

ОБОБЩЕНИЕ АЛГОРИТМА МПД НА НЕДВОИЧНЫЕ КОДЫ



В.В.Золотарёв,
старший научный
сотрудник ИКИ РАН

Применение многопороговых алгоритмов для недвоичных кодов в сетях мобильной связи позволяет существенно, иногда даже в несколько раз, повысить КПД использования весьма дорогих цифровых каналов передачи данных. Эффективное кодирование создает условия для существенно более полной реализации возможностей цифровых сетей.

Основные свойства QМПД

Результаты работы многопороговых декодеров (МПД) [1,3,4] в двоичных гауссовских каналах во многих случаях оказываются совпадающими с характеристиками оптимального декодирования или близкими к ним даже при высоком уровне шума.

Обобщение многопорогового декодирования (МПД) на недвоичные симметричные каналы рассматривалось в [2 — 6]. В [2] отмечалось, что оптимальные декодеры для большого основания кода $q > 16$ создать трудно, а помехоустойчивость традиционных декодеров для кодов Рида-Соломона (РС), просто в силу их небольшой длины, недостаточна. Именно поэтому возможность применения длинных недвоичных кодов с возможно меньшей сложностью декодирования представляется крайне желательной. Такими свойствами и обладают недвоичные (называемые также q -ичными) коды с мажоритарным декодированием, которое далее обозначается как QМПД.

В [1,5] доказано, что решения QМПД сходятся к решениям оптимальных переборных алгоритмов в том смысле, что в каналах с симметричными случайными ошибками все изменения в декодируемых символах приводят к переходу к более правдоподобным решениям. Проблема состоит только в том, чтобы при максимально высоком уровне шума было возмож-

но продолжать поиск все более правдоподобных кодовых слов до тех пор, пока не будет достигнуто наиболее правдоподобное решение, которое и является, как известно, решениями ОД, оптимальным решением. Как известно, обычно решения ОД являются результатом полного перебора. В то же время QМПД, обеспечивая достижение решения ОД при достаточно высоком уровне шума, остается алгоритмом с минимальной теоретически возможной линейной от длины кода сложностью, т.е. числом операций декодера. Поэтому применение недвоичных МПД особенно перспективно, поскольку областей применения кодов РС очень много, их эффективность весьма невелика, а потребность в значительном улучшении характеристик помехоустойчивости во всех подобных технических системах огромна.

Рассмотрим сравнительные характеристики QМПД и обычных декодеров РС. Собственно алгоритм декодирования QМПД детально описан в [1 — 5]. Предложенный новый алгоритм характеризуют два наиболее существенных момента. 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 сверточных кодах возможны конфигурации ошибок, не исправляемые в QМПД, но они могут быть ис-

правлены 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. Это задача решается при выборе кодов для QМПД по минимуму уровня проявления эффекта размножения ошибок [1, 3].

Два важных свойства QМПД оказываются полезными при рассмотрении характеристик этого алгоритма. Первое: как и в случае двоичных цифровых потоков, что было показано в [1], QМПД не покинет решение ОД, если он достиг его. А в случае отсутствия только одного отличия в текущем решении QМПД от единственного оптимального решения при последующих попытках декодирования такого сообщения декодер почти всегда достигнет оптимального решения. Если же декодер устроен так, что сначала оценивается наиболее правдоподобное изменение решения в сообщении, которое затем и реализуется, то декодер обязательно перейдет к оптимальному решению. Совокупность этих свойств очень важна для устойчивой сходимости решений QМПД к решению ОД, поэтому их так и называют устойчивостью относительно решения ОД.

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 относительного 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 сим-

вол d_j разностного регистра) правильными будут только 2, а остальные 7 — ошибочными. Такое невозможно 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 основания кода 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.

Оценки характеристик QМПД

Наиболее частые комбинации, приводящие к ошибкам даже при использовании оптимальных переборных методов в недвоичных симметричных каналах, рассмотрены в [1 — 6]. Нижние оценки вероятностей таких событий были предложены в [1,2,4,5]. Вероятности ошибки в первом символе кода при использовании QМПД были рассмотрены в [1,5]. Они важны при оценках вероятностей ошибок канала, при которых удастся хотя бы немного понизить плотность ошибок в принятом сообщении. Ясно, что если на первой итерации QМПД несколько снижает число оставшихся ошибок по сравнению с их первоначальным количеством, то работа декодера на остальных итерациях существенно облегчается и действительно появляется вполне реальная возможность достижения им решения ОД. Значит, эти вероятности можно отнести к верхним оценкам характеристик QМПД. Указанные совокупности верхних и нижних оценок вероятностей ошибки QМПД позволяют осу-

ществлять простое предварительное определение возможностей этого алгоритма в двоичных каналах.

