

Алгоритмы многопорогового декодирования для гауссовских каналов¹

В.В.Золотарёв*, Г.В.Овечкин**

*Институт космических исследований РАН, Москва, Россия

**Рязанский государственный радиотехнический университет, Рязань, Россия

Поступила в редколлегию 10.03.2008

Аннотация—Рассмотрены основные принципы метода многопорогового декодирования линейных кодов как поиска глобального экстремума функционала от большого числа переменных. Показано, что эффективность многопорогового декодирования близка к результатам, обеспечиваемым оптимальными переборными методами. Даются оценки сложности декодирования при программной и при аппаратной реализации.

1. ВВЕДЕНИЕ

Как известно, применение помехоустойчивого кодирования позволяет решать большое число задач в цифровых сетях, которые были принципиально недоступны при аналоговой обработке сигнала. Основное преимущество систем связи, использующих кодирование, состоит в том, что эффективность использования каналов, т.е. их к.п.д., оказывается во много раз более высокой, чем в случае, когда коды не используются. Мерой роста эффективности обычно выбирается энергетический выигрыш кодирования (ЭВК), который указывает, на сколько можно снизить удельную энергетическую нагрузку канала, т.е. отношение средней энергии передачи одного бита данных к спектральной плотности мощности шума E_b/N_0 при использовании некоторых методов кодирования и декодирования по сравнению с их отсутствием, чтобы обеспечить сохранение той высокой достоверности передачи, которая необходима в данной системе. Например, требуемая вероятность ошибки на бит $P_b(e)$ должна составлять 10^{-6} . Этими возможностями и определяется необходимость применения кодирования и для систем космической, спутниковой и мобильной связи.

Способность кодов обеспечивать высокодостоверную передачу данных при небольшом уровне сигнала позволяет минимизировать размеры аппаратуры, повысить скорость передачи по очень дорогим каналам цифровой связи, существенно уменьшить размеры антенн или многократно увеличить срок службы автономных источников питания. При этом во многих случаях величина ЭВК может достигать 10 дБ и более. Кроме того, важно подчеркнуть, что необходимая достоверность передачи данных в каналах с шумами и системах хранения цифровой информации в дальнейшем будет только расти, что при прочих равных условиях приведёт к ужесточению требований, предъявляемых к системам кодирования. А это, в свою очередь, будет способствовать росту обеспечиваемого ими ЭВК, что необходимо осуществить наименее дорогими способами именно на основе эффективных кодов и обязательно очень простых и быстрых декодеров.

В цифровой связи сейчас используются как декодеры, реализующие хорошо известный специалистам алгоритм Витерби (АВ) [1], так и значительно более сложные кодовые конструкции, такие как турбо коды [2] и низкоплотностные коды [3]. Однако применяемые в настоящее время системы кодирования, особенно для высокоскоростных каналов, всё ещё очень сложны или

¹ Работа выполнена при поддержке РФФИ (грант №08-07-00078а)

малоэффективны. Ниже рассмотрены теоретические основы и конкретные характеристики высокоэффективного, быстродействующего и очень простого итеративного алгоритма коррекции ошибок в каналах с большим уровнем шума, являющегося результатом развития идей мажоритарного декодирования линейных сверточных кодов [4].

2. ПРИНЦИП ПОВТОРНОГО ДЕКОДИРОВАНИЯ

За последние десятилетия теория и техника помехоустойчивого кодирования продвинулись далеко вперед. Предложенные в 70-х годах прошлого века многими авторами методы повторного декодирования принятых сообщений, оказались малоэффективными вследствие сильного группирования ошибок на выходе декодера. Пример такой схемы с пороговым декодером (ПД) [4] для сверточного кода приведен на рисунке 1.

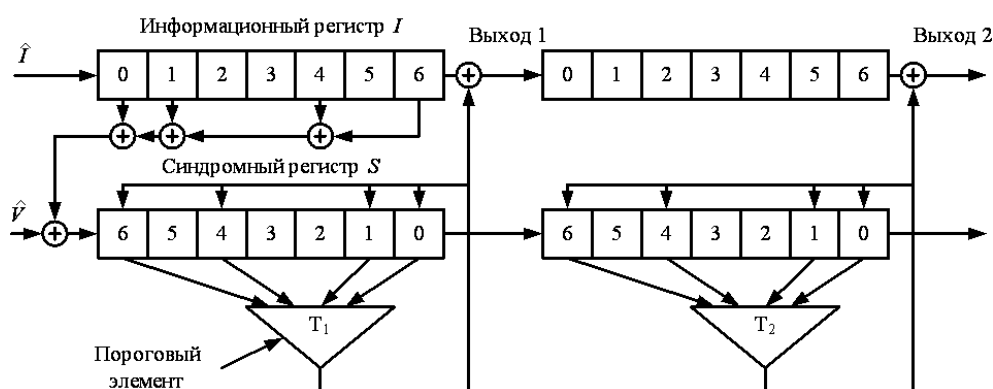


Рис. 1. Пример схемы повторного декодирования на основе порогового декодера сверточного кода

Малая эффективность подобной схемы декодирования была следствием сильного группирования, т.е. размножения ошибок в пороговом декодере. В самом деле, если при некотором уровне шума в двоичном симметричном канале с независимыми ошибками в какой-то момент ПД принял неправильное решение об очередном информационном символе, то обычно на выходе этого ПД далее появлялся очень плотный пакет ошибок. Например, пусть с выхода первого ПД на рисунке 1 на вход второго поступила немного улучшенная при первой попытке декодирования последовательность. Тогда если ошибок в некоторой части информационной последовательности после первого ПД нет, то второй декодер не нужен. Но при появлении на выходе первого ПД ошибки, которая обычно является началом типичного пакета ошибок этого ПД, оказывается, что второй декодер, точно повторяющий схему первого и настроенный на исправление только случайных ошибок, скорее всего, не исправит этот пакет. Следовательно, он не нужен и в этом случае.

Подчеркнем, что коды с малым уровнем размножения ошибок в ПД в те годы были совершенно неизвестны. Однако позже эта проблема была полностью решена методами, описанными в [5]–[15]. В связи с этим приобретает важное значение рассмотренный ниже новый подход к реализации простых эффективных процедур исправления ошибок, который развивается с 1972 г. и назван многопороговым декодированием (МПД) [5].

