

Обобщение алгоритма МПД на недвоичные коды.

В.В.Золотарёв, ИКИ РАН
Москва

Предложено обобщение основных принципов многопорогового декодирования (МПД) на недвоичные коды. Показано, что эффективность недвоичного МПД близка к результатам, обеспечиваемым оптимальными переборными методами, которые для недвоичных кодов практически вообще нереализуемы. Характеристики недвоичных МПД сравниваются с возможностями кодов Рида-Соломона.

1. Основная теорема для QМПД.

Результаты работы многопороговых декодеров (МПД) [1-6] в двоичных гауссовских каналах во многих случаях оказываются совпадающими с характеристиками оптимального декодирования или близкими к ним даже при высоком уровне шума. Однако эффективные методы мажоритарного декодирования для недвоичных кодов в литературе не описаны.

Рассмотрим обобщение многопорогового декодирования (МПД) на недвоичные симметричные каналы [8,9]. Ценность этого метода заключается в том, что мажоритарные алгоритмы имеют всего лишь линейный рост сложности (числа операций декодирования) от длины кода n . Поскольку обычно оптимальные методы характеризуются экспоненциально растущей с длиной кода сложностью, применение недвоичных МПД, обозначаемых далее как QМПД, представляется особенно желательным.

Ещё более существенно, что в случае больших значений основания кода q , $q > 10$, совершенно невозможно создать эффективные истинно оптимальные декодеры (ОД), в том числе и алгоритм Витерби, поскольку при этом их сложность в большинстве случаев будет иметь вид q^k , где k - длина кодирующего регистра. Это и определяет важность применения QМПД, поскольку возможности декодеров для кодов Рида-Соломона (РС), имеющих широкую область применения, очень ограничены, а их сложность реализации неоправданно велика.

Пусть задан q -ичный, $q > 2$, симметричный канал с вероятностью ошибки $p_0 > 0$, такой, что при передаче любой исходный символ кода переходит в один из оставшихся $q-1$ символов случайно, независимо и равновероятно. По аналогии с двоичным симметричным каналом без памяти (ДСК) назовём этот канал также q -ичным симметричным каналом (QСК). Для этого канала оптимальным решением при передаче любого символа будет такое, возможно, единственное кодовое слово из q^{nR} возможных, которое отличается от принятого сообщения в минимальном числе символов кода. (Здесь предполагалось, что n - длина кода, выраженная числом символов кода, R - кодовая скорость, $R < 1$.)

Рассмотрим линейный недвоичный код, проверочная матрица которого имеет такой же вид, как и в двоичном случае, т. е. состоит только из нулей и единиц. Пусть эта матрица соответствует самоортогональному систематическому блоковому или свёрточному коду [6,7]. В этом случае слова минимального веса d , где d - минимальное расстояние кода, имеют единственный ненулевой символ i_k , со значением q , $q > 0$, в его информационной части. Поскольку проверочные (а значит, и порождающие) матрицы кода содержат только нули и единицы, то операции кодера и декодера по

формированию проверочных символов кода и вычислению синдрома S принятого сообщения являются только сложениями. Таким образом, для кодирования и декодирования не требуется наличие недвоичного поля, а достаточно создать только некоторый вариант группы по сложению. Это дополнительно и очень существенно упрощает все процедуры кодирования и реализации последующего декодирования.

Рассмотрим далее формальное описание алгоритма QМПД.

Пусть задан линейный недвоичный систематический свёрточный или блочный код, проверочная матрица H которого имеет такой же вид, как и в двоичном случае, т.е. состоит только из нулей и единиц, за исключением того, что вместо 1 в единичной подматрице будут -1 . Предположим также, что все операции сложения и вычитания будут производиться в некоторой группе целых чисел, например, по $\text{mod } q$. После передачи кодового вектора \bar{A}_0 длины n с k информационными символами по QСК в декодер поступает вектор \bar{Q} , отличающийся, вообще говоря, от исходного кодового вектора из-за искажений в канале: $\bar{Q} = \bar{A}_0 + \bar{E}$, где \bar{E} – вектор шума канала типа QСК.

Будем, как и в двоичном случае, представлять каждый вектор \bar{X} длины n в виде пары векторов \bar{X}_I, \bar{X}_V длины k и $(n-k)$ соответственно.

