

ЭФФЕКТИВНОЕ МНОГОПороГОВОЕ ДЕКОДИРОВАНИЕ НЕДВОИЧНЫХ САОРТОГОНАЛЬНЫХ КОДОВ

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

¹Институт космических исследований

²Рязанский государственный радиотехнический университет

Введение

Помехоустойчивое кодирование применяется для исправления ошибок, возникающих при передаче данных по каналам с шумами. В настоящее время наибольшее внимание уделяется развитию методов коррекции ошибок в двоичных данных. Однако во многих случаях в реальных системах удобно работать с данными, имеющими байтовую структуру. Например, удобнее работать с байтами в системах хранения больших объемов информации (CD диски и др. носители). В подобных системах для защиты данных от ошибок целесообразно применение недвоичных помехоустойчивых кодов.

К настоящему времени среди недвоичных кодов практическое применение нашли только коды Рида-Соломона (РС) [1], обладающие рядом положительных свойств. В частности коды РС характеризуются тем, что для исправления в пределах кодового слова любой комбинации из t символьных ошибок достаточно использовать лишь $2t$ проверочных символов. Кроме того для коротких кодов Рида-Соломона существуют достаточно эффективные алгоритмы декодирования, в полной мере использующие корректирующие возможности кода. Однако короткие коды РС часто не могут обеспечить требуемой в настоящее время степени защиты данных от ошибок, а для длинных кодов РС практически невозможно создать эффективные декодеры.

Значительно лучшей эффективностью обладают недвоичные многопороговые декодеры (q МПД) [2–4]. Известно, что q МПД обладают линейной сложностью реализации и позволяют практически оптимально декодировать даже очень длинные, потенциально гораздо более эффективные коды [2]. В результате, применение недвоичных МПД вместо кодов РС может на много порядков повысить уровень защиты информации от ошибок при одновременном существенном упрощении процесса коррекции ошибок. Рассмотрим характеристики недвоичных многопороговых декодеров в q -ичном симметричном канале (q СК) и основные подходы к их улучшению.

Характеристики q МПД

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 1 и 2 показаны характеристики q МПД для кодов с длиной блока $n=4000$ и 60000 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 4 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. Характеристики q МПД при использовании двухбайтовых символов представлены на рис. 1 кривой 3. Здесь использовался код с $R=1/2$ и $n=32000$ символов. 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 5 на рис. 1), декодер для которого чрез-

вычайно сложен для реализации. Отметим, что для кодов РС существуют алгоритмы декодирования, позволяющие исправлять даже несколько большее, чем t , число ошибок, например, алгоритм Судана [5]. Данные методы очень интересны для теории кодирования, однако сложность их реализации становится пропорциональной n^3 , в то время как рост эффективности декодирования от такого усложнения, особенно при высоких кодовых скоростях, которые часто и требуется применять на практике, оказывается незначительным [2]. Это иллюстрируется кривой 7 на рис. 1, которая соответствует алгоритму декодирования Судана для кода РС с $n=255$, $q=256$ и $R=1/2$. При этом алгоритм декодирования оказывается сложнее q МПД в десятки тысяч раз и более (в зависимости от длина кода).