3. ПРИНЦИП ГЛОБАЛЬНОЙ ОПТИМИЗАЦИИ ФУНКЦИОНАЛА

Развитие методов декодирования помехоустойчивых кодов в течение длительного времени удивительным образом никак не было связано с методами решения задачи оптимизации

функционала от многих дискретных переменных. Тем не менее, декодирование, т.е. поиск единственного кодового слова из экспоненциально большого числа возможных сообщений, совершенно естественно было бы рассматривать именно с таких позиций. Однако большинство разработывавшихся ранее алгоритмов декодирования никак не использовало для поиска наилучших решений декодера хорошо известные разнообразные мощные оптимизационные процедуры, которые вполне можно было бы применить к поиску кодовых слов, находящихся на минимально возможном расстоянии от принятого сообщения. Заметим, что широко применяемый в технике связи алгоритм Витерби, используемый для декодирования по максимуму правдоподобия коротких свёрточных кодов, также не относится к классу оптимизационных процедур, поскольку он непосредственно ищет оптимальное решение на основе очень удобного в реализации метода полного перебора.

Вместе с тем некоторые алгоритмы декодирования, в частности, пороговые декодеры [4], относящиеся к простейшим методам коррекции ошибок, почти уже обладают именно теми свойствами, необходимыми для реализации полноценных эффективных и одновременно исключительно простых итеративных процедур декодирования, которые действительно были бы методами поиска глобального экстремума функционала от очень большого числа переменных.

Для подтверждения этого рассмотрим пример простейшей системы кодирования/порогового декодирования с кодовой скоростью $R = 1/2$ и минимальным кодовым расстоянием $d = 3$, показанный на рисунке 2.

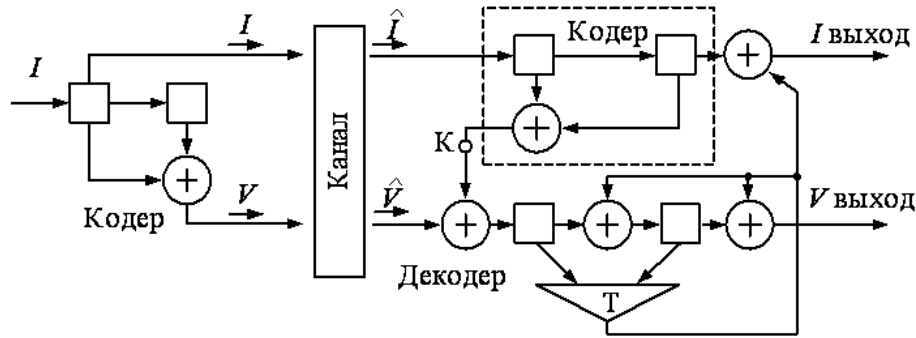


Рис. 2. Специальный вид системы кодирования, поясняющий новую интерпретацию вектора синдрома

Как следует из вида кодера и простейшего мажоритарного декодера, исправляющего в этом простом примере одну ошибку, в состав этого декодера входит точная копия кодера, которая формирует свои оценки проверочных символов кода по принятым из канала, возможно, с ошибками информационным символам кода. Эти символы появляются в точке K декодера и затем, после сложения на полусумматоре с принятыми из канала проверочными символами \hat{V} образуют символы вектора синдрома S , который зависит только от вектора ошибок канала. Эти символы и поступают потом на пороговый элемент декодера из синдромного регистра, как это показано на рисунке 2.

Уже сам вид ПД на представленной схеме кодирования/декодирования позволяет указать простой способ организации правильной процедуры оптимизации, т.е. поиска наилучшего возможного решения при декодировании. Укажем для этого на факт, который никогда не отмечался ранее: в регистре синдрома декодера находится разность по проверочным символам между принятым с искажениями из канала вектором $Q = [\hat{I}, \hat{V}]$ и таким кодовым словом A_r , информационные символы которого совпадают с принятой из канала информационной частью вектора Q .

Значит, полная разница между кодовым словом – текущей гипотезой-решением декодера A_i о переданном кодовом слове и принятым зашумленным вектором Q будет в таком модифицированном декодере мажоритарного типа, где в ПД будет добавлен ещё всего лишь один вектор, который всегда должен соответствовать разности между принятым вектором Q и A_i – текущей гипотезой декодера по информационным символам. В таком декодере и будет содержаться текущее значение полной разности и, следовательно, полное расстояние между решением декодера и принятым вектором. Это расстояние следует стремиться уменьшить до минимально возможного, что и будет соответствовать решению оптимального декодера.

4. ПРИНЦИПЫ РАБОТЫ МПД

Именно такой подход к проблеме высокоэффективного декодирования и является основой развиваемых с 1972 года специальных итеративных многопороговых декодеров [5]–[15], почти совпадающих с классическим ПД и таких же простых в реализации, как и их прототип.

Изменения, которые необходимо сделать в обычном ПД, чтобы преобразовать его в МПД, как следует из обсуждения принципа глобальной оптимизации в предыдущем разделе, состоят просто в том, что решения всех пороговых элементов об изменениях декодируемых символов сначала запоминаются в дополнительном разностном регистре D , первоначально, естественно, нулевым. Эти решения затем используются последующими пороговыми элементами декодера в качестве дополнительной проверки при дальнейшем уточнении значений декодируемых символов. Такой декодер уже измеряет полные расстояния между всё более новыми и более правдоподобными потенциальными решениями и принятым вектором Q . Он изменяет декодируемые символы так, что каждое новое решение такого МПД всегда ближе к принятому из канала вектору. Это позволяет во многих случаях практически полностью реализовать корректирующие возможности используемых кодов. Примеры конкретных схем МПД приведены в [9, 10].

Декодер после этого достаточно простого усовершенствования приобретает новые чрезвычайно полезные свойства. Решения МПД при каждом изменении декодируемых им информационных символов строго приближаются к решению оптимального декодера, обеспечивая во многих случаях реализацию этого процесса даже после нескольких десятков попыток коррекции кодового блока или потока символов свёрточного кода. Разумеется, для обеспечения высокой эффективности МПД при больших шумах канала необходимо выбирать только специальные коды с малым уровнем размножения ошибок. Этот важный вопрос рассматривался в [6, 8, 9].

Рассмотрим далее описанные возможности МПД более формально.

5. ОСНОВНАЯ ТЕОРЕМА МПД

Пусть задан двоичный линейный систематический блочный или свёрточный самоортогональный код [16] со скоростью передачи $R = k/n$, где k – число информационных символов, n – длина кодовой комбинации.

При передаче по ДСК без памяти оптимальный декодер, минимизирующий среднюю вероятность ошибки, из множества 2^k равновероятных кодовых слов $\{A\}$ выбирает такой вектор A_0 , для которого расстояние Хэмминга $r = |Q \oplus A|$, где Q – принятое сообщение, \oplus – сложение по mod 2, было бы минимальным по всему множеству $\{A\}$.