Пусть $\bar{Q} = \bar{A} + \bar{E}$, где \bar{E} – вектор ошибки, «+» и «-» – операции сложения и вычитания в определённой некоторым образом группе, \bar{A} – некоторое произвольное кодовое слово.

Определим \bar{D} – q -ичный вектор длины k , равный $\bar{D} = \bar{A}_I - \bar{Q}_I$, где \bar{Q}_I – информационная часть принятого сообщения $\bar{Q} = (\bar{Q}_I, \bar{Q}_V)$.

Тогда справедлива следующая лемма.

Лемма 1.

$$(\bar{D}, H(\bar{Q}_I + \bar{D}, \bar{Q}_V)) = \bar{A} - \bar{Q}. \quad (2.7)$$

Доказательство. В силу линейности кода справедлива цепочка равенств

$$\begin{aligned} \bar{S} &= H(\bar{Q}_I + \bar{D}, \bar{Q}_V) = H(\bar{Q}_I + \bar{D}, \bar{Q}_V + \bar{A}_V - \bar{A}_V) = \\ &= H\bar{A} + H(\bar{0}_I, \bar{Q}_V - \bar{A}_V), \end{aligned}$$

где $\bar{0}_I$ – нулевой вектор длины k .

Учитывая, что для систематического кода для $q > 2$ $H(\bar{0}_I, \bar{X}_V) = -\bar{X}_V$, получаем, что $\bar{S} = \bar{A}_V - \bar{Q}_V$. А так как $\bar{D} = \bar{A}_I - \bar{Q}_I$, то $(\bar{D}, \bar{S}) = \bar{A} - \bar{Q}$.

Лемма доказана.

Она устанавливает простое полезное соответствие между произвольным кодовым словом и принятым сообщением, аналогичное двоичному случаю [Ошибка! Источник ссылки не найден.,3]. Фактически она утверждает, что для рассматриваемых кодов вектор синдрома является расстоянием по проверочным между принятым сообщением \bar{Q}_I и кодовым вектором с информационной частью \bar{A}_I . Такая интерпретация вектора синдрома рассматривалась с различных сторон в [1,4,5]. Эта лемма позволяет доказать главное свойство QМПД алгоритма, который описан ниже.

Пусть при передаче по QСК кодового слова \bar{A}_0 в декодер поступил искажённый в канале связи вектор $\bar{Q} = \bar{A}_0 + \bar{E}$. Аналогично двоичному случаю, разностный вектор \bar{D} , теперь уже q -ичный, перед началом процедуры декодирования примем равным 0.

Пусть далее декодер QМПД устроен так, что после вычисления обычным образом вектора синдрома $\bar{S} = H\bar{Q}$ принятого сообщения процедура декодирования состоит в следующем.

1. Для произвольно взятого символа q -ичного декодируемого информационного символа i_j принятого сообщения подсчитывается число двух наиболее часто встречающихся значений проверок из общего числа J всех проверок, относящихся к символу i_j , а также символа d_j вектора \bar{D} , соответствующего символу i_j . Пусть значения

этих двух проверок равны h_0 и h_1 , а их количество равно m_0 и m_1 , соответственно, причем $m_0 \geq m_1$.

Эта процедура аналогична подсчёту суммы проверок на пороговом элементе двоичного МПД.

2. Если $m_0 - m_1 \leq T$, где $T = 0, 1, 2, \dots$ – целое неотрицательное число, то осуществляется переход к новому произвольному $i_m, m \neq j$, и далее к п.1.

Это – тоже аналог процедуры сравнения с порогом в двоичном декодере.

3. Если $m_0 - m_1 > T$, то из i_j, d_j и всех J проверок относительно i_j вычитается оценка ошибки, равная h_0 , затем происходит выбор нового $i_m, m \neq j$, и переход к п.1.

Этот последний шаг цикла декодирования очередного символа есть просто процесс изменения декодируемого символа и коррекции через обратную связь всех символов синдрома, являющихся проверками декодируемого символа. Нужно только учитывать, что процедуры сложения и вычитания в QМПД не тождественны, как это имеет место в двоичном МПД. Пример схемной реализации QМПД представлен в [6].

Такие попытки декодирования по пп.1÷3 могут быть повторены для каждого символа принятого сообщения, например, 3, 10 и более раз.

