кодовой скоростью R=7/8 для однобайтовых символов (q=256). Отметим, что теоретически при данных R и q можно работать при вероятности ошибки в канале около 0.076. Характеристики кодов РС с еще большей кодовой скоростью R=19/20 при q=256 представлены на рис. 10 кривой *2*. Для указанных параметров канала и кодирования предельно возможный уровень шума, при котором теоретически возможно эффективное декодирование, составляет P_0≈0.027.

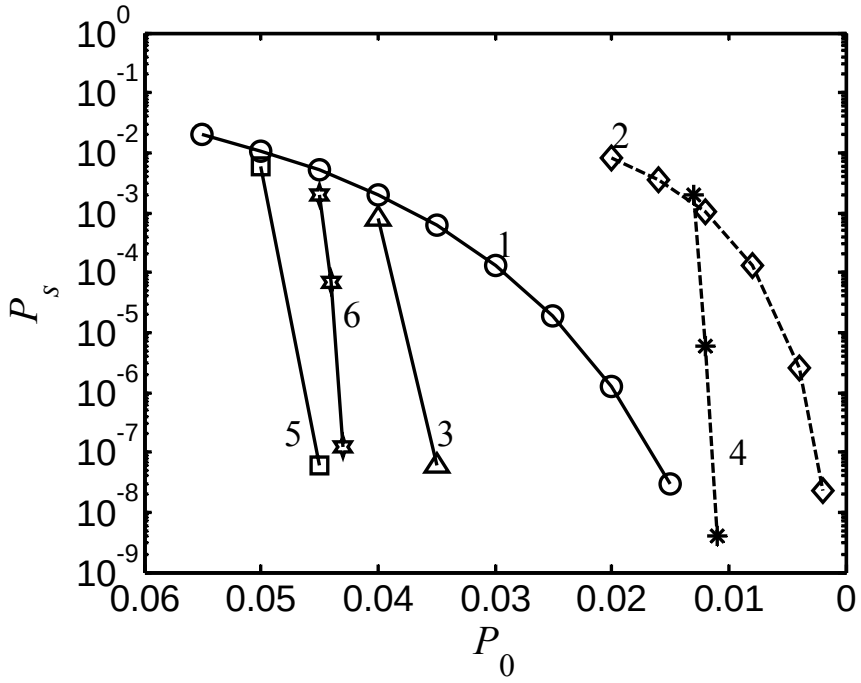

Рис. 10. Характеристики малоизбыточных недвоичных кодов

Заметим, что кроме кодов РС в настоящее время вообще нет других коротких недвоичных кодов, имеющих достаточно эффективные и одновременно простые методы декодирования. Однако короткие коды РС длины до n=255 однобайтовых символов, как следует из рис. 9 и 10, не обеспечивают необходимых в настоящее время уровней достоверности. А декодеры для длинных кодов РС оказываются слишком сложными для реализации и возможное существенное упрощение данных декодеров весьма проблематично. Отметим, что для кодов РС существуют алгоритмы декодирования, позволяющие исправлять даже несколько большее, чем t, число ошибок, например, алгоритм Судана. Данные методы очень интересны для теории кодирования, однако сложность их реализации становится пропорциональной n^3, в то время как рост эффективности декодирования от такого усложнения, особенно при высоких кодовых скоростях, которые часто и требуется применять на практике, оказывается незначительным. Это иллюстрируется кривой *3* на рис. 9, который соответствует алгоритму декодирования Судана для кода РС с n=255, q=256 и R=1/2.

Гораздо ближе к теоретическим границам работают разработанные в рамках

гранта q-ичные многопороговые декодеры (qМПД) недвоичных самоортогональных кодов. Они, как и обычные двоичные МПД, обладают свойством стремления к решению оптимального декодера при линейной от длины кода сложности реализации, которая свойственна только пороговым процедурам. В отличие от кодов РС для qМПД никаких ограничений по длине кода вообще нет, поскольку длина кода n и размер алфавита q в недвоичных кодах с мажоритарным декодированием совершенно не зависят друг от друга. При этом сложность декодирования кодового блока пропорциональна $n{\cdot}d{\cdot}I$, где n – длина кода, d – кодовое расстояние (обычно $d{\le}20$), I – число итераций декодирования (обычно $I{\le}30$).