В целом ряде случаев оказывается также очень полезным оценить предельные возможности QМПД при малом уровне шума канала, когда практически все его конечные решения с большой долей вероятности оказываются оптимальными. В этом случае нижняя оценка для вероятности ошибки ОД, совпадающая с вероятностью ошибки декодирования алгоритма QМПД для недвоичного самоортогонального кода [1,3,4] с минимальным кодовым расстоянием d , оказывается просто равной вероятности того, что декодируемый символ и все относящиеся к нему проверочные символы приняты ошибочно. Иначе говоря, вероятность ошибки декодера в отдельном символе равна $P_s(e) = p_0^d$, где p_0 — вероятность ошибки в рассматриваемом канале. Во многих случаях такая простая оценка позволяет на первом этапе определения возможностей QМПД найти его наименьшую достижимую вероятность ошибки с вполне

приемлемой точностью. В случае необходимости точность этой простейшей ошибки можно повысить, если рассмотреть также вероятность таких событий, когда один из проверочных символов принят правильно, а также вариант, при котором информационный символ принят правильно, но есть два проверочных символа, ошибки в которых имеют одинаковые значения. В этих двух группах событий решения QМПД и ОД также будут ошибочны. Отметим, что если основание кода q будет небольшим, одного порядка с кодовым расстоянием d , то необходимо оценивать гораздо более сложные комбинации ошибок в принятом сообщении, рассмотренные, например, в [1 — 4].

Характеристики помехоустойчивости QМПД

Ниже рассмотрены результаты моделирования работы QМПД в недвоичном симметричном канале qСК, а также возможности обычных декодеров кодов РС.

