МНОГОПОРОГОВОЕ ДЕКОДИРОВАНИЕ ДЛЯ ИНФОРМАЦИОННЫХ ПОТОКОВ С БАЙТОВОЙ СТРУКТУРОЙ

The author examines the multithreshold decoding method application for error correction in byte structure data, evaluates decoding characteristics and adduces modeling results in comparison with correcting possibilities of the Reed-Solomon codes. He makes the conclusion that nonbinary multithreshold decoding actually has high effectiveness that is unavailable for Reed-Solomon codes decoders.

В.В. ЗОЛОТАРЕВ,
ИКИ РАН

ВВЕДЕНИЕ

Микропроцессорная реализация методов помехоустойчивого кодирования позволяет решать широкий круг задач в цифровых сетях связи. Основное преимущество систем связи с помехоустойчивым кодированием состоит в том, что энергетическая эффективность использования каналов оказывается во много раз более высокой, чем в случае когда оно не используется. Ниже предлагается метод итеративного декодирования, реализованный на идеях многопорогового декодирования (МПД) [2 — 4, 9], который можно использовать при обработке цифрового потока пословно, например байтами. МПД является развитием мажоритарных декодеров. В этом случае происходит дополнительное ускорение по сравнению с побитной обработкой, которая в большей степени соответствует аппаратной реализации процессов обработки.

Поскольку в системах мобильной связи необходимо более полно реализовать как частотную, так и энергетическую эффективность, то программная реализация систем декодирования с небольшим объемом вычислений может оказаться более предпочтительной, чем аппаратная.

ОБОБЩЕНИЕ АЛГОРИТМА МПД НА НЕДВОИЧНЫЕ КОДЫ

Рассмотрим обобщение многопорогового декодирования (МПД) на недвоичные симметричные каналы [2, 3]. Ценность этого метода заключается в том, что мажоритарные алгоритмы имеют всего лишь линейный рост сложности от числа операций декодирования и длины кода n. Поскольку обычно оптимальные методы характеризуются экспоненциально растущей сложностью, применение недвоичных МПД, обозначаемых далее как QMПД, представляется особенно желательным.

Еще более существенно, что в случае больших значений основания недвоичного кода q, $q > 10$ вообще 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 QMПД, поскольку возможности декодеров для кодов Рида-Соломона очень ограниченны, а их сложность реализации достаточно велика. Увеличение длины кодов Рида-Соломона возможно только при росте основания q, что ведет к существенному и совершенно неоправданному росту сложности декодирования в случаях как аппаратной, так и программной реализации.

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) назовем этот канал также q-ичным симметричным каналом (QCK). 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 предполагается, 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 сверточному коду. 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 кодеры и декодеры выполняют только операцию сложения для формирования проверочных символов кода и вычисления синдрома S принятого сообщения. 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 реализацию последующего декодирования.

Пусть декодер типа QMПД 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 i_k происходит подсчет числа и определение значений двух относящихся к нему и наиболее часто встречающихся проверок кода, например q_1 и q_2, причем q_1 встречается m_1 раз, q_2 — m_2 раз, $m_1 > m_2$, а остальные значения проверок для декодируемого символа i_k встречаются также не более m_2 раз. Тогда QMПД при каждом изменении символа i_k будет переходить ко все более правдоподобным решениям. Если окажется, что два наиболее часто встречающихся значения проверок таковы, что $m_1 = m_2$, то символ i_k не изменяется и делается попытка декодирования любого другого информационного символа кода.

Наиболее существенным обстоятельством, значительно повышающим корректирующие возможности описанного недвоичного МПД, является возможность принимать безошибочные решения при больших значениях q всего при двух правильных проверках относительно i_k из d возможных. Это обычно происходит в том случае, когда все неправильные проверки $\boldsymbol{s_i}$ относительно декодируемого символа $\boldsymbol{i_k}$ имеют различные значения s_i, $q_i > s_i > 0$. При трех и более проверках в некоторых случаях правильное решение декодера о декодируемом символе возможно даже при совпадении значений ошибок в части проверок, поступающих на пороговый элемент.

