

ОТЧЕТ ЗА 2010 ГОД ПО ПРОЕКТУ РФФИ 08-07-00078-а

Статус отчета: не подписан

Дата последнего изменения: 12.12.2010

Отчёт создал: Золотарев Валерий Владимирович

Отчет распечатан: 12.12.2010

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

2011

1.6. Вид отчета

итоговый (2008-2010)

1.7. Аннотация

За время выполнения проекта выполнялись работы по повышению эффективности многопороговых декодеров (МПД). Одно из направлений работ связано с построением новых помехоустойчивых кодов с особо низким уровнем группирования ошибок при многопороговом декодировании. Для данных целей были создан набор программных средств, включающий средства анализа спектра самоортогональных кодов (СОК), средства генерации кодов с заданным уровнем размножения ошибок, а средства оптимизации структуры СОК для работы вблизи пропускной способности канала. Использование построенных с помощью данного ПО кодов при многопороговом декодировании позволило существенно (в ряде случаев более чем на 0,5 дБ) снизить допустимое отношение сигнал/шум при использовании МПД в каналах космической и спутниковой связи. В результате характеристики МПД в области обеспечения низких вероятностей ошибки стали сопоставимыми с характеристиками лучших современных методов коррекции ошибок. 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.

Создан демонстрационный аппаратно-программный комплекс, включающий МПД сверточного кода, реализованный на ПЛИС Altera, и позволяющий выполнять декодирование информационного потока на скорости до 1,6 Гбит/с. Применение данного комплекса позволяет ускоренно развивать методы и средства помехоустойчивого кодирования для спутниковых и космических линий связи в области еще больших скоростей коррекции ошибок при значительном уровне шума. По результатам этих работ получен патент на изобретение в области методов помехоустойчивого кодирования.

Выполнена разработка новых каскадных схем коррекции ошибок в двоичных данных, составляющим элементом которых является кодер самоортогональных кодов и МПД. Для данных кодов был сформулирован и доказан ряд теорем о стремлении решения декодеров каскадных кодов различных классов к решению оптимального декодера при

каждом изменении декодируемого символа декодером внешнего кода. Показано, что при использовании предложенных каскадных кодов возможно дополнительное улучшение эффективности работы МПД на 0.2..0.5 дБ по сравнению с ранее полученными результатами. Важно, что столь высокое повышение эффективности декодеров двоичных кодов в области, близкой к пропускной способности канала, особенно трудно и ценно.

Предложен и исследован новый подход к декодированию блоковых и сверточных самоортогональных кодов, основанный на применяемом для декодирования низкоплотностных кодов, min-sum алгоритме декодирования. Показано, что использование предложенного подхода позволяет улучшить эффективность декодирования на 0,5..1 дБ при примерно четырехкратном повышении сложности реализации декодера. Сложность кодера при этом остается неизменной, что очень важно для многих систем, например систем дистанционного зондирования земли, а сложность декодера все равно существенно меньше сложности сопоставимых по эффективности методов коррекции ошибок.

Завершен очень важный этап исследований и разработки уникальных алгоритмов недвоичного многопорогового декодирования для сверхвысокоскоростной записи и особо надёжного хранения цифровых символьных потоков данных. Как известно, символьные самоортогональные коды открыты ещё в СССР и до сих пор не исследуются вообще за рубежом, хотя характеристики этих кодов на много десятичных порядков превышают и эффективность и сложность алгоритмов, которые известны на Западе. Для данных декодеров построены новые самоортогональные коды с малым размножением ошибок, что позволило дополнительно примерно на 0,1..0.2 дБ улучшить обеспечиваемый энергетический выигрыш без изменения алгоритмов кодирования/декодирования. Разработаны новые каскадные схемы коррекции ошибок, основанные на символьных МПД. Применение данных схем позволяет повысить достоверность хранения цифровых данных на 2..5 порядков по сравнению с базовым некаскадным методом при усложнении алгоритма коррекции ошибок всего на 10..30%. Это позволяет утверждать, что завершённое исследование полностью решило проблему простой и очень быстрой записи для хранения цифровых данных с произвольно большой достоверностью на всё ближайшее обозримое будущее техники обработки цифровой информации.

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 разработан дополнительный веб-сайт www.mtdbest.ru, на котором представлена разнообразная 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 transmission, processing and storage for work near channel capacity

2.4. Год представления отчета

2011

2.5. Вид отчета

ИТОГОВЫЙ (2008-2010)

2.6. Аннотация

During the project works were performed on efficiency multithreshold decoders (MTD) increasing. One of work trend is connected with construction of new codes with very low error propagation during multithreshold decoding. For this purpose a set of software was created. It includes software for self-orthogonal code (SOC) spectrum analysis, software for construction of SOC with necessary error propagation and software for optimization structure of SOC. A using of generated with these software codes allows essentially (in many times more than 0,5 dB) improve coding gain for satellite and space channels. As a result of the MTD performance 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 decoding methods.

A demonstration hardware-software complex was created. This complex includes MTD for a convolutional SOC implemented on serial FPGA Altera and allows decode data with rate about 1,6 Gbps. Application of the complex 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. By results of these works the patent for the invention in the field of error-correcting coding methods is received.

The development of concatenated schemes for error correction in binary data carried out. These schemes include encoder for self-orthogonal codes and multithreshold decoder. For these schemes a number of theorems was formulated and proved. These theorems claim that decision of concatenated code decoder aspires to decision of an optimum decoder at every symbol correction. It is shown that using of submitted concatenated schemes allows to increase coding gain on 0,2..0,5 dB in comparison with previous results. Note that performance increasing for noise level near to channel capacity is very hard and valuable task. It was submitted new way to self-orthogonal codes decoding. This way is based on min-sum algorithm used for decoding of low-density parity-check codes. The simulation results for such decoding shows performance improvement on 0,5..1 dB at decoding complexity increasing in about four times.

The important stage of development of unique non-binary multithreshold decoders for q-ary self-orthogonal codes is finished. As it is known symbolic self-orthogonal codes was submitted in USSR. The symbol error rate performance of multithreshold decoders for these codes in many decimal orders better than performance of other known codes. Such performance can be obtained at liner (i.e. minimal possible!) implementation complexity. During last year new self-orthogonal codes with low

level error propagation was constructed. It allows increase coding gain on 0,1..0,2 dB additionally without any modification coding/decoding algorithm. New concatenated error correction schemes based on symbolic MTD were constructed also. These methods allow to raise reliability of storage in 2..5 decimal order at complication of decoding algorithm on 10..30 % in comparison with initial MTD. It allows to state that completed works solve problems of very simple and fast recording for digital data storage with any required reliability for near future.

During all period of the project specialized web site www.mtdbest.iki.rssi.ru is developed. The basic results of workings out of MTD algorithms are presented in it. It was created additional site www.mtdbest.ru which also contains different information about development of multithreshold decoders and other error correction methods.

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 2010 год*

Целью очередного годового этапа является разработка методов, методик и алгоритмов дальнейшего повышения эффективности многопороговых декодеров (МПД) и каскадных схем на его основе вблизи пропускной способности канала. При этом будут решены следующие основные задачи:

1. Разработка принципов функционирования расширенных пороговых элементов, направленного на исправление особо сложных для МПД конфигураций ошибок.
2. Разработка математического и программного обеспечения для анализа спектра самоортогональных кодов.
3. Разработка методики получения мягких решений многопорогового декодера, отражающих надежность декодированных битов.
4. Создание технологического макета высокоскоростного декодера МПД.

Также в 2010 г. коллективом авторов запланировано участие в зарубежных конференциях по проблемам передачи данных и публикация статей в зарубежных журналах.

3.5. *Степень выполнения поставленных в проекте задач*

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

1. Разработаны новые каскадные схемы коррекции ошибок, основанные на многопороговом декодере, и выполнена оптимизация параметров их работы. Применение предложенных каскадных кодов и методов их декодирования позволяет уменьшить вероятность ошибки декодирования на 3..5 десятичных порядков и более даже по сравнению с уже изначально очень эффективным двоичным и недвоичным МПД.
2. Разработано математическое и программное обеспечение для анализа спектра самоортогональных кодов. Результаты данного анализа позволили построить новые самоортогональные коды, значительно более устойчивые к эффекту размножения ошибок, чем ранее известные.
3. Разработка методики получения мягких решений многопорогового декодера каскадного кода, отражающих надежность декодированных битов. Данную информацию можно использовать декодерами внешних кодов для улучшения эффективности их работы.
4. Результаты работ опубликованы в ряде ведущих российских журналов. Две статьи в IEEE Transaction on Communication находятся на стадии рецензирования. Задача построения нового технологического макета высокоскоростного декодера МПД не была выполнена из-за уменьшения объема финансирования. Для проведения необходимых исследований использовался демонстрационно-измерительный стенд МПД, созданный на предшествующих этапах работ по гранту. На завершающем этапе находится решение задачи разработки принципов функционирования расширенных пороговых элементов, направленных на исправление особо сложных для МПД конфигураций ошибок, что позволит

улучшить эффективность декодирования при работе вблизи пропускной способности канала.

Кроме поставленных задач дополнительно была решена задача адаптации методов декодирования низкоплотностных кодов для декодирования самоортогональных кодов. Результаты исследования показали, что применение данных методов позволяет получить дополнительный энергетический выигрыш кодирования порядка 0,5..1 дБ при четырехкратном росте сложности реализации.

Таким образом, можно считать, что поставленные в проекте задачи решены.

3.6. *Полученные за отчетный период важнейшие результаты*

1. Разработаны новые каскадные схемы коррекции ошибок, основанные на многопороговом декодере, и выполнена оптимизация параметров их работы. Применение предложенных каскадных кодов и методов их декодирования позволяет уменьшить вероятность ошибки декодирования на 3..5 десятичных порядков и более даже по сравнению с уже изначально очень эффективным двоичным и недвоичным МПД.

В работе предложено организовать каскадирование внутреннего СОК, декодируемого с помощью МПД, с другим внешним СОК, также декодируемым с помощью МПД. Для данной схемы был сформулирован и доказан ряд теорем.

Рассмотрим теоретические основы построения каскадной схемы кодирования, состоящей из внутреннего СОК и внешнего СОК, декодируемых с помощью МПД. Пусть внутренний код C_1 имеет кодовое расстояние d_1 , длину кода N_1 и длину информационной части K_1 . Пусть внешний код C_2 имеет кодовое расстояние d_2 , длину кода N_2 и длину информационной части K_2 .

Пусть каскадный код представляет собой код-произведение, т.е. исходные данные при кодировании записываются в массив размером K_2 на K_1 . Затем данные кодируются по столбцам кодом C_2 , после чего результат кодируется по строкам кодом C_1 . В результате в силу линейности составляющих кодов каждая строка матрицы является кодовым словом внутреннего кода, а каждый столбец – кодовым словом внешнего кода. Общая длина кода получается равной N_1N_2 , длина информационной части K_1K_2 , минимальное кодовое расстояние d_1d_2 , кодовая скорость $R=K_1K_2/N_1N_2$. После завершения процедуры кодирования данные из массива считываются по строкам и передаются по каналу.

Подобная организация каскадирования иллюстрируется рис. 1, на котором символы I соответствуют информационным символам кода, символы $C^{(2)}$ – проверочным символам внешнего кода. Проверочные символы внутреннего кода для информационных символов I обозначены через $C^{(1)}$, а проверочные символы внутреннего кода для проверочных символов внешнего кода обозначены на рисунке через $C^{(*)}$.

Пусть после передачи по ДСК декодер каскадного кода принял искаженные в канале информационные символы U и проверочные символы $V^{(1)}$, $V^{(2)}$ и $V^{(*)}$ (рис. 2а).

При декодировании данного каскадного кода сначала МПД выполняет декодирование внутреннего СОК (декодирование всех строк), после чего с помощью другого МПД выполняется декодирование внешнего СОК (декодирование столбцов, соответствующих информационным символам каскадного кода).

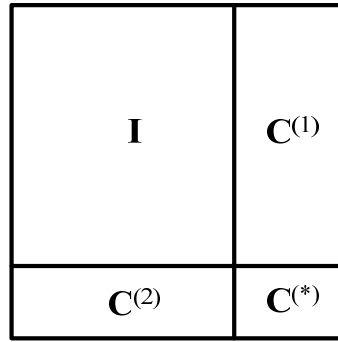


Рис. 1. Кодовое слово каскадного кода

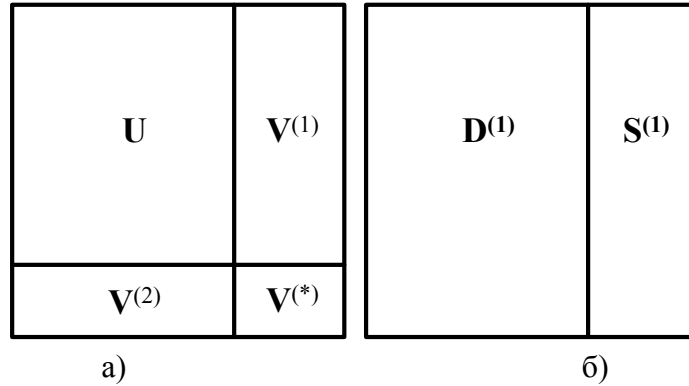


Рис. 2. Принятое сообщение каскадного кода

Пусть после декодирования внутреннего СОК МПД сохранил значения синдромного и разностного регистров $\mathbf{S}^{(1)}$ и $\mathbf{D}^{(1)}$ (рис. 2б), а также сформировал регистр \mathbf{L} , в который занес значение суммы на пороговом элементе для каждого из своих информационных символов

$$l_{ij} = \sum_{k \in \Theta_j} s_{ik}^{(1)} + d_{ij}^{(1)}.$$

Здесь Θ_j представляет множество номеров проверок внутреннего кода (элементов синдрома $\mathbf{S}^{(1)}$), участвующих при декодировании j -го символа в любой строке; $s_{ik}^{(1)}$ – элемент регистра $\mathbf{S}^{(1)}$; $d_{ij}^{(1)}$ – элемент регистра $\mathbf{D}^{(1)}$.

После этого в процесс декодирования включается МПД внешнего СОК, который в процессе работы сначала обычным образом вычисляет значение синдрома $\mathbf{S}^{(2)}$ и затем выполняет декодирование.

Для каскадного кода, построенного в соответствии с описанными принципами, справедлива следующая теорема.

Теорема 1. Для канала типа ДСК при каждом изменении декодируемых символов на первой итерации многопорогового декодера внешнего кода происходит переход к более правдоподобному решению всего каскадного кода в целом по сравнению с предыдущим решением декодера.

Доказательство.

Пусть МПД внешнего кода выполняет декодирование некоторого информационного символа u_{ij} . Сравним расстояние между принятым сообщением и кодовым словом полного каскадного кода до и после инвертирования символа u_{ij} . Отметим, что под расстоянием между кодовым словом \mathbf{C} и принятым сообщением \mathbf{B} в случае использования канала типа ДСК понимается расстояние Хэмминга между ними:

$$W = \sum_{i=0}^{N-1} (c_i \oplus b_i).$$

Здесь N – длина кодового слова; c_i – элемент вектора \mathbf{C} , равный 0 или 1; b_i – элемент вектора \mathbf{B} , равный 0 или 1. В дальнейшем для удобства изложения величину W будем называть метрикой кодового слова \mathbf{C} .