Будем любой двоичный вектор X длины n представлять парой векторов X_I и X_V длины k и $(n - k)$ соответственно, относящихся к информационной и проверочным частям вектора:

$$X = [X_I, X_V].$$

Тогда в предположении, что проверочная матрица кода представлена в систематическом виде: $H = [C, I]$, имеет место

Лемма. Для любого кодового вектора A и принятого сообщения Q справедливо соотношение

$$A \oplus Q = [D, H[Q_I \oplus D, Q_V]], \quad (1)$$

где вектор D длины k определяется из соотношения

$$A_I = Q_I \oplus D. \quad (2)$$

Доказательство. В силу линейности кода

$$S = H[Q_I \oplus D, Q_V] = H[A_I, A_V \oplus A_V \oplus Q_V] = HA \oplus H[0_I, A_V \oplus Q_V],$$

где 0_I – нулевое информационное слово.

Так как $HA = 0$, поскольку A – кодовое слово, а $H[0_I, A_V \oplus Q_V] = A_V \oplus Q_V$, так как $A_V \oplus Q_V$ умножается только на единичную подматрицу I матрицы H , то получаем, что вектор S равен

$$S = A_V \oplus Q_V. \quad (3)$$

Проводя в правой части (1) замены с учетом (2) и (3), находим, что

$$[D, S] = [D, A_V \oplus Q_V] = [D \oplus Q_I \oplus Q_I, A_V \oplus Q_V] = A \oplus Q.$$

Таким образом, вектор синдрома S действительно, как это и было представлено на рисунке 2, есть разница по проверочным символам между пришедшим из канала частично искажённым сообщением и определённым выше кодовым словом. **Лемма доказана.**

Ее содержание заключается в том, что разность $B = Q \oplus A$ для любого принятого вектора Q и кодового слова A определяется парой векторов $[D, S]$. Перебором всех векторов A можно найти вектор A_0 , минимизирующий $|B|$ и являющийся решением оптимального декодера. В силу определения при $D = 0$ вектор S является обычным синдромом принятого сообщения Q : $S = HQ$. Для простоты изложения будем в дальнейшем и при $D \neq 0$ называть S синдромом, поскольку это обобщение естественно и не приводит в дальнейшем к каким-либо противоречиям. Отметим также, что при каждом изменении A нет необходимости заново вычислять все компоненты синдрома. Достаточно на каждом шаге изменения инвертировать только те компоненты S , которые содержат нечетное число ошибок в изменяемых информационных символах. Однако переборные алгоритмы слишком сложны.

Поэтому рассмотрим алгоритм декодирования, который очень близок к пороговому и в связи с этим весьма просто реализуем.

1. Пусть на первом подготовительном этапе декодер выполняет вычисление и запоминание вектора S . Затем начинается выполнение собственно процедуры декодирования.
2. Выбирается некоторый информационный символ i_j и для него вычисляется обычная сумма компонент синдрома s_{j_k} , содержащих в качестве слагаемых ошибку e_j в декодируемом символе i_j (т.е. сумму проверок $s_{j_k} \in \{S_j\}$, где $\{S_j\}$ – множество проверок относительно компоненты e_j , соответствующей символу i_j) и символа d_j , компоненты вектора D , также относящегося к декодируемому символу i_j :

$$L_j = \sum_{s_{j_k} \in \{S_j\}} s_{j_k} + d_j. \quad (4)$$

Будем при этом полагать, что первоначально $D = 0$, потому что перед началом операций декодирования в памяти декодера есть только принятый вектор Q и декодер не имеет никаких других более предпочтительных гипотез о переданном сообщении.

Выберем порог равным половине всех слагаемых в (4). Для самоортогональных кодов это число равно $T = d/2 = (J + 1)/2$.

3. Пусть, наконец, все $J = d - 1$ проверок, i_j и d_j инвертируются при $L_j > T$ и остаются неизменными при $L_j \leq T$.
4. Если не принято решение о прекращении процедуры декодирования, декодер возвращается в п.2.

Предлагаемая процедура при первой попытке декодирования, пока все $d_j = 0$, совпадает с обычным алгоритмом для ПД. Будем в дальнейшем называть декодер, реализующий предлагаемый алгоритм, многопороговым декодером (МПД).

При этом справедлива

Теорема (Основная теорема многопорогового декодирования). *Если на произвольном j -м шаге МПД изменяет декодируемый информационный символ i_j , то:*

- а) *при этом МПД находит новое кодовое слово A_2 , более близкое к принятому сообщению Q , чем то кодовое слово A_1 , которому соответствовало значение i_j перед j -м шагом декодирования*

$$|B_1| = |A_1 \oplus Q| > |A_2 \oplus Q| = |B_2|;$$

- б) *после окончания j -го шага возможно декодирование любого очередного символа i_k , $k \neq j$, так что при его изменении будет осуществлено дальнейшее приближение к принятому сообщению.*

Доказательство. Перед началом декодирования символа i_j согласно лемме справедливо

$$[D_1, S_1] = [A_{1I} \oplus Q_I, H[Q_I \oplus D_1, Q_V]] = A_1 \oplus Q,$$

где

$$A_1 = [A_{1I}, A_{1V}], \quad A_{1I} = Q_I \oplus D_1.$$

Вес вектора B_1 перед этим шагом, равный $|B_1| = |D_1| + |S_1|$, можно представить в виде обычной суммы весов $W_1 = L_{1j} + X$, где L_{1j} определено выражением (4) и равно сумме проверок и символа d_j на пороговом элементе; X – вес остальных компонент S_1 и D_1 , не входящих в L_{1j} .

Рассмотрим кодовый вектор A_2 , отличающийся от A_1 только в одном информационном символе i_j , и соответствующую ему разность $B_2 = A_2 \oplus Q$. Поскольку B_1 и B_2 отличаются между собой только в тех компонентах, которые поступают на пороговый элемент, то $|B_2| = L_{2j} + X$, где $L_{1j} + L_{2j} = J + 1$, потому что в силу линейности кода каждая проверка и символ d_j точно в одном из двух векторов B_i равны 1.

Так как МПД изменяет i_j , если $L_{1j} > T$, то для этого необходимо, чтобы было $L_2 < L_1$ и, следовательно, $|B_1| > |B_2|$, чем доказан пункт а) теоремы.