ОЦЕНКИ ВЕРОЯТНОСТЕЙ ОШИБКИ ДЕКОДИРОВАНИЯ

Рассмотрим вычисление нижней оценки вероятности оптимального декодирования для кода, задаваемого описанным выше способом. Во всех анализируемых далее 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 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 наиболее частых событий, которые всегда приводят к ошибкам оптимального декодера (ОД).

— все проверочные символы и декодируемый символ i_0 ошибочны

$$P_1(e) = p_0^{J+1},$$

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

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

$$P_2(e) = (1-p_0)J(J-1)p_0^J \prod_{i=1}^{J-2} \frac{2\left(1-\frac{i}{q-1}\right)}{(q-1)};$$

— правильно принят один проверочный символ, а остальные ошибочны, как и i_0

$$P_3(e) = J(1-p_0)p_0^J;$$

— правильно принят один проверочный символ и i_0, но из всех остальных неправильно принятых символов есть три одинаковых значения ошибок

$$P_4 = (1-p_0)^2 p_0^{J-1} \prod_{i=1}^{J-4} \frac{\left(1-\frac{i}{q-1}\right) J!}{6(J-4)!(q-1)^2};$$

— есть два правильно проверочных символа, а все остальные, включая i_0, неправильны, причем два ошибочно принятых проверочных символа имеют одинаковые значения:

$$P_5 = (1-p_0)^2 p_0^{J-1} J! \prod_{i=1}^{J-4} \frac{\left(1-\frac{i}{q-1}\right)}{4(J-4)!(q-1)};$$

— правильно принято три проверочных символа, а все остальные, включая i_0, неправильно, причем три ошибочно принятых проверочных символа имеют одинаковые значения

$$P_6 = p_0^{J-2}(1-p_0)^3 J! \prod_{i=1}^{J-6} \frac{1-\left(\frac{i}{q-1}\right)}{36(J-6)!(q-1)^2}.$$

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 $d = J + 1$. Таким образом, нижняя оценка вероятности ошибки оптимального декодирования определяется суммой найденных выше вероятностей $P_1 — P_6$.

Более полное перечисление событий, приводящих к ошибкам недвоичного ОД, оценки вероятностей их появления, а также вероятности ошибки в первом символе недвоичного ПД приведены в [2, 3].

Перечисленных событий вполне достаточно, чтобы для большинства реальных условий применения кодов получать удовлетворительные по точности вероятностные оценки потенциальной помехоустойчивости кода. А поскольку QMПД 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.

ХАРАКТЕРИСТИКИ ДЕКОДИРОВАНИЯ

Во многих системах особенно удобно работать с данными, имеющими байтовую структуру. Это соответствует кодам с $q = 256$. Отметим, что кроме кодов Рида-Соломона в настоящее время вообще нет других сколько-нибудь эффективных методов декодирования недвоичных символьных данных. Сравним вероятностные характеристики кодов Рида-Соломона с возможностями QMПД. Выберем код Рида-Соломона длиной 255 символов (символ состоит из 8 битов). Подчеркнем, что для QMПД никаких ограничений по длине кода вообще нет, поскольку он выполняет только операции сложения по модулю 256 и сравнения.

Очевидно, что недвоичный пороговый элемент, рассмотренный выше при описании операций в QMПД, — простейшее устройство или подпрограмма с числом операций N сложения и сравнения небольших целых чисел $N \sim 20 — 50$ для всех тех небольших значений минимального кодового расстояния d, ($d < 15$), которое следует применять в таком декодере.

На рис. 1 представлены характеристики декодеров для кодов Рида-Соломона длины $n = 255$ (обозначены RS) и QMПД в QCK.

