(Раздел из книги **"Вычислительные сети",** авторы: С.И. Самойленко, А.А.Давыдов, В.В.Золотарёв, Е.И.Третьякова, "Наука", Москва, 1981, 278с.)

Главные принципы многопорогового декодирования

Сравнение различных алгоритмов декодирования показывает, что самые эффективные алгоритмы, например реализующие декодеры Витерби для длинных кодов чрезвычайно сложны, а характеристики простых алгоритмов в каналах с большим шумом весьма неудовлетворительны.

Ниже будут изложены основы многопорогового метода декодирования (МПД) линейных кодов, позволяющего существенно повысить эффективность пороговых декодеров. Опишем сначала качественно идею предполагаемого алгоритма.

Возьмем в качестве примера сверточный самоортогональный код (СОК) с R=1/2. Обычный ПД с обратной связью принимает решение о декодируемых символах на основе J=d-1 проверочных соотношений, содержащих ошибки в (d-1)(d-2)/2 информационных символах, которые еще не были декодированы, такого же числа ошибок декодера и d-1 ошибок в проверочных символах. В этом случае низкая достоверность проверок при больших d объясняется тем, что почти всегда проверки искажаются вследствие ошибок именно в информационных символах, причем если p_0 достаточно мала, т. е. $P_1(e)<<p_0$, то это в основном ошибки в символах, принятых из канала и еще не исправленных в ПД.

Предположим теперь, что используется схема декодирования, в которой после первого ПД исправленные им информационные символы, а также проверочные символы из канала связи вновь поступают в другой ПД такого же типа. Поведение второго ПД будет определяться двумя факторами. С одной стороны, достоверность проверок второго ПД в среднем выше, так как вероятности ошибок в информационных символах, наиболее сильно искажавших проверки, теперь стали существенно ниже. Это может обеспечить более высокое качество декодирования с использованием цепочки из двух ПД по сравнению с одним. В принципе число ПД может быть и большим, чем 2. Нижняя граница эффективности такой схемы определялась бы достоверностью приема трех проверочных символов, которые входят в проверки, поступающие на пороговый элемент ПД.

С другой стороны, все ошибки и проверки второго декодера оказываются теперь зависимыми, и даже вероятность первой ошибки $P_1(e)$ для второго ПД уже не может быть рассчитана столь просто, как для первого ПД. В худшем случае, возможно, что ошибки на выходе первого ПД группируются так, что пока первый ПД не ошибается, второй ПД не требуется, а пакеты ошибок первого вследствие РО окажутся такими, что второй ПД, который в силу выбора кода ориентирован на исправление независимых случайных ошибок, не сможет их исправить. Поэтому и в этом случае он может оказаться бесполезным.

Ниже будет показано, что, тем не менее, при выполнении достаточно простых условий эффективность рассматриваемого ниже многопорогового декодирования (МПД) может быть весьма высокой, причем многие излагаемые далее результаты справедливы как для сверточных, так и для блоковых кодов.

Алгоритм многопорогового декодирования.

Рассмотрим двоичный линейный систематический блоковый пли сверточный код со скоростью передачи R=k/n, где k – число информационных символов, n – длина кодовой комбинации.

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

Будем любой двоичный вектор $\overline{X}$ длины *n* представлять парой векторов $\overline{X}_I$ и $\overline{X}_V$ длины *k* и *(n-k)* соответственно, относящихся к информационной и проверочным частям вектора:

$X = (\overline{X}_I, \overline{X}_V)$.

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

Лемма. Для любого кодового вектора $\overline{A}$ и принятого сообщения $\overline{Q}$ справедливо

$$\overline{A} \oplus \overline{Q} = (\overline{D}, H(\overline{Q}_I \oplus \overline{D}, \overline{Q}_V)), \qquad (2.6.2)$$

где вектор $\overline{D}$ длины *k* определяется соотношением

$$\overline{A}_I = \overline{Q}_I \oplus \overline{D}. \qquad (2.6.3)$$

Доказательство. В силу линейности кода

$\overline{S} = H(\overline{Q}_I \oplus \overline{D}, \overline{Q}_V) = H(\overline{A}_I, \overline{A}_V \oplus \overline{A}_V \oplus \overline{Q}_V) = H \cdot \overline{A} \oplus H(\overline{0}_I, \overline{A}_V \oplus \overline{Q}_V)$,

где $\overline{0}_I$ – нулевое информационное слово.

