

ОБЗОР ИССЛЕДОВАНИЙ И РАЗРАБОТОК МЕТОДОВ ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ (По состоянию на 2005 год)

Золотарев В.В., Овечкин Г.В.

Аннотация. Передача информации по каналам связи существенно усложняется из-за помех и искажений в канале. Эффективным средством повышения достоверности передаваемой информации является помехоустойчивое кодирование. В обзоре производится сравнение основных алгоритмов декодирования помехоустойчивых кодов, сделанное по материалам научно-технических конференций и публикациям по теории кодирования.

Критерии эффективности кодирования. В последнее десятилетие теория помехоустойчивого кодирования продвинулась далеко вперед. Появились мощные коды и методы их декодирования, обеспечивающие работу систем связи вблизи пропускной способности канала. Наиболее общим показателем для качественной оценки методов декодирования является энергетический выигрыш кодирования (ЭВК), показывающий снижение энергии, необходимой для передачи одного бита данных (при некоторой выбранной средней вероятности ошибки на бит $P_b(e)$) в случае использования тех или иных алгоритмов кодирования и декодирования, по сравнению со случаем, когда кодирования нет.

Зарубежные специалисты более 20 лет назад оценивали каждый 1 дБ ЭВК в миллионы долларов [1]. Сейчас ценность ЭВК возросла еще больше, поскольку появилась возможность уменьшать размеры очень дорогих антенн или повышать дальность связи, увеличивать скорость передачи или снижать необходимую мощность передатчика, улучшать другие важные свойства современных систем связи. Заметим, что их стоимость растет все быстрее и уже совершенно несопоставима с теми затратами, которые были необходимы несколько десятилетий назад. Кроме того, существенно возрастают взаимные помехи приему между различными системами, появляется все больше экологических ограничений на мощность передатчиков, растет потребность в резком увеличении скоростей обмена данными между сетями, а также в значительном росте их достоверности.

И в дальнейшем, в условиях глобализации экономики и взрывной информатизации общества эти тенденции будут только усиливаться. Отсюда можно сделать очевидный вывод, что возрастание на несколько порядков (!) экономической (как и экологической, и вообще, системной) ценности ЭВК на базе методов помехоустойчивого кодирования становится чрезвычайно актуальным и требует внедрения теоретических достижений в области помехоустойчивого кодирования при создании компьютерных систем связи.

Характеристики декодеров. На рис. 1 представлена зависимость вероятности ошибки на бит $P_b(e)$ на выходе декодера от уровня шума E_b/N_0 в двоичном симметричном канале без памяти (ДСК). Ошибки возникают при работе жесткого модема с двоичной фазовой модуляцией в канале с аддитивным белым гауссовским шумом, когда в декодере не используются оценки достоверности принятых символов. Такая модель канала достаточно точно описывает реальные спутниковые и некоторые другие типы каналов.

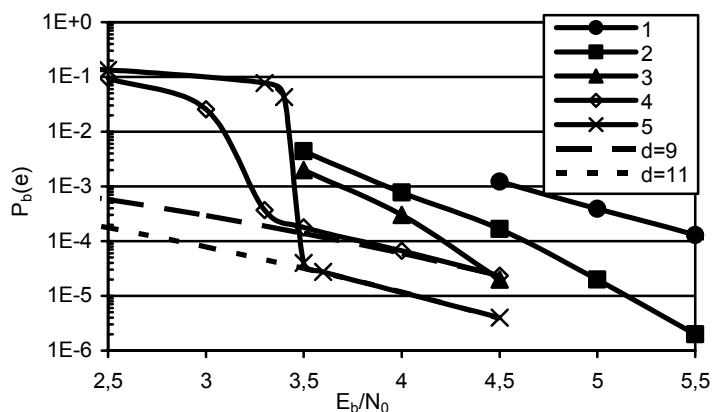


Рис. 1. Характеристики МПД и АВ в ДСК

Кривые 1, 2, 3 соответствуют широко используемому алгоритму Витерби (АВ) [2] для кодовой скорости $R=1/2$ и длины кодирующего регистра $K=7, 11$ и 15. Данный метод является оптимальным, однако его сложность растет экспоненциально с ростом K и поэтому на практике декодеры с $K>9$ не используются. В результате возникает необходимость поиска более простых с точки зрения практической реализации декодеров, обеспечивающих в то же время близкое к оптимальному декодирование.

Многopороговые алгоритмы. Один из простейших алгоритмов коррекции ошибок – пороговый декодер (ПД) Мессе [3], принимающий решение о значении каждого декодируемого символа на основе обычного «голосования» проверок. Схема порогового декодера сверточного самоортогонального кода (СОК) с кодовым расстоянием $d=5$, кодовой скоростью $R=1/2$ и длиной кодового ограничения $n_A=14$ представлена на рис. 2. Он состоит из двух двоичных регистров, нескольких полусумматоров (сумматоров по mod 2) и порогового элемента T , который просто суммирует двоичные проверки декодируемого символа и сравнивает их с порогом, изменяя этот символ и все относящиеся к нему проверки, если сумма проверок превысила некоторое пороговое значение. Но данный метод имеет невысокую корректирующую способность, из-за чего редко применяется в системах передачи данных.

Значительно лучшими характеристиками обладают многopороговые декодеры (МПД) [4-7], являющиеся модификацией представленного выше

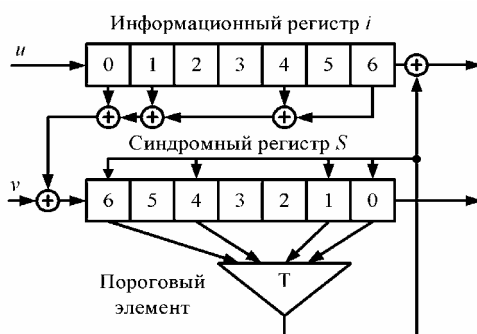


Рис. 2. Схема порогового декодера

ПД. МПД в процессе контроля принятых кодовых последовательностей многократно исправляют информационные символы пришедшего из канала сообщения. Эти декодеры обладают важнейшим строго доказанным свойством – сходимостью к решению оптимального декодера (ОД), сохраняя линейную от длины кода сложность реализации.

Схема МПД сверточного СОК с $d=5$, $n_A=14$ и двумя итерациями декодирования представлена на рис. 3. При большем числе итераций, обычно необходимом для работы в области больших шумов канала, последующие итерации полностью аналогичны второй. Как видно из представленной схемы, каждая итерация МПД отличается от обычного ПД только наличием «разностного» регистра, в котором отмечаются измененные пороговым элементом (ПЭ) информационные символы. Существенно, что решения ПЭ из разностного регистра затем используются другим ПЭ на следующей итерации декодирования. На каждой итерации МПД при декодировании информационного символа i_k на ПЭ – единственном активном элементе декодера (при использовании жесткого модема в ДСК) выполняются следующие операции.

1. Вычисляется сумма проверок (каждая из которых для случая ДСК равна 0 или 1), т. е. функция

$$L_i = \sum_{m=1}^J S_{g_m} + r_i,$$

где $J=d-1$ – количество проверок (ненулевых элементов дт порождающего полинома кода G); r_i – символ разностного регистра, относящийся к декодируемому символу i_k также равный 0 или 1; S_m – m -й элемент синдромного регистра, входящий в множество проверок относительно декодируемого символа i_k .

2. Если $L_i > T$, где $T \geq (d-1)/2$ – значение порога порогового элемента, то информационный символ i_k , все связанные с ним проверки $\{S_{g_m}\}_{m=1,J}$ и символ r_i инвертируются.

3. Переход к декодированию следующего символа (п. 1).

Заметим, что при применении мягкого модема, когда в гауссовском канале оценивается надежность приема каждого двоичного символа, в МПД

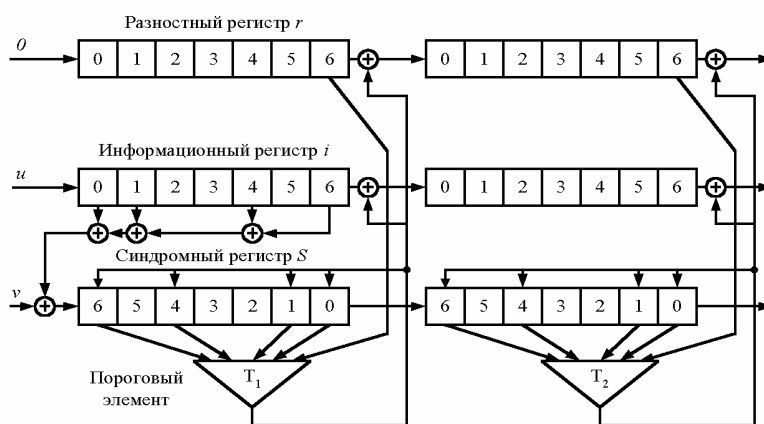


Рис. 3. Схема декодера МПД сверточного СОК

выполняются те же операции, но проверки суммируются уже с весами, определяющими надежность оценок принятых из канала битов. Пороги T для декодируемых символов будут переменными, а не фиксированными, как в случае ДСК.

Анализ характеристик МПД. Кривая 4 на рис. 1 соответствует работе МПД сверточного СОК с $R=1/2$, минимальным кодовым расстоянием $d=9$, длиной кодового ограничения $n_A=4168$ бит и $I=15$ итерациях декодирования. Возможности МПД с $R=1/2$, $d=11$ и $I=20$ представлены на рис. 1 кривой 5. Пунктиром на рисунке показаны вероятности ошибочного декодирования кода с $d=9$ и $d=11$ оптимальным декодером. Как следует из графиков, МПД (для достаточно длинных кодов) оказывается лучше даже заведомо нереализуемого оптимального АВ с $k=15$ и более. Отметим, что с ростом длины кодового ограничения n_A и увеличением числа итераций характеристики МПД быстрее сходятся к характеристикам оптимального декодера.

