Конференция «66-я Научная сессия, посвященная Дню радио». Москва 2011. Том 1. Стр. 245–247.

КАСКАДНЫЕ МЕТОДЫ ДЕКОДИРОВАНИЯ СИМВОЛЬНЫХ ПОМЕХОУСТОЙЧИВЫХ КОДОВ, ОСНОВАННЫЕ НА МНОГОПОРОГОВЫХ АЛГОРИТМАХ

Золотарёв В.В.[1], Овечкин Г.В.[2], Овечкин П.В.[2]

[1]Институт космических исследований
[2]Рязанский государственный радиотехнический университет

Повышение достоверности передачи и хранения цифровых данных реализуется с помощью методов помехоустойчивого кодирования. При этом часто оказывается более удобным работать с данными на уровне целых символов, например байтов. В частности, легче работать с символьной информацией при организации надежного хранения цифровых данных, коррекции пакетирующихся ошибок, поступивших из канала или от декодера внутреннего кода каскадной конструкции. В подобных случаях для защиты данных от ошибок целесообразно применение недвоичных помехоустойчивых кодов.

На сегодняшний день в теории кодирования известен ряд недвоичных кодов, различающихся корректирующей способностью, вносимой избыточностью, сложностью декодирования и многими другими важными параметрами. Среди них практическое применение в реальных системах нашли только коды Рида-Соломона (РС) [1], для которых существуют достаточно эффективные алгебраические алгоритмы декодирования, в полной мере использующие корректирующие возможности кода. Сложность реализации наиболее простых из них пропорциональна n^2 [2], где n – длина кода. Под сложностью реализации здесь понимается число арифметических операций, требуемых для декодирования кодового блока. В ряде публикаций [3] показано, что короткие коды РС часто не могут обеспечить требуемой в настоящее время степени защиты данных от ошибок, а для длинных кодов РС из-за высокой сложности реализации практически невозможно создать эффективные декодеры. В последнее время зарубежные специалисты стали активно развивать декодеры недвоичных низкоплотностных кодов [4]. Данные методы обладают очень высокой корректирующей способностью, однако их сложность, особенно при больших размерах алфавита q, оказывается слишком большой для применения в реальных системах.

Гораздо лучшей эффективностью, чем коды РС, обладают недвоичные многопороговые декодеры (qМПД) [5, 6], разрабатываемые в Институте космических исследований РАН и Рязанском государственном радиотехническом университете. Предложенные еще в 1984 году qМПД обладают линейной зависимостью сложности реализации от длины кода и позволяют практически оптимально декодировать даже очень длинные, потенциально гораздо более эффективные недвоичные самоортогональные коды (qСОК). В результате, применение qСОК, декодируемых с помощью qМПД, вместо кодов РС может на много порядков повысить уровень защиты информации от ошибок при существенном упрощении процесса коррекции ошибок. Рассмотрим характеристики данных методов.

На рис. 1 представлены зависимости вероятности символьной ошибки декодирования P_s от вероятности ошибки P_0 в q-ичном симметричном канале (qСК), в котором передаваемые символы искажаются независимо друг от друга с равной вероятностью. Характеристики qМПД для qСОК с кодовым расстоянием d=17 длиной n порядка 32000 однобайтовых символов (q=256) при кодовой скорости R=1/2 представлены кривой *1*. Отметим, что достаточно простой для реализации qМПД способен исправлять до 25% байтовых ошибок в канале. При использовании же кодов

Рида-Соломона даже с применением каскадирования удается обеспечить сопоставимую вероятность ошибки всего при 18% символьных ошибок в канале при кодовой скорости 1/2 и 10 итерациях декодирования.