Так, как $H\overline{A} = 0$, поскольку $\overline{A}$ – кодовое слово, а $H(\overline{0}_I, \overline{A}_V \oplus \overline{Q}_V) = \overline{A}_V \oplus \overline{Q}_V$, так как $(\overline{A}_V \oplus \overline{Q}_V)$ умножается только на единичную подматрицу *I* матрицы *H,* то получаем, что вектор $\overline{S}$ равен

$$\overline{S} = \overline{A}_V \oplus \overline{Q}_V. \qquad (2.6.4.)$$

Проводя в правой части (2.6.2) замены с учетом (2.6.3), находим, что

$(\overline{D}, \overline{S}) = (\overline{D}, \overline{A}_V \oplus \overline{Q}_V) = (\overline{D} \oplus \overline{Q}_I \oplus \overline{Q}_I, \overline{A}_V \oplus \overline{Q}_V) = \overline{A} \oplus \overline{Q}$.

Лемма доказана.

Ее содержание заключается в том, что разность $\overline{B} = \overline{Q} \oplus \overline{A}$ для любого принятого вектора $\overline{Q}$ и кодового слова $\overline{A}$ определяется парой векторов $(\overline{D}, \overline{S})$. Перебором всех векторов $\overline{A}$ можно найти вектор $\hat{A}$, минимизирующий $|\overline{B}|$ и являющийся решением оптимального декодера (ОД). В силу определения при $\overline{D} = 0$ вектор $\overline{S}$ является обычным синдромом принятого сообщения $\overline{Q} : \overline{S} = H\overline{Q}$. Для простоты изложения будем в дальнейшем и при $\overline{D} \neq 0$ называть $\overline{S}$ синдро-

мом, поскольку это обобщение естественно и не приводит в дальнейшем к каким-либо противоречиям. Отметим также, что при каждом изменении $\overline{A}$ нет необходимости заново вычислять все компоненты синдрома. Достаточно на каждом шаге изменения инвертировать только те компоненты $\overline{S}$, которые содержат нечетное число ошибок в изменяемых информационных символах.

Рассмотрим теперь новый алгоритм декодирования, который очень близок к пороговому. Пусть на первом подготовительном этапе декодер выполняет вычисление и запоминание вектора $\overline{S}$. Затем начинается выполнение собственно процедуры декодирования. На каждом шаге декодер вычисляет обычную сумму компонент синдрома s_{jk}, содержащих в качестве слагаемых ошибку e_j, в декодируемом символе $\mathbf{i_j}$ (т. е. сумму проверок $s_{jk} \in \{S_j\}$, где $\{S_j\}$ – множество проверок относительно компоненты $\mathbf{e_j}$, соответствующей символу $\mathbf{i_j}$) и символа $\mathbf{d_j}$, также относящегося к декодируемому символу $\mathbf{i_j}$:

$$L_j = \sum_{s_{jk} \in \{S_j\}} s_{jk} + d_j. \qquad (1)$$

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

Выберем порог T равным половине всех слагаемых в (1). Для СОК это число равно $T=d/2=(J+1)/2$. Пусть, наконец, все **J=d-1** проверок, $\mathbf{i_j}$ и $\mathbf{d_j}$ инвертируются при $L_j > T$ и остаются неизменными при $L_j \le T$.

Предлагаемая процедура при первой попытке декодирования, пока все $\mathbf{d_j=0}$, совпадает с обычным алгоритмом для ПД. Будем в дальнейшем называть декодер, реализующий предлагаемый алгоритм, многопороговым декодером (МПД). Выбор такого названия будет ясен из дальнейшего рассмотрения.

При этом справедлива теорема 1.

Основная теорема многопорогового декодирования - 1.