На рис. 1 представлены вероятности ошибки на символ

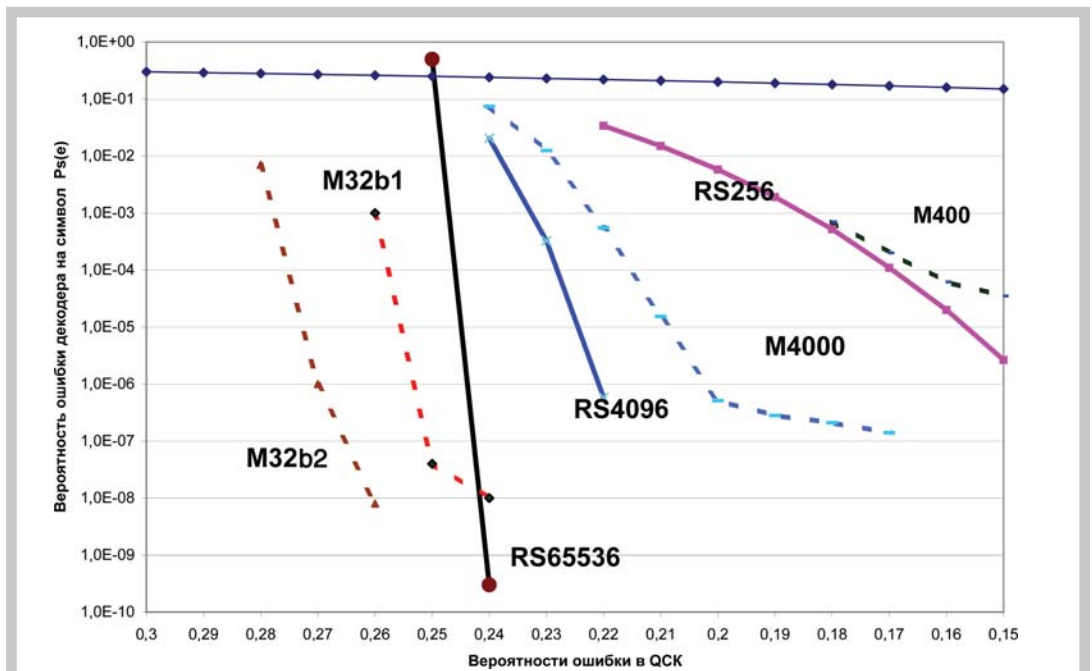


Рис. 1. Характеристики недвоичных блочных МПД и кодов РС с $R = 1/2$

для кодов Рида-Соломона, которые обозначены как RS_n , где n — длина кода, выраженная в числе символов. Отметим, что реально сейчас используются только коды РС длины 256 или менее. Коды длины 4096 символов и тем более длины $n = 65536$ (каждый символ — размером 16 битов) в обозримом будущем реализации не подлежат.

Здесь же пунктирными линиями показаны возможности кодов с мажоритарным декодированием при $R = 1/2$ для случая $q = 256$ (символ — 1 байт) для разных длин кодов, поскольку при любом $q > 2$, как и в двоичном случае, для QМПД можно строить сколь угодно длинные коды с различными значениями кодового расстояния d и кодовой скорости R . Эти коды отмечены как M400 и M4000 с числами, обозначающими длины кодов, выраженные числом символов. Далее обозначение M32b1 соответствует QМПД для кода длины 32 000 символов. Как видно из рис. 1, возможности QМПД во всех случаях сопоставимы или лучше, чем у весьма сложных декодеров

кодов РС. Более того, очень простой для реализации последний декодер для кода длины 32 000 оказывается способным обеспечить простейшими мажоритарными методами помехоустойчивость, принципиально недостижимую даже для кода РС длины 65 536 двухбитовых символов, декодер для которого не будет создан никогда. А если перейти к двухбайтовым недвоичным кодам с мажоритарным декодированием, то его характеристики для длины кода 32 000 символов будут соответствовать графику M32b2, еще более показательному по уровню помехоустойчивости в области, где коды РС уже не работают. При этом QМПД для двухбайтовых символов практически ни в чем не сложнее однобайтового, так как даже обычные микропроцессоры одинаково просто и быстро работают и с однобайтовыми символами, и с двух- и даже иногда с восьмибайтовыми словами.

Далее на рис. 2 показаны возможности QМПД и кодов РС при кодовой скорости

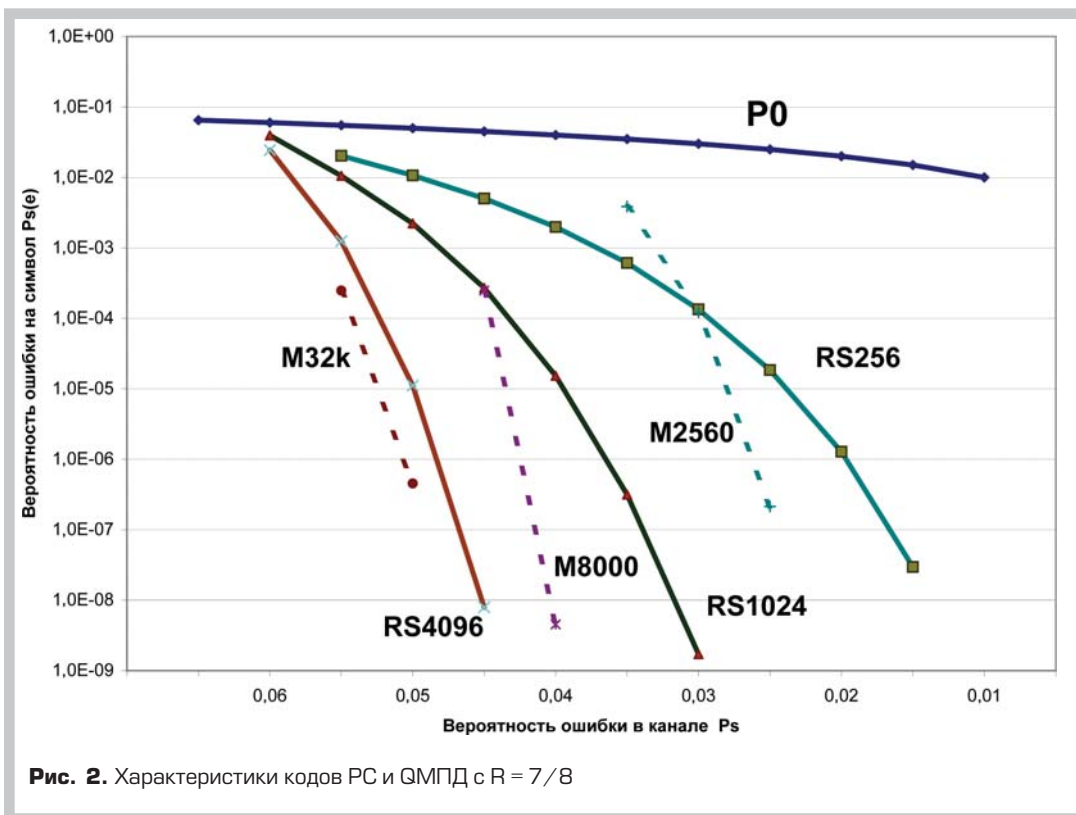
$R = 7/8$. Сплошными линиями в тех же обозначениях, что и на рис. 1, представлены вероятности ошибки на символ для кодов РС.