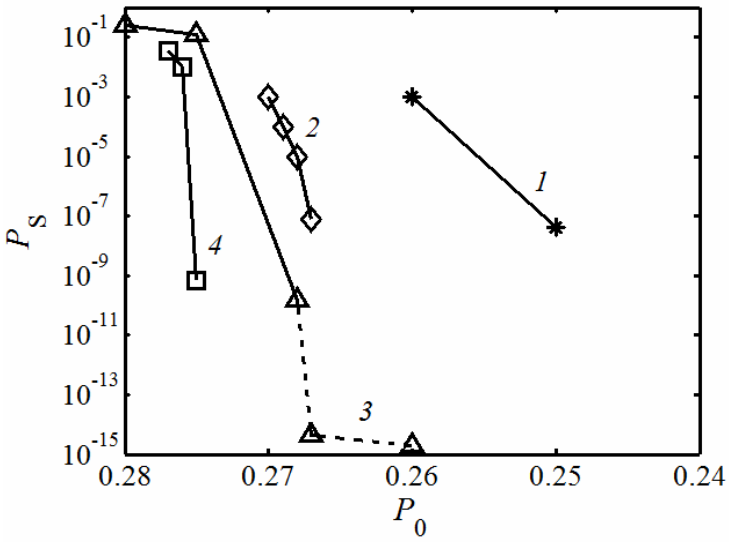

Рис. 1. Характеристики qМПД в qСК для различных кодов с R≈1/2 и q=256

Для qМПД дополнительно предложен ряд подходов к повышению его эффективности. В частности в [7] предложен алгоритм оптимизации структуры кода, позволяющий найти qСОК, для которых qМПД обеспечивает лучшую корректирующую способность при большом уровне шума в канале связи. Зависимость вероятности ошибки декодирования от вероятности ошибки в qСК для одного из таких найденных кодов с d=17, n=32000, q=256, R=1/2 отражены на рис. 1 кривой *2*. Отметим, что только за счет выбора лучшей структуры кода удалось повысить долю исправляемых ошибок в qСК до 26,5% без усложнения декодера.

Еще более значительное повышение корректирующей способности qМПД обеспечивается при использовании каскадных методов коррекции ошибок, основанных на qМПД.

Первый метод используется для декодирования каскадного кода, состоящего из внутреннего qСОК и предложенных внешних недвоичных кодов Хэмминга (как обычных, так и расширенных) [8]. При кодировании каскадным кодом исходные данные сначала кодируются внешним кодом, в результате чего получается несколько кодовых слов недвоичного кода Хэмминга, которые кодируются кодером внутреннего кода, образуя кодовое слово qСОК.

В работе [8] показано, что известные в литературе недвоичные коды Хэмминга обладают рядом недостатков, которые не допускают применения таких кодов в данной каскадной схеме. Поэтому вместо них используются модифицированные недвоичные коды Хэмминга, основанные на обычных двоичных. Данные коды имеют длину 2^m–1 (m – число проверочных символов кода), не зависящую от размера символа, при кодировании/декодировании используется арифметика по модулю q, которая позволяет легко работать с символами практически любой размерности, и с помощью предложенных кодов в большинстве случаев возможно исправление двух ошибок в кодовом блоке.

Для разработанного декодера такого каскадного кода получены как аналитические оценки эффективности, так и результаты компьютерного моделирования. Из данных результатов следует возможность уменьшения с помощью предложенных методов каскадирования вероятности ошибки декодирования на 5 и более порядков по сравнению с исходным qМПД при сохранении минимально возможной, линейной сложности

реализации декодера. Пример характеристик каскадной схемы, состоящей из qСОК с R=8/16, q=256, d=17, n=32000 и предложенного недвоичного расширенного кода Хэмминга с длиной N_2=128, показан на рис. 1 кривой *3*. Часть кривой, представленная пунктиром, получена с использованием нижней оценки вероятности ошибки декодирования, поскольку за время моделирования (объем моделирования 10^{14} символов) не было получено ни одной ошибки декодирования. Отметим, что сложность декодирования из-за добавления декодера недвоичного расширенного кода Хэмминга увеличивается не более чем на 35% по сравнению с исходным qМПД.

Второй метод используется для декодирования каскадного кода, состоящего из внутреннего qСОК и внешнего qСОК. Данные коды образуют обычный код-произведение. При декодировании каскадного кода сначала выполняется декодирование внутреннего qСОК с помощью обычного qМПД, после чего в соответствии со сформулированным правилом работы недвоичного порогового элемента выполняется декодирование внешнего qСОК.