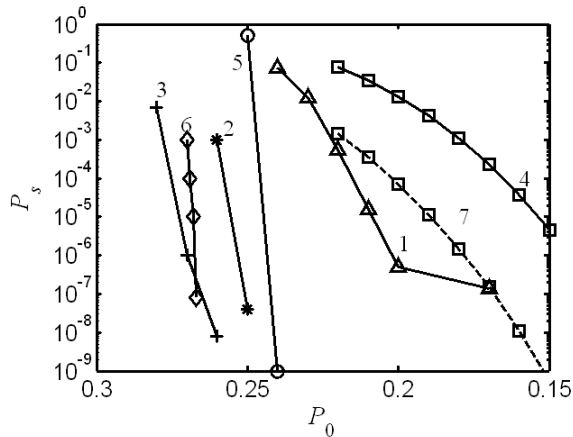


Рис. 1. Характеристики недвоичных кодов с $R=1/2$ в q СК

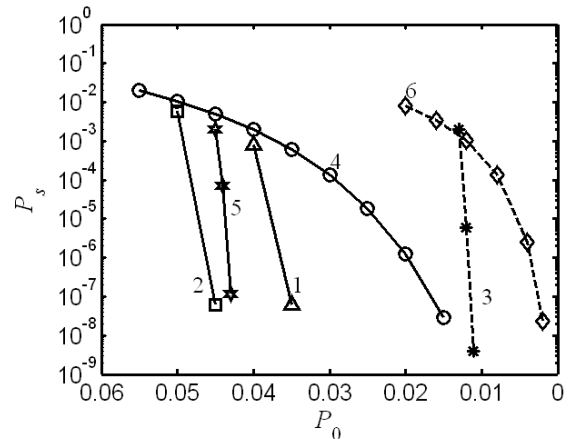


Рис. 2. Характеристики малоизбыточных недвоичных кодов

Интерес для систем передачи и хранения данных часто представляют малоизбыточные помехоустойчивые коды. Характеристики q МПД для недвоичных кодов с $R=7/8$, $n=100000$ символов и $q=256$ представлены на рис. 2 кривой 1, а характеристики кодов РС с $R=7/8$ и $q=256$ отражены кривой 4. Здесь также видно заметное преимущество q МПД над кодами РС. Аналогичная ситуация наблюдается и при использовании кодов с еще более высокой кодовой скоростью $R=19/20$. Для данной кодовой скорости при $q=256$ эффективность q МПД показана кривой 3, а для кодов РС – кривой 6. Такие же высокие характеристики обеспечивает q МПД при использовании алфавита большего объема. На рис. 2 кривой 2 представлена эффективность q МПД для кода с $R=7/8$ при использовании двухбайтовых символов ($q=65536$).

Отметим, 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. При этом наилучшими характеристиками обладают коды для схем с параллельным кодированием [2, 6].

Самоортогональные коды для схем параллельного кодирования

В основе построения схем параллельного кодирования лежит выделение в самоортогональном коде C_0 с кодовым расстоянием d_0 и кодовой скоростью $R_0=k/(k+m)$ ($m>1$) некоторого составляющего кода C_1 с кодовой скоростью $R_1>R_0$, тоже являющегося самоортогональным кодом (СОК). Кодовое расстояние d_1 выделенного кода выбирается значительно меньшим d_0 , и, следовательно, область его эффективной работы будет ближе к границе Шеннона. При декодировании параллельного кода сначала выполняются несколько итераций декодирования составляющего кода C_1 , позволяющие примерно на порядок снизить вероятность ошибки в принятой из канала информационной последовательности, после чего в процесс декодирования включается оставшаяся часть кода C_0 . Отличительной особенностью данной схемы кодирования является то, что

здесь внешний код работает с кодовой скоростью R_0 , в то время как в обычных каскадных кодах кодовая скорость внешнего кода близка к единице. Данное свойство обеспечивает существенное преимущество параллельному кодированию перед другими каскадными конструкциями.

Пример структуры кода с кодовой скоростью $R_0=8/16$ и кодовым расстоянием $d_0=17$ для схемы параллельного кодирования приведен на рис. 3. Здесь строки таблицы соответствуют проверочным ветвям, столбцы – информационным ветвям, а в каждой ячейке с индексами i и j таблицы указано количество элементов информационной ветви j , которое участвует в формировании каждого символа проверочной ветви i . В данном коде используется 8 информационных и 8 проверочных ветвей. В процессе декодирования этого кода на первых итерациях используется только код C_1 с кодовой скоростью $R_1=8/15$ и кодовым расстоянием $d_1=8$, содержащий первые 7 проверочных ветвей. Проверки в данных ветвях имеют малую размерность, и поэтому декодер такого “уменьшенного” кода хорошо работает при больших вероятностях ошибки в канале. Когда вероятность ошибки декодирования в информационных ветвях станет невысокой (порядка 10^{-3}), включается и последняя проверочная ветвь с большой размерностью проверок. С помощью этой ветви исправляются оставшиеся ошибки в информационных ветвях, и вероятность ошибки на выходе декодера снижается еще на несколько порядков.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|----|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 8 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 8 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 8 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 8 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 8 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 8 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 8 |
| 9 | 9 | 9 | 9 | 9 | 9 | 9 | 9 | 72 |

| | | | | | | | |
|----|----|----|----|----|----|----|----|
| 16 | 16 | 16 | 16 | 16 | 16 | 16 | 16 |
|----|----|----|----|----|----|----|----|

Рис. 3. Структура параллельного кода

Сложность q МПД при параллельном кодировании (в смысле количества выполняемых операций) оказывается даже меньше сложности обычного q МПД [2], поскольку в данном случае на первых итерациях декодирования некоторые элементы синдромного регистра просто не участвуют в процессе вычисления суммы на пороговом элементе.

Заметим, что интуитивный выбор размерностей проверок для каждой информационной и проверочной ветви при построении СОК для схем параллельного кодирования является чрезвычайно трудоемкой задачей.