Далее, очевидно, если символ i_j не изменялся, то можно декодировать любой другой символ i_k , $k \neq j$, поскольку при этом сохраняются условия леммы. В случае же изменения i_j в соответствии с правилами работы МПД после декодирования i_j имеют место равенства $A_{2I} = Q_I \oplus D_2$ и $S_2 = H[Q_I \oplus D_2, Q_V]$, где D_2 отличается от D_1 в символе d_j , поскольку при изменении через

обратную связь с порогового элемента проверок, относящихся к i_j , инвертируются именно те компоненты S_1 , в которых S_2 отличается от S_1 . Отсюда получаем, что после изменения i_j для определенных выше векторов D_2 , A_2 и S_2 также имеет место равенство

$$[D_2, S_2] = A_2 \oplus Q,$$

аналогичное тому, которое имело место перед изменением i_j . Тем самым при последующих шагах декодирования и изменениях символов i_k , $k \neq j$, также будет осуществляться дальнейшее приближение к принятому из канала сообщению Q . **Основная теорема МПД доказана.**

Из этой теоремы следует, что МПД при каждом изменении декодируемых символов приближается к принятому вектору Q , отыскивая тем самым все более близкие к оптимальному решению, более правдоподобные вектора A_i . МПД просматривает и сравнивает не экспоненциально большое количество кодовых слов, а только пары, отличающиеся между собой лишь в одном информационном символе, причем, одно из сравниваемых слов находится в декодере. В случае, если второе кодовое слово окажется ближе к вектору Q , чем то, которое находится в МПД, декодер переходит к нему и дальнейшие сравнения производятся уже с новым промежуточным вектором A_i . Ясно, что в принципе можно проводить достаточно большое число попыток декодирования всех символов кода. Тем самым будет осуществляться сходимость к решению оптимального декодера – вектору A_0 . Принципиально важно, что при этом сложность МПД остаётся такой же, как и у обычного ПД – линейной.

Допустим далее, что МПД достиг решения оптимального декодера, т.е. в информационном регистре МПД находятся символы вектора A_0 . Тогда справедливо

Следствие. *МПД не изменит решения оптимального декодера.*

Доказательство. Если бы МПД изменил на некотором шаге хотя бы один информационный символ в векторе A_0 , то это означало бы, что нашелся другой кодовый вектор A^* , который ближе к Q , чем A_0 , что невозможно, потому что, по определению, ближайшим к Q словом является вектор A_0 . **Следствие доказано.**

Таким образом, показана устойчивость решения МПД относительно оптимального решения: достигнув его, МПД останется в нём. Это очень важно, поскольку алгоритм предполагает возможность многократного изменения декодируемых символов.

Можно также заметить, что при доказательстве основной теоремы МПД единственность декодируемого символа i_j не использовалась сколько-нибудь существенным образом. Отсюда следует, что данная процедура декодирования может применяться и к любой группе информационных символов [6, 8, 9].

Для применения алгоритма МПД при декодировании в канале с аддитивным белым гауссовским шумом (АБГШ) с квантованием принимаемого двоичного потока на M уровней, $M > 2$, удобно сначала переписать функцию правдоподобия L_j в виде

$$L_j = \sum_{s_{jk} \in \{S_j\}} w_{i_k} (2s_{jk} - 1) + w_{d_j} (2d_j - 1). \quad (5)$$

Для обычного двоичного симметричного канала это выражение с весами проверок w_{j_k} , равными 1, очевидно эквивалентно (4). При переходе к гауссовскому каналу, т.е. в случае $M > 2$ уровней квантования сигнала весовые коэффициенты при вычислении L_j могут выбираться как относительно небольшие вещественные или целые числа. Тогда декодируемые символы в МПД для гауссовского канала следует изменять при $L_j > 0$. При этом, если $M \gg 1$, то, как

известно, корректирующие возможности используемых кодов и хороших алгоритмов их декодирования, в том числе МПД, обычно улучшаются примерно на 2 дБ по уровню отношения сигнал/шум на входе декодера.

6. РАЗМНОЖЕНИЕ ОШИБОК ДЕКОДИРОВАНИЯ В МАЖОРИТАРНЫХ ДЕКОДЕРАХ

Из доказанных выше результатов следует, что увеличение числа попыток исправления ранее декодированных символов с помощью МПД может быть действительно полезным, поскольку при каждом изменении информационных битов кода происходит переход к более правдоподобным решениям. Однако из этого не следует, что МПД обязательно достигнет оптимального решения. Для многих кодов существует весьма большое число таких сочетаний ошибок канала, что они исправляются при оптимальном декодировании, но не исправляются с помощью МПД. В значительной мере это связано с тем, что пороговые декодеры действительно в довольно большой степени подвержены влиянию эффекта размножения ошибок. Второй и другие последовательно соединенные улучшенные ПД, из которых состоят, например, свёрточные МПД, обычно вынуждены работать в основном с потоками пакетов ошибок от предыдущих итераций декодирования декодеров.

В [6,8,9] представлен метод оценки размножения ошибок для самоортогональных кодов [16], состоящий в том, что с помощью многомерных производящих функций вероятности вычисляются оценки вероятности появления одиночных ошибок и пакетов на выходе ПД. Этот метод помогает как при отборе кодов, в наименьшей степени подверженных влиянию размножению ошибок, так и при выборе оптимальных весов и порогов в МПД, обеспечивающих наименьшие значения вероятности его ошибок декодирования.

Основой нового подхода к оценкам размножения ошибок является достаточно удобная возможность оценивать вероятности появления двух ошибок в пределах длины кодового ограничения или внутри любого кодового блока. Это позволяет обобщить этот метод на пакеты ошибок декодирования любого веса. Для обеспечения высокой эффективности МПД обычно достаточно рассматривать пакеты веса не более 3. При этом приходится проводить вычисления в пространстве параметров размерности 2^{3d} , где d – минимальное кодовое расстояние кода. Но при анализе кодов с $d \sim 7$ и более эта задача слишком сложна для вычислений.

Однако при дальнейших исследованиях были найдены методы значительного упрощения оценок вероятностей появления пакетов, которые затем позволили сформулировать комплекс критериев, по которым необходимо строить коды с очень малыми вероятностями появления пакетов ошибок при мажоритарном декодировании. Соответствующие алгоритмы построения таких кодов длины n требуют выполнения порядка n^4 операций, что позволяет искать эффективные коды до длин порядка 500000 битов. Недавно эти алгоритмы были ещё немного улучшены.

При декодировании вблизи пропускной способности канала необходимо применение только очень длинных кодов. Поэтому завершённая разработка конструктивных методов построения кодов требуемого качества полностью решила проблему выбора кодов с незначительным уровнем размножения ошибок для высокоэффективных декодеров класса МПД.

В следующих разделах рассмотрим характеристики различных декодеров многопорогового типа.

7. БАЗОВЫЕ ХАРАКТЕРИСТИКИ ЭФФЕКТИВНОСТИ МПД

Зависимость вероятности битовой ошибки $P_b(e)$ от отношения сигнал/шум E_b/N_0 в канале с АБГШ при использовании мягкого модема для многопорогового декодера самоортогональных кодов с кодовой скоростью $R = 1/2$ и различным кодовым расстоянием d представлена

на рисунке 3. Пунктиром на рисунке показана достаточно точная оценка вероятности ошибки декодирования тех же кодов с помощью оптимального декодера. Из представленных графиков видно, что МПД действительно обеспечивает близкое к оптимальному декодирование правильно выбранных кодов при весьма высоком уровне шума в канале связи.