При реализации алгоритма QМПД, как и в двоичном случае, удобно все информационные символы перебирать последовательно, а останавливать процедуру декодирования после фиксированного числа попыток коррекции ошибки или если при очередной такой попытке ни один из символов не изменил своего значения.

Для описанного алгоритма QМПД справедлива следующая теорема.

Теорема 2. Основная теорема многопорогового декодирования недвоичных кодов.

Пусть декодер реализует алгоритм QМПД для описанного выше СОК. Тогда при каждом изменении декодируемых символов происходит переход к более правдоподобию решению по сравнению с предыдущими состояниями декодера.

Предварительное обсуждение.

Напомним, что для классического канала типа QСК из двух кодовых векторов более близким к принятому из канала сообщению i , следовательно, более правдоподобным будет тот из них, который отличается от принятого вектора в меньшем числе символов. Поэтому доказательство роста правдоподобия решений QМПД при каждом изменении декодируемых символов состоит просто в том, чтобы показать, что число символов нового кодового слова, совпадающих с символами принятого сообщения, увеличилось, т.е. расстояние Хемминга между ними уменьшилось. Для недвоичных символов это расстояние как раз соответствует количеству несовпадающих символов в двух векторах равной длины.

Итак, согласно свойствам вектора синдрома и разностного регистра по лемме 1 для QМПД расстояние между принятым вектором и текущим решением QМПД равно числу ненулевых символов синдрома. Значит, для уменьшения этого расстояния, что будет соответствовать росту правдоподобия решений этого декодера, нужно найти другое кодовое слово, для которого общее число нулевых символов синдрома \bar{S} и разностного вектора \bar{D} увеличится. Напомним, что, как и в двоичном случае, здесь имеется в виду то кодовое слово, информационные символы которого находятся в соответствующих регистрах декодера.

Доказательство.

Пусть декодер содержит векторы

$$\bar{A}_{0l}, \bar{D} = \bar{A}_{0l} - \bar{Q}_l \text{ и } \bar{S} = H(\bar{Q}_l + \bar{D}, \bar{Q}_l), \quad (2.8) (1)$$

где $\bar{A}_0 = (\bar{A}_{0l}, \bar{A}_{0r})$ – произвольное кодовое слово, \bar{Q} – принятое сообщение.

Покажем, что в случае использования алгоритма QМПД при изменении очередного декодируемого символа i_j в текущем информационном векторе-решении декодера \bar{A}_{0l} получается такой новый вектор \bar{A}_{1l} , что расстояние Хемминга до принятого

вектора \bar{Q} у кодового слова \bar{A}_1 меньше, чем у предыдущего решения декодера \bar{A}_0 , т.е. $|\bar{A}_0 - \bar{Q}| > |\bar{A}_1 - \bar{Q}|$.

В самом деле, если некоторый символ i_j изменен, значит, нашлось единственное значение h_0 , $h_0 \neq 0$, на множестве проверок символа i_j , которое встречается строго чаще всех других, m_0 раз, а все другие – не более m_1 раз, $m_0 > m_1$. Отметим, что если $h_0 = 0$, декодируемый символ не изменяется.

В этом случае при изменении i_j , d_j и всех имеющихся J проверок в регистре синдрома, т.е. после вычитания из них величины h_0 , все m_0 проверок (и, может быть, символ d_j), которые были равны h_0 , станут равными 0. Количество нулевых проверок в векторе синдрома (конечно, с учётом и значения символа d_j), которые до изменения символа i_j были равны нулю, не может быть больше m_1 . Но это значит, что при изменении i_j за счет этих символов вес вектора синдрома не может возрасти на этих позициях более, чем на m_1 . Тогда общее изменение веса равно $m_1 - m_0 < 0$, т.е. суммарный вес векторов \bar{D} и \bar{S} после изменения декодируемого символа i_j уменьшится.