Запишем выражение для расстояния метрики кодового слова полного каскадного кода, которое является решением декодера до изменения информационного символа u_{ij} . При этом в выражении для метрики выделим элементы, связанные с данным информационным символом и не связанные с ним (рис. 3). Заметим, что с информационным символом u_{ij} связаны:

- 1) d_1-1 проверка внутреннего кода (обозначены на рис. 3 кружочками).
- 2) d_2-1 проверка внешнего кода (обозначены на рис. 3 крестиками).
- 3) $(d_2-1)(d_1-1)$ проверок внешнего кода для проверок внутреннего кода, связанных с рассматриваемым информационным символом (обозначены на рис. 3 треугольниками).

- 4) Элемент разностного регистра $\mathbf{D}^{(1)}$ (обозначен на рис. 3 квадратом).

Таким образом, с информационным символом u_{ij} связано всего d_2d_1-1 проверок и один элемент разностного регистра.

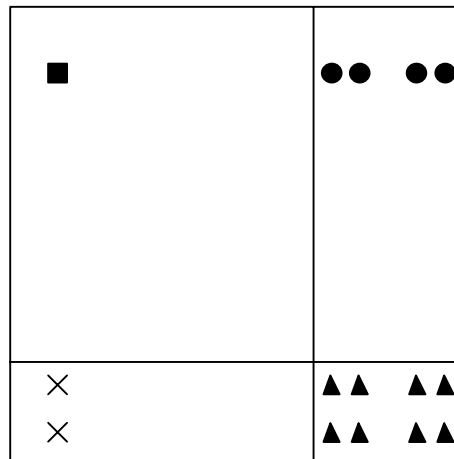


Рис. 3. Символы, связанные с декодируемым символом

В результате метрика кодового слова полного каскадного кода до инвертирования символа u_{ij} определяется как:

$$\begin{aligned}
 W_0 &= X + d_{ij}^{(1)} + \sum_{k \in \Theta_j} s_{ik}^{(1)} + \\
 &+ \sum_{m \in \Omega_i} \left((1 - s_{mj}^{(2)})(d_{mj}^{(1)} + \sum_{k \in \Theta_j} s_{mk}^{(1)}) + s_{mj}^{(2)}(d_1 - (d_{mj}^{(1)} + \sum_{k \in \Theta_j} s_{mk}^{(1)})) \right) = \\
 &= X + l_{ij} + \sum_{m \in \Omega_i} \left((1 - s_{mj}^{(2)})l_{mj} + s_{mj}^{(2)}(d_1 - l_{mj}) \right).
 \end{aligned} \tag{1}$$

Здесь X – константа, содержащая компоненты синдромов и разностного регистра, не зависящие от u_{ij} ; Ω_i – множество номеров проверок для внешнего кода, участвующих при декодировании символа u_{ij} ; $s_{ik}^{(1)}$ – элемент регистра $\mathbf{S}^{(1)}$; $s_{mj}^{(2)}$ – элемент регистра $\mathbf{S}^{(2)}$; $d_{ij}^{(1)}$ – элемент регистра $\mathbf{D}^{(1)}$; l_{mj} – элемент регистра \mathbf{L} ; d_1 – кодовое расстояние внутреннего СОК.

В сумме $\sum_{m \in \Omega_i} \left((1 - s_{mj}^{(2)})(d_{mj}^{(1)} + \sum_{k \in \Theta_j} s_{mk}^{(1)}) + s_{mj}^{(2)}(d_1 - (d_{mj}^{(1)} + \sum_{k \in \Theta_j} s_{mk}^{(1)})) \right)$ часть

$(1 - s_{mj}^{(2)})(d_{mj} + \sum_{k \in \Theta_j} s_{mk}^{(1)})$ соответствует проверочным символам внешнего кода, для

которых проверка $s_{mj}^{(2)}$ выполняется, а часть $s_{mj}^{(2)}(d_1 - (d_{mj} + \sum_{k \in \Theta_j} s_{mk}^{(1)}))$ соответствует

проверочным символам внешнего кода, для которых проверка не выполняется (соответствующий проверочный символ в кодовом слове должен быть инвертирован).

После инверсии символа u_{ij} все элементы, связанные с ним будут также инвертированы. Это приведет к тому, что метрика нового кодового слова станет равной

$$W_1 = X + d_1 - l_{ij} + \sum_{m \in \Omega_i} (d_1 - (1 - s_{mj}^{(2)})l_{mj} - s_{mj}^{(2)}(d_1 - l_{mj})). \quad (2)$$

Определим условия, при выполнении которых данная метрика при инвертировании символа u_{ij} уменьшается, т.е. будет выполняться условие

$$W_1 - W_0 < 0. \quad (3)$$

$$X + d_1 - l_{ij} + \sum_{m \in \Omega_i} (d_1 - (1 - s_{mj}^{(2)})l_{mj} - s_{mj}^{(2)}(d_1 - l_{mj})) - \\ - \left(X + l_{ij} + \sum_{m \in \Omega_i} ((1 - s_{mj}^{(2)})l_{mj} + s_{mj}^{(2)}(d_1 - l_{mj})) \right) < 0.$$

$$d_1 - 2l_{ij} + \sum_{m \in \Omega_i} (d_1 - 2(1 - s_{mj}^{(2)})l_{mj} - 2s_{mj}^{(2)}(d_1 - l_{mj})) = \quad (4)$$

$$= d_1 - 2l_{ij} + \sum_{m \in \Omega_i} (d_1 - 2l_{mj})(1 - 2s_{mj}^{(2)}) < 0$$

Обозначим $d_1 - 2l_{ij}$ через Δ_{ij} . Тогда выражение (4) примет вид

$$d_1 - 2l_{ij} + \sum_{m \in \Omega_i} (d_1 - 2l_{mj})(1 - 2s_{mj}^{(2)}) = \Delta_{ij} + \sum_{m \in \Omega_i} \Delta_{mj}(1 - 2s_{mj}^{(2)}) < 0.$$

Или

$$- \Delta_{ij} + \sum_{m \in \Omega_i} (2s_{mj}^{(2)} - 1)\Delta_{mj} > 0. \quad (5)$$

Таким образом, при инверсии символа u_{ij} метрика кодового слова полного каскадного кода, а, следовательно, и расстояние между ним и принятым сообщением уменьшается, если выполняется условие (5). При этом происходит переход к более правдоподобному решению декодера. Но данное условие совпадает с условием принятия решения о наличии ошибки для первой итерации работы МПД. При этом вес символов внешнего кода определяется как $\Delta_{ij} = d_1 - 2l_{ij}$.

Таким образом, если МПД внешнего кода на первой итерации изменяет некоторый информационный символ, то происходит переход к более правдоподобному решению декодера.

Теорема доказана.

Далее рассмотрим работу МПД внешнего кода при выполнении второй и последующих итераций декодирования. При этом справедлива следующая теорема.

Теорема 2. Для канала типа ДСК при каждом изменении декодируемых символов на второй и последующей итерациях многопорогового декодера внешнего кода происходит переход к более правдоподобному решению всего каскадного кода в

целом по сравнению с предыдущим решением декодера.

Доказательство.

Пусть МПД внешнего кода выполнил первую итерацию декодирования в соответствии с принципами работы МПД, в результате выполнения которой были получены вектор синдрома $\mathbf{S}^{(2)}$ и разностный регистр $\mathbf{D}^{(2)}$ (рис. 4).

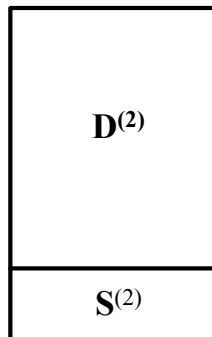


Рис. 4. Регистры МПД внешнего кода

Перепишем для данных условий выражение (1) для метрики кодового слова полного каскадного кода, являющегося решением декодера до изменения информационного символа u_{ij} . При этом на данное выражение будут оказывать дополнительное влияние элементы регистра $\mathbf{D}^{(2)}$.

$$W_0 = X + (1 - d_{ij}^{(2)})l_{ij} + d_{ij}^{(2)}(d_1 - l_{ij}) + \sum_{m \in \Omega_i} [(1 - s_{mj}^{(2)})l_{mj} + s_{mj}^{(2)}(d_1 - l_{mj})] \quad (6)$$

Здесь $d_{ij}^{(2)}$ – элемент регистра $\mathbf{D}^{(2)}$. Отметим, что в данном выражении в сумме $(1 - d_{ij}^{(2)})l_{ij} + d_{ij}^{(2)}(d_1 - l_{ij})$ слагаемое $(1 - d_{ij}^{(2)})l_{ij}$ соответствует случаю, когда на предшествующих итерациях декодирования МПД внешнего кода не изменил декодируемый символ, а слагаемое $d_{ij}^{(2)}(d_1 - l_{ij})$ – когда на предшествующих итерациях декодирования МПД внешнего кода изменил декодируемый символ.

После инверсии декодируемого символа u_{ij} метрика нового кодового слова будет равна

$$W_1 = X + d_1 - ((1 - d_{ij}^{(2)})l_{ij} + d_{ij}^{(2)}(d_1 - l_{ij})) + \sum_{m \in \Omega_i} (d_1 - ((1 - s_{mj}^{(2)})l_{mj} + s_{mj}^{(2)}(d_1 - l_{mj}))) \quad (7)$$

Тогда изменение метрики при инвертировании декодируемого символа будет следующим:

$$\begin{aligned}
W_1 - W_0 &= X + d_1 - \left((1 - d_{ij}^{(2)})l_{ij} + d_{ij}^{(2)}(d_1 - l_{ij}) \right) + \\
&+ \sum_{m \in \Omega_i} \left(d_1 - \left((1 - s_{mj}^{(2)})l_{mj} + s_{mj}^{(2)}(d_1 - l_{mj}) \right) \right) - \\
&- \left(X + (1 - d_{ij}^{(2)})l_{ij} + d_{ij}^{(2)}(d_1 - l_{ij}) + \sum_{m \in \Omega_i} \left((1 - s_{mj}^{(2)})l_{mj} + s_{mj}^{(2)}(d_1 - l_{mj}) \right) \right) = \\
&= d_1 - 2 \left((1 - d_{ij}^{(2)})l_{ij} + d_{ij}^{(2)}(d_1 - l_{ij}) \right) + \sum_{m \in \Omega_i} \left(d_1 - 2 \left((1 - s_{mj}^{(2)})l_{mj} + s_{mj}^{(2)}(d_1 - l_{mj}) \right) \right) = \\
&= d_1(1 - 2d_{ij}^{(2)}) - 2l_{ij}(1 - 2d_{ij}^{(2)}) + \sum_{m \in \Omega_i} \left(d_1(1 - 2s_{mj}^{(2)}) - 2l_{mj}(1 - 2s_{mj}^{(2)}) \right) = \\
&= (d_1 - 2l_{ij})(1 - 2d_{ij}^{(2)}) + \sum_{m \in \Omega_i} (d_1 - 2l_{mj})(1 - 2s_{mj}^{(2)}) = \\
&= \Delta_{ij}(1 - 2d_{ij}^{(2)}) + \sum_{m \in \Omega_i} \Delta_{mj}(1 - 2s_{mj}^{(2)}). \tag{8}
\end{aligned}$$

Здесь снова используется обозначение $\Delta_{ij} = d_1 - 2l_{ij}$.

Для того, чтобы метрика при декодировании уменьшалась, необходимо, чтобы

$$W_1 - W_0 = \Delta_{ij}(1 - 2d_{ij}^{(2)}) + \sum_{m \in \Omega_i} \Delta_{mj}(1 - 2s_{mj}^{(2)}) < 0. \tag{9}$$

Или

$$\Delta_{ij}(2d_{ij}^{(2)} - 1) + \sum_{m \in \Omega_i} \Delta_{mj}(2s_{mj}^{(2)} - 1) > 0. \tag{10}$$

Данное выражение совпадает с выражением о принятии решения об инвертировании декодируемого символа для МПД на второй и последующих итерациях декодирования при надежности символов Δ_{ij} . Таким образом, даже при нескольких итерациях декодирования МПД внешнего кода при изменении информационного символа расстояние между кодовым словом-решением декодера и принятым сообщением уменьшается и, следовательно, происходит переход к более правдоподобному решению.

Теорема доказана.

Отметим, что в данном случае, как и в случае некаскадного МПД, для того, чтобы декодер внешнего кода был способен достигнуть решения оптимального декодера следует выбирать коды, в наименьшей степени подверженные эффекту размножения ошибок, анализ которого был проведен в [ЗВВ] и кратко изложен в данной работе.

Обобщение на мягкие решения (канал с АБГШ)

Рассмотрим особенности работы предложенной каскадной схемы коррекции ошибок в случае использования канала с АБГШ и двоичной фазовой модуляции. Сначала математически опишем процесс модуляции, передачи по каналу и демодуляции.

Пусть необходимо передать по каналу кодовое слово $\mathbf{C}^{(0)}$ ($c_i^{(0)} \in \{0,1\}$). Для этого сначала выполняется двоичная ФМ сигнала. В матричном виде данное преобразование записывается в виде:

$$\mathbf{Y}^{(0)} = 2\mathbf{C}^{(0)} - 1.$$

В результате получается вектор передаваемых сигналов $\mathbf{Y}^{(0)}$ ($y_i^{(0)} \in \{-1, +1\}$).

Затем данный вектор искажается в канале под действием АБГШ, в результате чего принимается вектор \mathbf{R} :

$$\mathbf{R} = \mathbf{Y}^{(0)} + \mathbf{N}.$$

Здесь \mathbf{N} – вектор независимых нормально распределенных случайных величин с нулевым математическим ожиданием и дисперсией σ^2 , зависящей от отношения сигнал/шум.

Далее на основании принятого сообщения демодулятор выносит решения относительно каждого из принятых битов:

$$b_i = \begin{cases} 0, & \text{если } r_i < 0 \\ 1, & \text{в противном случае} \end{cases}.$$

При этом каждому значению b_i соответствует вес $w_i = |r_i|$, характеризующий надежность вынесенного решения.

Запишем выражение для расстояния между принятым сообщением и произвольным кодовым словом \mathbf{C} , результат модуляции которого равен $\mathbf{Y} = 2\mathbf{C} - 1$. Отметим, что при этом используется не расстояние Хэмминга, как для ДСК, а Евклидово расстояние. При данных обозначениях квадрат Евклидова расстояния равен

$$D^2 = \|\mathbf{Y} - \mathbf{R}\|^2 = \sum_{i=0}^{N-1} (y_i - r_i)^2. \quad (11)$$

Здесь N – длина кода. При декодировании необходимо найти такое кодовое слово $\mathbf{C}^{(*)}$, для которого расстояние D^2 до принятого сообщения будет минимально.

Выполним преобразование данного выражения

$$\begin{aligned} D^2 &= \sum_{i=0}^{N-1} (y_i - r_i)^2 = \sum_{i=0}^{N-1} (y_i^2 - 2y_i r_i + r_i^2) = \\ &= \sum_{i=0}^{N-1} y_i^2 + \sum_{i=0}^{N-1} r_i^2 - 2 \sum_{i=0}^{N-1} r_i y_i = P - 2 \sum_{i=0}^{N-1} r_i y_i \end{aligned} \quad (12)$$

Здесь $P = \sum_{i=0}^{N-1} y_i^2 + \sum_{i=0}^{N-1} r_i^2$ – константа, не зависящая от кодового слова \mathbf{C} .