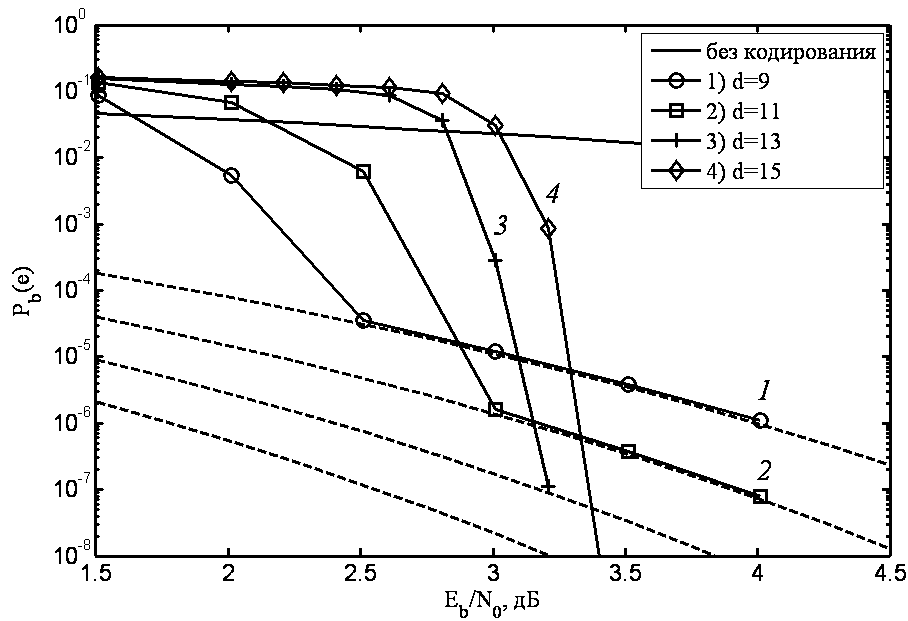


Рис. 3. Характеристики МПД для кода с $R = 1/2$ в канале с АБГШ

8. СЛОЖНОСТЬ РЕАЛИЗАЦИИ АЛГОРИТМА МПД

Главным достоинством МПД является крайне малая сложность декодирования. Как и в случае обычного ПД, в МПД на каждой итерации суммируются взвешенные проверки, которые сравниваются с порогом и изменяются вместе с декодируемым символом, если этот порог превышен. Число итераций декодирования I в этом случае обычно не более 50, а общая сложность декодирования с помощью МПД, очевидно, оценивается для $d < 25$ как

$$N_1 \sim (d + 2)(I + 4).$$

Но объём повторяющихся вычислений сумм на пороге можно значительно снизить, поскольку символы на каждом из пороговых элементов изменяются в процессе декодирования весьма редко. Если при тех же условиях на I и d возможно ухудшение характеристик МПД всего на 0,1 дБ по энергетике, что обычно вполне допустимо, то объём вычислений в МПД ещё более уменьшается:

$$N_2 \sim c_1 d + c_2 I,$$

где константы c_1 и c_2 – небольшие целые числа [8, 9, 10].

То, что при декодировании фактически каждая итерация в МПД требует всего несколько простейших операций типа сложение и сравнение, приводит к тому, что рост числа итераций почти не снижает реального быстродействия декодера, например, в программном варианте реализации. В качестве хорошей иллюстрации этого свойства алгоритма можно сослаться на демонстрационную программу МПД для свёрточного кода с $R = 3/4$. Она используется в системе специального

цифрового телевидения и обеспечивает на обычном персональном компьютере производительность порядка $4 \dots 10$ Мбит/с, чего с огромным запасом хватает для обработки телевизионного цветного сигнала при весьма низком отношении сигнал/шум. Применяемые в ней коды проходят процедуру стандартизации. Демопрограмма и простая инструкция по её использованию может быть переписана с большого тематического веб-сайта ИКИ РАН www.mtdbest.iki.rssi.ru, где она размещена на учебной страничке. Действительно, сравнение МПД с другими методами показало, что скорость обработки на основе МПД оказывается примерно на 2 порядка более высокой, чем, например, у турбо декодеров с сопоставимыми параметрами энергетической эффективности [17]. Там же можно найти демопрограмму для LDPC кода.

В случае аппаратной реализации МПД, например, на ПЛИС Xilinx или Altera, проведённые испытания подтвердили хорошие параметры их эффективности при одновременно очень высокой производительности, вплоть до 1,6 Гбит/с. Такая возможность появилась после реализации запатентованных технических решений для аппаратного МПД. Согласно этим решениям такой декодер превращается в одноктактную решающую схему, причём на каждом такте работы он может принимать до 40 решений о декодируемых символах, а предельная частота тактов определяется максимально возможной скоростью сдвига принятых из канала данных по регистрам сдвига декодера, из которых он в основном и состоит. Типичная скорость продвижения информации по регистрам сдвига указанных ПЛИС находится в пределах от 100 до 250 Мбит/с, а число параллельно работающих регистров такого вида в МПД может превышать сотню. Это значит, что производительность МПД в аппаратном варианте реализации формально может существенно превышать даже 10 Гбит/с. По существу это снимает все ограничения по скорости обработки на такие устройства, что при обеспечиваемых многопороговыми алгоритмами энергетических параметрах эффективности делает их единоличными лидерами среди всех методов высокоскоростной передачи цифровых потоков по дорогим спутниковым и прочим каналам. В частности, особенно полезны уже разработанные аппаратные версии МПД для систем дистанционного зондирования Земли, поскольку как раз их высокоскоростные потоки цифровых данных при ограниченной мощности передатчиков следует всемерно защищать методами помехоустойчивого кодирования. Фото быстродействующего макета МПД декодера на ПЛИС Altera приведено на рисунке 4.