Характеристики qМПД также представлены на рис. 9. Здесь кривыми *4* и *5* показана эффективность qМПД для самоортогональных кодов с R=1/2 и длиной блока 4000 и 32000 однобайтовых символов (q=256). Объем моделирования в нижних точках данных графиков составлял от $5{\cdot}10^{10}$ до $2{\cdot}10^{12}$ символов, что свидетельствует о крайней простоте метода. Из рисунка видно, что характеристики qМПД оказываются гораздо лучше характеристик кодов РС с такими же q и R. При увеличении длины блока, что для qМПД не вызывает никаких сложностей, разница в эффективности становится еще более существенной. Характеристики qМПД при использовании двухбайтовых символов представлены на рис. 9 кривой *6*. Здесь также использовался код с R=1/2 и n=32000 символов. Отметим, что очень простой для реализации qМПД для двухбайтового кода длины 32000 оказывается способным обеспечить помехоустойчивость, недостижимую даже для кода РС длины 65535 двухбайтовых символов, декодер для которого на данный момент слишком сложен для реализации. При этом qМПД для двухбайтовых символов практически ни в чем не сложнее однобайтового, так как его сложность совершенно не зависит от размера алфавита q.

Высокой корректирующей способностью обладают и qМПД для малоизбыточных недвоичных самоортогональных кодов, пример характеристик которых для R=7/8, n=48000 символов и q=256 представлен на рис. 10 кривой *3*. Здесь также видно заметное преимущество qМПД над кодами РС. Аналогичная ситуация наблюдается и при использовании кодов с еще более высокой кодовой скоростью R=19/20. Для данной кодовой скорости при q=256 эффективность qМПД показана кривой *4*, а для кодов РС – кривой *2*. Такие же высокие характеристики обеспечивает qМПД малоизбыточных кодов при использовании алфавита большего объема, при котором создание других декодеров представляется очень сложным. На рис. 10 кривой *5* представлена эффективность qМПД для кода с R=7/8 при использовании двухбайтовых символов (q=65536).

Отметим, что для достижения с помощью qМПД таких результатов требуется очень тщательно выбирать применяемые коды, основным критерием при отборе которых является степень устойчивости к эффекту размножения ошибок, который проявляется в том, что после первой ошибки декодирования существенно увеличивается вероятность последующих ошибок. Известно, что размножению ошибок в наименьшей степени подвержены коды для схем с параллельным кодированием. В работе показано, что оптимизируя структуру данных кодов можно еще улучшить эффективность работы qМПД. В частности, характеристики найденных кодов с q=256 и кодовыми скоростями 1/2 и 7/8 представлены на рис. 9 и 10 кривыми *7* и *6* соответственно. Видно, что данные коды обеспечивают эффективную работу при б*о*льших вероятностях ошибки в qСК, чем ранее

представленные, при такой же сложности их декодирования.

Согласно общим принципам теории кодирования, переход к каскадным принципам кодирования еще более улучшит характеристики qМПД без существенно усложнения декодера. Показано, что применение совместно с qМПД простейшего кода с контролем по модулю q, разработанного в рамках гранта, позволяет на несколько порядков снизить вероятность ошибки на блок по сравнению с обычным qМПД при всего лишь 2% росте избыточности. При этом увеличение объема вычислений в каскадном коде составляет менее 20% по сравнению с исходным алгоритмом qМПД.

Таким образом, недвоичный аналог алгоритма МПД может обеспечить при весьма высоких уровнях шума вероятности ошибки декодирования, в ряде случаев недоступные для кодов Рида-Соломона сколько угодно большой длины. При этом сложность реализации такого алгоритма оказывается незначительной, линейно растущей с длиной кода, т.е. теоретически минимально возможной.