Таким образом, минимизация выражения (11) эквивалентна максимизации выражения

$$M = \sum_{i=0}^{N-1} r_i y_i \quad (13)$$

по всем возможным кодовым словам \mathbf{C} .

Из анализа выражения (13) видно, что M увеличивается, если знаки r_i и y_i совпадают (другими словами, если $c_i = b_i$) и уменьшается в противном случае. Тогда выражение (13) можно переписать в виде

$$M = \sum_{i=0}^{N-1} (1 - 2p_i)w_i = - \sum_{i=0}^{N-1} (2p_i - 1)w_i, \quad (14)$$

где $p_i = b_i \oplus c_i$, w_i – надежность решения b_i .

Следовательно, решением декодера должно являться кодовое слово, которое минимизирует выражение

$$W = \sum_{i=0}^{N-1} (2p_i - 1)w_i. \quad (15)$$

В дальнейшем величину W будем называть метрикой кодового слова. Отметим, что данная величина оказывается пропорциональной Евклидовому расстоянию между кодовым словом и принятым сообщением.

Сформулируем и докажем теорему, характеризующую работу МПД внешнего кода

предложенной каскадной схемы в данных условиях.

Теорема 3. Для канала с АБГШ и двоичной ФМ при каждом изменении декодируемых символов на произвольной итерации многопорогового декодера внешнего кода происходит переход к более правдоподобию решению всего каскадного кода в целом по сравнению с предыдущим решением декодера.

Доказательство.

Пусть в данных условиях МПД выполнил декодирование внутреннего кода в соответствии с обычным алгоритмом работы. После декодирования МПД внутреннего кода запомнил суммы на ПЭ после последней итерации для всех информационных символов:

$$l_{ij} = \sum_{k \in \Theta_i} (2s_{ik}^{(1)} - 1)w_{ik} + (2d_{ij} - 1)w_{ij}. \quad (16)$$

Запишем выражение для метрики кодового слова полного каскадного кода до изменения символа u_{ij} с помощью МПД внешнего кода, выделив части, связанные с декодируемым символом и не связанные с ним. По аналогии с ДСК имеем:

$$\begin{aligned} W_0 &= X + (1 - 2d_{ij}^{(2)}) \left[(2d_{ij}^{(1)} - 1)w_{ij} + \sum_{k \in \Theta_j} (2s_{ik}^{(1)} - 1)w_{ik} \right] + \\ &+ \sum_{m \in \Omega_i} \left((1 - 2s_{mj}^{(2)}) \left[(2d_{mj}^{(1)} - 1)w_{mj} + \sum_{k \in \Theta_j} (2s_{mk}^{(1)} - 1)w_{mk} \right] \right) = \\ &= X + (1 - 2d_{ij}^{(2)})l_{ij} + \sum_{m \in \Omega_i} (1 - 2s_{mj}^{(2)})l_{mj}. \end{aligned} \quad (17)$$

В данном выражении в слагаемом $(1 - 2d_{ij}^{(2)}) \left[(2d_{ij}^{(1)} - 1)w_{ij} + \sum_{k \in \Theta_j} (2s_{ik}^{(1)} - 1)w_{ik} \right]$

сомножитель $(1 - 2d_{ij}^{(2)})$ показывает, что если МПД внешнего кода ранее не изменял информационным символ u_{ij} (т.е. $d_{ij}^{(2)} = 0$), то для него сумма на ПЭ не изменяется.

Если же МПД внешнего кода на предшествующих итерациях декодирования изменил символ u_{ij} (т.е. $d_{ij}^{(2)} = 1$), то следует инвертировать сумму на ПЭ.

После изменения символа u_{ij} все суммы l_{ij} на ПЭ изменят знак, и вес станет равным

$$W_1 = X - (1 - 2d_{ij}^{(2)})l_{ij} - \sum_{m \in \Omega_i} (1 - 2s_{mj}^{(2)})l_{mj}. \quad (18)$$

Следовательно, общее изменение метрики при инвертировании символа u_{ij} равно

$$\begin{aligned} W_1 - W_0 &= X - (1 - 2d_{ij}^{(2)})l_{ij} - \sum_{m \in \Omega_i} (1 - 2s_{mj}^{(2)})l_{mj} - \\ &- \left(X + (2d_{ij}^{(2)} - 1)l_{ij} + \sum_{m \in \Omega_i} (1 - 2s_{mj}^{(2)})l_{mj} \right) = \\ &= -2l_{ij}(1 - 2d_{ij}^{(2)}) - 2 \sum_{m \in \Omega_i} (1 - 2s_{mj}^{(2)})l_{mj}. \end{aligned} \quad (19)$$

Данная метрика уменьшается, если

$$W_1 - W_0 < 0$$

или

$$(1 - 2d_{ij}^{(2)})l_{ij} - \sum_{m \in \Omega_i} (2s_{mj}^{(2)} - 1)l_{mj} > 0. \quad (20)$$

Обозначим $\Delta_{ij} = -l_{ij}$. Тогда выражение (20) примет вид

$$(2d_{ij}^{(2)} - 1)\Delta_{ij} + \sum_{m \in \Omega_i} (2s_{mj}^{(2)} - 1)\Delta_{mj} > 0. \quad (21)$$

Данное выражение совпадает с правилом принятия решения МПД об инвертировании декодируемого символа на произвольной итерации декодирования. При этом вес символов определяется как $\Delta_{ij} = -l_{ij}$. Таким образом, если МПД внешнего кода на произвольной итерации изменит декодируемый символ, то метрика и, соответственно, расстояние между полученным кодовым словом и принятым сообщением станет меньше, и, следовательно, произойдет переход к более правдоподобному решению декодера.

Теорема доказана.

Подобные схемы можно построить и для недвоичных СОК. Для данного варианта каскадирования были сформулированы правила декодирования, при выполнении которых декодер внешнего кода при каждом изменении декодируемых символов будет переходить к кодовому слову всего каскадного кода в целом, находящимся на меньшем расстоянии от принятого сообщения, чем предыдущее решение декодера. Результаты экспериментального исследования данных каскадных схем показали их высокую исправляющую способность при работе вблизи пропускной способности канала.

2. Разработано математическое и программное обеспечение для анализа спектра самоортогональных кодов. Результаты данного анализа позволили построить новые самоортогональные коды, значительно более устойчивые к эффекту размножения ошибок, чем ранее известные.

Спектр кода представляет собой набор значений a_{ij} , определяющих число кодовых слов веса j , информационный вес которых равен i . Знание спектра кода может быть полезным при оценивании характеристик, которые можно получить при оптимальном декодировании данного кода. Для этого может использоваться, например, аддитивная граница вероятности ошибки, которая характеризуется достаточной точностью при малом шуме в канале. В тоже время задача получения спектра для реальных кодов достаточно сложна для решения из-за огромного объема требуемых вычислений, пропорционального 2^K , где K – длина кода. Кроме оценивания параметров кода спектр можно использовать при выборе кодов, в наименьшей степени подверженных размножению ошибок.

В работе решена задача получения начальной части спектра кодов, которая наиболее сильно влияет на характеристики кодов. Для этого была разработана и реализована в программных средствах методика получения спектра кодов, позволяющую за приемлемое время получать спектр кода.

Основная идея предложенной методики заключается в постепенном формировании списка кодовых слов сначала с информационным весом 1, затем с информационным весом 2 и т.д. При этом каждое следующее кодовое слово строится на основании того из ранее построенных, которое имеет минимальный вес при максимальном информационном весе. Полученное кодовое слово сохраняется в том случае, если оно имеет вес, строго меньший nd , где n – число информационных единиц, d – кодовое расстояние кода.

После построения всех возможных кодовых слов из некоторого базового переходят к следующему по весу из ранее построенных кодовых слов. Данный процесс повторяется до тех пор, пока не будет построено заданное число кодовых слов, на основании которых и рассчитывается спектр кода.

Определим влияние спектра кода на эффективность его многопорогового

декодирования. Для этого получим спектры для кодов с различным уровнем размножения ошибок и выполним их анализ.

Для анализа выберем сверточные коды с небольшим кодовым расстоянием $d=5$ и различной длиной. Данные коды заданы в табл. 1 путем перечисления ненулевых коэффициентов порождающих полиномов. Заметим, что полином g_{ij} определяет информационные символы i -й информационной ветви, участвующих в получении j -го проверочного символа.

Таблица 1. Порождающие полиномы самоортогональных кодов

№	R	d	n_A	g
1	1/2	5	14	$g_{1,1}=\{0,1,4,6\}$
2	1/2	5	338	$g_{1,1}=\{0,4,38,168\}$
3	2/4	5	56	$g_{1,1}=\{0,1\}, g_{1,2}=\{0,6\}, g_{2,1}=\{0,4\}, g_{2,2}=\{1,15\}$
4	2/4	5	172	$g_{1,1}=\{0,6\}, g_{1,2}=\{0,15\}, g_{2,1}=\{0,32\}, g_{2,2}=\{7,42\}$
5	4/8	5	788	$g_{1,1}=\{0\}, g_{1,2}=\{0\}, g_{1,3}=\{0\}, g_{1,4}=\{0\}, g_{2,1}=\{0\}, g_{2,2}=\{6\}, g_{2,3}=\{9\}, g_{2,4}=\{10\}, g_{3,1}=\{0\}, g_{3,2}=\{13\}, g_{3,3}=\{27\}, g_{3,4}=\{56\}, g_{4,1}=\{0\}, g_{4,2}=\{21\}, g_{4,3}=\{47\}, g_{4,4}=\{98\}$

Для данных кодов спектр представлен в нижеследующих таблицах. В данных таблицах в заголовке столбцов указан информационный вес кодовых слов n , в заголовках строк – общий вес кодовых слов w , а в остальных ячейках – число кодовых слов с информационным весом n и общим весом w .

Таблица 2. Спектр кода 1 из табл. 1

$w \backslash n$	1	2	3	4	5	6	7
5	1	0	0	0	0	0	0
6	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0
8	0	6	0	4	0	0	0
9	0	0	11	0	7	0	0
10	0	0	0	14	0	4	0
11	0	0	21	0	35	0	3
12	0	0	0	64	0	64	0
13	0	0	0	0	133	0	65
14	0	0	0	77	0	258	0
15	0	0	0	0	235	0	354
16	0	0	0	0	0	382	0
17	0	0	0	0	99	0	545
18	0	0	0	0	0	321	0
19	0	0	0	0	0	0	480
20	0	0	0	0	0	80	0

Таблица 3. Спектр кода 2 из табл. 1

$w \backslash n$	1	2	3	4	5	6	7
5	1	0	0	0	0	0	0
6	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0
8	0	6	0	1	0	0	0
9	0	0	4	0	0	0	0

10	0	0	0	0	0	0	0
11	0	0	42	0	12	0	0
12	0	0	0	63	0	0	0
13	0	0	0	0	36	0	0
14	0	0	0	296	0	133	0
15	0	0	0	0	629	0	61
16	0	0	0	0	0	583	0
17	0	0	0	0	2166	0	1359
18	0	0	0	0	0	5963	0
19	0	0	0	0	0	0	7657
20	0	0	0	0	0	15680	0

Таблица 4. Спектр кода 3 из табл. 1

$n \backslash w$	1	2	3	4	5	6	7
5	2	0	0	0	0	0	0
6	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0
8	0	12	0	0	0	0	0
9	0	0	3	0	0	0	0
10	0	0	0	0	0	0	0
11	0	0	99	0	0	0	0
12	0	0	0	74	0	1	0
13	0	0	0	0	41	0	1
14	0	0	0	904	0	34	0
15	0	0	0	0	1212	0	56
16	0	0	0	0	0	1250	0
17	0	0	0	0	8467	0	1456
18	0	0	0	0	0	16632	0
19	0	0	0	0	0	0	24137
20	0	0	0	0	0	81939	0

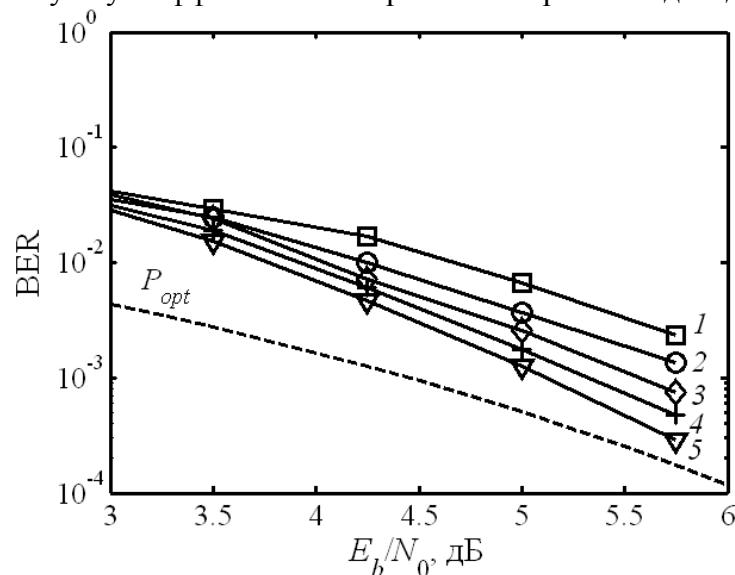
Таблица 5. Спектр кода 4 из табл. 1

$n \backslash w$	1	2	3	4	5	6	7
5	2	0	0	0	0	0	0
6	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0
8	0	12	0	0	0	0	0
9	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0
11	0	0	108	0	0	0	0
12	0	0	0	4	0	0	0
13	0	0	0	0	0	0	0
14	0	0	0	1152	0	0	0
15	0	0	0	0	149	0	0
16	0	0	0	0	0	24	0
17	0	0	0	0	13140	0	1
18	0	0	0	0	0	3452	0
19	0	0	0	0	0	0	1043
20	0	0	0	0	0	160771	0

Таблица 6. Спектр кода 5 из табл. 1

$w \backslash n$	1	2	3	4	5	6	7
5	4	0	0	0	0	0	0
6	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0
8	0	24	0	0	0	0	0
9	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0
11	0	0	216	0	0	0	0
12	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0
14	0	0	0	2376	0	0	0
15	0	0	0	0	31	0	0
16	0	0	0	0	0	0	0
17	0	0	0	0	29329	0	0
18	0	0	0	0	0	1194	0
19	0	0	0	0	0	0	24
20	0	0	0	0	0	464713	0

Характеристики этих же кодов в ДСК показаны на рис. 5 кривыми 1, 2, 3, 4 и 5. Отметим, что для кодов, имеющих более разреженный спектр, характеристики оказываются лучше. Таким образом, при построении кодов следует выбирать такие коды, для которых число кодовых слов с информационным весом n и полным весом $w < nd - 2(n - 1)$ является минимально возможным. Такие коды позволяют обеспечить наилучшую эффективность при многопороговом декодировании.

Рис. 5. Эффективность МПД для кодов с $d=5$ в ДСК

3. Создана методика получения мягких решений многопорогового декодера, отражающих надежность декодированных битов. Данную информацию можно использовать декодерами внешних кодов для улучшения эффективности их работы.

