

ОВЕЧКИН Г.В.

(Рязанский государственный радиотехнический университет, г. Рязань)

МЕТОДЫ УЛУЧШЕНИЯ ЭФФЕКТИВНОСТИ МНОГОПороГОВЫХ ДЕКОДЕРОВ СИМВОЛЬНЫХ САМООРТОГОНАЛЬНЫХ КОДОВ

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 (q МПД) [5, 6] символьных самортогональных кодов (q СОК), разрабатываемые в Институте космических исследований РАН и Рязанском государственном радиотехническом университете. Отметим, что эти коды и q МПД алгоритмы являются открытиями в теории помехоустойчивого кодирования. Предложенные еще в 1984 году q МПД обладают линейной зависимостью сложности реализации от длины кода и позволяют практически оптимально декодировать даже очень длинные, потенциально гораздо более эффективные q СОК. В результате, применение q СОК, декодируемых с помощью q МПД, вместо кодов РС может на много порядков повысить уровень защиты информации от ошибок при существенном упрощении процесса коррекции ошибок.

Рассмотрим характеристики q МПД в q -ичном симметричном канале (q СК). В таком канале каждый символ искажается независимо от других с вероятностью P_0 , причем при искажении символ с равной вероятностью переходит в один из $q-1$ оставшихся символов. Подобная модель, например, соответствует каналу с пакетами ошибок при использовании перемежения/деперемежения на уровне символов. Зависимости вероятности символьной ошибки P_s после декодирования от вероятности символьной ошибки P_0 в q СК для кодов с кодовой скоростью $R=1/2$ представлены на рис. 1. Здесь кривыми 4 и 5 показаны характеристики q МПД для кодов с длиной блока $n=4000$ и 32000 символов при использовании 8-ми битовых символов (размер алфавита $q=256$). Объем моделирования в нижних точках данных графиков составлял от $5 \cdot 10^{10}$ до $2 \cdot 10^{12}$ символов, что свидетельствует о крайней простоте метода. Для сравнения на данном рисунке кривой 1 показаны характеристики (255, 128) кодов РС для $q=256$. Из рис. 1 видно, что эффективность q МПД оказывается гораздо лучше эффективности кодов РС для символов такого же размера. При увеличении длины блока

q МПД разница в эффективности становится еще более существенной. Отметим, что разнообразные методы повышения корректирующей способности кодов РС, в том числе все вариации алгоритма Судана, обладают сложностью порядка n^3 . Для кодов длины 32000 символов это приводит к разнице в порядке сложности около $n^2 = 32000^2 \approx 10^9$, т.е. в миллиард раз, при этом улучшение помехоустойчивости оказывается весьма незначительным. Это продемонстрировано на рис. 1 кривой 3, которой представлены характеристики алгоритма Судана для (255, 128) кода РС. Дополнительно отметим, что достаточно простой для реализации q МПД 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.

Дополнительным преимуществом q МПД над другими методами коррекции ошибок является то, что он позволяет легко работать с символами практически любого размера, обеспечивая при этом такую же высокую корректирующую способность. Это подтверждается представленными на рисунке характеристиками q МПД для кода длиной 32000 двухбайтовых символов (кривая 6) и длиной 100000 четырехбайтовых символов (кривая 9). Отметим, что очень простой для реализации q МПД декодер для двухбайтового кода длины 32000 оказывается способным обеспечить помехоустойчивость, принципиально недостижимую даже для кода РС длины 65535 двухбайтовых символов (кривая 2 на рис. 1, декодер для которого не подлежит реализации в обозримом будущем. Кроме того, q МПД для четырехбайтовых символов превосходит по эффективности даже на три порядка более сложный декодер не двоичных низкоплотных кодов длиной 100000 четырехбайтовых символов, пример характеристик которого представлен на рис. 3 кривой 8 [7].