9. ПРИМЕНЕНИЕ МНОГОПороГОВЫХ ДЕКОДЕРОВ В СХЕМАХ С ПАРАЛЛЕЛЬНЫМ КОДИРОВАНИЕМ

Для приближения границы эффективной работы МПД к пропускной способности канала возможно его применение в схемах параллельного каскадирования [9, 10, 18]. В основе построения данных схем лежит выделение в самоортогональном коде 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 самоортогональным. Кодовое расстояние d_1 выделенного кода выбирается значительно меньшим d_0 , и, как следует из рисунка 3, 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 параллельного каскадирования 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 рисунке 5 представлены результаты моделирования схем с параллельным кодированием в канале с АБГШ для самоортогонального кода с $R_0 = 6/12$, $d_0 = 13$



Рис. 4. Макет МПД декодера на ПЛИС Altera

и $R_0 = 5/10$, $d_0 = 15$ (кривые «Параллельный»). 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 $d = 7, 9, 13$ и 15 . Для сравнения на рисунке 5 также показаны характеристики декодируемых с помощью МПД обычных самоортогональных кодов с аналогичными d и R (кривые «Обычный»). Отметим, что при получении данных характеристик использовались достаточно короткие коды, длиной до нескольких тысяч битов, и от 10 до 20 итераций декодирования. При некотором увеличении объема памяти декодера и числа выполняемых итераций с помощью параллельного каскадирования уже удалось получить характеристики, представленные на рисунке 5 кривой «Длинный». Как следует из анализа представленных графиков, применение параллельного кодирования позволяет МПД работать чуть больше чем в 1,5 дБ от пропускной способности канала.

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.

10. КАСКАДНЫЕ КОДЫ ДЕКОДИРУЕМЫЕ С ИСПОЛЬЗОВАНИЕМ МПД

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

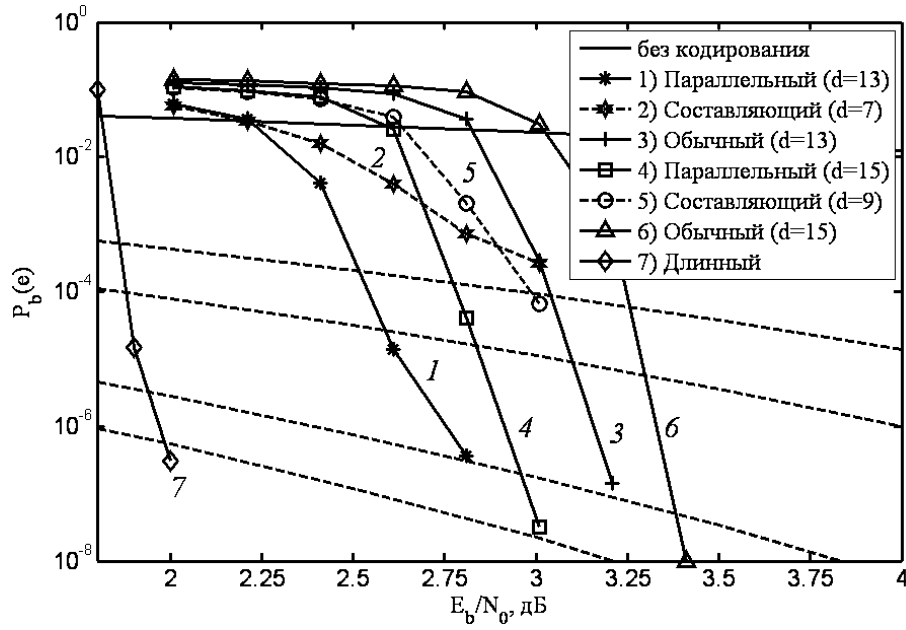


Рис. 5. Результаты моделирования параллельного кода на базе МПД в канале с АБГШ

Особое место среди кодовых схем на базе МПД занимает его каскадирование с кодами контроля по четности, использование которых позволяет существенно повысить эффективность применения кодирования. Особенность данной схемы заключается в том, что такое каскадирование практически не требует дополнительных затрат на оборудование (например, в схему кодирования требуется добавить лишь один сумматор по модулю 2), тогда как использование в каскадном коде, например, кодов Рида-Соломона несравненно труднее. Подробно принципы каскадирования МПД с кодом контроля четности рассмотрены в [9, 10, 18].

Эффективность работы каскадных схем, состоящих из самоортогонального кода с $d = 7$ и 9 и кода контроля четности с длиной 50, для канала с АБГШ отражена на рисунке 6. Как видно из графиков, каскадный код на основе МПД оказывается значительно лучше некаскадного. При этом использование простейшего кода контроля четности совместно с самоортогональным кодом позволяет получить дополнительный энергетический выигрыш около 1...1,5 дБ при вероятности ошибки на выходе декодера $P_b(e) = 10^{-5}$. Также отметим, что каскадный код, состоящий из кода Рида-Соломона (255, 223, 33) и сверточного кода с кодовой скоростью 1/2 и конструктивной длиной $K = 7$, декодируемый с помощью оптимального алгоритма Витерби, даже при меньшей общей кодовой скорости ($R \approx 0,437$) уступает каскадной схеме на базе МПД при $P_b(e) > 10^{-6}$. Заметим, что при использовании каскадирования с кодом контроля четности совместно с ранее рассмотренным параллельным кодированием, возможно получение значительного дополнительного энергетического выигрыша. Пример характеристик одной из таких схем показан на рисунке 6 кривой «МПДп+ККЧ». Использование малоизбыточного кода во внешнем каскаде данной схемы позволит получить сколь угодно малую вероятность ошибки при потерях в энергетике около 0,1...0,2 дБ.

Сложность декодирования рассмотренной каскадной схемы по сравнению со сложностью обычного МПД увеличивается на сложность декодера кода с контролем четности, примерно равную всего двум операциям на информационный бит.

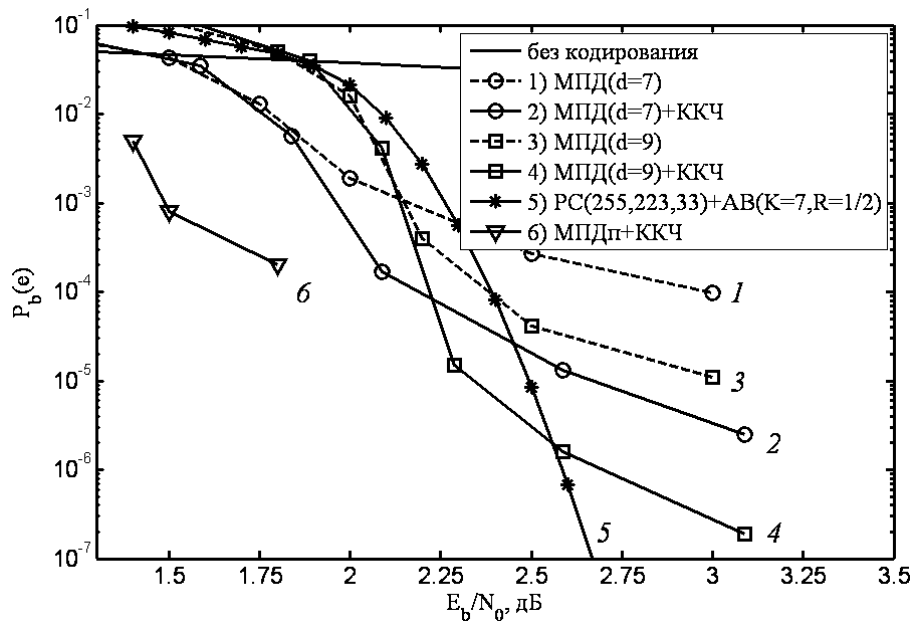


Рис. 6. Результаты моделирования каскадного кода на базе МПД в канале с АБГШ

11. МНОГОПороГОВЫЕ АЛГОРИТМЫ В КАНАЛАХ С НЕРАВНОМЕРНОЙ ЭНЕРГЕТИКОЙ

Опишем типичный пример очень простой модификации алгоритма МПД, которая с учётом конкретных свойств метода очень точно использует его свойства и фактически вообще без усложнения самого метода решающим образом улучшает его характеристики энергетической эффективности в полном соответствии с принципом «от простого к эффективному». Происходит просто согласование системы сигналов со свойствами кода и декодера.