На рис. 4 показаны характеристики тех же алгоритмов декодирования при использовании мягкого модема, оценивающего достоверность принимаемых двоичных символов с квантованием выхода на $Q=16$ уровней для вышеперечисленных кодов. Из сопоставления рис. 1 и 4 видно, что переход к мягкому модему при использовании АВ позволяет получить дополнительный ЭВК порядка 2 дБ, а при использовании МПД – 1.4...1.7 дБ. Но и в этом случае МПД, сохраняя простоту обычного ПД, существенно превосходит АВ по эффективности. Основные соотношения между этими алгоритмами имеют место и при других кодовых скоростях.

Приведенные выше данные показывают, что доступные для реализации оптимальные АВ уступают МПД, в котором могут легко декодироваться длинные коды, в широком диапазоне кодовых скоростей при использовании как жесткого, так и мягкого модемов. При этом МПД выполняет только простейшие операции сложения и сравнения небольших целых чисел, что обуславливает его крайнюю простоту при всех вариантах программной или аппаратной реализации.

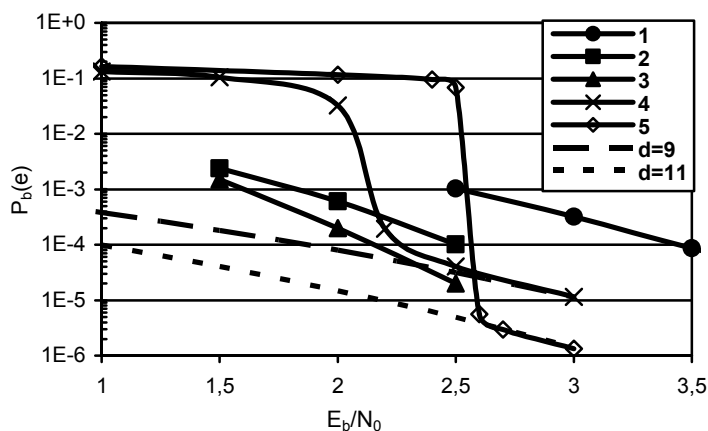


Рис. 4. Характеристики МПД и АВ в канале с АБГШ

Каскадные коды. Важным этапом в развитии теории кодирования является появление каскадных кодов [8], в основе построения которых лежит идея совместного использования нескольких составляющих кодов. Данный подход позволил существенно повысить эффективность применения кодирования по сравнению с базовыми некаскадными методами.

Наиболее широкое распространение в реальных системах связи нашла каскадная схема, в которой внешним кодом является код Рида-Соломона, а внутренним – сверточный код, обычно декодируемый с помощью оптимального алгоритма Витерби. Часто в данной схеме между внешним и внутренним кодером/декодером включаются устройства перемежения и восстановления (деперемежения), осуществляющие псевдослучайную перестановку символов внешнего кода и восстановление исходного порядка символов соответственно. Рассмотренные устройства предназначены для разбиения пакетов ошибок, появляющихся при декодировании принятого из канала сообщения с помощью декодера внутреннего кода (алгоритма Витерби), что позволяет существенно улучшить эффективность всей каскадной конструкции.

Результаты моделирования каскадного кода, состоящего из кода Рида-Соломона (255, 223, 33) и сверточного кода с $K=7$ и $R=1/2$, при разной глубине перемежения I представлены на рис. 5. При получении данных графиков использовался обычный прямоугольный перемежитель, представляющий собой массив, состоящий из I строк (определяющих глубину перемежения) по 255 q -ичных символов (в каждом символе содержится 8 бит, поскольку $q=256$). В процессе кодирования кодовые слова кода Рида-Соломона построчно записывались в массив перемежителя, а затем считывались по столбцам и кодировались с помощью кодера сверточного кода. При декодировании принятая последовательность сначала обрабатывалась декодером внутреннего кода (декодером Витерби). Далее информация с выхода декоде-

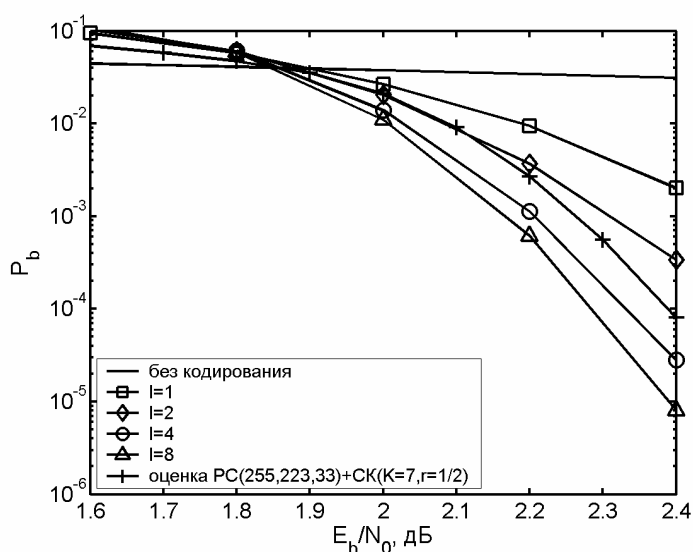


Рис. 5. Характеристики каскадного кода, состоящего из кода Рида-Соломона (255, 223, 33) и сверточного кода ($K=7$, $R=1/2$) в канале с АБГШ

ра Витерби группировалась в q -ичные символы и по столбцам записывалась в массив деперемежителя (т.е. первый символ записывается в первый столбец первой строки, второй – в первый столбец второй строки и т.д.), а затем построчно считывалась декодером кода Рида-Соломона и декодировалась. Анализируя данные графики можно заметить, что оценка эффективности рассматриваемого каскадного кода оказывается несколько завышенной. Это можно объяснить неточностью границы для характеристик сверточного кода при очень высоком уровне шума.

В настоящее время на рынке существует много кодеков, реализующих каскадный код PC+AB, одним из которых является кодек ANA4210 RSVP компании АНА (Advanced Hardware Architecture), обеспечивающий работу с информационной скоростью до 68 Мбит/с.

Турбо коды. Дальнейшим развитием каскадных кодов стали турбо коды, образующиеся путем каскадирования двух или более составляющих кодов. Первые турбо коды, предложенные Беру и соавторами в [9], состояли из двух параллельно соединенных через перемежитель сверточных кодов. В общем случае турбо коды могут получаться как при параллельном, так и последовательном соединении кодов, разделенных перемежителем (рис. 6).

Для примера на рис. 6а представлена схема кодера параллельного турбо кода с общей кодовой скоростью $R=1/3$. Для повышения кодовой скорости турбо кода может применяться выкалывание символов то одной, то другой проверочной ветви. В результате скорость кода R увеличивается до $1/2$. Дальнейшее повышение кодовой скорости может осуществляться выкалыванием большего числа проверочных символов.

Наиболее важным моментом при проектировании турбо кодов является правильный выбор составляющих кодов и перемежителя. Результаты исследований показали, что для параллельного турбо кода наилучшими составляющими кодами являются рекурсивные систематические сверточные коды, поскольку их применение позволяет значительно уменьшить число кодовых слов низкого веса, определяющих эффективность турбо кода [10]. Получающийся в результате турбо код обычно называется сверточным турбо кодом (Turbo Convolutional Code – TCC). Роль перемежителя в турбо кодах состоит в уменьшении корреляции между соседними символами кодового слова, что позволяет на каждой итерации декодирования уменьшать вероятность ошибки. Кроме этого, перемежитель также оказывает огромное влияние на минимальное кодовое расстояние турбо кода и количество кодовых слов низкого

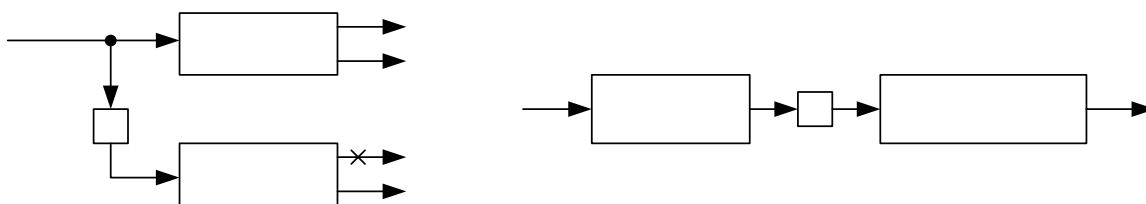


Рис. 6. Кодер параллельного (а) и последовательного (б) турбо кода

веса, определяющих эффективность турбо кода. Наилучшими характеристиками обладают турбо коды с псевдослучайными перемежителями, однако часто они слишком сложны для построения и поэтому на практике приходится использовать перемежители с регулярной структурой (например, диагональные перемежители).

Для декодирования турбо кодов используется итеративное декодирование с мягким решением (рис. 7), позволяющее получить очень близкие к пропускной способности канала характеристики. В процессе итеративного декодирования турбо кодов выполняются несколько итераций декодирования, на каждой из которых происходит декодирование каждого из составляющих кодов. Для этого могут использоваться любые алгоритмы декодирования, способные формировать мягкие решения относительно декодированных символов. Наибольшее практическое применение нашли такие алгоритмы декодирования, как Log-MAP (LM), Max-Log-MAP (MLM) и Soft Output Viterby Algorithm (SOVA). Сложность реализации данных методов в смысле количества выполняемых операций для декодирования одного информационного символа представлена в табл. 1 [11]. В этой таблице K определяет конструктивную длину составляющих кодов. Зная сложность реализации методов декодирования составляющих кодов $N_{\text{сост}}$ можно оценить сложность декодирования всего турбо кода:

$$N_{\text{турбо}} = IN_{\text{сост}}M,$$

где I – число итераций декодирования; M – число составляющих кодов (обычно два).