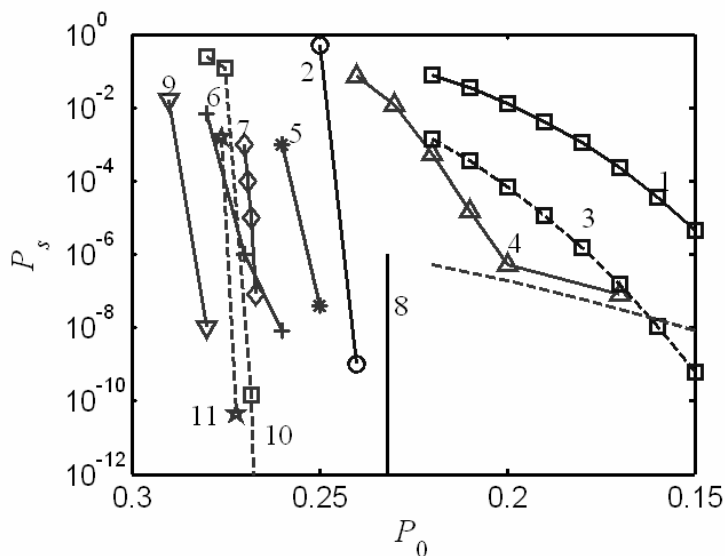


Рис. 1. Характеристики не двоичных кодов с кодовой скоростью $R=1/2$ в q СК

Следует заметить, что для достижения с помощью q МПД таких результатов требуется очень тщательно выбирать применяемые коды, основным критерием при отборе которых является степень устойчивости к эффекту размножения ошибок [8], который проявляется в том, что после первой ошибки декодирования существенно увеличивается вероятность последующих ошибок. Известно, что размножению ошибок в наименьшей степени подвержены коды для схем с параллельным кодированием [8]. В [9] показано, что оптимизируя структуру данных кодов можно еще улучшить эффективность работы q МПД. В частности, характеристики найденных в [9] кодов с $q=256$ и кодовой скоростью 1/2 представлены на рис. 1

кривой 7. Отметим, что только за счет выбора лучшей структуры кода удалось повысить долю исправляемых ошибок в q СК до 26,5% без усложнения декодера.

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

Первый метод используется для декодирования каскадного кода, состоящего из внутреннего q СОК и предложенных внешних не двоичных кодов Хэмминга (как обычных, так и расширенных) [10]. При кодировании каскадным кодом исходные данные сначала кодируются внешним кодом, в результате чего получается несколько кодовых слов не двоичного кода Хэмминга, которые кодируются кодером внутреннего кода, образуя кодовое слово q СОК.

В работе [10] показано, что известные в литературе не двоичные коды Хэмминга обладают рядом недостатков, которые не допускают применения таких кодов в данной каскадной схеме. Поэтому вместо них используются модифицированные не двоичные 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 q МПД при сохранении минимально возможной, линейной сложности реализации декодера. Пример характеристик каскадной схемы, состоящей из q СОК с $R=8/16$, $q=256$, $d=17$, $n=32000$ и предложенного не двоичного расширенного кода Хэмминга с длиной $N_2=128$, показан на рис. 1 кривой 10. Отметим, что сложность декодирования из-за добавления декодера не двоичного расширенного кода Хэмминга увеличивается не более чем на 35% по сравнению с исходным q МПД.

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

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 q СОК, 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 q СОК.

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 q МПД, который при работе не будет использовать информацию, полученную от q МПД внутреннего кода.

Пример характеристик данного метода каскадирования представлен на рис. 1 кривой 11, которая соответствует эффективности работы декодера каскадного кода, состоящего из

внутреннего q СОК с $d=5$, $R=8/16$ и внешнего q СОК с $d=7$, $R=19/20$ при работе с однобайтовыми символами. При этом q МПД 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 q СК, что недостижимо для других практически реализуемых методов коррекции ошибок в символьных данных.

Дополнительно следует отметить, что сложность реализации q МПД 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 q МПД 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].

Библиографический список

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. Zhang F., Pfister H. List-Message Passing Achieves Capacity on the q -ary Symmetric Channel for Large q // In Proc. IEEE Global Telecom. Conf., Washington, Nov. 2007. P.283–287.
8. Золотарёв В.В. Теория и алгоритмы многопорогового декодирования. М.: Радио и связь, Горячая линия – Телеком, 2006.
9. Овечкин Г.В., Овечкин П.В. Оптимизация структуры недвоичных самоортогональных кодов для схем параллельного кодирования // Труды НИИР. – М., 2009. – №2. – С.34–38.
10. 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.

G.V.OVECHKIN

METHODS FOR PERFORMANCE IMPROVEMENT OF MULTITHRESHOLD DECODERS FOR NON-BINARY SELF-ORTHOGONAL CODES

Error-correcting coding is applied to correction of the errors arising at data transmission over physical channels. In many cases in real systems it is convenient to work with data having byte structure. By this time among non-binary codes only Reed-Solomon codes was found practical application. Considerably better efficiency q -ary multithreshold decoders (q MTD) of non-binary self-orthogonal codes possess. In paper several methods for q MTD performance improvement are discussed. It's shown these methods allow to provide efficient error correction in data containing even 27,5% byte errors. Such performance is not achievable for existing methods of error correction in non-binary data.