Пунктирными линиями помечены коды с QМПД-декодированием и длинами от 2 560 до 32 000 байтов (символ — 8 битов): M2560, M8000 и M32k. Аналогично случаю $R = 1/2$, возможность создания кодов РС длины 4096 при $R = 7/8$ в ближайшее время останется очень проблематичной, в то время как даже для кодов длины 32 000 байтов рассматриваемые недвоичные мажоритарные декодеры останутся очень простыми.

Наконец, на рис. 3 для кодов с малой избыточностью с $R = 0,95$ представлены аналогичные характеристики для QМПД и кодов РС. Для сопоставления на рис. 3 приведен также график для кода РС с $n = 256$ и $R = 7/8$ с рис. 2. Пунктирами M80Kb1 и M80Kb2 указаны возможности двух QМПД для кодов длины $n = 80 000$ и символов размером 1 и 2 байта.

Из сопоставления кодов РС длины $n = 256$ при $R = 7/8$ и $R = 19/20$ видно, насколько последний менее эффективен первого и насколько труднее обеспечивать хорошую эффективность при уменьшении избыточности. Тем не менее характеристики малоизбыточных кодов с мажоритарным декодированием на основе QМПД оказываются весьма высокими и могут обеспечивать очень высокие уровни помехоустойчивости, если выбранные коды имеют достаточные большие длины.

Подчеркнем также, что, согласно общим принципам теории кодирования, переход к каскадным принципам кодирования еще более улучшит характеристики QМПД. При этом сложность декодирования увеличится по сравнению с исходным алгоритмом очень незначительно. Детально сложность



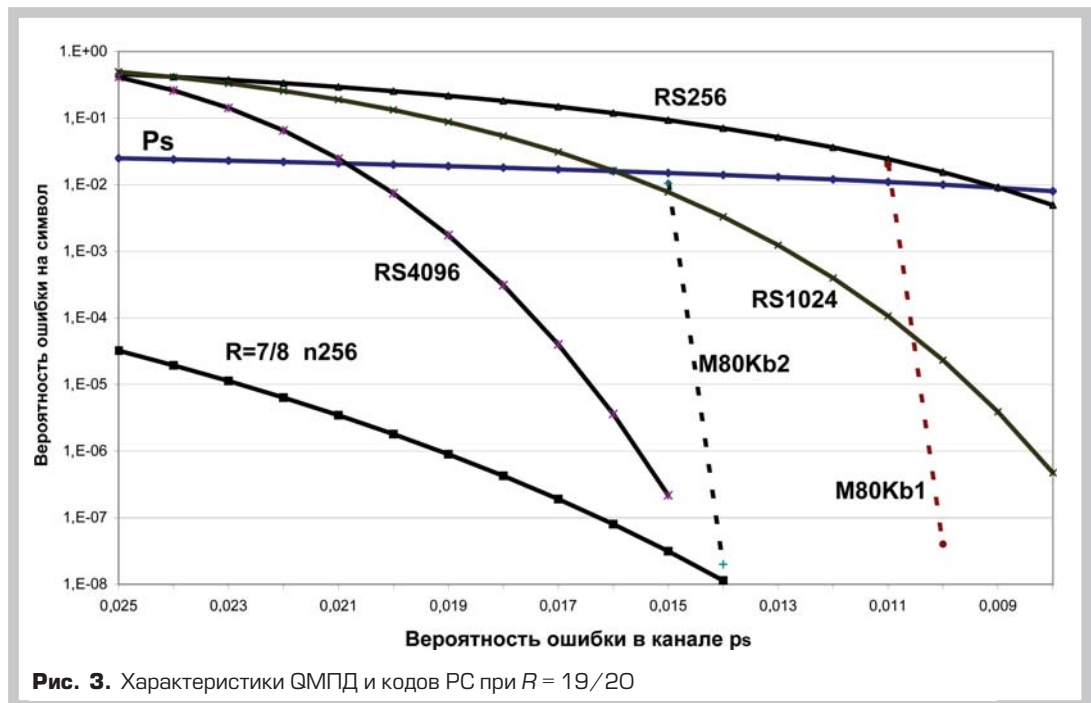
QMПД рассматривалась в [1]. Реальная очень незначительная сложность QMПД-декодера, выполняющего только операции сложения и сравнения, подтверждается скоростью работы этого алгоритма на ПК средней производительности для ряда типичных параметров кода и канала, которая составляла около 1 млрд декодированных символов за 1 ч полного моделирования функционирования кодера, имитатора шума канала и собственно декодера рассматриваемого класса.