Многопороговый декодер самоортогональных кодов может декодировать как принятое сообщение, представляющее собой как жесткие решения демодулятора (когда демодулятор оценивает только значение принятых битов), так и мягкие решения (когда демодулятор дополнительно оценивает надежность своего

решения). При этом использование мягких решений позволяет повысить выигрыш от применения кодирования примерно на 1,5 дБ. Результатом работы классического МПД являются оценка жестких решений для декодированных битов. В тоже время при использовании МПД в составе сложных кодовых конструкций, например, в составе каскадных кодов, для повышения общей эффективности схемы декодирования целесообразно формировать для декодера внешнего кода и надежность этих решений. При доказательстве вышеописанных теорем были рассмотрены разные варианты формирования мягких решений. Наиболее общим вариантом является подход, при котором надежность решения МПД относительно i -го информационного символа оценивается в соответствии с выражением

$$\Delta_i = -l_i,$$

где l_i – сумма на пороговом элементе, определяемая следующим образом:

$$l_i = \sum_{k \in \Theta_i} (2s_k - 1)w_k + (2d_i - 1)w_i.$$

Здесь Θ_i представляет множество номеров проверок (элементов синдромного регистра), участвующих при декодировании i -го информационного символа; s_k – элемент синдромного регистра; d_i – элемент разностного регистра, w_i – канальная надежность i -го символа (для ДСК $w_i = 1$).

Отметим, что именно этот подход использовался при получении результатов для каскадных кодов, предложенных в работе.

Далее рассмотрим, как меняются мягкие решения, сформированные таким образом, на различных итерациях многопорогового декодирования.

Пусть задан код с кодовой скоростью $1/2$, кодовым расстоянием 9 и канал типа ДСК с отношением сигнал/шум 4 дБ. Также пусть по каналу передается только нулевая последовательность. Для данных условий гистограмма мягких решений до первой итерации декодирования (суммы на ПЭ до декодирования) представлена на рис. 6. Здесь по оси ОХ – представлено значение мягкого решения, а по оси ОУ – частота появления такого значения.

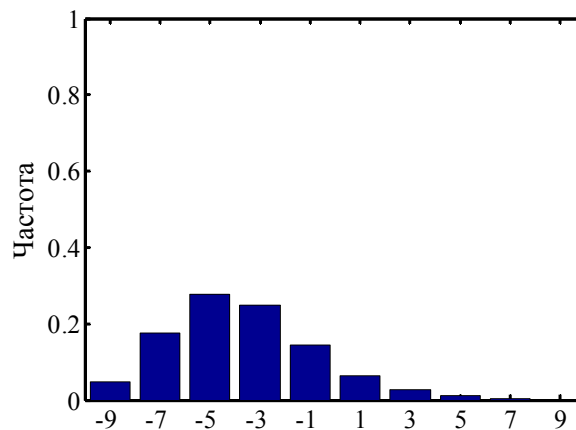


Рис. 6. Гистограмма мягких решений перед декодированием

Гистограмма мягких решений после первой итерации декодирования представлена на рис. 7. Заметно, что надежность решений декодера несколько возросла и доля ошибочных значений стала меньше.

Гистограмма мягких решений после второй итерации декодирования представлена на рис. 8. Надежность решений декодера еще более увеличивается.

В дальнейшем с ростом числа итераций декодирования надежность решений еще более возрастает, а доля ошибочных битов при этом существенно уменьшается. После финальной итерации декодирования (в данном случае было использовано 10 итераций) гистограмма мягких решений имеет вид, показанный на рис. 9.

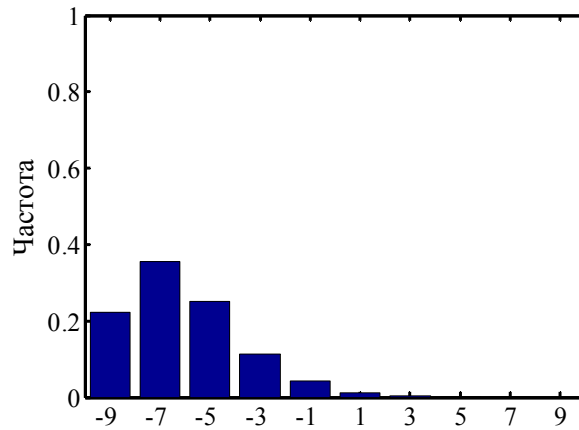


Рис. 7. Гистограмма мягких решений после первой итерации декодирования

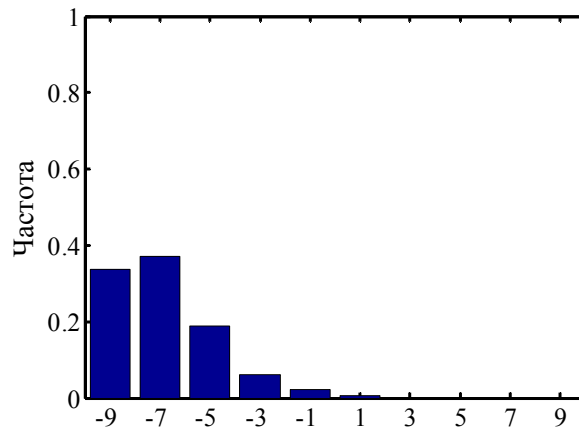


Рис. 8. Гистограмма мягких решений после второй итерации

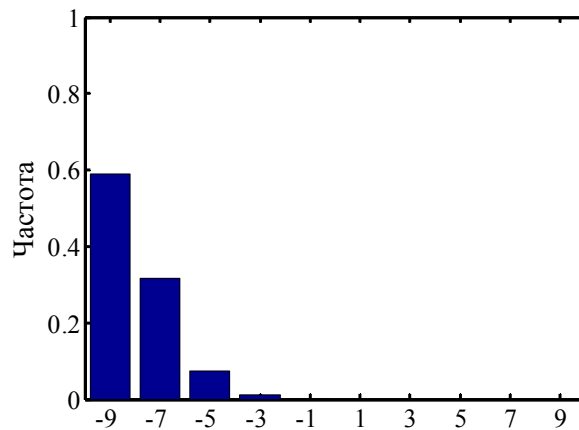


Рис. 9. Гистограмма мягких решений после десятой итерации

Отметим, что в результате выполнения ряда итераций декодирования мягкие решения относительно декодированных битов улучшаются. Другими словами при этом увеличивается уверенность многопорогового декодера в правильности декодирования.

Аналогичным образом изменяются мягкие решения и при работе МПД в канале с гауссовским шумом и двоичной ФМ. Для данных условий гистограмма частот мягких решений до декодирования представлена на рис. 10, а после десятой итерации декодирования – на рис. 11. И в этом случае надежность решений МПД с ростом числа выполняемых итераций увеличивается.

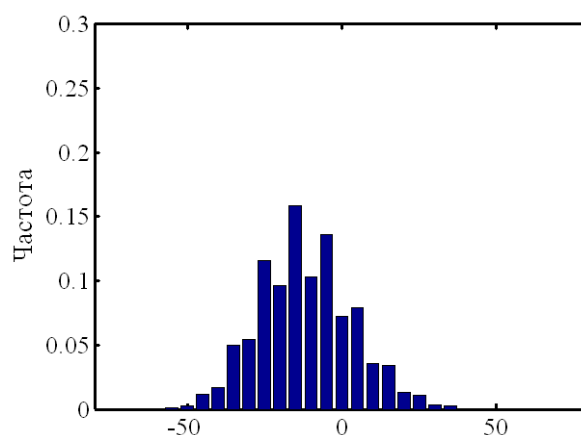


Рис. 10. Гистограмма мягких решений перед декодированием

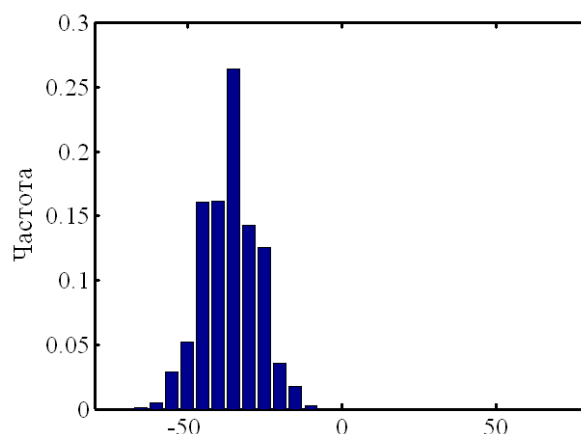


Рис. 11. Гистограмма мягких решений после десятой итерации

4. Решена задача адаптации методов декодирования низкоплотностных кодов для декодирования самоортогональных кодов. Результаты исследования показали, что применение данных методов позволяет получить дополнительный энергетический выигрыш кодирования порядка 0,5..1 дБ при четырехкратном росте сложности реализации.

В настоящее время зарубежными и отечественными специалистами активно развиваются чрезвычайно эффективные алгоритмы декодирования низкоплотностных (Low-Density Parity-Check – LDPC) кодов, обладающие при этом не очень высокой сложностью как программной, так и аппаратной реализации. Некоторые сведения про данные коды были изложены в первой главе диссертации. Рассмотрим LDPC коды и методы их декодирования немного более подробно.

LDPC коды представляют собой линейные блочные (N, K) коды, задаваемые с помощью проверочной матрицы H , характеризуемой относительно малым числом единиц в строках и столбцах (рис. 12а). В результате для длинных кодов плотность единиц в проверочной матрице оказывается очень малой. Проверочной матрице кода ставится в соответствие граф Таннера, в котором для представления строк и столбцов проверочной матрицы используются определенным образом связанные между собой битовые и проверочные узлы. Битовые узлы соответствуют кодовым битам, а проверочные – проверкам, в которых эти кодовые биты участвуют. Например, для кода с матрицей H с рис. 12а граф Таннера представлен на рис. 12б. Степенью узла называется число входящих в него ветвей. Например, для графа Таннера с рис. 12б степень битовых узлов равна 3 (число единиц в столбцах проверочной матрицы), а степень проверочных – 6 (число единиц в строках проверочной матрицы). Если степени всех узлов одного типа одинаковы, то LDPC коды называются регулярными, иначе – нерегулярными.

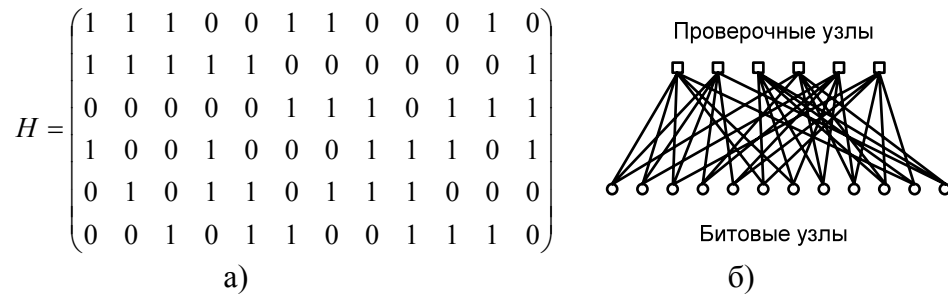


Рис. 12. Проверочная матрица и граф Таннера регулярного LDPC кода

Для декодирования LDPC кодов обычно используются разновидности message passing алгоритма, работающего с графом Таннера кода. В основе работы данного метода лежит итеративный обмен сообщениями между битовыми (нижними на рис. 12б) и проверочными (верхними на рис. 12б) узлами графа кода. При правильном выборе кода (проверочной матрицы) удастся получить близкие к оптимальным результаты.

Сообщения, посылаемые i -м битовым узлом к j -му проверочному, определяются как сумма всех сообщений, поступивших от других проверочных узлов, и канального решения для кодового бита:

$$q_{i,j} = L_i + \sum_{k \in C_i, k \neq j} r_{k,i}. \quad (22)$$

Здесь $q_{i,j}$ – сообщение от i -го битового к j -му проверочному узлу; L_i – мягкое решение демодулятора относительно всех канальных битов; C_i – множество номеров проверочных узлов, связанное с i -м битовым узлом; $r_{k,i}$ – сообщение от k -го проверочного к i -му битовому узлу (эти сообщения на первой итерации декодирования инициализируются нулями).

Сообщения, посылаемые j -м проверочным узлом к i -му битовому, определяются как:

$$r_{j,i} = 2 \tanh^{-1} \left(\prod_{k \in R_j, k \neq i} \tanh \frac{q_{k,j}}{2} \right). \quad (23)$$

Здесь R_j – множество номеров битовых узлов, связанное с j -м проверочным узлом; $\tanh(x)$ – гиперболический тангенс.

Процесс обмена сообщениями между битовыми и проверочными узлами повторяется многократно, несколько десятков или даже сотен раз. После этого результатом работы декодера будут мягкие решения, определяемые в соответствии с выражением

$$b_i = L_i + \sum_{k \in C_i} r_{k,i}. \quad (24)$$

Знак решений будет определять значение декодируемого бита, а модель надежность решения. Алгоритмы декодирования, реализующие подобный подход, называются message-passing (MP) декодерами.

Отметим, что формирование сообщений от битовых узлов к проверочным является достаточно простой задачей, поскольку для этого используются только операции сложения. Этого нельзя сказать о формировании сообщений от проверочных узлов к битовым, так как при этом используются достаточно сложные для вычисления функции определения гиперболического тангенса и обратной от нее, а также операции умножения. В результате вместо данного алгоритма на практике используется его модификации, имеющие существенно меньшую вычислительную сложность за счет незначительно худшей корректирующей способности. Одним из таких алгоритмов является min-sum алгоритм, в котором для вычисления сообщений от проверочных узлов к битовым используется выражение

$$r_{j,i} = \prod_{k \in R_j, k \neq i} \text{sign}(q_{k,j}) \cdot \min_{k \in R_j, k \neq i} (|q_{k,j}|). \quad (25)$$

В ряде публикаций показано, что проигрыш от применения подобного упрощения составляет порядка 0,5 дБ. Однако наряду с меньшей сложностью реализации данный алгоритм не чувствителен к неточности информации о состоянии канала. Это дополнительно существенно снижает сложность приемника.

Заметим, что min-sum алгоритм может подойти и для декодирования самоортогональных кодов, проверочная матрица для которых также является разреженной. Например, проверочная матрица для блочного СОК, заданного образующим полиномом $g(x) = 1 + x + x^4 + x^6$, имеет вид

$$\mathbf{H} = \begin{bmatrix} 1100101000 & 0001000000 & 000000 \\ 0110010100 & 0000100000 & 000000 \\ 0011001010 & 0000010000 & 000000 \\ 0001100101 & 0000001000 & 000000 \\ 0000110010 & 1000000100 & 000000 \\ 0000011001 & 0100000010 & 000000 \\ 0000001100 & 1010000001 & 000000 \\ 1000000110 & 0100000000 & 100000 \\ 0100000011 & 0010000000 & 010000 \\ 1010000001 & 1000000000 & 001000 \\ 0101000000 & 1100000000 & 000100 \\ 0010100000 & 0110000000 & 000010 \\ 1001010000 & 0010000000 & 000001 \end{bmatrix} = [\mathbf{P} : \mathbf{I}]. \quad (26)$$

Для таких кодов число единиц в строках и столбцах подматрицы \mathbf{P} равно $d-1$ (d – кодовое расстояние), а число единиц в строках и столбцах подматрицы \mathbf{I} равно 1. По сравнению с существующими LDPC кодами при одинаковых параметрах СОК будут обладать существенно меньшей сложностью кодирования, что немаловажно для многих систем.