Построение наиболее эффективных СОК для схем параллельного кодирования

Для того чтобы автоматизировать процесс построения СОК, можно перебирать все возможные варианты кодов с различными размерностями проверок и выбирать тот, декодер которого оставляет после себя наименьший процент ошибок. Вычислительная сложность такого алгоритма равна $m^{nk \cdot nr} \cdot C_{q\text{МПД}}$ операций, где nk и nr – число информационных и проверочных ветвей, m – количество возможных вариантов числа проверок каждой пары информационная–проверочная ветвь, $C_{q\text{МПД}}$ – вычислительная сложность q МПД [2]. Данный алгоритм чрезвычайно эффективен при построении недвоичных СОК с небольшим количеством информационных и проверочных ветвей, так как осуществляется полный перебор возможных вариантов кодов. Однако при построении кодов с большим количеством информационных и проверочных ветвей применение алгоритма полного перебора из-за большой вычислительной сложности оказывается не-

возможным. Поэтому для построения недвоичных СОК целесообразно использовать немного менее эффективный алгоритм, предложенный в [7]. Данный алгоритм обладает вычислительной сложностью $m \cdot nk \cdot nr \cdot N \cdot C_{q\text{МПД}}$ операций и, как показывают представленные далее результаты экспериментальных исследований, достаточно хорошей эффективностью.

На рис. 1 приведены результаты моделирования декодера для найденного с помощью предложенного алгоритма недвоичного СОК в q -ичном симметричном канале (кривая б). Кодовая скорость этого недвоичного СОК $R=1/2$, длина кода $n=60000$, минимальное кодовое расстояние $d=17$. При использовании данного кода достигаются гораздо лучшие результаты декодирования, чем ранее полученные. Вероятность ошибки на выходе декодера такого СОК составляет 10^{-7} при вероятности ошибки в канале $P_0=0.267$. При этом область эффективной работы найденного кода оказывается на 13% ближе к пропускной способности канала, равной для $q=256$ $P_c=0.38$, по сравнению с известным недвоичным СОК, использованным в [8]. Еще более значительным получается улучшение характеристик $q\text{МПД}$ для малоизбыточных кодов. На рис. 2 приведены результаты моделирования декодера найденного с помощью программы недвоичного СОК с кодовой скоростью $R=7/8$, минимальным кодовым расстоянием $d=7$ и длиной блока $n=100000$ в q -ичном симметричном канале (кривая 5). Вероятность ошибки на выходе декодера такого СОК составляет 10^{-7} при вероятности ошибки в канале $P_0=0.043$. При этом область эффективной работы найденного кода оказывается примерно на 20% ближе к пропускной способности канала $P_c=0.076$ по сравнению с известным недвоичным СОК с $R=7/8$ (кривая 1 на рис. 2) [8].

Заключение

Сравнение кодов РС и недвоичных самоортогональных кодов, декодируемых $q\text{МПД}$, показало, что коды Рида-Соломона уступают недвоичным СОК по эффективности и при этом имеют гораздо большую вычислительную сложность декодирования. Кроме того, для $q\text{МПД}$ возможно еще существенное улучшение эффективности за счет оптимизации структуры используемых кодов, что делает превосходство $q\text{МПД}$ над кодами Рида-Соломона еще более существенным. Это позволяет считать, что в дальнейшем $q\text{МПД}$ смогут заменить коды Рида-Соломона в разнообразных системах передачи и хранения данных, обеспечивая работу подобных систем в значительно более сложных условиях.

Работа выполнена при финансовой поддержке РФФИ (грант №08-07-00078).

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. Золотарев В.В. Теория и алгоритмы многопорогового декодирования – М.: Радио и связь, Горячая линия – Телеком, 2006. 232 с.
3. Золотарев В.В. Обобщение алгоритма МПД на недвоичные коды // Мобильные системы, М., 2007, №2, С.36-39.
4. Веб-сайт ИКИ РАН www.mtdbest.iki.rssi.ru.
5. Sudan M. Decoding of Reed Solomon codes beyond the error-correction bound // Journal of Complexity, 1997, vol.13, P.180–193.
6. Золотарев В.В. Параллельное кодирование в каналах СПД // Вопросы кибернетики, 1986, вып. 120, С.56–58.
7. Овечкин Г.В., Овечкин П.В. Оптимизация структуры недвоичных самоортогональных кодов для схем параллельного кодирования // Труды НИИР, 2009, №2, С.34–38.
8. Золотарев В.В. Каскадные схемы МПД декодирования для больших баз данных // Мобильные системы, М., 2008, №1.