Дальнейшее улучшение эффективности декодирования возможно при переходе к сверточным кодам, методам параллельного кодирования, применения кодов с выделенными ветвями и другим мерам, часть из которых описана в [1].

Новые области применения новых методов кодирования

Кроме естественных областей применения простых высокоэффективных методов кодирования в сетях связи следует отметить хорошие возможности применения QMПД для кодирования информации на дисках и других носителях больших объемов информации, в сверхбольших базах аудио- и видеоданных с намного более высоким уровнем достоверности, чем это было доступно до недавнего времени, а также при обновлении, восстановлении и использовании хранимых данных. При этом легко обеспечить и оперативный постоянный контроль за качеством хранимой информации, а также корректировку данных вследствие старения и возникающих дефектов носителя.

Принципиально новый уровень помехоустойчивости, достигаемый с помощью QMПД, позволяет решать перечисленные задачи без дополнительной доработки этих алгоритмов или всего лишь при незначительной



их адаптации к возможным дополнительным требованиям, возникающим в подобных масштабных цифровых системах.

Таким образом, возможность очень простого исправления ошибок в длинных двоичных кодах при эффективности, близкой к уровню, доступному только оптимальным переборным алгоритмам, открывает принципиально новые возможности для кодирования символической информации, т.е. основным видам данных, практически непосредственно используемым современным информационным обществом. Кодирование обеспечивает высокое контролируемое качество хранимой, передаваемой и формируемой информации. Применение простых и одновременно высокоэффективных методов кодирования может создать новые высокие стандарты информационного обеспечения бизнеса и государственных структур.

Разработка алгоритмов МПД поддерживались научным советом по комплексной проблеме "Кибернетика" АН СССР и ИКИ РАН.

Дополнительная информация — на специализированном

тематическом двуязычном Web-сайте ИКИ РАН www.mtdbest.iki.rssi.ru.

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

Литература

1. Золотарев В.В. Теория и алгоритмы многопорогового декодирования. — М.: Радио и связь, Горячая линия — Телеком, 2006. — 270 с.
2. Золотарев В.В. Многопороговое декодирование для информационных потоков с байтовой структурой // Мобильные системы. — М. — 2006. — №3. — С. 25 — 27.
3. Золотарев В.В. Многопороговые декодеры. — Web-сайт www.mtdbest.iki.rssi.ru.
4. Золотарев В.В., Овечкин Г.В. Помехоустойчивое кодирование. Методы и алгоритмы. Справочник. "Горячая линия — Телеком", М. — 2004. — С.124.
5. Золотарев В.В. Алгоритмы кодирования символических данных в вычислительных сетях. — В сб. "Вопросы кибернетики", Научный совет по комплексной проблеме "Кибернетика" АН СССР, ВК-106, М., 1985. — С. 54 — 62.
6. Золотарев В.В. Многопороговое декодирование в двоичных каналах. — В сб. "Вопросы радиоэлектроники", серия ЭВТ, вып.12, М.:1984.