Граф Таннера для рассмотренного СОК представлен на рис. 13. Отметим, что в данном графе отсутствуют циклы длиной 4, существенно ухудшающие эффективность МР декодеров, и минимальная длина цикла равна 6. Один из циклов минимальной длины выделен на рисунке жирными линиями. Всего в графе 54 разных цикла длиной 6, начинающихся с нулевого информационного символа.

Эффективность min-sum декодирования СОК

Представим результаты экспериментального исследования эффективности min-sum алгоритма декодирования самоортогональных кодов. На рис. 14 представлены графики зависимости вероятности ошибки декодирования от отношения сигнал/шум в ДСК для различных самоортогональных кодов. При декодировании использовалось до 20 итераций min-sum алгоритма декодирования. Кривая 1 соответствует блочному СОК с $R=1/2$ и $d=5$, заданного полиномом $g(x) = 1 + x + x^4 + x^6$. Для сравнения кривой 2 показаны результаты многопорогового декодирования того же кода. Кривая $P_{opt,h}$ соответствует вероятности ошибки оптимального декодера для данного СОК в ДСК.

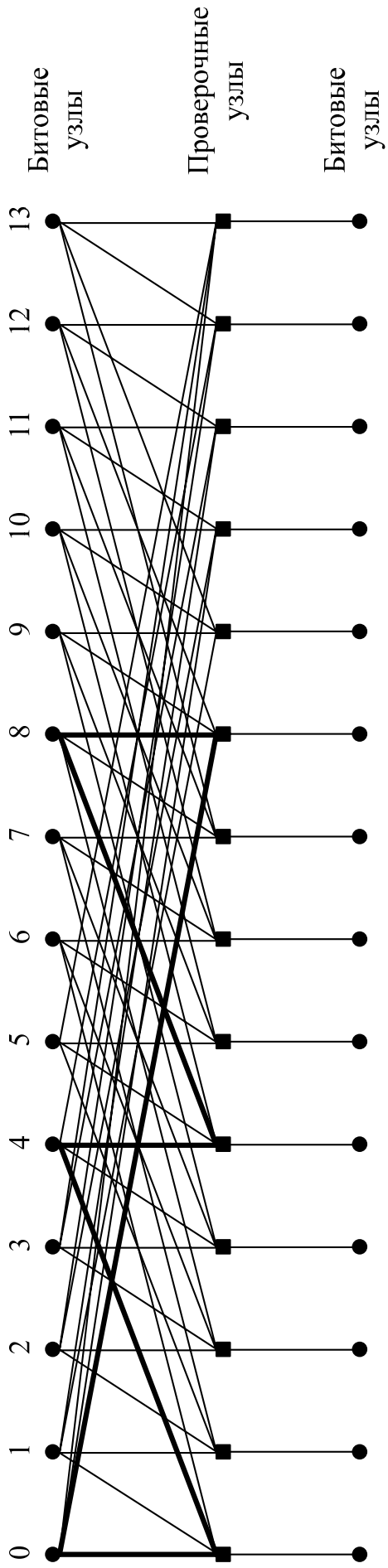


Рис. 13. Проверочная матрица и граф Таннера регулярного LDPC кода

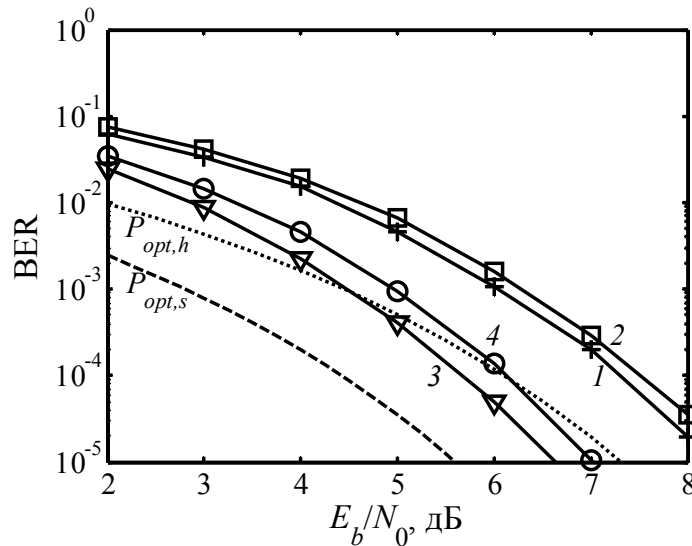


Рис. 14. Результаты моделирования min-sum декодера СОК с $d=5$

Из рисунка следует, что результаты, показываемые min-sum алгоритмом декодирования, оказываются несколько (примерно на 0,2 дБ) лучше результатов, показываемых МПД. Характеристики тех же алгоритмов для канала с АБГШ показаны на рис. 14 кривыми 3 и 4. Здесь улучшение от применения min-sum алгоритма декодирования по сравнению с МПД оказывается около 0,5 дБ. Отметим, что в данном случае оба алгоритма коррекции ошибок для такого короткого кода не способны обеспечить близкое к оптимальному декодирование. Также заметим, что переход к мягким решениям демодулятора в данном случае дает выигрыш в 1,5 дБ по сравнению с жесткими решениями.

Рассмотрим эффективность min-sum алгоритма декодирования для более длинных СОК с кодовым расстоянием $d=9$. Характеристики min-sum декодера в ДСК для данных СОК показаны на рис. 15. Кривая 1 соответствует коду с $R=1/2$ и $n=1350$, кривая 2 – коду с $R=2/4$ и $n=1188$, кривая 3 – коду с $R=2/4$ и $n=7604$, кривая 4 – коду с $R=4/8$ и $n=9704$. При получении данных графиков выполнялось не более 50 итераций декодирования. Из сравнения данных графиков с известными характеристиками МПД для этих же кодов следует, что min-sum алгоритм оказывается лучше МПД примерно на 0,5 дБ.

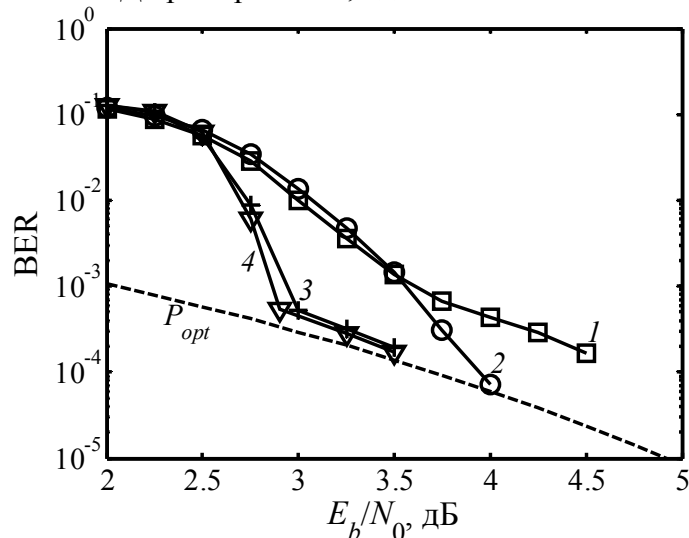


Рис. 15. Результаты моделирования min-sum декодера СОК с $d=9$ в ДСК

Результаты моделирования min-sum декодера этих же кодов в канале с АБГШ представлены соответствующими кривыми на рис. 16. В данном случае область

эффективной работы min-sum декодера, в которой он почти оптимально декодирует используемые коды, находится ближе к пропускной способности канала по сравнению с МПД примерно на 1 дБ и располагается всего в 1,3 дБ от пропускной способности канала. Хотя обеспечиваемая при этом вероятность ошибки декодирования из-за небольшого кодового расстояния используемых кодов оказывается достаточно большой (10^{-3} и ниже) даже для оптимального, т.е. наилучшего, декодера.

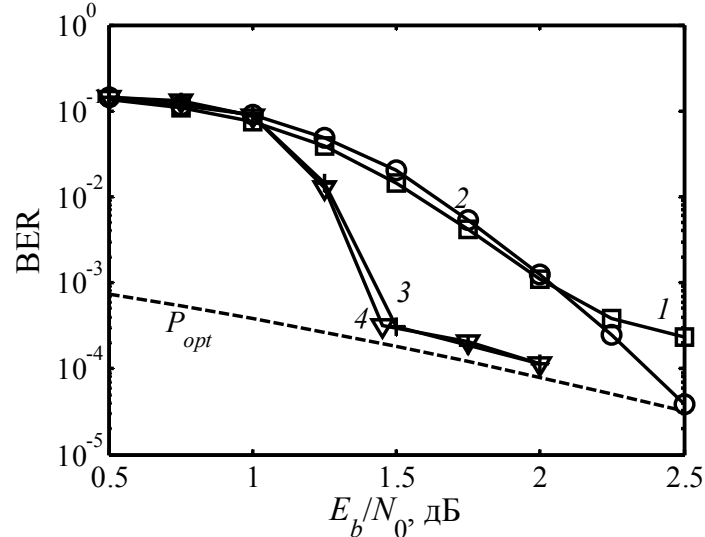


Рис. 16. Результаты моделирования min-sum декодера СОК с $d=9$ в канале с АБГШ

При анализе длин циклов графов Таннера используемых кодов оказывается, что код с $R=1/2$ имеет 204 цикла длины 6, начинающихся в нулевом битовом узле, 4255 циклов длины 8, 139089 циклов длины 10. Число циклов различной длины, начинающихся в нулевом символе, для остальных кодов представлено в таблице 7. Таким образом, более длинные коды с переменными связями, более устойчивые к размножению ошибок при многопороговом декодировании, имеют меньшее число коротких циклов, оказывающих наибольшее влияние на эффективность min-sum алгоритма декодирования. Поэтому использование кодов с переменными связями большей длины, как и в случае с МПД, позволяют существенно увеличить эффективность min-sum декодирования.

Таблица 7. Число циклов различной длины для некоторых СОК

Код	Длина цикла			
	6	8	10	12
$R=1/2, d=9, n=1350$	204	4255	139089	1310707
$R=2/4, d=9, n=1188$	104	5318	135548	136798
$R=2/4, d=9, n=7604$	28	965	40273	904535
$R=4/8, d=9, n=9704$	0	815	36065	833902

Далее рассмотрим эффективность min-sum декодирования СОК с различным кодовым расстоянием. Для этого выберем достаточно длинные коды, обладающие большей устойчивостью к размножению ошибок. Результаты моделирования min-sum декодера данных кодов в ДСК представлены на рис. 17. Здесь кривыми 1, 2, 3, 4 и 5 показаны характеристики кодов с $d=7, 9, 11, 13$ и 17. Аналогичные результаты для канала с АБГШ показаны на рис. 18. На данных рисунках пунктирными кривыми показана эффективность оптимального декодера для используемых кодов. Отметим, что коды с большим кодовым расстоянием, как и в случае с МПД, обладают лучшей корректирующей способностью в данных типах канала. Однако

декодирование, для кодов с меньшим кодовым расстоянием лежит ближе к пропускной способности канала. Это объясняется тем, что проверочные узлы для кодов с большим d имеют большую размерность, что несколько ухудшает качество сообщений, поступающих от них к битовым узлам.

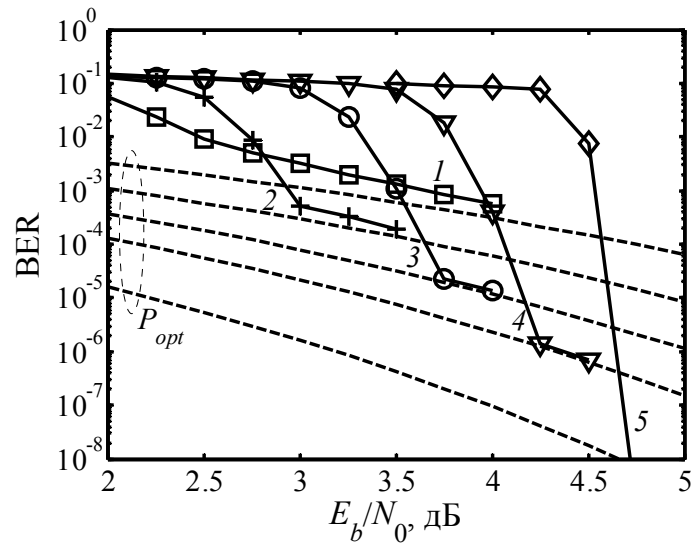


Рис. 17. Результаты моделирования min-sum декодера СОК с различным d и $R=1/2$ в ДСК

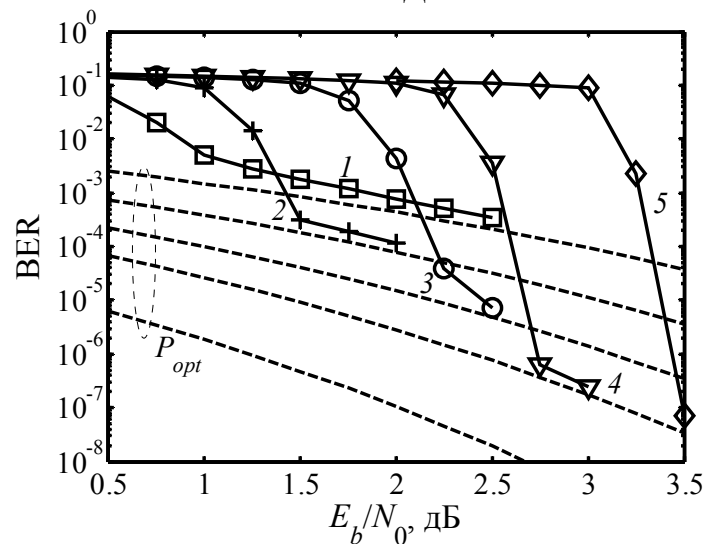


Рис. 18. Результаты моделирования min-sum декодера СОК с различным d и $R=1/2$ в канале с АБГШ

Эффективность min-sum декодера для кодов с различной кодовой скоростью представлена на рис. 19 для ДСК и рис. 20 для канала с АБГШ. Здесь использовались коды с $R=1/3$ и $d=13$, $R=1/2$ и $d=9$ и $R=2/3$ и $d=7$. Отметим, что вероятности оптимального декодирования данных кодов примерно одинаковы. Из анализа графиков следует, что наилучшей энергетической эффективностью обладают коды с кодовой скоростью $1/2$. Коды с кодовой скоростью $2/3$ обеспечивают несколько лучшую спектральную эффективность, однако уступают по энергетике порядка $0,5$ дБ. А коды с малым R , проигрывают по обоим параметрам.