Таблица 1. Сложность алгоритмов декодирования помехоустойчивых кодов

Вид операции	Алгоритм Витерби	Max-Log-MAP	Log-MAP	SOVA
Выбор максимума		$5 \cdot 2^{K-1} - 2$	$5 \cdot 2^{K-1} - 2$	$2^{K-1} + 3K$
Сложение	$2 \cdot 2^{K-1} + 5$	$10 \cdot 2^{K-1} + 11$	$15 \cdot 2^{K-1} + 9$	$2 \cdot 2^{K-1} + 8$
Умножение на ± 1		8	8	8
Сравнение	2^{K-1}			$6K$
Поиск в таблице			$5 \cdot 2^{K-1} - 2$	

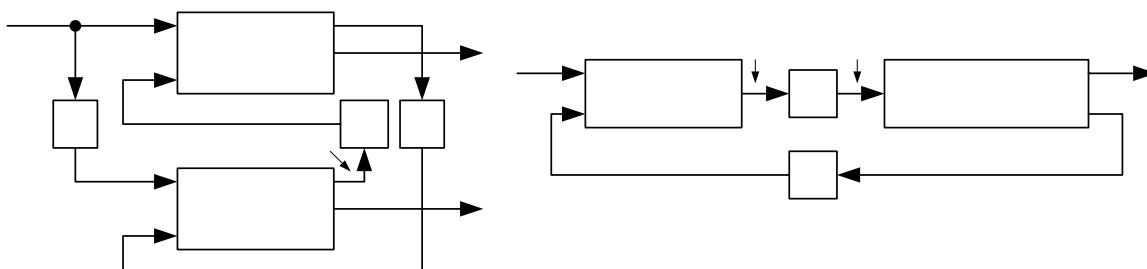


Рис. 7. Декодер параллельного (а) и последовательного (б) турбо кода

Далее рассмотрим результаты моделирования турбо кода в канале с АБГШ при использовании двоичной фазовой модуляции. Как следует из описания кодера и декодера турбо кодов, на их эффективность оказывают влияние много параметров, основными из которых являются алгоритм декодирования составляющих кодов, количество итераций декодирования, тип и длина перемежителя, составляющие коды. На рис. 8 представлены характеристики турбо кода с кодовой скоростью $R=1/2$, конструктивной длиной составляющих рекурсивных систематических сверточных кодов $K=4$, образующими полиномами составляющих кодеров $g_0=13$ и $g_1=15$ в восьмеричной системе счисления, Max-Log-MAP алгоритмом декодирования составляющих кодов, 8 итерациями декодирования и псевдослучайным перемежителем длиной L от 190 до 12282 бит. Для сравнения на данном рисунке также представлены характеристики сверточного кода с $K=11$, декодируемого с помощью алгоритма Витерби. Данный код был выбран потому, что $K=11$ является наименьшей конструктивной длиной, при которой сложность декодирования сверточного кода, исходя из табл. 1, становится больше сложности декодирования рассматриваемого турбо кода. Как видно из рисунка, турбо код с длиной блока всего 190 бит по эффективности соответствует сверточному коду с $K=11$, а с ростом длины перемежителя характеристики турбо кода значительно улучшаются при сохранении сложности декодирования.

Основным недостатком турбо кодов является относительно высокая сложность их практической реализации. Например, сложность SOVA алгоритма декодирования примерно в 2 раза больше сложности обычного алгоритма Витерби. Учитывая, что при декодировании турбо кода выполняется порядка 10 итераций декодирования, на каждой из которых декодируется два составляющих кода получается, что сложность турбо кода примерно в 40 раз больше сложности декодера Витерби. При использовании более эффективных Max-Log-MAP и Log-MAP алгоритмов разница в сложности еще в несколько раз увеличивается. К недостаткам турбо кодов также следует отнести наличие так называемой области насыщения вероятности ошибки (error

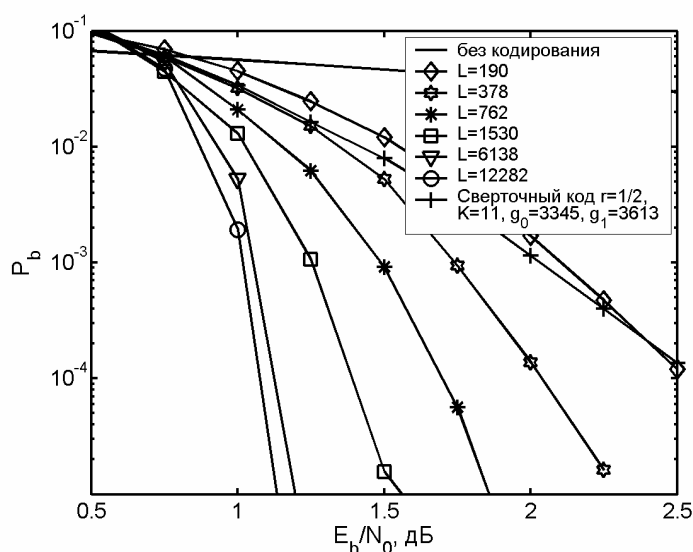


Рис. 8. Характеристики турбо кода в канале с АБГШ для разных длин перемежителей

floor), в которой скорость уменьшения вероятности ошибки при повышении отношения сигнал/шум значительно замедляется. Данный эффект вызван небольшим кодовым расстоянием турбо кодов.

Для декодирования сверточных турбо кодов на рынке представлено множество кодеков, позволяющие декодировать данные со скоростями до сотен Мбит/с. Примером турбо кодека является высокоскоростной FPGA турбо декодер S4000, построенный на базе ПЛИС Spartan типа Virtex™-E.

Низкоплотностные коды (LDPC). Прекрасные характеристики, получаемые при итеративном декодировании турбо кодов, стимулировали активные исследования по применению данного метода к декодированию других кодов. В результате оказалось возможным получить еще лучшие характеристики при декодировании низкоплотностных (Low Density Parity Check – LDPC) кодов [13], предложенных Галлагером еще в 1962 г. [14]. Данные коды представляют собой линейные блочные (N, K) коды, задаваемые с помощью проверочной матрицы H , характеризуемой относительно малым числом единиц в строках и столбцах (рис. 9а). Часто LDPC коды удобно представлять с помощью графа Таннера, в котором для представления строк и столбцов проверочной матрицы используются определенным образом связанные между собой битовые и проверочные узлы. Например, для кода с матрицей H с рис. 9а граф Таннера представлен на рис. 9б.

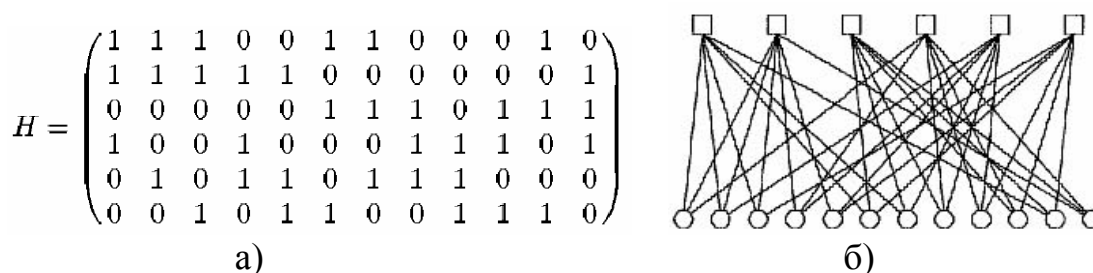


Рис. 9. Проверочная матрица и граф Таннера регулярного LDPC кода

Среди LDPC кодов выделяют регулярные и нерегулярные коды [15-17]. Проверочная матрица первых характеризуется тем, что во всех столбцах и строках имеется одинаковое число единиц λ и ρ соответственно. В нерегулярных LDPC кодах данное свойство не соблюдается, и веса столбцов и строк описываются с помощью функций $\lambda(i)$ и $\rho(i)$, задающих долю столбцов и строк с весом i . Для примера на рис. 10 представлена проверочная матрица и граф Таннера для нерегулярного LDPC кода, в котором $\lambda(2) = 8/9$, $\lambda(3) = 1/9$, $\rho(3) = 1/5$, $\rho(4) = 4/5$.

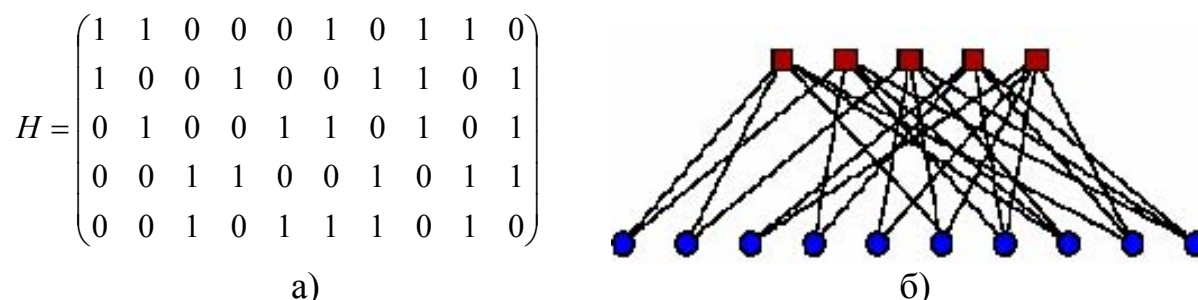


Рис. 10. Проверочная матрица и граф Таннера нерегулярного LDPC кода

Для декодирования LDPC кодов обычно используется разновидность итеративного декодирования, называемая алгоритмом распространения надежности (Belief Propagation – BP) [18], работающего с графом кода. Также возможно применение различных модификаций данного алгоритма, характеризующихся меньшей сложностью реализации. В основе работы данных методов лежит итеративный обмен мягкими решениями между битовыми и проверочными узлами графа кода. В случае если на графе отсутствуют циклы, то применение такого способа декодирования позволяет получить оптимальное решение. Поэтому желательно проектировать коды таким образом, чтобы в их графе отсутствовали короткие циклы. При выполнении данного требования удастся получить близкие к оптимальным результаты.

