Недвоичные многопороговые декодеры

В.В.Золотарёв
Москва
Институт космических исследований РАН

Рассмотрены простые декодеры мажоритарного типа для декодирования символьных данных. По аналогии с соответствующими алгоритмами для двоичных данных соответствующие алгоритмы названы q-ичными многопороговыми декодерами (QМПД). Они обладают свойством приближения к решению оптимального декодера при сохранении линейной сложности реализации, которая свойственна только пороговым процедурам. Возможности QМПД сравниваются с эффективностью декодеров для кодов Рида-Соломона.

Многопороговые декодеры (МПД) являются дальнейшим развитием обычных мажоритарных алгоритмов [1] и обеспечивают декодирование, во многих случаях просто совпадающее с оптимальными переборными методами.

Рассмотрим обобщение многопорогового декодирования (МПД) для двоичных данных в гауссовских каналах [2-5] на недвоичные симметричные каналы. 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 нарастающей 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, практически невозможно создать эффективные истинно оптимальные декодеры (ОД), поскольку при этом их сложность в большинстве случаев будет иметь вид $\mathbf{q}^{\mathbf{k}}$, где **k** - длина кодирующего регистра. Это и определяет важность применения QМПД, поскольку возможности декодеров для кодов Рида-Соломона (РС) очень ограничены, а их сложность реализации неоправданно велика.

Пусть задан **q**-ичный, **q**>2, симметричный канал с вероятностью ошибки $\mathbf{p_o}$>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 $\mathbf{q}^{nR}$ 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 [8,9]. В этом случае слова минимального веса **d**, где **d** - минимальное расстояние кода, имеют единственный ненулевой символ $\mathbf{i}_k$, со значением **q,** **q**>0, в его информационной части. Поскольку проверочные (а значит, и порождающие) матрицы кода содержат только нули и единички, 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 кольца целых чисел. Это дополнительно и очень существенно упрощает все процедуры кодирования и реализации последующего декодирования.

Пусть декодер типа QМПД устроен так, что после вычисления обычным образом вектора синдрома **S** принятого сообщения процедура декодирования состоит просто в том, что для очередного контролируемого пороговым (недвоичным!) элементом информационного символа кода $\mathbf{i}_k$ происходит подсчёт числа и определение значений двух относящихся к нему и наиболее часто встречающихся проверок кода, например, **q**1 и **q**2, причём **q**1 встречается **m1** раз, **q**2 - **m**2 раз, **m**1>**m**2, а остальные значения проверок для декодируемого символа $\mathbf{i}_k$ встречаются также не более **m**2 раз. Тогда QМПД при каждом изменении символа $\mathbf{i}_k$ будет переходить ко всё более правдоподобным решениям [6,7]. Если окажется, что два наиболее часто встречающихся значения проверок таковы, что **m1**=**m**2, то символ $\mathbf{i}_k$ не изменяется и делается попытка декодирования любого другого информационного символа кода. Наиболее существенным обстоятельством, повышающим корректирующие возможности описанного недвоичного МПД, является возможность принимать безошибочные решения при больших значениях **q** всего при 2-х правильных проверках относительно $\mathbf{i}_k$ из **d** возможных. Это обычно происходит в том случае, когда все неправильные проверки $\mathbf{s}_i$ относительно декодируемого символа $\mathbf{i}_k$ имеют различные значения $\mathbf{s}_i$, $\mathbf{q}_i$>$\mathbf{s}_i$>0.

Рассмотрим, как можно вычислить нижнюю оценку вероятности оптимального декодирования для кода, задаваемого описанным выше способом. Во всех подобных случаях это будет выявление наиболее часто встречающихся условий того, что вектор ошибки будет иметь расстояние Хемминга до ближайшего кодового слова меньшее, чем его собственный вес. В силу линейности кода этого достаточно для вынесения неправильного решения даже оптимальным переборным алгоритмом. Рассматривая такой вектор ошибки, будем учитывать, что нужно анализировать только те символы этого вектора, которые соответствуют позициям проверок относительно

очередного декодируемого символа $\mathbf{i_k}$. Выпишем вероятности таких наиболее частых событий, которые приводят к ошибкам оптимального декодера (ОД).