В последнее время зарубежными специалистами стали активно развиваться декодеры недвоичных низкоплотностных (qLDPC) кодов. Данные методы, безусловно, обладают очень высокой корректирующей способностью, однако сложность их реализации при больших значениях основания кода q оказывается слишком большой для практического применения в реальных системах. В частности сложность одной итерации декодирования кодового блока для одного из наиболее простых из известных алгоритмов декодирования qLDPC кодов пропорциональна $n \cdot q \cdot \log_2 q$. В результате разница в сложности реализации qМПД и декодеров qLDPC кодов при использовании всего четырехбайтовых символов ($q=2^{32}$) превышает миллиард раз. qМПД же при этом будет иметь ту же символьную скорость работы, как и для однобайтовых символов, а его битовая производительность даже возрастет в 4 раза. Известен метод декодирования qLDPC кодов, который обладает сложностью, пропорциональной $n \cdot s^2$, где $s \le q$ – максимальный размер списка, передаваемого по ветвям графа qLDPC кода и содержащего наиболее вероятные символы, соответствующие этим ветвям. Такое ограничение размера списка существенно упрощает процесс декодирования, но приводит к некоторому ухудшению характеристик. Например, для размера алфавита $q=2^{32}$ декодер регулярного qLDPC кода длиной 100000 символов и кодовой скоростью $R=1/2$ при $s=q$ теоретически способен работать при вероятности ошибки в канале $P_0=0.429$, а при $s=32$ работает только при $P_0=0.232$ (пунктир *8* на рис. 9). Следует особо отметить что декодер qLDPC кода с $s=32$ обладает существенно меньшей корректирующей способностью, чем qМПД при символах такого же размера (кривая *9* на рис. 9), и примерно в тысячу раз большей вычислительной сложностью.

3.9. Методы и подходы, использованные в ходе выполнения проекта

Разработки и исследования проводились на основе теории вероятностей, математической статистики, системного анализа, математического и имитационного моделирования, технологий модульного и объектно-ориентированного программирования.

Особенностью данного проекта является то, что в нем повышение достоверности передачи данных по каналам с шумами осуществлялось на основе развития максимально простых методов кодирования/декодирования, к которым относятся многопороговые декодеры (МПД). Все проведенные исследования по МПД, в отличие от западных работ, базируются на принципе развития этого

предельно простого метода, позволяющего практически оптимально декодировать произвольно длинные коды всего лишь с линейной сложностью. Особо показательными в этом отношении являются недвоичные декодеры, которые при некоторых типичных наборах параметров кодирования оказываются лучше и проще декодеров кодов Рида-Соломона в десятки тысяч или даже в миллионы раз для самых длинных из уже проанализированных коллективом проекта кодов. И только после тонкой и точной отработки основного метода исследования мы проводим доработку методов декодирования в плане повышения эффективности. Имея огромное преимущество методов МПД перед другими алгоритмами, коллектив разработчиков имеет возможность и ресурсы для небольшого увеличения числа операций декодирования, если при этом возможно очень значительное дополнительное улучшение характеристик таких улучшенных декодеров. Эта особенность исследовательских работ, проводимых коллективом сотрудников гранта, позволила нашему коллективу приблизиться к уровню результатов для упоминавшихся выше турбо и LDPC кодов при числе сотрудников, работающих по теме гранта, в тысячи раз меньшем, чем по указанным наиболее популярным темам теории кодирования за рубежом. Укажем также, что сфера работы нескольких оставшихся отечественных коллективов специалистов по теории кодирования много у̀же. Мы уверены, что именно предложенный нами стиль от простейших методов к их более эффективным модификациям, а не максимальная эффективность за счет сложности и последующее – обычно очень проблемное! – упрощение (стиль западных исследований), сможет помочь решить в ближайшем будущем проблему декодирования максимально просто и быстро.