Рассмотрим двухканальную схему передачи цифровых данных по спутниковым, космическим или иным каналам связи с достаточно большим уровнем гауссовского шума. Выберем для некоторого отношения сигнал/шум, первоначально одинакового для каждого из двух рассматриваемых каналов связи, такое перераспределение общей суммарной энергии, чтобы было обеспечено максимально возможное независимое последующее декодирование принятых информационных символов на основе многопорогового декодирования двоичных блоковых или свёрточных кодов. Иначе говоря, критерием наилучшего перераспределения энергии между каналами следует выбрать минимальный уровень проявления эффекта размножения ошибок при мажоритарном декодировании. В теории МПД эти вопросы достаточно полно проработаны [6, 9]. Снижение данного эффекта позволяет значительно улучшить сходимость решений МПД к оптимальным, что и создаёт условия для более эффективной работы алгоритмов МПД при больших уровнях шума.

При формировании такой совершенно простой новой сигнально-кодовой конструкции можно рассматривать различные способы балансировки энергетики. Например, каналы могут быть организованы так, что по одному из них передаются информационные символы кода, а по другому – проверочные. В этом случае анализ размножения ошибок упрощается в наибольшей степени, что позволяет достаточно быстро и полно рассматривать применимость максимального числа кодов и соответствующих им МПД алгоритмов в подобных схемах кодирования. Такие модели получили название каналов с неравномерной энергетикой [9, 19]. Они могут быть просто реализованы в обычных трактах передачи цифровых данных.

Как показал детальный анализ ряда кодов и некоторых модификаций МПД алгоритмов для каналов с неравномерной энергетикой с различными параметрами, перемещение границы области эффективной работы МПД в сторону более высокого уровня шума канала в диапазоне кодовых скоростей R от $1/4$ до $3/4$ может составлять до 1 дБ, что очень важно, поскольку уже исходная эффективность МПД в каналах обычного типа также оказывается весьма высокой. При этом отношение энергетики каналов должно находиться в диапазоне от 1,3 до 3,2.

Необходимость работы при более высоких уровнях шума требует увеличения числа итераций декодирования в МПД, но такое увеличение обычно оказывается не более чем двукратное, что сохраняет небольшую сложность реализации МПД как в программном, так и в аппаратном вариантах.

Новые полученные результаты в этой области иллюстрируются графиками на рисунке 7, на которых представлены возможности предложенных алгоритмов и уже известных методов. График «1) МПД-Х» соответствует эффективности МПД декодера на ПЛИС Xilinx, кривые «5) МПД+КК1», «6) МПД+КК2» и «7) МПД+КК3» даны для применения МПД в простейших каскадных схемах с кодом контроля четности. Все они детально обсуждались в [15]. На рисунке 7 также представлены кривые эффективности для алгоритма Витерби со стандартным кодом с конструктивной длиной $K = 7$ (кривая «3) АВ, $K=7$ ») и для каскадной схемы декодера Витерби с кодом Рида-Соломона (кривая «4) АВ+РС»), а также для турбо кода (кривая «9) Турбо») [2] и низкоплотностного кода, рекомендованного в стандарте DVB-S2 [20] (кривая «10) LDPC»). Отметим, что при реализации высокоскоростного декодера низкоплотностных кодов на ПЛИС потери в эффективности составляют более 0,5 дБ (кривая «11) LDPC (PLIS)»). Вертикаль « $C = 1/2$ » определяет пропускную способность гауссовского канала, к которой стремятся разработчики при улучшении характеристик декодирования при кодовой скорости $R = 1/2$. «МПД-L» – длинный код и МПД декодер с $I = 40$ итерациями, реализованный в ИКИ РАН на ПЛИС Altera. Новый результат для МПД и канала с неравномерной энергетикой – пунктир «8) МПД+НЭК» – соответствует возможности очень простого и значительного повышения эффективности декодирования кода при задержке принятия решения не более 400000 битов, при котором сохраняется хорошо известная достаточно большая скорость работы МПД как в программном, так и, особенно, в аппаратном варианте.

С учетом уже достигнутой близости области эффективной работы МПД к пропускной способности канала связи, можно считать, что МПД имеет хорошие перспективы по дальнейшему приближению его характеристик к границе Шеннона. При этом значительное преимущество МПД перед другими алгоритмами по числу операций, составляющее один-два десятичных порядка для различных сочетаний параметров кодирования, дает основание полагать, что МПД можно активно использовать при разработках современной аппаратуры передачи цифровых данных для космических и спутниковых каналов связи.

12. ВЫВОДЫ

Применение МПД в спутниковых и прочих дорогих каналах позволяет реализовать произвольно высокие скорости обработки и существенно повысить к.п.д. их использования. Крайне простое устройство МПД по сравнению с прочими сопоставимыми с ним по эффективности методами делает их предпочтительными в быстрых широкополосных каналах при аппаратной реализации. В достаточно медленных каналах связи даже программные реализации МПД очень эффективны и требуют написания лишь нескольких десятков команд программного кода для порогового элемента. Простые методы согласования кода и сигналов ещё более повышают возможности МПД и делают их реализацию особенно простой. Совершенно незначительная разница в эффективности МПД по сравнению с некоторыми особенно сложными декодерами