К искомым векторам ошибки относятся такие, что [6,7]:

- все проверочные символы и декодируемый символ **io** ошибочны:

$$P_1(e)=p_o^{J+1},$$

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

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

$$P_2(e)=(1-p_o)J(J-1)p_o^{J}\prod_{i=1}^{J-2}(1-i/(q-1))/(q-1)/2;$$

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

$$P_3(e)=J(1-p_o)p_o^{J};$$

- есть один правильно принятый проверочный символ, а также io, но из всех остальных неправильно принятых символов есть 3 одинаковых значения ошибок:

$$P_4=(1-p_o)^2p_o^{J-1}\prod_{i=1}^{J-4}(1-i/(q-1))J!/(6(J-4)!(q-1)^2);$$

- есть 2 правильных проверочных символа, а все остальные, включая **io**, неправильны, причем есть 2 ошибочно принятых проверочных символа с одинаковыми значениями:

$$P_5=(1-p_o)^2p_o^{J-1}J!\prod_{i=1}^{J-4}(1-i/(q-1))/(4(J-4)!(q-1));$$

- есть 3 правильных проверочных символа, а все остальные, включая **io**, неправильны, причем есть 3 ошибочно принятых проверочных символа с одинаковыми значениями:

$$P6=p_o^{J-2}(1-p_o)^3J!\prod_{i=1}^{J-6}(1-i/(q-1))/(36(J-6)!(q-1)^2).$$

Заметим, что если кодовое расстояние **d**<7, то уже последний случай рассматривать не следует, так как он предполагает наличие **J**=6 проверок в коде, тогда как для самоортогональных кодов **d**=**J**+1 [8,9]. Таким образом нижняя оценка вероятности ошибки оптимального декодирования определяется суммой найденных выше вероятностей $P_1 \div P_6$

Перечисленных событий вполне достаточно, чтобы для большинства реальных условий применения кодов получать удовлетворительные по точности вероятностные оценки потенциальной помехоустойчивости кода. А поскольку ОМПД на каждом шаге стремится к решению ОД, то можно ожидать, что при некотором достаточно высоком уровне шума он в большинстве случаев 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 ОМПД. Будем считать, что выбран код РС длины 255 (символ - 8 бит). Подчеркнём, что для ОМПД никаких ограничений по длине кода вообще нет, поскольку он работает просто в кольце целых чисел, выполняя в нем только операции сложения и сравнения в выбранном множестве. Очевидно, что недвоичный пороговый элемент, рассмотренный выше при описании операций в ОМПД, - простейшее устройство или подпрограмма с числом операций **N** сложения и сравнения небольших целых чисел **N**~10÷50 для всех тех небольших значений минимального кодового расстояния **d**, **d**<15, которое следует применять в таком декодере.