На рис. 11 представлены характеристики регулярных (кривая LDPC) и нерегулярных (кривые iLDPC) LDPC кодов различной длины с кодовой скоростью $1/2$ [17]. Как следует из данного рисунка, эффективность нерегулярных LDPC кодов оказывается лучше эффективности регулярных кодов. Это объясняется тем, что в нерегулярных кодах из-за различного числа единиц в строках и столбцах информационные символы защищены по-разному. В результате при декодировании проявляется так называемый эффект волны, когда более защищенные биты декодируются быстрее и затем как бы помогают при декодировании менее защищенных бит.

Из сравнения характеристик турбо кодов с характеристиками LDPC кодов следует, что последние оказываются более эффективными, что особенно заметно при больших длинах кодов и при малых вероятностях ошибки декодирования. При этом сложность практической реализации LDPC кодов, определяемая как $N_{LDPC} = I \cdot 4 \cdot s$ (I – число итераций декодирования, s – средний вес столбцов проверочной матрицы), существенно ниже сложности турбо кодов.

К одному из основных недостатков LDPC кодов, возникающему из-за специфической структуры проверочной матрицы H , следует отнести квадра-

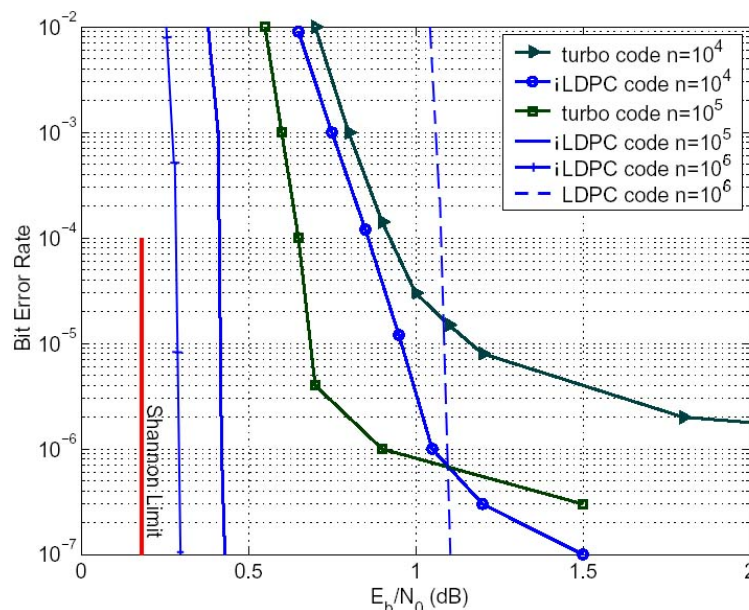


Рис. 11. Эффективность LDPC кодов и турбо кодов различной длины

тичную зависимость сложности кодирования от длины кода, хотя существуют подходы, позволяющие при тщательном предварительном проектировании снизить сложность кодирования до линейной. Кроме того, аппаратная реализация LDPC кодов часто бывает очень сложна и не позволяет простого изменения кодовой скорости и длины блока, поскольку при этом необходимо формировать новую проверочную матрицу H .

В настоящее время на рынке LDPC кодеков можно отметить кодек компании АНА, позволяющий работать с LDPC кодами длиной до 30 кбит со скоростью до 30 Мбит/с.

Турбо коды произведения (TPC). Турбо коды произведения (Turbo Product Codes – TPC) [19, 20] представляют собой многомерный набор кодовых слов составляющих линейных блоковых кодов, таких как коды с контролем четности, коды Хэмминга, Коды Боуза-Чоудхури-Хоквингема (Bose-Chaudhuri-Nosquenghem – BCH). Для примера на рис. 12 представлена структура двумерного TPC. Здесь код образован кодами C_1 с параметрами (N_1, K_1, d_1) и C_2 с параметрами (N_2, K_2, d_2) . При кодировании набор информационных битов D записывается в матрицу размером $K_2 \times K_1$, затем строки этой матрицы кодируются кодом C_1 , в результате чего получаются проверочные биты P_1 . После этого столбцы матрицы кодируются кодом C_2 , образуя проверочные биты P_2 для информационных символов и проверочные биты P_p для проверочных символов P_1 первого кода. В результате получается код с параметрами $(N_1 N_2, K_1 K_2, d_1 d_2)$.

Среди множества TPC кодов наибольший интерес представляют коды, построенные с помощью кодов Хэмминга и кодов с проверкой на четность. Последние коды часто называются TPC/SPC (Turbo Product Codes / Single Parity Check) кодами.

При декодировании TPC кодов также используется итеративный подход, основанный на мягком декодировании составляющих кодов. Причем, если в случае применения в качестве составляющих кодов Хэмминга и кодов BCH для их декодирования часто используется алгоритм Чейза, то TPC/SPC коды допускают достаточно простое представление в виде графа Таннера, что позволяет применить к ним более эффективный и с вычислительной точки зрения более простой ВР алгоритм декодирования, используемый при декодировании LDPC кодов.

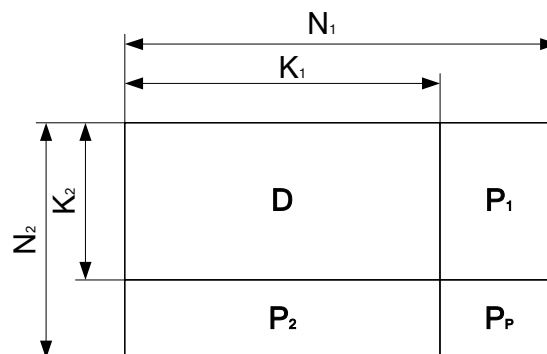


Рис. 12. Кодовое слово последовательного каскадного кода

На рис. 13 представлены характеристики ТРС, построенного с помощью кодов ВСН и расширенных кодов Хэмминга. Общая кодовая скорость ТРС кодов равна $21^2/32^2=0.43$, $26^2/32^2=0.66$, $51^2/64^2=0.635$, $57^2/64^2=0.79$. Видно, что данные коды показывают неплохие характеристики при высоких кодовых скоростях и у них практически отсутствует область насыщения вероятности ошибки.

На рис. 14 показаны характеристики ТРС/СПС кода, построенного из нескольких (8, 7) кодов с контролем четности. При использовании i кодов с контролем четности общая кодовая скорость ТРС/СПС кода оказывается равной $7^i/8^i$. Например, для двумерного кода (2D) кодовая скорость примерно равна 0.77, а для пятимерного (5D) – 0.51.

В настоящее время на рынке ТРС кодеков можно отметить кодеки АНА4501, АНА4540 компании АНА, позволяющие работать с двух и трех мерными ТРС кодами длиной до 4096 бит со скоростью до 36 Мбит/с и длиной 16384 бит со скоростью 155 Мбит/с соответственно.