Также заметим, что вектор \bar{S}_1 отличается от \bar{S}_0 только в тех символах, которые являются для i_j проверками, а разностные векторы \bar{D}_1 и \bar{D}_0 не совпадают только в позиции d_j на величину h_0 , как и соответствующие символу i_j проверки. Но это значит, что после изменения i_j в декодере типа QМПД содержатся векторы \bar{S}_1 и \bar{D}_1 , соответствующие разности принятого вектора и нового решения декодера, т.е. выполняются условия, соответствующие (1). Но тогда получаем, что и в новом состоянии декодера снова справедливы условия леммы 1, что позволяет перейти к очередной попытке коррекции символа i_m , $m \neq j$, после которой изменение следующего декодируемого символа снова гарантирует переход к новому ещё более правдоподобному решению и т.д.

Теорема доказана.

Как видим, при переходе от двоичного к недвоичному МПД стиль доказательства основной теоремы [1,5] изменился довольно незначительно.

Отметим два наиболее существенных момента, характеризующих предложенный новый алгоритм. Во-первых, как и в случае двоичных кодов, нельзя утверждать, что улучшение решения при многократных попытках декодирования будет иметь место до тех пор, пока не будет достигнуто решение ОД. На самом деле и в блоковых, и в свёрточных кодах возможны конфигурации ошибок, не исправляемые в QМПД, но которые могут быть исправлены в ОД. Поэтому основной способ повышения эффективности QМПД состоит в поиске кодов, в которых такие неисправляемые конфигурации ошибок довольно редки даже при большом уровне шума.

Другим важнейшим моментом является то, что по сравнению с традиционным подходом к двоичным мажоритарным схемам, в QМПД для изменения декодируемого символа достаточно наличие не абсолютного, а только относительно строгого большинства проверок, как это следует из условия $m_0 - m_1 > T$. Например, в самоортогональном коде с $d = 9$ ошибка в декодируемом символе будет исправлена даже в том случае, если из 9 его проверок (включая и символ d_j разностного регистра) правильными будет только 2, а остальные 7 – ошибочными. Такого невозможно вообразить для двоичных кодов, а для QМПД данная ситуация типична. Единственным условием для этого частного примера являются разные значения проверок относительно декодируемого символа i_j . А для больших значений q именно это условие практически всегда и реализуется. Эти свойства QМПД существенно расширяют возможности недвоичного многопорогового алгоритма при работе в больших шумах, сохраняя при этом весьма малую сложность процедур мажоритарного типа и в q -ичных каналах.

2. Нижние оценки вероятности ошибки декодирования.

Рассмотрим вычисление нижней оценки вероятности оптимального декодирования для кода, задаваемого описанным выше способом. Во всех этих случаях это будет выявление наиболее часто встречающихся условий того, что вектор ошибки будет иметь расстояние Хемминга до ближайшего кодового слова меньше, чем его собственный вес. В силу линейности кода этого достаточно для вынесения неправильного решения даже оптимальным переборным алгоритмом. Рассматривая вектор ошибки с такими свойствами, будем учитывать, что нужно анализировать только те символы этого вектора, которые соответствуют позициям проверок относительно очередного декодируемого символа i_k . Выпишем вероятности некоторых наиболее простых событий, которые приводят к ошибкам оптимального декодера (ОД).

К искомым векторам ошибки относятся такие, что [8,9]:

- все проверочные символы и декодируемый символ i_0 ошибочны:

$$P_1(\epsilon) = p_0^{J+1}, \quad (2)$$

где $d=J+1$, d - минимальное кодовое расстояние самоортогонального кода;

- все проверочные символы ошибочны, но два из них одинаковы, а i_0 принят верно:

$$P_2(\epsilon) = (1-p_0)^{J-2} p_0^J \prod_{i=1}^{J-2} (1-i/(q-1)) / (q-1)/2; \quad (3)$$

- есть один правильно принятый проверочный символ, а остальные ошибочны, как и i_0 :

$$P_3(\epsilon) = J(1-p_0)p_0^J. \quad (4)$$

Более полное перечисление различных событий, приводящих к ошибкам недвоичного ОД, и оценки их вероятностей, а также вероятностей ошибки в первом символе недвоичного ПД приведены в [6,8,9]. Простая схема QМПД дана в [6].

Перечисленных событий вполне достаточно, чтобы для большинства реальных условий применения кодов получать удовлетворительные по точности вероятностные оценки потенциальной помехоустойчивости кода. А поскольку QМПД на каждом шаге стремится к решению ОД, то можно ожидать, что при некотором достаточно высоком уровне шума он во многих случаях достигнет искомого оптимального решения.