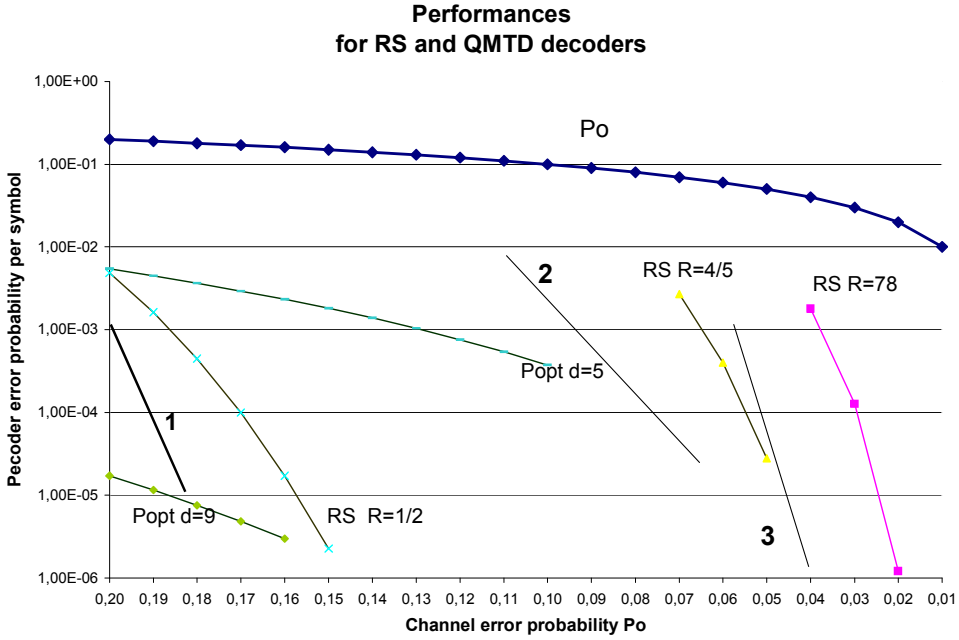

Рис.1.

На рис.1 представлены характеристики декодеров для кодов РС длины n=255 (обозначены: RS) и ОМПД в ОСК. По горизонтальной оси отложены вероятности ошибки $\mathbf{p_0}$ в указанном канале, а по оси ординат - средние вероятности ошибки на символ в результате декодирования. Для достижения решения, обычно совпадающего с оптимальным или близкого к решению ОД, ОМПД для q=256 необходимо 5÷20 итераций (повторных

попыток) декодирования принятого сообщения. Это полностью соответствует методу МПД для двоичных кодов [2-5].

Как следует из вида графиков зависимостей средней вероятности ошибки декодирования на символ **Ps**(e) от вероятности $\mathbf{p_o}$ канала QCK 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. 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.

Очевидно, что каскадирование нескольких недвоичных МПД также значительно улучшит вероятностные характеристики декодирования без значительного увеличения сложности, т. е. числа операций, осуществляемых декодером, работающим только с целыми числами и не выполняющего никаких операций умножения или деления. Это является его решающим преимуществом перед алгоритмами для кодов РС при сопоставлении их по сложности реализации.

Представленные результаты позволяют утверждать, что описанные почти 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.

Литература

1. Месси Дж. Пороговое декодирование. - М.: Мир, 1966.
2. Самойленко С.И., Давыдов А.А., Золотарёв В.В., Третьякова Е.И. Вычислительные сети. – М.: Наука, 1981, с. 277.
3. Золотарёв В.В.. Эффективные многопороговые алгоритмы декодирования. - АН СССР, Научный совет по комплексной проблеме "Кибернетика", препринт, М., 1981,с.75.
4. Золотарёв В.В. Использование помехоустойчивого кодирования в технике связи. - Электросвязь, №7, с.7-10, 1990.
5. Золотарёв В.В. Реальный энергетический выигрыш кодирования для спутниковых каналов. - В кн.: 4-я Международная Конференция “Спутниковая связь – ICSC-2000”, Т.2, с. 20-25, М.: МЦНТИ, 2000.
6. Золотарёв В.В.. Алгоритмы кодирования символьных данных в вычислительных сетях. - В сб.: "Вопросы кибернетики", ВК-106, М.,1985.
7. Золотарёв В.В.. Многопороговое декодирование в недвоичных каналах. - В сб.: "Вопросы радиоэлектроники", Серия ЭВТ, вып.12, М.,1984.
8. Townsend R.L., Weldon E.J. Self-Orthogonal Quasi-cyclic Codes. IEEE Trans., IT-13, 1967, pp.183-195.
9. Robinson J.P., Bernstein A.J. A Class of Binary Recurrent Codes with Limited Error Propagation. - IEEE Trans., vol. IT-13, NO.1,1967, pp.106-113.