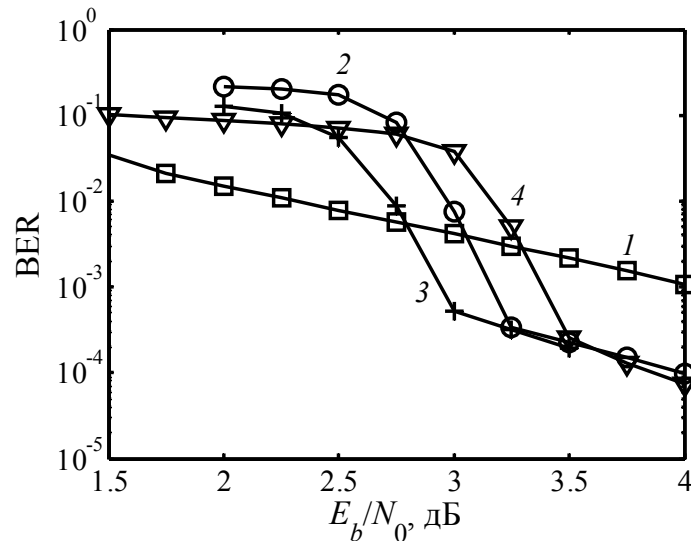


Рис. 19. Результаты моделирования min-sum декодера СОК с различным R в ДСК

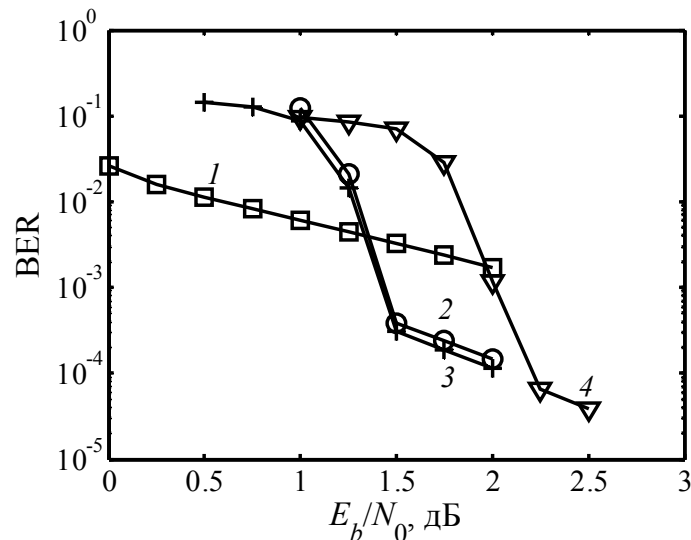


Рис. 20. Результаты моделирования min-sum декодера СОК с различным R в канале с АБГШ

Из представленных результатов можно сделать вывод о том, что min-sum декодер для различных самоортогональных кодов ведет себя так же, как и МПД. В результате можно предположить, что подходы к улучшению эффективности МПД, такие как использование кодов, наиболее устойчивых к размножению ошибок, применение параллельного каскадирования, кодов с выделенными ветвями, каскадирование с простейшими внешними кодами и др., позволят получить большой энергетический выигрыш для min-sum алгоритма декодирования самоортогональных кодов.

Рассмотрим получаемые характеристики при использовании min-sum алгоритма для декодирования кодов с параллельным каскадированием. На рис. 21 представлены характеристики ряда кодов в ДСК. Здесь кривая 1 соответствует обычному СОК с $R=1/2$, $d=9$, кривая 2 – СОК с параллельным каскадированием с такими же параметрами. В данном случае параллельное каскадирование позволило обеспечить дополнительный выигрыш всего порядка 0,3 дБ. При использовании кодов с большим кодовым расстоянием выигрыш от параллельного каскадирования оказывается значительно больше. Например, на данном рисунке кривой 3 представлены характеристики обычного СОК с $R=1/2$, $d=13$, а кривой 4 –

характеристики СОК с параллельным каскадированием с $R=1/2$, $d=13$. Дополнительный ЭВК в данном случае составляет порядка 1,2 дБ. Для $d=17$ характеристики обычного СОК и СОК с параллельным каскадированием представлены кривыми 5 и 6 соответственно. Здесь выигрыш от перехода к параллельному каскадированию составил уже около 1,3 дБ. Также отметим, что за счет оптимизации структуры кода с параллельным каскадированием с помощью разработанных программных средств возможно еще незначительное улучшение эффективности, что иллюстрируется кривой 7 на данном рисунке.

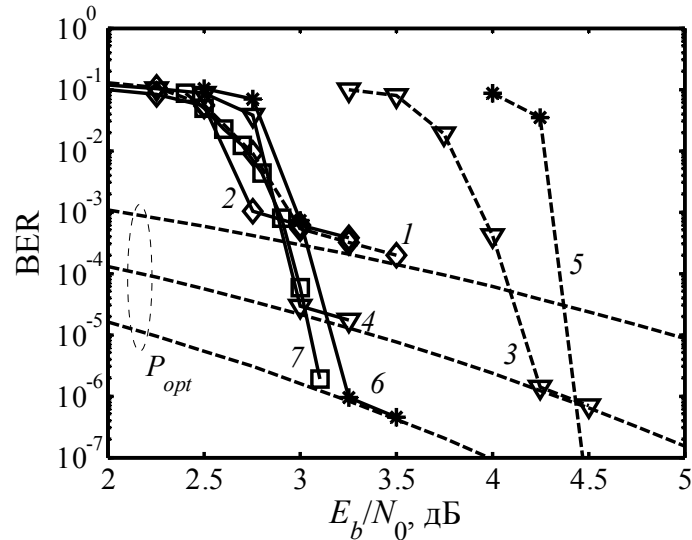


Рис. 21. Результаты моделирования min-sum декодера СОК с параллельным каскадированием в ДСК

На следующем рис. 22 соответствующими кривыми представлены характеристики тех же кодов, что и на рис. 21, в канале с АБГШ при использовании двоичной ФМ. Отметим, что в данном случае эффект от применения параллельного каскадирования оказывается таким же, как и для ДСК. В удалось обеспечить эффективную работу декодера СОК при уровне шума, всего на 1 дБ превышающем пропускную способность канала.

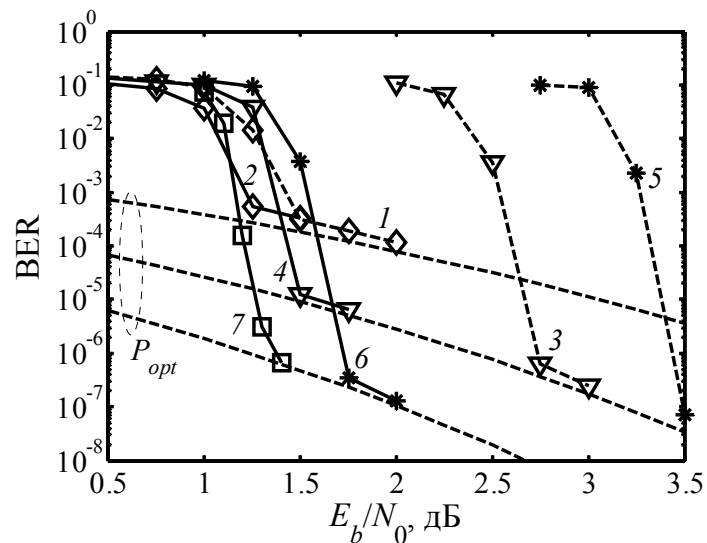


Рис. 22. Результаты моделирования min-sum декодера СОК с параллельным каскадированием в канале с АБГШ

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 проблемами.

За время выполнения проекта также был разработан дополнительный веб-сайт www.mtdbest.ru, на котором представлена разнообразная 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 2010 году получены новые научные результаты по разработке методов анализа устойчивости самоортогональных кодов к размножению ошибок. Для данного анализа были разработаны новые программные средства построения спектра самоортогональных и других кодов. Результаты данного анализа позволили построить ранее неизвестные самоортогональные коды, применение которых обеспечивает лучшую эффективность работы МПД при близком к предельном уровне шума в канале связи.

Научной новизной обладают новые разработанные каскадные схемы коррекции ошибок, основанные на многопороговом декодере. Применение предложенных каскадных кодов и методов их декодирования позволяет уменьшить вероятность ошибки декодирования на 3..5 десятичных порядков и более даже по сравнению с уже изначально очень эффективным двоичным и недвоичным МПД!

Для декодирования самоортогональных кодов впервые были адаптированы методы декодирования низкоплотностных кодов. Результаты исследования показали, что применение данных методов позволяет получить дополнительный энергетический выигрыш кодирования порядка 0,5..1 дБ при четырехкратном росте сложности реализации.

Разработана новая методика получения мягких решений двоичных МПД, содержащих информацию о надежности декодированных битов. Данную информацию можно использовать декодерами внешних кодов для улучшения эффективности их работы.

3.8. *Сопоставление полученных результатов с мировым уровнем*

1. Эффективность декодеров двоичных кодов

В настоящее время для обмена информацией широко используются различные системы цифровой связи. Подобные системы используют для передачи данных как проводные, так и беспроводные каналы связи, в которых под действием различного рода помех передаваемая информация может исказиться. Это является недопустимым для многих приложений. Поэтому в любой системе передачи цифровых данных применяются средства помехоустойчивого кодирования, использование которых позволяет снизить долю необнаруженных ошибок до приемлемой. Подобные проблемы возникают и в системах хранения данных, в которых для повышения надежности долговременного хранения данных также используют помехоустойчивое кодирование.

На сегодняшний день в теории помехоустойчивого кодирования известно всего несколько методов коррекции ошибок в цифровых данных, обеспечивающих работу вблизи пропускной способности канала. Рассмотрим их эффективность при работе в канале с аддитивным белым гауссовским шумом, двоичной фазовой модуляцией при использовании кодов с кодовой скоростью $1/2$. Отметим, что при таких параметрах канала и кодирования теоретически можно работать при отношении сигнал/шум, равным 0,2 дБ (кривая «С=1/2» на рис.1).

Наиболее широкое практическое применение в реальных системах связи нашли сверточные коды, для декодирования которых часто используется оптимальный алгоритм Витерби (кривая «1) Витерби(K=7)» на рис. 1), и различные каскадные коды, например, каскадные коды, состоящие из кода Рида-Соломона и сверточного кода (кривая «2) РС(204,188,8)+АВ(K=7)» на рис. 1). Характеристики данных методов коррекции ошибок, как следует из представленных графиков, существенно хуже теоретически возможных. В последнее время зарубежными специалистами активно развиваются турбо и низкоплотностные коды, эффективность которых очень высока. Например, методы декодирования турбо кодов, рекомендованных стандартом CDMA2000, обеспечивают характеристики, представленные кривой «3) TCC CDMA2000(n=3600)». А с помощью низкоплотностных кодов длиной в миллион битов можно обеспечить сколь угодно малую вероятность ошибки декодирования при работе менее чем в 0,1 дБ от пропускной способности гауссовского канала (кривая «4) LDPC(n=1000000)» на рис. 1). Эффективность декодеров низкоплотностных кодов меньшей длины, представлена на рисунке кривыми «5) 802.16e LDPC(n=2304)» и «6) DVB-S2 LDPC(n=64800)». К сожалению, все эти методы при работе в условиях большого шума все еще обладают весьма большой сложностью реализации, что затрудняет их практическое применение в высокоскоростных системах передачи и хранения данных.

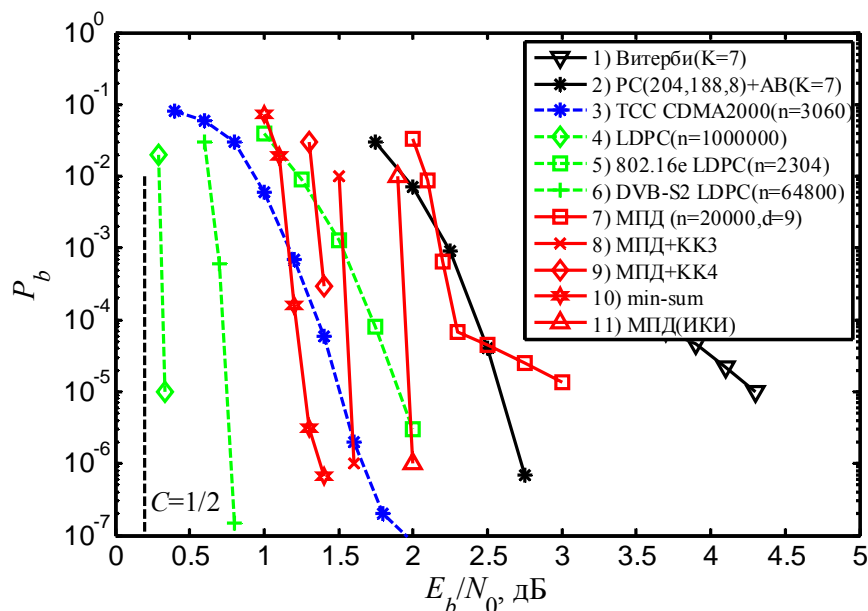


Рис. 1. Эффективность методов коррекции ошибок в канале с АБГШ и ФМ2

Интересным направлением в области разработки алгоритмов коррекции ошибок является многопороговое декодирование (МПД), развиваемое в данной работе. Для этих декодеров показано, что они позволяют почти оптимально декодировать даже очень длинные коды с линейной от длины кода сложностью исполнения, демонстрируя при этом достаточно хорошие корректирующие способности, пример которых для кода длиной 20000 битов, кодовым расстоянием $d=9$ и кодовой скорости $R=1/2$ представлен на рис. 1 кривой «7) МПД (n=20000, d=9)». При этом

МПД выполняют только простейшие операции сложения и сравнения целых чисел, что делает их очень привлекательными для применения в существующих и вновь создаваемых высокоскоростных цифровых системах передачи данных.

В рамках выполненных по проекту работ был предложен ряд каскадных схем коррекции ошибок, составляющей частью которых является МПД. При этом каскадирование осуществляется только с очень простыми кодами (коды с контролем четности, коды Хэмминга, короткие самоортогональные коды) для того, чтобы общая сложность схемы сильно не увеличилась. Применение подобных схем, как показали аналитические расчеты и результаты компьютерного моделирования, позволяет приблизить область эффективной работы МПД к пропускной способности канала на 1..2 дБ и уменьшить вероятность ошибки декодирования на 2..5 порядков без существенного усложнения схемы декодирования. Для примера на рис. 1 кривой «8) МПД+КК3» показаны характеристики одной из каскадных схем, построенной из МПД и достаточно простого самоортогонального кода. Данная схема позволяет обеспечить эффективность, сопоставимую с эффективностью лучших методов коррекции ошибок. При этом сложность этой каскадной схемы остается очень небольшой. В результате такой каскадный МПД легко реализовать, как и обычный МПД декодер, для скоростей порядка 500 Мбит/с и даже выше. Заметим, что с помощью МПД при увеличении числа итераций декодирования и выбора кодов с наименьшим на данный момент уровнем размножения ошибок возможно достижение вероятности ошибки порядка $3 \cdot 10^{-4}$ при $E_b/N_0 = 1,4$ дБ (кривая «9) МПД+КК4» на рис. 1) при использовании не более 50 итераций декодирования.

Еще лучшую эффективность можно обеспечить при использовании более сложного min-sum алгоритма для декодирования лучших из построенных в рамках данной работы СОК. Пример подобных характеристик представлен на рисунке кривой «10) min-sum». В результате были разработаны алгоритмы, обладающие сопоставимыми по эффективности с лучшими современными методами коррекции ошибок при в десятки и даже сотни раз меньшей сложности реализации.

За время выполнения проекта был реализован на ПЛИС Altera МПД сверточного кода, работающий на информационной скорости более 1 Гбит/с. Такой скорости удалось достичь за счет использования конвейера при реализации процедур вычислений на пороговом элементе декодера и максимально эффективного использования вычислительных ресурсов ПЛИС. Энергетическая эффективность и общие размеры наземной части комплекса (декодера) в общем случае определяются выбором конкретных типов ПЛИС приёмной части системы кодирования. Пример характеристик, обеспечиваемых данной ПЛИС, представлен на рис.1 кривой «11) МПД (ИКИ)».