Особенно удобно в технических системах работать с данными, имеющими байтовую структуру. Отметим, что кроме кодов Рида-Соломона (РС) в настоящее время вообще нет других сколько-нибудь эффективных методов декодирования недвоичных символьных данных. Сравним вероятностные характеристики кодов РС с возможностями QМПД. Будем считать, что выбран код РС длины 255 (символ - 8 бит). Подчеркнём, что для QМПД никаких ограничений по длине кода вообще нет, поскольку он выполняет только операции сложения по mod 256 и сравнения.

Очевидно, что недвоичный пороговый элемент, рассмотренный выше при описании операций в QМПД, - простейшее устройство или подпрограмма с числом операций N сложения и сравнения небольших целых чисел $N \sim 10 \div 50$ для всех тех небольших значений минимального кодового расстояния d , $d < 15$, которое следует применять в таком декодере.

3. Характеристики декодирования.

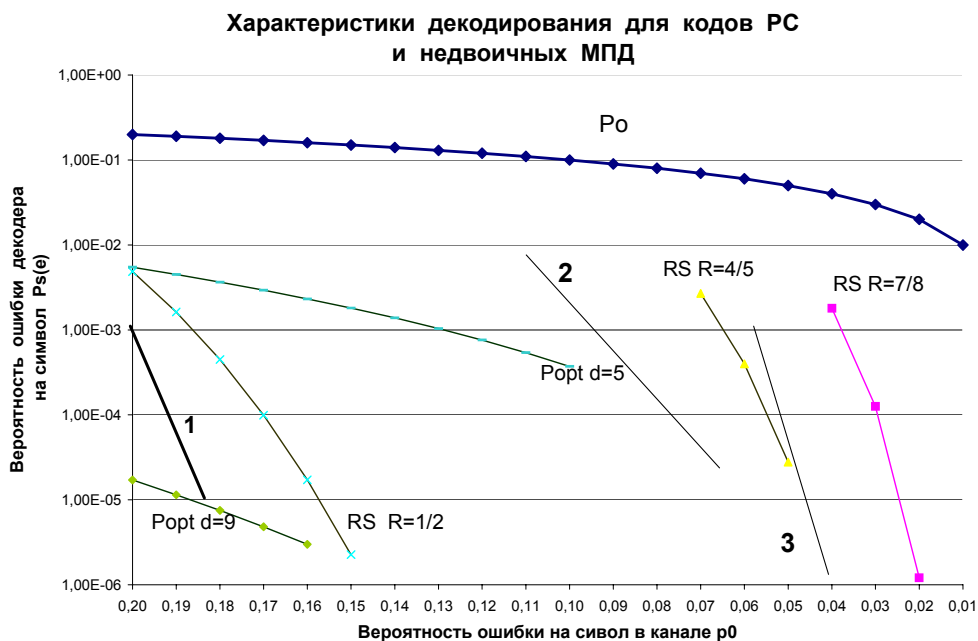


Рис.1.

На рис.1 представлены характеристики декодеров для кодов РС длины $n=255$ (обозначены: RS) и QМПД в QСК. По горизонтальной оси отложены вероятности ошибки p_0 в указанном канале, а по оси ординат - средние вероятности ошибки на символ в результате декодирования.

Для достижения решения, совпадающего с оптимальным или близкого к решению ОД, QМПД для $q=256$ необходимо $5 \div 20$ итераций (повторных попыток) декодирования принятого сообщения. Это полностью соответствует методу МПД для двоичных кодов [1-6].

Как следует из вида графиков зависимостей средней вероятности ошибки декодирования на символ $P_s(e)$ от вероятности p_0 канала QСК на входе декодеров для кодовых скоростей $R=1/2$, $R=4/5$ и $R=7/8$, простейший по своему устройству QМПД представлен графиками 1, 2 и 3 соответственно для указанных выше кодовых скоростей и обеспечивает гораздо более высокие характеристики, чем декодеры для кода РС, благодаря несколько большей длине $n=1000$ используемых кодов и хорошей сходимости решений QМПД к решению ОД.

Для сопоставления на рис.1 приведены также нижние оценки для использованных недвоичных СОК при оптимальном декодировании для $d=5$ и 9.