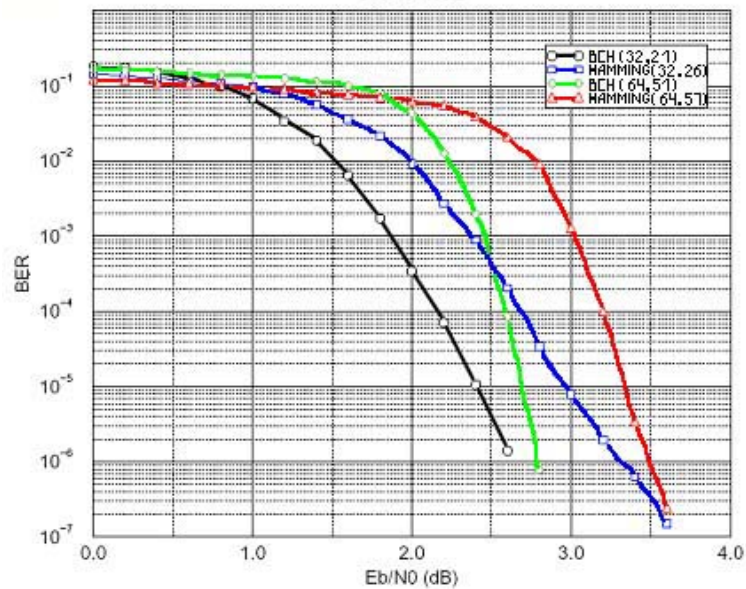


Рис. 13. Характеристики ТРС, состоящих из кодов ВСН и из кодов Хэмминга

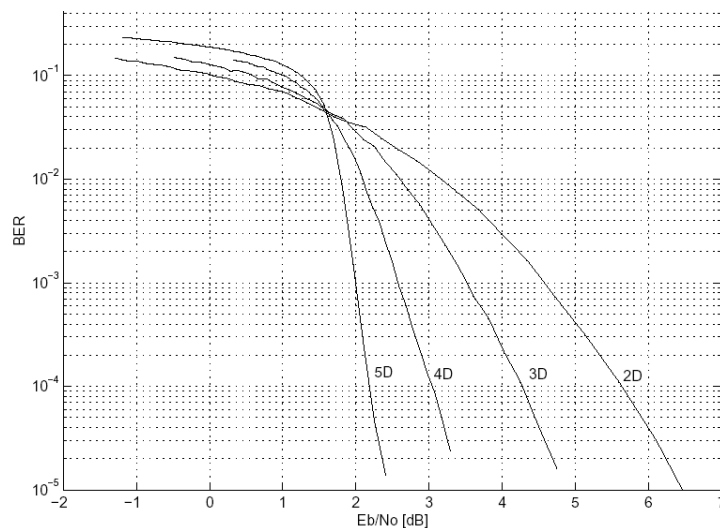


Рис. 14. Характеристики (8,7) ТРС/СПС разной размерности

Коды повторения-накопления (RA). Коды повторения-накопления (Repeat-Accumulate – RA) [21] сочетают в себе достоинства турбо кодов (линейная сложность кодирования) и низкоплотностных кодов (линейная сложность декодирования). Данные коды являются разновидностью кодов с последовательным каскадированием. Общая схема кодера RA кода представлена на рис. 15. Кодер состоит из повторителя, перемежителя и аккумулятора. В роли последнего обычно выступает рекурсивный сверточный кодер с кодовой скоростью 1. Итоговая кодовая скорость RA кода оказывается равной $1/q$, где q – число повторений информационных символов кода повторителем. Код с такой структурой легко описывается с помощью графа Таннера и, следовательно, к нему можно применять итеративный BP алгоритм декодирования или его разновидности. Пример графа Таннера для RA кода показан на рис. 16.



Рис. 15. Кодер RA кода

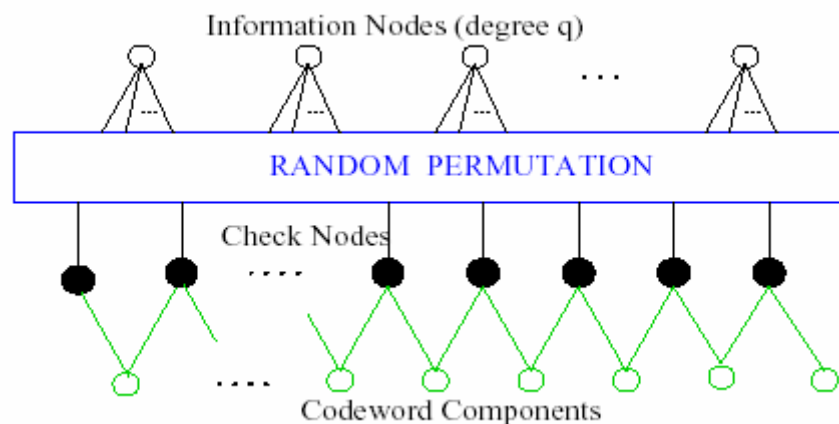


Рис. 16. Граф Таннера для RA кода

Рис. 17 отражает характеристики обычных RA кодов для длин блоков 4096 и 16384 и числа повторений информационных символов $q=3$ и 4.

Развитием RA кодов являются нерегулярные RA (Irregular Repeat Accumulate – IRA) коды. Введение нерегулярности в структуру RA кодов позволяет так же, как в случае LDPC кодов, существенно улучшить их эффективность. Обычно IRA коды строятся путем повторения различных информационных символов различное число раз. В этом случае код задается набором значений f_i , определяющих долю информационных бит, повторяющихся i раз. Пример графа Таннера для нерегулярного RA кода показан на рис. 18. На рис. 19 отражены характеристики IRA кодов с кодовой скоростью $1/2$ для различных длин кода. Видно, что эффективность IRA кодов оказывается лучше эффективности регулярных RA кодов. Для сравнения на данном рисунке также приведены характеристики турбо кодов с сопоставимыми параметрами.

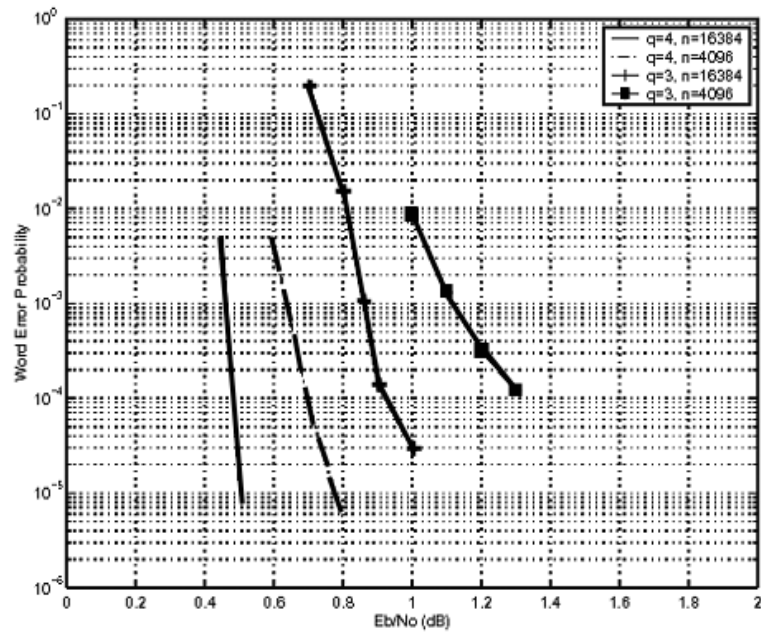


Рис. 17. Эффективность RA кодов для длин блока 4096, 16384 и $q = 3$ и 4

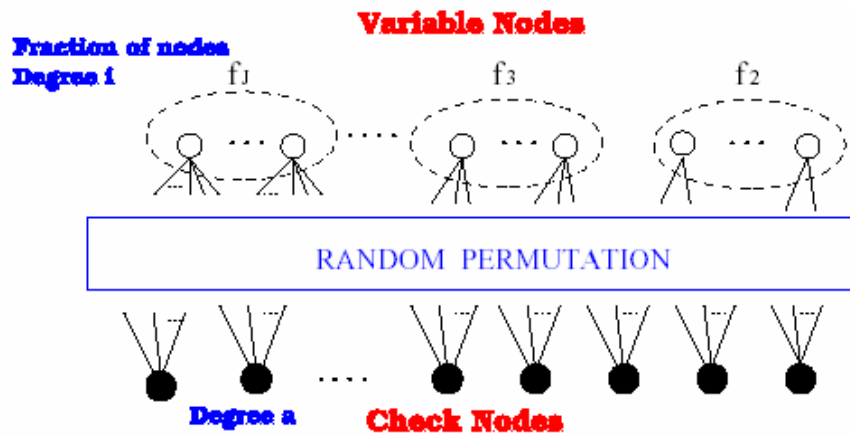


Рис. 18. Граф Таннера для IRA кода

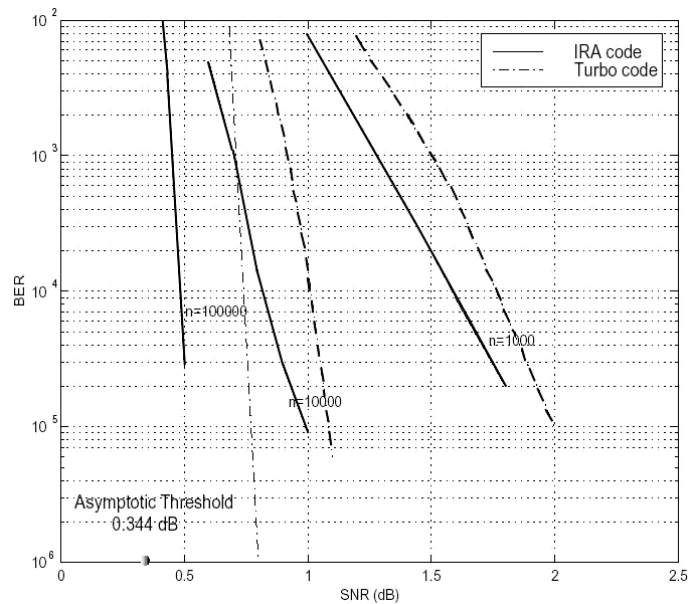


Рис. 19. Эффективность IRA кодов с $R=1/2$ для длин блока $10^3, 10^4, 10^5$

К недостаткам IRA кодов можно отнести значительное число итераций декодирования, которое при работе вблизи пропускной способности канала может достигать нескольких сотен, что приводит к значительному времени декодирования информационных символов.

Коды произведения-накопления (РА). Еще одним классом кодов с последовательным каскадированием являются коды произведения-накопления (Product Accumulate – PA) [22]. В данных кодах осуществляется каскадирование внешнего TPC/SPC кодов и рекурсивного сверточного кода с кодовой скоростью 1, в качестве которого обычно выступает аккумулятор. РА коды, также как и RA коды, характеризуются линейной сложностью кодирования и декодирования.

Среди РА кодов выделяют две разновидности: РА-I и РА-II коды. Внешний декодер РА-I кодов образуется путем параллельного соединения двух кодов с контролем четности через перемежитель (рис. 20). В случае использования блочного перемежителя, в котором информация записывается по строкам, а считывается по столбцам, внешний код становится обычным TPC/SPC кодом. Как следует из описания схемы кодирования, кодовая скорость РА-I кода равна $t/(t+2)$, где t – число информационных символов кода с контролем четности.