Для достижения решения, совпадающего с оптимальным или близкого к решению ОД, QMПД для $q = 256$ необходимо 5 — 20 итераций (повторных попыток) декодирования принятого сообщения. Это полностью соответствует методу МПД для двоичных кодов.

Как следует из рис. 1 для кодовых скоростей $R = 1/2$, $R = 4/5$ и $R = 7/8$, простейший по своему устройству QMПД (графики 1, 2 и 3) обеспечивает гораздо более высокие характеристики, чем декодеры для кода Рида-Соломона, благодаря несколько большей длине (n = 1000) используемых кодов и вследствие этого хорошей сходимости решений QMПД к решению ОД.

Для сопоставления на рис.1 приведены также нижние оценки для применявшихся при моделировании недвоичных самоортогональных кодов в случае оптимального декодирования для $d = 5, 9$, полученные с использованием приведенных выше формул.

Заметим, что в настоящее время неизвестны другие алгоритмы декодирования с приемлемой сложностью реализации, которые могут обеспечить такие же характеристики. При увеличении длины кодов характеристики QMПД могут быть дополнительно существенно улучшены.

Несомненно, что проблемы сложности реализации кодирования сохранятся в обозримом будущем, а благодаря росту скоростей обмена информацией требования более простой реализации декодеров станут все более актуальными.

Очевидно, что каскадирование нескольких недвоичных МПД также значительно улучшит вероятностные характеристики декодирования без значительного увеличения сложности. Это является его решающим преимуществом перед алгоритмами для кодов Рида-Соломона при сопоставлении их по сложности реализации.

ВЫВОДЫ

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

Несомненно, проблемы сложности реализации кодирования сохранятся в обозримом будущем, а благодаря росту скоростей обмена информацией требования более простой реализации декодеров станут все более актуальными.

Финансовую поддержку разработки QMПД осуществлял РФФИ по гранту №90024-05-07.

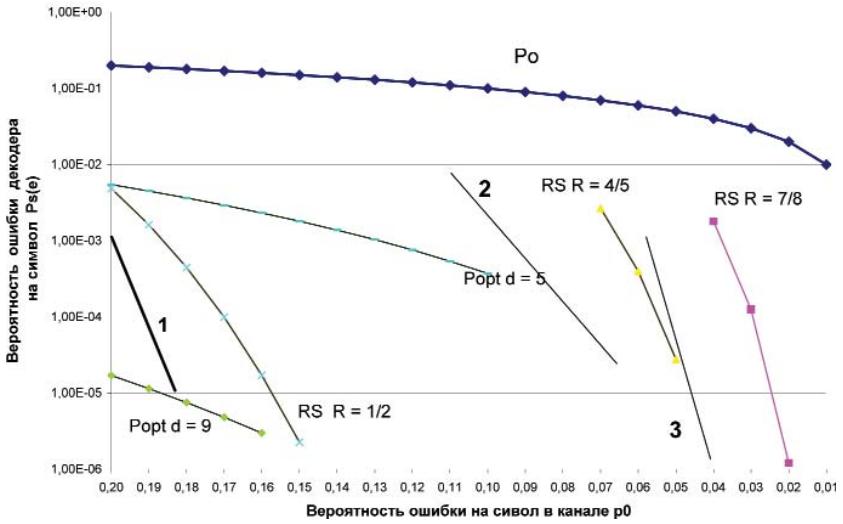

Рис.1. Эффективность QMПД и кодов Рида-Соломона

ЛИТЕРАТУРА

1. **Золотарев В.В.** Алгоритмы многопортового декодирования линейных кодов// Мобильные системы. — 2005. — № 12.

2. **Золотарев В.В.** Алгоритмы кодирования символьных данных в вычислительных сетях//Вопросы кибернетики, ВК-106. — М.,1985. — С. 45 — 49.

3. **Золотарев В.В.** Многопороговое декодирование в недвоичных каналах//Вопросы радиоэлектроники. — Серия ЭВТ. Вып.12. — М.,1984. — С. 14 — 17.