Заметим, что в настоящее время неизвестны другие алгоритмы декодирования с приемлемой сложности реализации, которые могут обеспечить такие же характеристики.

При увеличении длин кодов характеристики QМПД могут быть дополнительно существенно улучшены. Для недвоичных мажоритарно декодируемых кодов при длинах порядка $(3 - 8) \cdot 10^4$ при $p_0 \sim 0,27$ с помощью QМПД при $R=1/2$ можно достичь вероятности ошибки декодера на символ менее 10^{-6} . Такая помехоустойчивость недоступна для кодов РС сколько угодно большой длины. Сложность QМПД в пересчете на символ данных с ростом длины кода не меняется.

Для длинных кодов с $R=7/8$ QМПД работает эффективно при $p_0 \sim 0,040$, а при $R=19/20$ эта граничная вероятность составляет $p_0 \sim 0,012$. Высокие характеристики QМПД позволяют применять этот алгоритм для обеспечения хранения данных в сверхбольших долгоживущих базах данных при уровнях достоверности, на много порядков превышающих возможности кодов РС.

Свёрточные QМПД дополнительно улучшают характеристики декодирования.

Очень небольшие затраты на декодировании в QМПД ещё более повышают привлекательность их применения для различных систем. Например, обычные ПК позволяют без применения специальных мер набрать за час статистику декодированных данных для программных QМПД объёмом $\sim 10^{10}$ битов.

Очевидно, что каскадирование нескольких недвоичных МПД ещё более улучшит вероятностные характеристики декодирования практически без увеличения его сложности.

4. Выводы

Представленные результаты позволяют утверждать, что описанные впервые более 20 лет назад недвоичные МПД обладают действительно высокой эффективностью, недоступной для декодеров кодов РС. При этом сложность их реализации весьма невелика и, как показывает детальный анализ, может быть дополнительно значительно снижена.

Исследования МПД свидетельствуют, что те алгоритмы, которые нерационально используют вычислительные ресурсы, все же значительно проигрывают гораздо более простым, 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 требования более простой реализации декодеров будут все более актуальными. Более предпочтительными при всех вариантах реализации окажутся те алгоритмы, которые выполняют только очень простые, однородные и быстрые операции. Наиболее полно этим требованием удовлетворяют МПД и ряд его модификаций, включая недвоичные. А соответствие его возможностей характеристикам самых сложных алгоритмов делает многопороговые алгоритмы еще более перспективными..

Разработки алгоритмов МПД поддерживались Научным советом по комплексной проблеме "Кибернетика" АН СССР, ИКИ РАН, а также НИИ Радио Министерства связи.

Исследования велись при финансовой поддержке РФФИ по гранту №05-07-90024в.

Литература

1. Золотарёв В.В. Теория и алгоритмы многопорогового декодирования. – М., Радио и связь, Горячая линия - Телеком, 2006, 270с.
2. Золотарёв В.В. Устройство для декодирования линейных свёрточных кодов. - Авторское свидетельство на изобретение СССР №492878, БИ №43, 1975.
3. Самойленко С.И., Давыдов А.А., Золотарёв В.В., Третьякова Е.И. Вычислительные сети. – М.: Наука, 1981, с. 277.
4. V.V.Zolotarev. The Multithreshold Decoder Performance in Gaussian Channels. -In Proc.: 7-th International Symposium on Communication Theory and applications, held on 13-18 July 2003, St. Martin's College, Ambleside, UK, pp.18-22.
5. Золотарёв В.В. Многопороговые декодеры. - Веб-сайт www.mtdbest.iki.rssi.ru.
6. Золотарёв В.В., Овечкин Г.В. Помехоустойчивое кодирование. Методы и алгоритмы. Справочник. "Горячая линия - Телеком", Москва, 2004, с.124.

7. Townsend R.L., Weldon E.J. Self-Orthogonal Quasi-Cyclic Codes. - IEEE Trans., IT-13, 1967, pp.183-195.
8. Золотарёв В.В.. Алгоритмы кодирования символьных данных в вычислительных сетях. - В сб.: "Вопросы кибернетики", ВК-106, М.,1985.
9. Золотарёв В.В. Многопороговое декодирование в двоичных каналах. - В сб.: "Вопросы радиоэлектроники", Серия ЭВТ, вып.12, М.,1984.