Если на произвольном j-м шаге МПД изменяет декодируемый информационный символ $\mathbf{i_j}$, то:

а) при этом МПД находит новое кодовое слово $\overline{A}_2$, более близкое к принятому сообщению $\overline{Q}$, чем то кодовое слово $\overline{A}_1$, которому соответствовало значение $\mathbf{i_j}$ перед j-м шагом декодирования

$$|\overline{B}_1| \stackrel{\Delta}{=} |\overline{A}_1 \oplus \overline{Q}| > |\overline{A}_2 \oplus \overline{Q}| \stackrel{\Delta}{=} |\overline{B}_2|;$$

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

Доказательство. Перед началом декодирования символа $\mathbf{i_j}$ согласно приведённой выше лемме справедливо

$$(\overline{D}_1, \overline{S}_1) = (\overline{A}_{1I} \oplus \overline{Q}_1, H(\overline{Q}_I \oplus \overline{D}_1, \overline{Q}_V)) = \overline{A}_1 \oplus \overline{Q},$$

где

$$\overline{A}_1 = (\overline{A}_{1I}, \overline{A}_{1V}), \overline{A}_{1I} = \overline{Q}_I \oplus \overline{D}_1.$$

Вес вектора $\overline{B}_1$ перед этим шагом, равный $|\overline{B}_1| = |\overline{D}_1| + |\overline{S}_1|$, можно представить в виде обычной суммы весов $W_1 = L_{1j} + X$, где L_{1j} определено выражением (1) и равно сумме проверок и символа d_j, на пороговом элементе; X – вес остальных компонент $\overline{S}_1$, и $\overline{D}_1$, не входящих в L_{1j}.

Рассмотрим вектор $\overline{A}_2$, отличающийся от $\overline{A}_1$ только в одном символе $\mathbf{i_j}$, и соответствующую ему разность $\overline{B}_2 = \overline{A}_2 \oplus \overline{Q}$. Поскольку $\overline{B}_1$ и $\overline{B}_2$ отличаются между собой только в тех компонентах, которые поступают на пороговый элемент, то $|\overline{B}_2| = L_{2j} + X$, 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 $\overline{B}_i$, равны 1.

Так как МПД изменяет $\mathbf{i_j}$, если $L_{1j} > T$, то для этого необходимо, чтобы было $L_2 < L_1$ и, следовательно, $|\overline{B}_1| > |\overline{B}_2|$, чем доказан пункт а) теоремы.

Далее, очевидно, если символ $\mathbf{i_j}$ не изменялся, то можно декодировать любой другой символ $i_k, k \neq j$, поскольку при этом сохраняются условия леммы. В случае же изменения $\mathbf{i_j}$ в соответствии с правилами работы МПД после декодирования $\mathbf{i_j}$ имеют место равенства $\overline{A}_{2I} = \overline{Q}_I \oplus \overline{D}_2$ и $\overline{S}_2 = H(\overline{Q}_I \oplus \overline{D}_2, \overline{Q}_V)$, где $\overline{D}_2$ отличается от D_1 в символе d_j, поскольку при изменении (согласно базовому алгоритму ПД - через обратную связь (ОС) с порогового элемента) проверок, относящихся к $\mathbf{i_j}$, инвертируются именно те компоненты $\overline{S}_1$, в которых $\overline{S}_2$ отличается от $\overline{S}_1$. Отсюда получаем, что после изменения i_j для определенных выше векторов $\overline{D}_2$, $\overline{A}_2$ и $\overline{S}_2$:

$$(\overline{D}_2, \overline{S}_2) = (\overline{A}_2 \oplus \overline{Q}),$$

аналогичное тому, которое имело место перед изменением $\mathbf{i_j}$. Тем самым при последующих шагах декодирования и дальнейших изменениях символов $i_k, k \neq j$, также будет осуществляться приближение к принятому из канала сообщению $\overline{Q}$.

Основная теорема МПД доказана.

Мы показали, что МПД при каждом изменении декодируемых символов приближается к вектору $\overline{Q}$, отыскивая тем самым все более близкие к оптимальному решению, более правдоподобные вектора $\overline{A}_i$. 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, чем то, которое находится в МПД, декодер переходит к нему и дальнейшие сравнения производятся уже с новым

вектором $\overline{A_i}$. Ясно, что в принципе можно проводить достаточно большое число попыток декодирования и приближения к решению ОД – вектору $\widetilde{A}$. Принципиально важно, что при конечном числе просмотров декодером принятого вектора, что, конечно, выполняется всегда, сложность МПД такая же, как и у обычного ПД - линейная.

Допустим, что МПД достиг решения ОД, т.е. в информационном регистре МПД находятся символы вектора $\widetilde{A}$. Тогда справедливо

Следствие. МПД не изменит решения ОД.