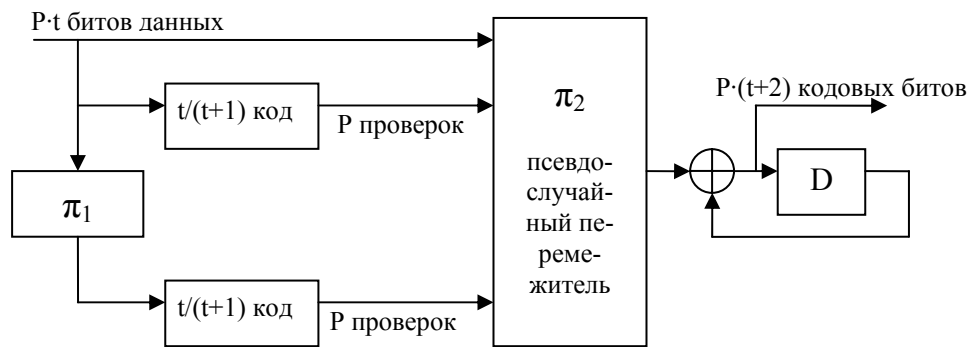


Рис. 20. Кодер РА-I кода

Внешний кодер РА-II кода состоит из параллельно связанных двумерных TPS/SPC кодов (рис. 21). В результате формируется $(P(t+1)^2, Pt^2)$ блочный код с кодовой скоростью $t^2/(t+1)^2$.

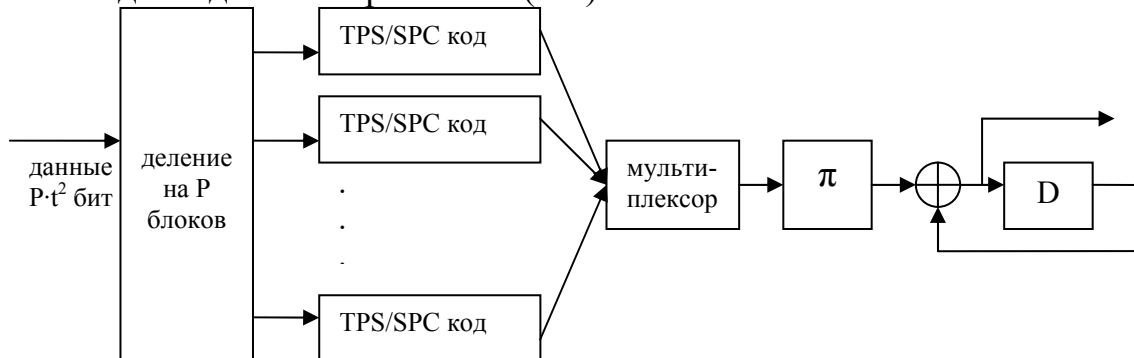


Рис. 21. Кодер РА-II кода

Для декодирования РА кодов используется ВР алгоритм, работающий с графом Таннера РА кода (рис. 22). Эффективность РА-I и РА-II кодов в гауссовском канале представлена на рис. 23 и 24. Отметим, что характеристики

РА-I кода получены для кодовой скорости 1/2, а характеристики РА-II кодов – для более высоких кодовых скоростей.

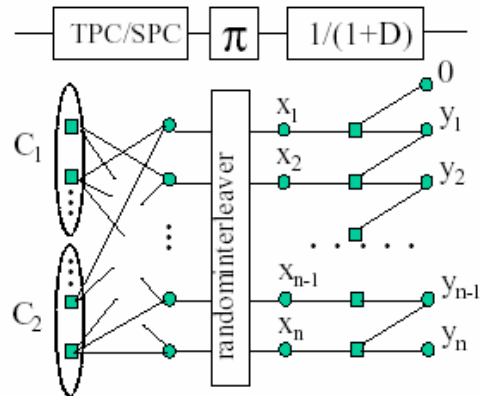


Рис. 22. Граф Таннера РА кода

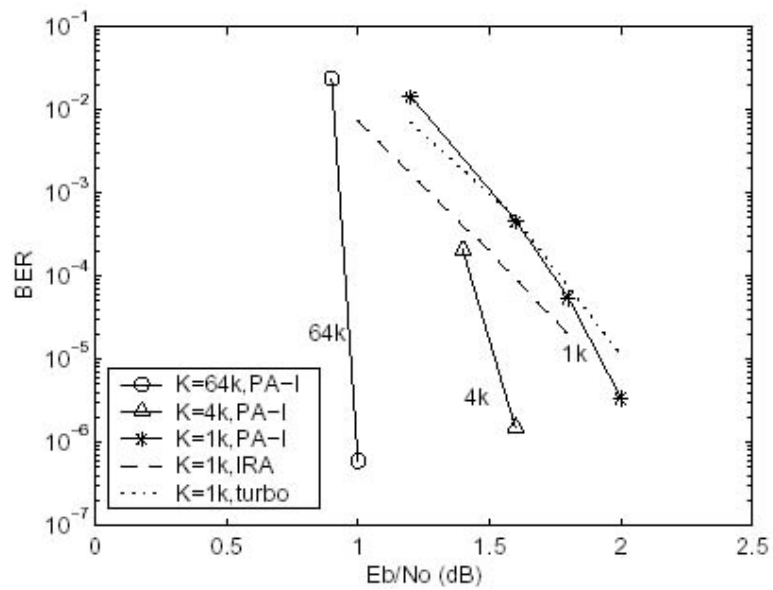


Рис. 23. Характеристики РА-I кода с кодовой скоростью 1/2

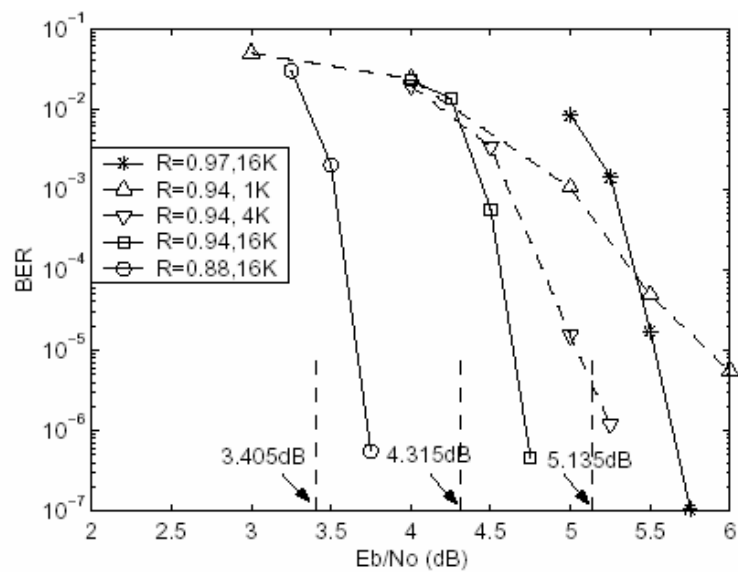


Рис. 24. Характеристики РА-II кода

Сложность декодирования РА кодов оказывается примерно равной $(7+13/R)$ операций для декодирования одного информационного бита на одной итерации [22].

Каскадные коды, декодируемые с использованием многопорогового декодера. Высокие характеристики МПД способствуют его широкому применению в составе различных кодовых конструкций, поскольку эффективность последних непосредственно связана с эффективностью их составных элементов.

Среди возможных подходов к улучшению характеристик МПД следует выделить такие схемы кодирования, как параллельные коды [23], коды с неравномерной энергетикой и коды с выделенными ветвями. Хотя отдельное использование каждого из данных подходов приводит лишь к незначительному (0,3...0,7 дБ) повышению эффективности по сравнению с обычным МПД, совместное применение этих схем позволяет добиться превосходных результатов.

Особое место среди кодовых схем на базе МПД занимает каскадирование с кодами контроля по четности (ККЧ) [24] использование которых также позволяет повысить эффективность применения кодирования. Особенность данной схемы заключается в том, что такое каскадирование практически не требует дополнительных затрат на оборудование (в схему кодирования требуется добавить лишь один сумматор по модулю 2), тогда как использование в каскадном коде, например, кодов Рида-Соломона несравненно труднее.

На рис. 25 представлены верхние оценки вероятностей ошибки для СОК с $d=7, 9, 11$ (здесь и далее считается, что данные СОК декодируются с помощью МПД) и каскадной схемы на его основе (длина ККЧ $n_1=25$). Методика оценки вероятности ошибки подробно рассмотрена в [24]. На этом же рисунке показаны результаты моделирования каскадного кода на базе СОК с $r=1/2$, $d=7$ и $d=9$. Заметим, что использование простейшего ККЧ совместно с СОК позволяет получить дополнительный энергетический выигрыш около 1...1,5 дБ при вероятности ошибки на выходе декодера $P_b=10^{-5}$.