2. Эффективность декодеров символьных кодов

В работе также развиваются схемы недвоичного многопорогового декодирования для перспективных систем передачи и хранения больших объемов цифровых данных, характеризующиеся повышенным быстродействием. Данные схемы могут быть использованы также для цифровых спутниковых трактов передачи данных и в других каналах, в которых, например, группирование ошибок из-за разных причин может быть весьма значительным.

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 (q СК), 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.

Одной из основных характеристик канала связи является его пропускная способность C , которая определяет максимальную кодовую скорость используемого кода, при которой с помощью правильно выбранных кодера и декодера можно вести передачу по каналу с шумом со сколь угодно малой вероятностью ошибки. Для q СК пропускная способность канала определяется как

$$C_{qCK} = 1 + P_0 \cdot \log_q(P_0) + (1 - P_0) \cdot \log_q(1 - P_0) - P_0 \cdot \log_q(q - 1),$$

где P_0 – вероятность ошибки в канале.

Из данного выражения также можно определить максимальную вероятность ошибки, при которой способен работать код с заданной кодовой скоростью.

Коды Рида-Соломона

На сегодняшний день среди двоичных кодов практическое применение нашли только коды Рида-Соломона (РС), обладающие рядом положительных свойств. Коды РС характеризуются тем, что для исправления в пределах кодового слова любой комбинации из t символьных ошибок можно использовать лишь $2t$ проверочных символов. При этом длина кода n у обычных кодов РС должна быть строго меньше размера алфавита q . 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 q СК представлены на рис. 2 кривой 1. По оси абсцисс на рисунке отложена вероятность ошибки P_0 в q СК, а по оси ординат – оценка вероятности ошибки на символ после декодирования, полученная путем компьютерного моделирования. При этом теоретически в q СК 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. Потенциальные возможности более длинных кодов РС с кодовой скоростью $R=1/2$ и длиной $n=65535$ двухбайтовых символов ($q=2^{16}$) отражены на рис. 2 кривой 2. И такие коды работают при вероятности ошибки в канале, значительно меньшей теоретически возможной, равной $P_0=0.438$ для данных условий.

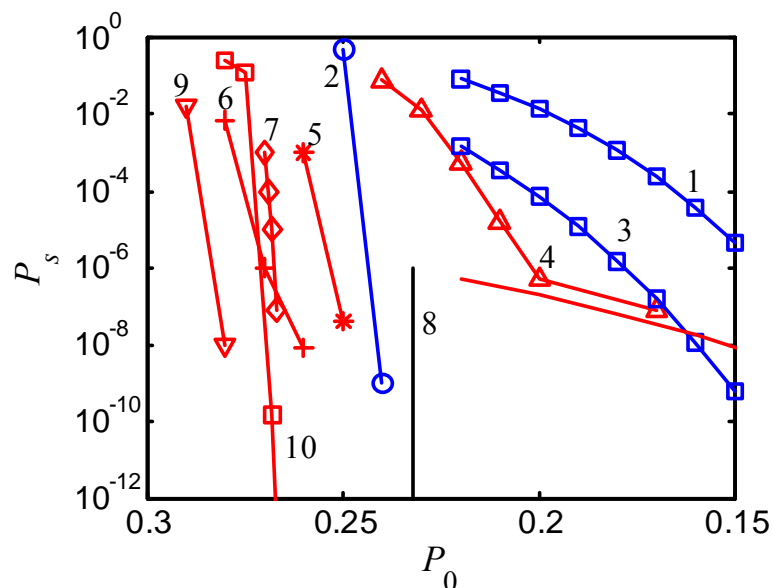


Рис. 2. Эффективность декодеров двоичных кодов с $R=1/2$

Особый интерес для систем передачи и хранения данных часто представляют малоизбыточные помехоустойчивые коды. Для таких кодов РС характеристики представлены на рис. 3. 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. 3 кривой 2. Для указанных параметров канала и кодирования предельно возможный уровень шума, при котором теоретически возможно эффективное декодирование, составляет $P_0 \approx 0.027$. 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. 2 и 3, не обеспечивают необходимых в настоящее время уровней достоверности. А декодеры для длинных кодов РС оказываются слишком сложными для реализации, так как их сложность пропорциональна $n \cdot \log^2 n$ 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. 2, который соответствует алгоритму декодирования Судана для кода РС с $n=255$, $q=256$ и $R=1/2$.

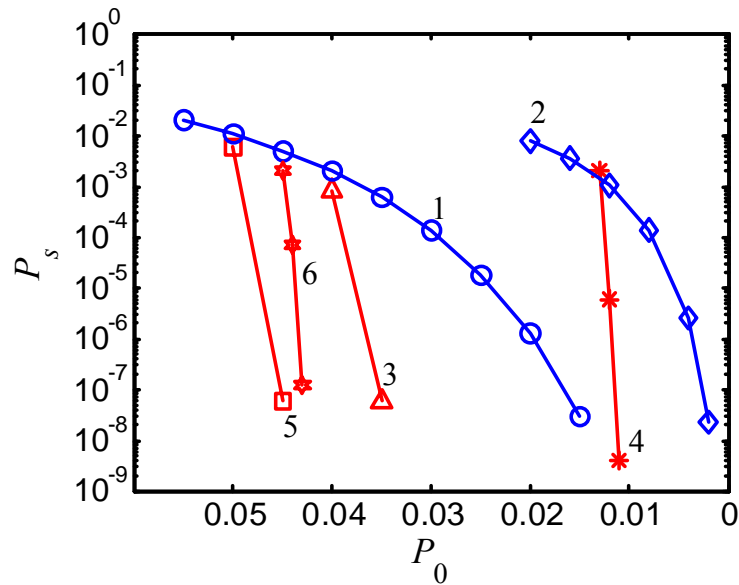


Рис. 3. Характеристики малоизбыточных недвоичных кодов в q СК

Недвоичные многопороговые декодеры

Гораздо ближе к теоретическим границам работают развиваемые в данной работе q -ичные многопороговые декодеры (q МПД) 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 q МПД 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

$d \leq 20$), I – число итераций декодирования (обычно $I \leq 30$).

Характеристики q МПД также представлены на рис. 2. Здесь кривыми 4 и 5 показана эффективность q МПД 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 q МПД оказываются гораздо лучше характеристик кодов РС с такими же q и R . При увеличении длины блока, что для q МПД не вызывает никаких сложностей, разница в эффективности становится еще более существенной. Характеристики q МПД при использовании двухбайтовых символов представлены на рис. 2 кривой 6. Здесь также использовался код с $R=1/2$ и $n=32000$ символов. Отметим, что очень простой для реализации q МПД 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 q МПД 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 q МПД для малоизбыточных недвоичных самоортогональных кодов, пример характеристик которых для $R=7/8$, $n=48000$ символов и $q=256$ представлен на рис. 3 кривой 3. Здесь также видно заметное преимущество q МПД 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 q МПД показана кривой 4, а для кодов РС – кривой 2. Такие же высокие характеристики обеспечивает q МПД малоизбыточных кодов при использовании алфавита большего объема, при котором создание других декодеров представляется очень сложным. На рис. 3 кривой 5 представлена эффективность q МПД для кода с $R=7/8$ при использовании двухбайтовых символов ($q=65536$).

Отметим, что для достижения с помощью q МПД 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 каскадированием. В публикациях авторов данной работы показано, что оптимизируя структуру данных кодов можно еще улучшить эффективность работы q МПД. В частности, характеристики найденных кодов с $q=256$ и кодовыми скоростями $1/2$ и $7/8$ представлены на рис. 2 и 3 кривыми 7 и 6 соответственно. Видно, что данные коды обеспечивают эффективную работу при больших вероятностях ошибки в q СК, чем ранее представленные, при такой же сложности их декодирования.

Еще большую эффективность практически без усложнения процедуры коррекции ошибок можно получить при переходе к каскадным схемам кодирования. В данной работе показано, что применение совместно с q МПД простейшего кода с контролем по модулю q позволяет на 1..3 порядков снизить вероятность ошибки на блок по сравнению с обычным q МПД при всего лишь 2% росте избыточности. При этом увеличение объема вычислений в каскадном коде составляет менее 20% по сравнению с исходным алгоритмом q МПД. А за счет применения совместно с q МПД модифицированного недвоичного расширенного кода Хэмминга можно уменьшить вероятность ошибки декодирования на 3..5 порядков (кривая 10 на рис. 2). 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.

Недвоичные низкоплотностные коды

В последнее время зарубежными специалистами стали активно развиваться декодеры недвоичных низкоплотностных (q LDPC) 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 q LDPC кодов пропорциональна $n \cdot q \cdot \log_2 q$. В результате разница в сложности реализации q МПД и декодеров q LDPC кодов при использовании всего четырехбайтовых символов ($q=2^{32}$) превышает миллиард раз. q МПД же при этом будет иметь ту же символьную скорость работы, как и для однобайтовых символов, а его битовая производительность даже возрастет в 4 раза. Для q LDPC известен метод декодирования, который обладает сложностью, пропорциональной $n \cdot s^2$, где $s \leq q$ – максимальный размер списка, передаваемого по ветвям графа q LDPC 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 q LDPC 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. 2). Следует особо отметить что декодер q LDPC кода с $s=32$ обладает существенно меньшей корректирующей способностью, чем q МПД при символах такого же размера (кривая 9 на рис. 2), и примерно в тысячу раз большей вычислительной сложностью.

В заключение отметим, что уникальность характеристик, обеспечиваемых такими МПД алгоритмами для символьных кодов, позволяет говорить об их абсолютном преимуществе над кодами Рида-Соломона, до сих пор повсеместно применяемых для защиты информации от ошибок. Это определяется уровнем теоретических изысканий по символьным кодам, проводимым в ИКИ РАН, аналогов которым в мире нет, и прикладных достижений, которые можно охарактеризовать как открытия в области алгоритмов цифровой обработки. Недвоичные МПД алгоритмы этого типа на 2 – 4 десятичных порядка проще по сравнению с конкурирующими алгоритмами при одновременно достигаемой на 3 – 5 порядков большей достоверности записи и хранения даже на малонадёжных носителях информации. Это – уникальная ситуация в истории обработки данных. Абсолютные приоритеты российских исследований в этой сфере алгоритмов цифровой обработки неоспоримы. Видимо, они сохранятся в ближайшие 10-15 лет. Именно поэтому и экономическая эффективность использования разработанных при поддержке РФФИ кодов и методов их декодирования будет очень высокой, поскольку они значительно, иногда многократно увеличивают к.п.д. очень дорогих высокоскоростных цифровых каналов связи или повышают скорость и на много порядков увеличивают достоверность записи принятых данных на носителях информации сверхбольшой емкости.

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 уже. 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.

- 3.10.1. *Количество научных работ, опубликованных в ходе выполнения проекта*
42
- 3.10.2. *Количество научных работ, подготовленных в ходе выполнения проекта и принятых к печати в 2010 г.*
15
- 3.11. *Участие в научных мероприятиях по тематике проекта, которые проводились при финансовой поддержке Фонда*
6
- 3.12. *Участие в экспедициях по тематике проекта, проводимых при финансовой поддержке Фонда*
- 3.13. *Финансовые средства, полученные от РФФИ*
250000 руб.
- 3.14. *Вычислительная техника и научное оборудование, приобретенные на средства Фонда*
- 3.15. *Адреса (полностью) ресурсов в Internet, подготовленных авторами по данному проекту*
<http://www.mtdbest.iki.rssi.ru>
<http://www.mtdbest.ru>
- 3.16. *Библиографический список всех публикаций по проекту*
1. Золотарев В.В. Каскадные схемы МПД декодирования для больших баз данных // Мобильные системы. М., 2008. С.66–71.
 2. Зубарев Ю.Б., Золотарев В.В., Овечкин Г.В. Обзор методов помехоустойчивого кодирования с использованием многопороговых декодеров //

Цифровая обработка сигналов. М., 2008. №1. С.2–11.

3. Золотарев В.В., Овечкин Г.В. Алгоритмы многопорогового кодирования для гауссовских каналов // Информационные процессы. М., 2008. Том 8. №1. С.68–83.
4. Зубарев Ю.Б., Овечкин Г.В. Обзор методов помехоустойчивого кодирования с использованием многопороговых декодеров // Электросвязь. М., 2008. №12. С.2–11.
5. Овечкин Г.В., Овечкин П.В. Оптимизация структуры недвоичных самоортогональных кодов для схем параллельного кодирования // Труды НИИР, №2, 2009. С.34–38.
6. Золотарев В.В., Назиров Р.Р., Чулков И.В., Овечкин Г.В. Алгоритмы МПД // Российский космос. №1, 2009. С. 60–63.
7. Овечкин Г.В., Овечкин П.В. Использование недвоичного многопорогового декодера в каскадных схемах коррекции ошибок // Вестник РГРТУ, 2009, №4 (Вып. 30), С.7–12.
8. Золотарев В.В., Овечкин Г.В. Эффективное многопороговое декодирование недвоичных кодов // Радиотехника и электроника. 2010. в печати
9. Зубарев Ю.Б., Золотарев В.В. Каскадные схемы декодирования для баз данных на основе МПД // В сб.: «10 Международная конференция «Цифровая обработка сигналов и ее приложения- DSPA-08». М., 2008.
10. Золотарев В.В., Овечкин Г.В. Применение многопорогового декодирования для повышения достоверности передачи данных // В сб.: 15-я Международная научно-техническая конференция «Проблемы передачи и обработки информации в сетях и системах телекоммуникаций». Рязань, 2008. С.3–5.
11. В.В.Золотарев, Р.Р.Назиров. Сверхнадежное исправление ошибок на основе МПД алгоритмов для баз данных систем ДЗЗ // В сб.: ИКИ по дистанционному зондированию Земли. М.: ИКИ РАН, 2008.
12. Овечкин Г.В., Овечкин П.В. Использование многопороговых декодеров в системах дистанционного зондирования Земли // Фундаментальные и прикладные космические исследования: V Конференция молодых ученых, посвященная Дню космонавтики. М.: ИКИ РАН, 2008. С.33.
13. Овечкин П.В. Использование недвоичных многопороговых декодеров в магнитных и оптических запоминающих устройствах // В сб.: «10 Международная конференция «Цифровая обработка сигналов и ее приложения- DSPA-08». М., 2008.
14. Овечкин П.В. Каскадные схемы на основе недвоичного многопорогового декодера // В сб.: 15-я Международная научно-техническая конференция «Проблемы передачи и обработки информации в сетях и системах телекоммуникаций». Рязань, 2008. С.34–35.
15. Овечкин Г.В., Овечкин П.В. Многопороговое декодирование недвоичных самоортогональных кодов // Научно-техническая конференция «Информационные и телекоммуникационные технологии», Рязань, РВВКУС, 2009 г.
16. Овечкин Г.В., Чикин А.В. Помехоустойчивость приемника спутниковых сигналов DVB-S2 // 11-я межд. конф. и выст. «Цифровая обработка сигналов и ее применение». М.: 2009. С.578–580.
17. Овечкин Г.В., Зубарев Ю.Б., Золотарев В.В. Новые алгоритмы декодирования для высокоскоростных спутниковых каналов // 11-я межд. конф. и выст. «Цифровая обработка сигналов и ее применение». М.: 2009. С. 6–9.
18. Овечкин П.В. Применение недвоичного многопорогового декодера для защиты файлов от искажений // 11-я Межд. конф. «Цифровая обработка сигналов и ее применение, DSPA-09». М.: 2009, С. 200–202.
19. Овечкин Г.В., Овечкин П.В. Использование многопороговых декодеров в системах дистанционного зондирования Земли // Седьмая всероссийская открытая ежегодная конференция «Современные проблемы дистанционного зондирования

Земли из космоса» Москва, ИКИ РАН, 2009 г.