Доказательство. Если бы МПД изменил на некотором шаге хоть один символ в векторе $\widetilde{A}$, то это означало бы, что нашелся другой кодовый вектор $\widetilde{A}^*$, который ближе к $\overline{Q}$, чем $\widetilde{A}$, что невозможно, потому что, по определению, ближайшим к $\overline{Q}$ словом является вектор $\widetilde{A}$.

Следствие доказано.

Принципиальным моментом является то, что следствие доказывает устойчивость решения МПД относительно оптимального решения: достигнув его, МПД останется в нём. Это очень важно в тех случаях, когда алгоритм предполагает возможность многократного изменения декодируемых символов.

Можно также заметить, что при доказательстве основной теоремы МПД не использовалось существенным образом единственность декодируемого символа. Так что данная процедура приложима и сразу к группе информационных символов.

Эффективность МПД.

Получать оценки эффективности МПД только расчетными методами чрезвычайно сложно. Поэтому для больших уровней шума более целесообразно часть исследований проводить с помощью моделирования, потому что при этом достаточно просто получать необходимую статистику при одновременной более точной непосредственной оценке основного параметра, который представляет интерес – средней вероятности ошибки на бит $P_b(e)$ на выходе МПД.

Для оценки качества работы МПД и интерпретации получаемых результатов моделирования представляются полезными следующие приведенные ниже данные.

Пусть в результате постепенного приближении к решению ОД МПД нашел кодовый вектор $\widetilde{A}^*$, отличающийся от $\widetilde{A}$ только в одном информационном символе $\mathbf{i_j}$. Ниже сформулированы условия, при которых МПД достигнет решения ОД.

Теорема 2. Пусть МПД осуществляет декодирование с задержкой, т. е. он изменит i_j, только если соответствующая ему сумма проверок больше, чем любая сумма проверок, относящаяся к другим символам. Тогда если решение $\widetilde{A}$ для данного принятого вектора $\overline{Q}$ единственно, то после завершения процедуры декодирования МПД изменит $\mathbf{i_j}$, и его решение будет совпадать с оптимальным.

Доказательство. Пусть векторы на входе МПД соответствуют решению, отличающемуся от оптимального в символе $\mathbf{i_j}$, а соответствующая ему сумма на пороговом элементе равна $a_j, a_j > T$. Покажем, что она строго больше суммы a_k, относящейся к любому символу $i_k, k \neq j$.

Докажем это от противного.

Пусть найдется $i_k, k \neq j$, такое, что $a_k \geq a_j$. Тогда, поскольку в символе i_j $\widetilde{A}^*$ отлично от $\widetilde{A}$, то $a_j = T + b_j > T, b = 9{,}5; 1{,}5\ldots$ и $a_k = T + b_k > T, b_k \geq b_j$.

Обозначим $W_j = a_j + x = |\overline{B}_j| = |\overline{Q} \oplus \widetilde{A}^*|$, где x – вес всех оставшихся компонент $\overline{S}$ и $\overline{D}$ не поступивших на вход порогового элемента.

Если $b_k \geq b_j$, то после инверсии i_k и соответствующих ему компонент векторов $\overline{S}$ и $\overline{D}$ вес суммы на пороге уменьшается па величину $\Delta = a_k - (J + 1 - a_k) = 2a_k - J - 1 = 2T + 2b_k - J - 1 = 2b_k > 0$. После инверсии $\mathbf{i_j}$ вес суммы на пороге уменьшился бы на $2b_j$. Поскольку входным вектором, который изменялся бы в обоих этих случаях, был $\widetilde{A}^*$, то это соответствует случаю, когда кодовый вектор $\widetilde{A}_k^*$, отличающийся от $\widetilde{A}^*$ в символе i_k, ближе к $\overline{Q}$, чем $\widetilde{A}$, что невозможно. В силу единственности $\widetilde{A}$ невозможен также и случай $a_k = a_j$. Но это значит, что сумма a_j максимальная среди всех a_i и МПД действительно изменит i_j.

Теорема доказана.

Отметим, что введенным в теореме ограничениям удовлетворяют многие самоортогональные сверточные коды и что данный результат справедлив независимо от того, верное или ошибочное решение об $\mathbf{i_j}$ принял ОД. Таким образом, рассматриваемый пороговый декодер не ухудшает оптимальное решение и может исправлять одиночные отклонения от оптимального решения. Это свойство МПД естественно назвать устойчивостью относительно решения ОД.