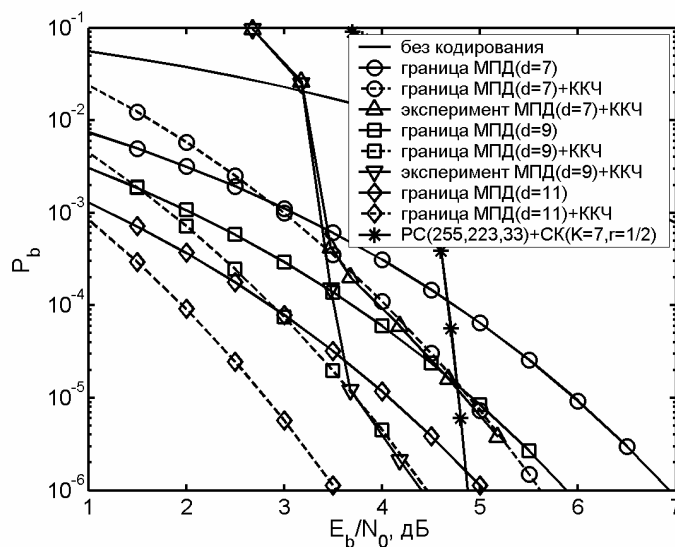


Рис. 25. Эффективность каскадного кода на базе МПД в ДСК

Эффективность работы каскадной схемы, состоящей из тех же СОК, что и на рис. 25 и ККЧ с $n_1=50$, для канала с АБГШ отражена на рис. 26. Как видно из рисунков, и в данном случае каскадный код оказывается значительно лучше некаскадного. Следует отметить, что при получении представленных графиков ККЧ использовался на нескольких итерациях декодирования, тем самым как бы «помогая» МПД при декодировании внутреннего СОК. Также отметим, что каскадный код, состоящий из кода Рида-Соломона (255, 223, 33) и сверточного кода с кодовой скоростью $1/2$ и длиной кодового ограничения $K=7$, декодируемый с помощью оптимального алгоритма Витерби, даже при меньшей общей кодовой скорости ($R \approx 0,437$) сильно уступает каскадной схеме на базе МПД при $P_b > 10^{-6}$. К сожалению, рассмотренный способ каскадирования позволяет улучшить характеристики МПД только в области его эффективной работы.

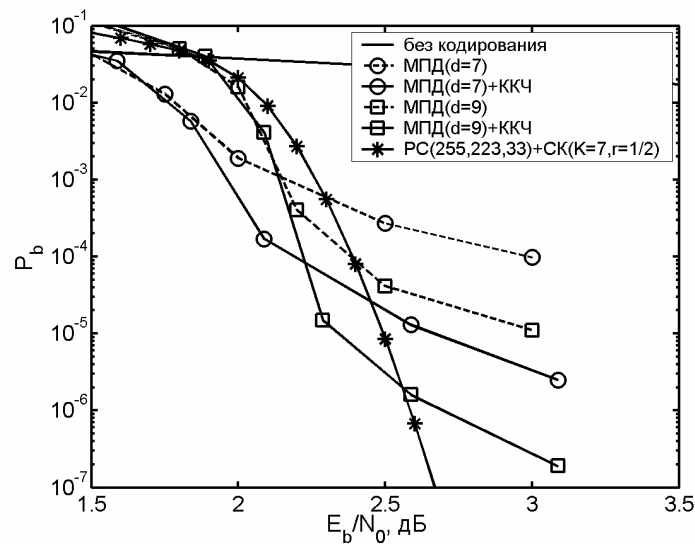


Рис. 26. Результаты моделирования каскадного кода на базе МПД в канале с АБГШ

Сложность декодирования рассмотренной каскадной схемы по сравнению со сложностью обычного МПД увеличивается на сложность декодера ККЧ. Из описания принципа работы данного декодера ясно, что при декодировании блока ККЧ, длиной n_1 символов, требуется выполнить n_1-1 сложений по модулю 2 и 1 сравнение при определении наличия ошибки в блоке, n_1-1 операций выбора максимума из двух чисел для определения символа с минимальной достоверностью и $d+1$ операций сложения по модулю 2 (инверсий) в случае необходимости коррекции информационного символа (также корректируются элементы разностного и синдромного регистров). Причем, так как коррекция осуществляется с вероятностью $P_{МПД} \ll 1$, при определении общей сложности ей можно пренебречь. В результате при декодировании одного информационного бита декодером ККЧ в среднем требуется всего $(n_1 - 1)/(n_1 - 1) \approx 2$ операции, эквивалентных сложению.

Применение многопорогового декодера в схемах с параллельным кодированием. Для приближения границы эффективной работы МПД к пропускной способности канала возможно его применение в ранее упомянутых схемах параллельного кодирования [23]. В основе построения данных схем лежит выделение в СОК C_0 с кодовым расстоянием d_0 и кодовой скоростью r_0 некоторого составляющего кода C_1 с кодовой скоростью $r_1 > r_0$, тоже являющегося СОК. Кодовое расстояние d_1 выделенного кода выбирается значительно меньшим d_0 , и, следовательно, область его эффективной работы будет ближе к границе Шеннона. При декодировании параллельного кода сначала выполняются несколько итераций декодирования составляющего кода C_1 , позволяющие примерно на порядок снизить вероятность ошибки в принятой из канала информационной последовательности, после чего в процесс декодирования включается оставшаяся часть кода C_0 . Отличительной особенностью данной схемы кодирования является то, что здесь внешний код работает с кодовой скоростью r_0 , в то время как в обычных каскадных кодах кодовая скорость внешнего кода близка к единице. Данное свойство обеспечивает существенное преимущество МПД перед другими каскадными конструкциями.

Для примера на рис. 27 представлены результаты моделирования схем с параллельным кодированием в канале с АБГШ для СОК с $r_0=6/12$, $d_0=13$ и $r_0=5/10$, $d_0=15$. В параллельном коде с $d_0=13$ в данном случае был выделен внешний код с $r_1=6/11$, $d_1=7$, а в коде с $d_0=15$ был выделен код с $r_1=5/9$, $d_1=9$. Кривые «составляющий» на рисунках отражают вероятность ошибки на выходе выделенных кодов параллельной схемы. Пунктирными линиями без маркеров на данных рисунках показаны вероятности ошибки оптимального декодирования кодов с $d=7, 9, 11, 13$ и 15 . Для сравнения на рисунке также показаны характеристики декодируемых с помощью МПД обычных СОК с аналогичными d и r .

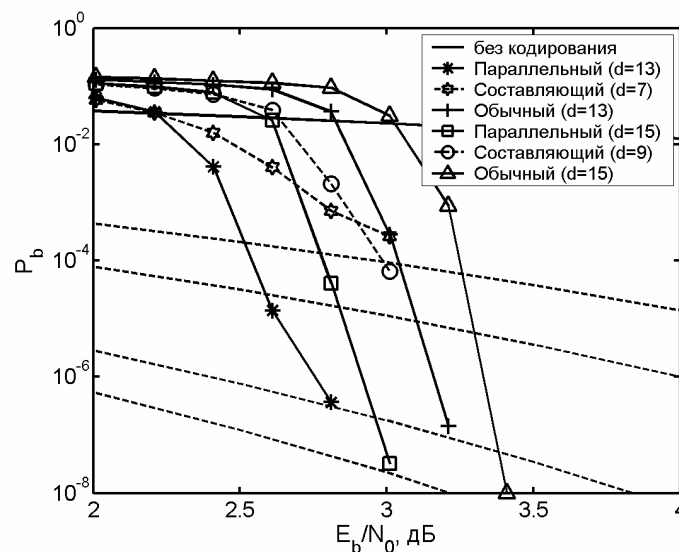


Рис. 27. Результаты моделирования параллельного кода на базе МПД в канале с АБГШ

Как следует из анализа представленных графиков, применение параллельного кодирования позволяет приблизить границу эффективной работы МПД к пропускной способности канала примерно на 0,5 дБ.

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

Приведенные результаты относились к двоичным кодам и системам с двоичной фазовой модуляцией. Но на основе важнейшего свойства сходимости решения МПД к оптимальному при всех изменениях декодируемых символов [25] реализованы недвоичные МПД, обеспечивающие характеристики, близкие или несколько более высокие, чем у кодов Рида–Соломона. Аналогично, высокие характеристики МПД, обеспечиваемые ими в каналах со стираниями и в системах с многопозиционной модуляцией делают их универсальным средством простого достижения высокого уровня помехозащищенности сообщений в системах широкого спектра применения. При этом сохраняется такая же сложность реализации, как и в простейшем пороговом декодере.

Большой объем дополнительной научной и учебно-методической информации об алгоритмах класса МПД можно найти на тематическом веб-сайте по алгоритмам МПД www.mtdbest.iki.rssi.ru.

Аппаратная реализация МПД. На сегодняшний день в НИИР уже разработан один их вариантов реализации МПД на ПЛИС Xilinx. Этот МПД является развитием с 1975 года серии декодеров сверточных кодов на базе МПД и может считаться представителем их пятого поколения.

Характеристики ПЛИС сверточного МПД при кодовой скорости $R=1/2$ представлены на рис. 28. В нем полностью реализованы все возможности алгоритмов этого класса по распараллеливанию операций декодирования на

Характеристики МПД на ПЛИС XILINX

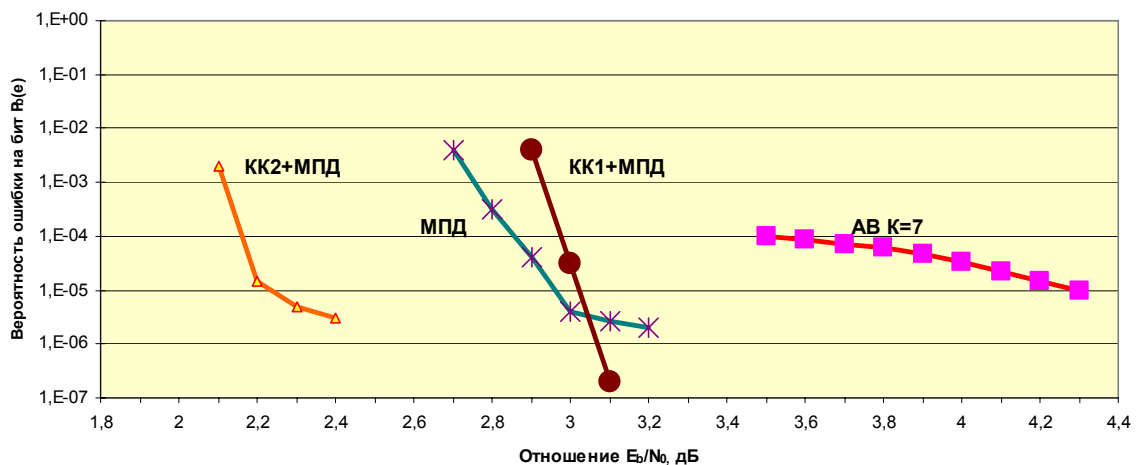


Рис. 28. Результаты ПЛИС МПД сверточного кода в канале с АБГШ

аппаратном уровне. Поэтому производительность декодера ограничивается только скоростью движения данных по его регистрам сдвига, которые относятся к самым быстрым элементам схемотехники ПЛИС. Этим и определяется очень высокая производительность МПД на ПЛИС, которая составляет в различных реализованных вариантах этого декодера от 160 до 480 Мбит/с и может быть еще существенно увеличена.