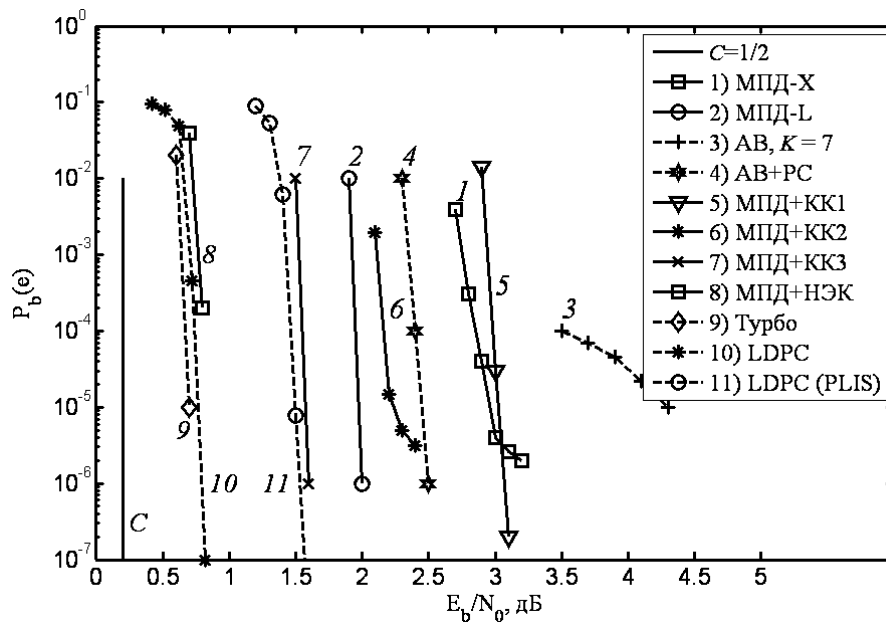


Рис. 7. Характеристики МПД, декодера Витерби, турбо и низкоплотностных кодов в гауссовском канале при $R = 1/2$

других типов, как показывает динамика улучшения характеристик МПД в последние годы, будет преодолена, видимо, в самое ближайшее время.

Таким образом, в результате почти 40-летних исследований разработан широкий класс многопороговых алгоритмов, которые могут быть полезны для многих современных высокоскоростных систем связи с предельно возможными уровнями энергетического выигрыша и недостижимым для других алгоритмов быстродействием.

Исследования МПД свидетельствуют, что те алгоритмы, которые нерационально используют вычислительные ресурсы, все же значительно проигрывают гораздо более простым методам, которые решают проблему декодирования более эффективно и экономно. Несомненно, что проблемы сложности реализации кодирования сохранятся в обозримом будущем, а в связи с ростом скоростей обмена информацией и необходимостью повышения её достоверности при передаче и хранении требования более простой реализации декодеров будут все более актуальными. Особенно предпочтительными 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 многопороговые алгоритмы еще более привлекательными.

Дополнительные сведения и результаты исследований МПД представлены на специализированном веб-сайте ИКИ РАН www.mtdbest.iki.rssi.ru.

Проведение исследований по алгоритмам МПД поддерживалось Научным советом по комплексной проблеме «Кибернетика» СССР, ИКИ РАН, ФГУП НИИРадио и грантами РФФИ №05-07-90024, №08-07-00078.

СПИСОК ЛИТЕРАТУРЫ

1. Витерби А. Границы ошибок для сверточных кодов и асимптотически оптимальный алгоритм декодирования. Некоторые вопросы теории кодирования. М.: Мир, 1970. стр. 142–165.

2. Berrou C., Glavieux A., Thitimajshima P. Near Shannon Limit Error-Correcting Coding and Decoding: Turbo-Codes. ICC'93, Geneva, 1993, pp. 1064–1070.
3. MacKay D.J.C., Neal R.M. Near Shannon limit performance of low density parity check codes. IEEE Electronics Letters, 1996, vol. 32, no. 18, pp. 1645–1646.
4. Мессис Дж. Пороговое декодирование. М.: Мир, 1966.
5. Золотарёв В.В. Устройство для декодирования линейных свёрточных кодов. Авторское свидетельство на изобретение СССР №492878, Бюллетень изобретений №43, 1975.
6. Самойленко С.И., Давыдов А.А., Золотарёв В.В., Третьякова Е.И. Вычислительные сети. М.: Наука, 1981.
7. Золотарёв В.В., Овечкин Г.В. Эффективные алгоритмы помехоустойчивого кодирования для цифровых систем связи. Электросвязь, 2003, №9, стр. 34–37.
8. Многопороговые декодеры. Веб-сайт ИКИ РАН www.mtdbest.iki.rssi.ru.
9. Золотарёв В.В. Теория и алгоритмы многопорогового декодирования. М.: Радио и связь, Горячая линия-Телеком, 2006.
10. Золотарёв В.В., Овечкин Г.В. Помехоустойчивое кодирование. Методы и алгоритмы. Справочник. М.: Горячая линия-Телеком, 2004.
11. Зубарев Ю.Б., Золотарёв В.В. Многопороговые декодеры: перспективы аппаратной реализации. 7-я Международная конференция и выставка «Цифровая обработка сигналов и её применение». М., 2005, Вып. VII-1, стр. 68–69.
12. Zolotarev V.V., Nazirov R.R., Chulkov I.V. The Quick Almost optimal multithreshold decoders for Noisy Gaussian Channels. RSCGSO International Conference ESA in Moscow. 2007.
13. Зубарев Ю.Б., Золотарёв В.В., Овечкин Г.В., Строков В.В. Многопороговые декодеры для высокоскоростных спутниковых каналов связи: новые перспективы. Электросвязь, 2005, №2, стр. 10–12.
14. Золотарёв В.В., Овечкин Г.В. Многопороговые декодеры для каналов с предельно высоким уровнем шума. Телекоммуникации, 2005, №9, стр. 29–34.
15. Зубарев Ю.Б., Золотарёв В.В., Овечкин Г.В., Дмитриева Т.А. Многопороговые алгоритмы для спутниковых сетей с оптимальными характеристиками. Электросвязь, 2006, №10, стр. 9–11.
16. Townsend R.L., Weldon E.J. Self-Orthogonal Quasi-Cyclic Codes. IEEE Trans., IT-13, 1967, pp. 183–195.
17. Золотарев В.В., Овечкин Г.В. Сложность реализации эффективных методов декодирования помехоустойчивых кодов. 6-я между. конф. и выст. «Цифровая обработка сигналов и ее применение». М., 2004, Т.1, стр. 220–221.
18. Золотарёв В.В., Овечкин Г.В. Использование многопорогового декодера в каскадных схемах. Вестник РГРТА, 2003, Вып.11, стр. 112–115.
19. Zolotarev V.V., Averin S.V., Chulkov I.V. Optimum Decoding Characteristics Achievement on the Basis of Multithreshold Algorithms. 9-th ISCTA'07, Ambleside, 2007.
20. European Telecommunications Standards Institute. Digital video broadcasting (DVB) second generation framing structure, channel coding and modulation systems for broadcasting, interactive services, news gathering and other broadband satellite applications. DRAFT EN 302 307 (v.1.1.2 06.2006).

Статью представил к публикации член редколлегии Н.А.Кузнецов