Для систематических сверточных кодов теорема 2 может быть переформулирована так, что сумма a_j должна быть максимальная среди всех a_i только в пределах длины кодового ограничения n_A от $\mathbf{i_j}$. Это связано с тем, что суммы, относящиеся к информационным символам, которые находятся на более далеких расстояниях, оказываются обязательно состоящими из различных компонент векторов $\overline{S}$ и $\overline{D}$ и, следовательно, не зависящими друг от друга. При этом МПД сверточного кода будет исправлять все одиночные отклонения от оптимального решения, разделенные интервалом не менее $2n_A$.

Наконец, сформулируем критерии качества декодирования МПД, который может быть использован при анализе результатов моделирования работы декодеров.

Теорема 3. Пусть МПД неоднократно декодирует в некотором порядке каждый информационный символ сообщения. Тогда, если он совершил единственную ошибку в символе $\mathbf{i_j}$ и не может ее исправить при вторичной попытке декодирования, ОД также ошибочно декодирует это сообщение.

Доказательство. Пусть ошибка совершена в символе $\mathbf{i_j}$. Поскольку никакие символы не были изменены при следующей попытке декодирования, то суммы на пороге во всех случаях были меньше *T*. Но это значит, что правильное кодовое слово с инвертированными $\mathbf{i_j}$ не может быть решением, потому что сумма a_j будет в этом случае больше *T* и, значит, оно будет дальше от $\overline{Q}$, чем то, которому соответствует состояние МПД. Может найтись другое кодовое слово, отличающееся от истинного кодового вектора в большем числе информационных символов и находящееся ближе к $\overline{Q}$, чем решение МПД. Но это значит, что ОД все равно совершит ошибку.

Теорема доказана.

Для сверточного кода может быть также сформулирована следующая теорема.

Теорема 4. Пусть МПД сверточного кода не изменяет решение после некоторого числа попыток улучшить принятое сообщение. Тогда число ошибок ОД при декодировании этого сообщения не меньше числа одиночных ошибок в решении МПД, находящихся на расстоянии более $2n_A$ от других ошибок.

Доказательство. Инверсия информационных символов, находящихся на расстоянии более $2n_A$ друг от друга, не влияет на значения соответствующих им сумм a_i. Поэтому либо эти символы будут неправильно декодированы и при использовании ОД, либо вместо одиночных ошибок на выходе ОД будут пакеты ошибок.

Покажем, что каждой одиночной ошибке МПД можно поставить во взаимно однозначное соответствие одну ошибку ОД. Если МПД и ОД совершают ошибку в одном и том же одиночном символе, то можно установить соответствие между этими двумя ошибками декодеров. Если для некоторой одиночной ошибки МПД найдется пакет ошибок ОД, содержащий эту ошибку, то снова можно установить такое же соответствие. Наконец, если одиночной ошибке $\xi_j = 1$ МПД соответствует правильное решение ОД, то ближайший ошибочный символ пакета ошибок ОД должен находиться на расстоянии не более $\mathbf{n_A}$ от ξ_j, поскольку иначе ОД не может правильно декодировать $\mathbf{i_j}$. Поставим ближайшую к $\mathbf{i_j}$ ошибку ОД из этого пакета в соответствие ξ_j. Так как эта ошибка из пакета находится на расстоянии не более $\mathbf{n_A}$ от ξ_j, то ее расстояние до других одиночных ошибок МПД более $\mathbf{n_A}$, и она не может быть поставлена в соответствие этим ошибкам. Но это и значит, что ошибок ОД больше, чем одиночных ошибок МПД.

Теорема доказана.

Последняя теорема позволяет легко идентифицировать те ошибки, возникающие при использовании МПД, которые сделал бы и ОД: все одиночные ошибки МПД, не исправляемые при повторном декодировании, приводят к ошибкам и при использовании ОД.

Заметим, что наибольшая необходимость кодирования проявляется в каналах с умеренным и значительным шумом, а не с малым, когда уменьшить вероятность ошибки можно многими методами. Поведение ПД при большом

уровне шума исследовать значительно сложнее, и польза от применения последовательно соединенных декодеров не столь очевидна. Поэтому наиболее быстро получить вероятностные характеристики МПД при больших уровнях шума получают в результате компьютерного моделирования. Разумеется, для всех других алгоритмов декодирования компьютерное моделирование также является единственным методом изучения их эффективности при большом уровне шума.