Как следует из вида графиков, представленных на рис. 28, очень простой сверточный МПД с быстродействием порядка 200 Мбит/с и с задержкой около 10000 битов оказывается на 1,5 дБ лучше стандартного АВ с длиной кодового регистра $R=7$. Напомним, что улучшение ЭВК даже на 0,1 дБ считается очень серьезным достижением. Поэтому такая большая разница в ЭВК между АВ и МПД при фактически неограниченной производительности последнего позволяет утверждать, что создание в НИИР современных версий алгоритмов МПД на новейшей элементной базе является важнейшим научным и технологическим достижением в области методов помехоустойчивого кодирования.

На рис. 28 графики КК1 и КК2 показывают возможности ранее рассмотренных каскадных схем с МПД, использующих в качестве внешнего кода коды контроля на четность. Общая кодовая скорость этих каскадных схем остается близкой к $R \sim 1/2$. В первом случае для КК1 задержка декодирования составляет порядка 10000 битов, во втором, для КК2, она близка к 40000 битов. В обоих вариантах реализации каскадных схем производительность декодеров превышает 150 Мбит/с и также может быть значительно увеличена. Подчеркнем, что реализованное в МПД каскадирование с кодами контроля по четности, для чего в схему кодирования добавляется всего один полусумматор, оказывается несравненно проще, чем в каскадной схеме АВ с кодами Рида-Соломона. При этом каскадная схема с МПД оказывается эффективнее как по ЭВК, так и по кодовой скорости.

Заключение. Огромное преимущество МПД перед всеми другими схемами декодирования по числу операций и возможность их полного распараллеливания при аппаратной реализации позволяют считать, что в результате 30-летних исследований в НИИРадио разработан широкий класс многопороговых алгоритмов, которые могут быть признаны основным методом кодирования для многих современных высокоскоростных систем связи с предельно возможными уровнями энергетического выигрыша и очень высоким быстродействием.

Методы МПД в области высоких шумов канала уже сейчас позволяют обеспечить требуемый уровень энергетичности канала наиболее простыми способами. Декодеры МПД много лет успешно работают в уже разработанных в НИИР системах спутниковой связи.

Возможности современной технологии позволяют даже для высокоскоростных каналов разрабатывать аппаратно-программные версии МПД декодеров, которые будут успевать выполнять достаточно большое число операций с каждым декодируемым символом. Это создает условия для реализации все более сложных кодовых конструкций. Высокие характеристики МПД

очень наглядно иллюстрируют ту очевидную истину, что те алгоритмы, которые нерационально используют вычислительные ресурсы, будут всегда значительно проигрывать гораздо более простым методам, которые решают проблему декодирования более эффективно.

Несомненно, что проблемы сложности реализации кодирования сохранятся в обозримом будущем, а в связи с ростом скоростей обмена информацией требования более простой реализации декодеров будут все актуальнее. Самыми дешевыми при всех вариантах реализации окажутся те алгоритмы, которые выполняют только очень простые, однородные и быстрые операции. Наиболее полно этим требованием удовлетворяют МПД. А соответствие его возможностей характеристикам самых сложных алгоритмов делает МПД еще более привлекательным.

Таким образом, последнее десятилетие создало условия для достижения в реальной каналообразующей аппаратуре систем связи уровня энергетики, весьма близкого к теоретическим пределам для каналов космической и спутниковой связи. Высокие характеристики, кроме МПД, могут обеспечить всего несколько методов. Но учет проблемы сложности при сопоставимых уровнях ЭВК показывает, что в этом случае алгоритмы на базе МПД сохраняют близость по своей сложности реализации к простейшему декодеру порогового типа и поэтому в большинстве случаев применения кодирования являются наиболее предпочтительными методами декодирования в приемлемых по стоимости высокоскоростных системах связи.

ЛИТЕРАТУРА

1. Берлекэмп Э.Р. Техника кодирования с исправлением ошибок // ТИИЭР, 1980, Т. 68, №5. С. 24–58.
2. Витерби А. Границы ошибок для сверточных кодов и асимптотически оптимальный алгоритм декодирования // Некоторые вопросы теории кодирования. М.: Мир, 1970. С. 142–165.
3. Месси Дж. Пороговое декодирование / Пер. с англ.; Под ред. Э.Л. Блоха. М.: Мир, 1966. 208 с.
4. Самойленко С.И., Давыдов А.А., Золотарев В.В., Третьякова Е.И. Вычислительные сети. М.: Наука, 1981. 277 с.
5. Zolotarev V.V. The Multithreshold Decoder Performance in Gaussian Channels // Proc. 7th Intern. Symp. on Commun. Theory and Applications 7ISCTA'03 (St. Martin's College, Ambleside, UK, 13–18 July). 2003. P. 18–22.
6. Золотарев В.В., Овечкин Г.В. Помехоустойчивое кодирование. Методы и алгоритмы. Справочник. М.: Горячая линия – Телеком, 2004. 126 с.
7. Золотарев В.В., Овечкин Г.В. Эффективные алгоритмы помехоустойчивого кодирования для цифровых систем связи // Электросвязь. 2003. № 9. С. 34–37.
8. Форни Д. Каскадные коды: Пер. с англ. под ред. Самойленко С.И. – М.: Мир, 1970. 208 с.
9. Berrou C., Glavieux A., Thitimajshima P. Near Shannon Limit Error-Correcting Coding and Decoding: Turbo Codes // Proc. of the Intern. Conf. on Commun (Geneva, Switzerland). 1993, May. P. 1064–1070.
10. Seghers J., On the Free Distance of TURBO Codes and Related Product Codes,» Final Report, Diploma Project SS 1995, Number 6613, Swiss Federal Institute of Technology Zurich, Switzerland, August 1995.

11. Золотарев В.В., Овечкин Г.В. Сложность реализации эффективных методов декодирования помехоустойчивых кодов // Проблемы передачи и обработки информации в сетях и системах телекоммуникаций: Тез. докл. 12-й Междунар. науч.-техн. конф. – Рязань: РГРТА, 2004. – С. 12–14
12. Andrews K., Berner J., Chen V. et al. Turbo-decoder implementation for the deep space network // IPN Progress Report 42–148. – Feb. 15, 2002.
13. D. J. C. MacKay and R. M. Neal, “Near Shannon limit performance of low density parity check codes,” IEEE Electronics Letters, vol. 32, no. 18, pp. 1645–1646, Aug. 1996.
14. Gallager R. Low-density parity-check codes // IRE Trans. Information Theory, pp. 21–28, January 1962.
15. M. G. Luby, M. Mitzenmacher, M. A. Shokrollahi, and D. A. Spielman, “Improved low-density parity-check codes using irregular graphs,” IEEE Trans. Inform. Theory, vol. 47, no. 2, pp. 585–598, Feb. 2001.
16. M. Ardakani, “Efficient Analysis, Design and Decoding of Low-Density Parity-Check Codes” Ph.D. dissertation, University of Toronto, 2004
17. Richardson T., Shokrollahi M., Urbanke R. Design of capacity-approaching irregular low-density parity-check codes // IEEE Trans. Inform. Theory, vol. 47, pp. 638–656, Feb. 2001.
18. Y. Weiss and W. T. Freeman, “On the optimality of solutions of the max-product belief-propagation algorithm in arbitrary graphs,” IEEE Trans. Inform. Theory, vol. 47, no. 2, pp. 736–744, Feb. 2001.
19. Press Release, AHA announces Turbo Product Code Forward Error Correction Technology (Nov. 2). – 1998.
20. Williams D. Turbo Product Code FEC Contribution // IEEE 802.16.1pc-00/35. – 2000. – June 19.
21. Jin H., Khandekar A., McEliece R. Irregular repeat-accumulate codes // Proc. 2nd Int. Symp. on Turbo Codes and Related Topics (Brest, France). 2000, Sept. P. 1–8.
22. J. Li, K.R. Narayanan, C.N. Georghiades, “Product accumulate codes: A class of capacity-approaching, low-complexity codes”, submitted to IEEE Trans. Inform. Theory, 2001.
23. Золотарев В.В. Параллельное кодирование в каналах СПД // Вопросы кибернетики. 1986. Вып. 120. С. 56-58.
24. Золотарев В.В., Овечкин Г.В. Использование многопорогового декодера в каскадных схемах // Вестник РГРТА. 2003. Вып. 11. С. 112–115.
25. Золотарев В.В. Недвоичные многопороговые декодеры // Цифровая обработка сигналов. 2003. № 3. С. 10–12.
26. Веб-сайт www.mtdbest.iki.rssi.ru.