20. Овечкин П.В. Использование многопороговых декодеров в системах хранения больших объемов данных // VI Конференция молодых ученых, посвященная Дню космонавтики «Фундаментальные и прикладные космические исследования». М.: ИКИ РАН, 2009, С. 33–34.
21. Ovechkin G.V., Zolotarev V.V., Averin S.V. Algorithm of multithreshold decoding for self-orthogonal codes over Gaussian channels – 11-th ISCTA'09, July, UK, Ambleside, 2009.
22. Ovechkin G.V., Zolotarev V.V. Non-binary multithreshold decoders of symbolic self-orthogonal codes for q-ary symmetric channels – 11-th ISCTA'09, July, UK, Ambleside, 2009.
23. Золотарёв В.В., Овечкин П.В. Алгоритм ускорения работы недвоичного многопорогового декодера // Межвуз. сб. науч. тр. «Математическое и программное обеспечение информационных систем». Рязань: РГРТУ, 2009, С. 17–19.
24. Овечкин П.В. Основная теорема декодирования каскадного кода, состоящего из недвоичного самоортогонального кода и кода контроля по модулю q // Межвуз. сб. науч. тр. «Математическое и программное обеспечение информационных систем». Рязань: РГРТУ, 2009, С. 101–103.
25. Золотарев В.В., Назиров Р.Р., Никифоров А.В., Чулков И.В. Новые возможности многопорогового декодирования по высокодостоверной передаче данных ДЗЗ // Современные проблемы дистанционного зондирования земли из космоса. Сборник научных статей. Выпуск 6. Том I. Москва, ООО «Азбука-2000», 2009. С.167–173.
26. Золотарев В.В., Овечкин Г.В., Овечкин П.В. Свидетельство РОСПАТЕНТ №2009612632 о регистрации программы для ЭВМ «Имитационная модель многопорогового декодера помехоустойчивых кодов» (MTDProtect) от 25.05.09.
27. Золотарёв В.В. «Способ декодирования помехоустойчивого кода». Патент на изобретение №2377722 с приоритетом от 21.06.2007, выдан в 2009 году. Опубликовано в БИ №36 за 2009 г.
28. Золотарев В.В., Овечкин Г.В. Эффективное многопороговое декодирование недвоичных кодов // Радиотехника и электроника. 2010. Том 55, №3, С. 324–329.
29. Кузнецов Н.А., Золотарев В.В., Овечкин Г.В., Овечкин П.В. Недвоичные многопороговые декодеры и другие методы коррекции ошибок в символьной информации // Радиотехника, №6, вып. 141, 2010. С. 4–9.
30. Овечкин Г.В. Многопороговые декодеры для систем передачи и хранения больших объемов данных // Задачи системного анализа, управления и обработки информации : межвузовский сборник научных трудов. Вып. 3 – М. : МГУП, 2010. С. 100–105.
31. Золотарев В.В., Зубарев Ю.Б., Овечкин Г.В. Высокоскоростной многопороговый декодер для систем передачи больших объемов данных // Научно-технический сборник «Техника средств связи», серия «Техника телевидения», юбилейный выпуск, МНИТИ, 2010. С. 41–43.
32. Овечкин Г.В. Применение min-sum алгоритма для декодирования блочных самоортогональных кодов // Межвуз. сб. науч. тр. «Математическое и программное обеспечение вычислительных систем» – Москва, Горячая линия – Телеком, 2010. С. 99–105.
33. Золотарев В.В., Зубарев Ю.Б., Овечкин Г.В. Высокоскоростной многопороговый декодер для систем передачи больших объемов данных // 12-я межд. конф. и выст. «Цифровая обработка сигналов и ее применение». М.: 2010. С. 10–13. Пленарный доклад.
34. Золотарев В.В., Овечкин Г.В., Овечкин П.В. Эффективное многопороговое декодирование недвоичных самоортогональных кодов // 12-я межд. конф. и выст.

«Цифровая обработка сигналов и ее применение». М.: 2010. С. 21–24.

35. Золотарев В.В., Овечкин Г.В., Овечкин П.В. Исследование недвоичных многопороговых декодеров в каналах связи с пакетирующимися ошибками // 65 Научная сессия, посвященная Дню радио: Тезисы докладов. М.: РНТОРЭС, 2010. С. 376–378.

36. Зубарев Ю.Б., Овечкин Г.В., Овечкин П.В. Недвоичное многопороговое декодирование для перспективных систем цифрового телевидения // Материалы 5-й международной научно-технической конференции "Современные телевизионные технологии. Состояние и направления развития". МНИТИ, 2010. С. 33–34.

37. Зубарев Ю.Б., Золотарев В.В. Применение многопороговых алгоритмов декодирования для перспективных систем цифрового телевидения // Материалы 5-й международной научно-технической конференции "Современные телевизионные технологии. Состояние и направления развития". МНИТИ, 2010. С. 19–20.

38. Золотарев В.В., Овечкин Г.В. Применение многопорогового декодирования для повышения достоверности передачи данных // Проблемы передачи и обработки информации в сетях и системах телекоммуникаций: Материалы 16-й Межд. науч.-техн. конф. Рязань: РГРТУ, 2010. С. 3–5.

39. Золотарев В.В., Овечкин Г.В., Назиров Р.Р., Овечкин П.В., Чулков И.В. Эффективное недвоичное многопороговое декодирование помехоустойчивых кодов для систем дистанционного зондирования земли // Современные проблемы дистанционного зондирования Земли из космоса. Сборник статей, ИКИ РАН, 2010. Том. 7, №2, С. 269–274

40. Золотарев В.В., Овечкин Г.В., Овечкин П.В. Недвоичное многопороговое декодирование для систем ДЗЗ // VIII открытая всероссийская конференция «Современные проблемы дистанционного зондирования земли из космоса», Институт космических исследований РАН, 2010. С.37.

41. Золотарев В.В., Назиров Р.Р., Чулков И.В. Применение многопороговых алгоритмов декодирования для перспективных высокоскоростных систем ДЗЗ // VIII открытая всероссийская конференция «Современные проблемы дистанционного зондирования земли из космоса», Институт космических исследований РАН, 2010. С.120.

42. Золотарев В.В. Теория и методы разработки алгоритмов многопорогового декодирования // VIII открытая всероссийская конференция «Современные проблемы дистанционного зондирования земли из космоса», Институт космических исследований РАН, 2010. С.130–131.

3.17. *Приоритетное направление развития науки, технологий и техники РФ, в котором, по мнению исполнителей, могут быть использованы результаты данного проекта информационно-телекоммуникационные системы*

3.18. *Критическая технология РФ, в которой, по мнению исполнителей, могут быть использованы результаты данного проекта технологии обработки, хранения, передачи и защиты информации*

Подпись руководителя проекта

Форма 511. ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ РЕЗУЛЬТАТОВ ЗАВЕРШЕННОГО ПРОЕКТА РФФИ В ПРИКЛАДНОЙ ОБЛАСТИ

11.1. Номер проекта
08-07-00078

11.2.1. Приоритетное направление развития науки, технологий и техники РФ, в котором, по мнению исполнителей, могут быть использованы результаты завершенного проекта

информационно-телекоммуникационные системы

11.2.2. Критическая технология РФ, в которой, по мнению исполнителей, могут быть использованы результаты завершенного проекта

технологии обработки, хранения, передачи и защиты информации

11.3. Предлагаемое авторами название работы в прикладной области

Многопороговые декодеры для спутниковых, космических и иных цифровых систем связи

11.4. Ожидаемые результаты работы в прикладной области

В настоящее время весь мир переживает трудный очень дорогой в финансовом плане период перехода на полностью цифровые методы создания, обработки и передачи информации. В этих условиях именно простые методы обеспечения высокодостоверной передачи данных на основе методов помехоустойчивого кодирования могут создать огромную экономию финансовых средств при создании новейших систем и сетей связи. Большой экономический эффект от применения кодирования проявляется в том, что с уменьшением допустимого отношения сигнал/шум на передаче вследствие применения кодирования появляется возможность очень значительного роста скорости передачи, увеличения дальности связи или уменьшения размера используемых обычно очень дорогих антенн. А поскольку и дальше требования к достоверности передаваемых цифровых данных будут только расти, то важность кодирования и его экономическая необходимость будут только увеличиваться. Поэтому оценивавшаяся в 80-х годах экономическая ценность кодирования в миллионы долларов в настоящее время для широкомасштабных систем уже исчисляется десятками миллионов долларов и в дальнейшем будет только быстро увеличиваться.

К сожалению, сейчас в России создаются модемы (одним из важнейших узлов которых и являются устройства помехоустойчивого кодирования), которые обычно не могут работать при достаточно большом уровне шума в канале связи и на достаточно высоких скоростях передачи. Тем не менее, постепенно у заказчиков различных ведомств постепенно появляются средства на создание цифровых модемов высокого качества. При их весьма трудоемкой разработке особое внимание уделяется созданию самого главного узла такого модема – помехоустойчивому кодеку, – который должен обладать достаточно большим запасом прочности по наиболее важным для такого модема параметрам: производительности, энергетической эффективности, совместимости с различными системами сигналов и адаптивности к прочим параметрам систем связи. Высококачественные кодеки создают возможность для успешной передачи цифровых данных этими модемами при гораздо меньших уровнях сигнала по сравнению со случаем, когда кодирование не используется. Именно решение фундаментальной научной проблемы – простого декодирования (восстановления достоверности цифровых потоков) при экстремально большом уровне шума и позволяет непосредственно решить экономически сверхважную техническую задачу обеспечения высокого к.п.д. используемых дорогих цифровых спутниковых каналов путем создания действительно эффективных модемов.

В настоящее время для ряда современных высокоскоростных систем связи основным методом кодирования могут быть признаны развиваемые в рамках гранта многопороговые методы декодирования (МПД) помехоустойчивых кодов, характеризующиеся предельно возможными уровнями энергетического выигрыша и очень высоким быстродействием. Данные методы при декодировании требуют в 10-100 раз меньшее число операций по сравнению с другими сопоставимыми по эффективности методами, причем эти операции могут быть полностью распараллелены при аппаратной реализации. В результате реализованные на ПЛИС МПД смогут обеспечивать декодирование со скоростью до нескольких Гбит/с. Это позволяет уже сейчас решить проблему эффективного кодирования в высокоскоростных каналах с большим уровнем шума.

Разработки алгоритмов типа МПД ведутся уже в течение 35 лет, и к настоящему времени данные алгоритмы находятся в высокой степени готовности к непосредственному применению в различных системах цифровой связи. Сейчас в ИКИ, НИИРадио, Воронежском НИИ связи и в других организациях уже создано несколько поколений успешно работающих МПД декодеров. Дополнительным подтверждением полезности многопороговых декодеров является глубокая заинтересованность многих крупных организаций («Энергия», КБ им. Лавочкина и др.) в продолжении разработок по проекту.

Таким образом, МПД алгоритмы являются уникальными технически высокоэффективными алгоритмами, дающими огромный экономический эффект в новых и модернизируемых сетях связи, которые гораздо более эффективны и одновременно менее дороги в разработке, чем другие сопоставимые с ними по основным параметрам декодеры. Идеология МПД является чисто российским направлением исследований и достижением. Поэтому все технические решения и наработки абсолютно доступны для всех организаций соответствующего профиля.

Внедрение МПД в разработки систем связи ведомств всех уровней обеспечит достижение уникально высоких характеристик этих систем в самые короткие сроки и с минимальными затратами. Именно в таких системах и следует применять многопороговые декодеры, способные работать при очень низких отношениях сигнал/шум. При этом кодирование фактически увеличивает, причем, иногда многократно (!) к.п.д. использования очень дорогих каналов связи только за счет более эффективных вычислений при обработке сигнала без увеличения объема прочих необходимых частотных и финансовых ресурсов создаваемых сверхдорогих ныне коммуникационных систем. Это и является основанием для самого широкого внедрения исследований по кодам в технику связи во всем мире именно из-за огромной нормы прибыли по разработкам такого типа, которая может достигать в некоторых случаях десятков тысяч процентов.

11.5. *Планируемая продолжительность работы*
до 2 лет

11.6. *Предполагаемые авторами пути дальнейшего продвижения проект*
участие в лотах ФЦП Минобрнауки

11.7. *Информация, связанная с интеллектуальной собственностью*
патент (свидетельство на полезную модель) имеется

11.8. *Реквизиты охранных документов (номер патента, исходящий номер заявки на патент)*

Патенты на изобретения №2017333, №2119252, №2377722

Патенты на полезную модель №44215, №44216

Подпись руководителя проекта

Форма 511. ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ РЕЗУЛЬТАТОВ ЗАВЕРШЕННОГО ПРОЕКТА РФФИ В ПРИКЛАДНОЙ ОБЛАСТИ

11.1. *Номер проекта*
08-07-00078

11.2.1. *Приоритетное направление развития науки, технологий и техники РФ, в котором, по мнению исполнителей, могут быть использованы результаты завершенного проекта*
информационно-телекоммуникационные системы

11.2.2. *Критическая технология РФ, в которой, по мнению исполнителей, могут быть использованы результаты завершенного проекта*
технологии обработки, хранения, передачи и защиты информации

11.3. *Предлагаемое авторами название работы в прикладной области*

Многopороговые декодеры для защиты файлов сверхбольших баз данных от искажений

11.4. *Ожидаемые результаты работы в прикладной области*

Ни одно современное устройство для хранения информации не может работать без использования схем коррекции ошибок. Среди таких устройств и 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, которые для файла или набора файлов создают дополнительный файл, используя который, можно восстановить исходную информацию, даже если она была искажена.

Все известные методы для защиты файлов от искажений основаны на использовании кодов Рида-Соломона. Данные методы часто не обеспечивают требований по скорости работы и корректирующей способности. Поэтому предлагается для защиты файлов от искажений использовать методы, основанные на применении недвоичных многопороговых декодеров (QMПД). Данный декодер обеспечивает близкое к оптимальному декодирование с линейной от длины кода сложностью реализации, что позволяет ему эффективно декодировать информацию со скоростью более 10 Мбит/с при работе на обычном персональном компьютере.

Использование QMПД для защиты файлов от искажений позволит повысить скорость кодирования/восстановления информации примерно в сто раз по сравнению с известными аналогами. Также QMПД одинаково эффективно будет исправлять как независимые ошибки так и пакеты ошибок. 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.

11.5. *Планируемая продолжительность работы*
до 2 лет

11.6. *Предполагаемые авторами пути дальнейшего продвижения проекта*
участие в лотах ФЦП Минобрнауки

11.7. *Информация, связанная с интеллектуальной собственностью*
патент (свидетельство на полезную модель) имеется

11.8. *Реквизиты охраняемых документов (номер патента, исходящий номер заявки на патент)*
Патенты на изобретения №2017333, №2119252, №2377722
Патенты на полезную модель №44215, №44216

Подпись руководителя проекта