Данное правило заключается в том, что если среди всех проверок и элементов разностного регистра, связанных с декодируемым символом u_{ij}, выбрать ненулевое значение проверки h, для которого сумма $n_{ij}^{(h)} + \sum_{m\in\Omega_i} n_{mj}^{(s_{mj}^{(2)}-h)}$ максимальна и удовлетворяет условию

$$n_{ij}^{(0)} + \sum_{m\in\Omega_i} n_{mj}^{(s_{mj}^{(2)})} < n_{ij}^{(h)} + \sum_{m\in\Omega_i} n_{mj}^{(s_{mj}^{(2)}-h)},$$

то при изменении символа u_{ij} на значение h расстояние между принятым сообщением и кодовым словом полного каскадного кода уменьшится и, следовательно, произойдет переход к более правдоподобному решению. Здесь $n_{ij}^{(x)}$ – число элементов синдромного и разностного регистров внутреннего qСОК, соответствующих информационному символу u_{ij}, значение которых равно x; Ω_i – множество номеров проверок, участвующих при декодировании i-го символа внешнего кода; $s_{mj}^{(2)}$ – элемент массива синдрома декодера внешнего qСОК.

Следует заметить, что непосредственное использование данного правила при большом числе проверок, связанных с декодируемым символом, может оказаться вычислительно сложным. При незначительных потерях в эффективности можно организовать декодирование внешнего кода с помощью обычного qМПД, который при работе не будет использовать информацию, полученную от qМПД внутреннего кода.

Пример характеристик данного метода каскадирования представлен на рис. 1 кривой *4*, которая соответствует эффективности работы декодера каскадного кода, состоящего из внутреннего qСОК с d=5, R=8/16 и внешнего qСОК с d=7, R=19/20 при работе с однобайтовыми символами. При этом qМПД внешнего кода работал без учета дополнительной информации от декодера внутреннего кода. Отметим, что предложенный метод декодирования способен эффективно работать даже при 27,5 % байтовых ошибок в qСК, что недостижимо для других практически реализуемых методов коррекции ошибок в символьных данных.

Дополнительно следует отметить, что сложность реализации qМПД не зависит от размера используемых символов, что позволяет создавать декодеры многопорогового типа (в том числе и каскадные), эффективно исправляющие ошибки даже в многобайтовых символах (например, в четырехбайтовых символах и более), для которых создание декодеров других типов представляется очень затруднительным. Все это позволяет считать, что в дальнейшем qМПД смогут заменить коды Рида-Соломона в самых разных системах передачи и хранения данных, обеспечивая работу подобных систем в значительно более сложных условиях, чем возможно в настоящее время.

Работа выполнена при финансовой поддержке РФФИ (грант №08-07-00078), ИКИ РАН, РГРТУ. Большой объем дополнительной информации о декодерах многопорогового типа можно найти на веб-сайтах [6].

Литература

1. Reed I. S., Solomon G. Polynomial codes over certain finite fields // J. Soc. Industrial Appl. Math. – 1960. – Vol. 8. – P. 300–304.

2. Ning C., Zhiyuan Y. Complexity analysis of Reed-Solomon decoding over GF(2^m) without using syndromes // EURASIP Journal on Wireless Communications and Networking. – January 2008. – №4. – P. 1-11.

3. Золотарёв В.В., Кузнецов Н.А., Овечкин Г.В., Овечкин П.В. Недвоичные многопороговые декодеры и другие методы коррекции ошибок в символьной информации // Радиотехника. – М., 2010. – №6. – Вып. 141. – С. 4–9.

4. Davey M.C., MacKay D.J.C. Low density parity check codes over GF(q) // IEEE Comm. Letters. – 1998. – V.2(6). – P.165–167.

5. Золотарёв В.В., Овечкин Г.В. Эффективное многопороговое декодирование недвоичных кодов // Радиотехника и электроника. – М., 2010. – Т.55. – №3. – С.324–329.

6. Веб-сайты ИКИ РАН www.mtdbest.iki.rssi.ru и РГРТУ www.mtdbest.ru.

7. Овечкин Г.В., Овечкин П.В. Оптимизация структуры недвоичных самоортогональных кодов для схем параллельного кодирования // Труды НИИР. – М., 2009. – №2. – С.34–38.

8. Овечкин Г.В., Овечкин П.В. Использование недвоичного многопорогового декодера в каскадных схемах коррекции ошибок // Вестник РГРТУ. – Рязань, 2009. – №4 (выпуск 30). – С.7-12.