УДК 519.673

И.А. РАТАЙЧУК, В.И. ШУЛЬГИН

Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Украина

ИССЛЕДОВАНИЕ ПОМЕХОУСТОЙЧИВОСТИ ЦИФРОВОГО КАНАЛА СВЯЗИ С ИСПОЛЬЗОВАНИЕМ НЕДВОИЧНЫХ КОДОВ РИДА-СОЛОМОНА

Проведено исследование помехоустойчивости цифрового канала связи с использованием недвоичных кодов Рида-Соломона. Рассматриваемая задача относится к классу задач моделирования и статистической обработки данных. Дана характеристика недвоичных кодов Рида-Соломона и приведены теоретические границы вероятности ошибки. Построена модель канала связи с использованием данных кодов. Определены зависимости вероятности ошибки от соотношения сигнал/шум для кодов с различными алфавитами, длинами кодовых слов и избыточностью. Проведено исследование качества работы канала связи и показано преимущество недвоичных кодов Рида-Соломона перед двоичными.

Ключевые слова: *недвоичные коды Рида-Соломона, помехоустойчивость, моделирование канала связи.*

Введение

Недвоичные коды Рида-Соломона (РС) занимают важное место в теории и практике помехоустойчивого кодирования. Они были изобретены сотрудниками Массачуссетского технологического института Ирвином Ридом и Густавом Соломоном в 1960 году. Но только начиная с 1969 года, когда были предложены эффективные алгоритмы декодирования, они начинают получать практическое применение в системах связи.

Впервые код Рида-Соломона был использован в составе каскадного кода в системе передачи изображений с зонда Вояджер в 1977 году. Первым коммерческим применением РС кодов в массовом производстве было их использование в записи компакт-дисков в 1982. С тех пор они получили широкое распространение при архивации данных, в контроллерах оперативной памяти, устройствах записи CD/DVD. В системах спутниковой связи и цифрового телевидения они вместе со сверточными кодами применяются как компоненты каскадных кодов. Коды Рида-Соломона также являются неотъемлемой частью систем беспроводной и мобильной связи [1].

Такая массовость их применения объясняется их эффективностью в исправлении как одиночных, так и пакетированных ошибок. Это свойство особо важно в системах передачи данных, использующих алгоритм сверточного кодирования Виттерби, т.к. на выходе сверточного декодера неисправленные ошибки обычно группируются в пакеты. Особо удобными для использования в цифровых системах недвоичные коды делает то, что символами кода являются не одиночные биты, а группы из нескольких бит. Поэтому наиболее часто используемыми кодами Рида-Соломона являются коды над полем Галуа $GF(2^8)$ в которых символы представлены 8 битами или байтом.

Таким образом, в настоящее время коды Рида-Соломона являются неотъемлемой частью уже давно получивших распространение каскадных кодов и быстро набирающих популярность турбо-кодов.

К сожалению в отечественных периодических изданиях уделяется мало внимания недвоичным кодам, а западные статьи носят по большей части прикладной характер. В работе [2] рассматривается применение кодов Рида-Соломона для схемотехнического решения кодека с низким потреблением энергии.

Постановка задачи

По сравнению с аналоговыми системами, цифровые системы передачи данных намного сильнее подвержены влиянию шумов и помех. В этих системах данные передаются с высокой степенью сжатия и поэтому они особо чувствительны к возникающим ошибкам, особенно к пакетам ошибок. Если для аналоговых систем для качественной работы достаточно обеспечить вероятность появления ошибки в пределах 10^{-4}, то для цифровых систем эта величина составляет 10^{-9} – 10^{-11}. Одиночный кодер не в состоянии удовлетворить таким требованиям, поэтому на практике применяется каскадное кодирование или турбо-коды. В данной работе рассматривается применение РС кода в каскадном коде, где он последовательно соединен со сверточным кодом. Учитывая характеристики сверточных кодов, для качественной работы канала связи кодер Рида-Соломона должен обеспечивать вероятность ошибки в преде-

© И.А. Ратайчук, В.И. Шульгин

лах 10^{-4} – 10^{-6}. Для проверки показателей качества работы РС кодов и их сравнения с двоичными кодами в среде моделирования MATLAB была создана модель цифрового канала связи. В качестве критерия качества кода использовалась зависимость вероятности ошибки от соотношения сигнал/шум.

Характеристика кодов Рида-Соломона

Коды Рида-Соломона относятся к классу циклических блоковых кодов. Свойство цикличности означает, что циклический сдвиг кодового слова на один символ порождает новое кодовое слово из этого же кода. Кодовое слово обрабатывается и передается блоками из n символов, из которых k символов являются информационными, а остальные n – k – проверочные. Каждый символ кодового слова представлен m битами. Обычно в системах передачи данных используется систематическое кодирование, при котором кодовое слово состоит из двух последовательных блоков информационных и проверочных символов (рис.1). Такой подход позволяет уменьшить затраты ресурсов на извлечение исходной информации, если в кодовом слове не возникло ошибок.

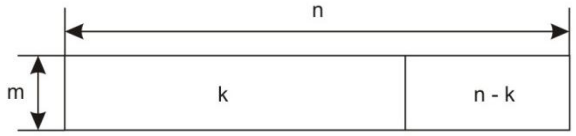

Рис. 1. Структура систематического кодового слова

Коды Рида-Соломона являются алгебраическими кодами, т.е. все операции и преобразования над ними выполняются в соответствии с арифметикой полей Галуа. Одной из особенностей РС кодов является их жесткая архитектура. При построении таких кодов задаются величина алфавита m и количество исправляемых ошибок t. Длина кодового слова задается соотношением $n = 2^m - 1$. Количество проверочных символов равно $n - k = 2t$. Такая особенность РС кодов позволяет заранее подобрать необходимые параметры кода, а не искать коды, соответствующие требуемым характеристикам. При этом для полученного кода можно увеличивать или уменьшать длину слова при помощи специальных процедур, что делает коды Рида-Соломона весьма гибкими в практическом применении [3].

Недвоичные РС коды являются частным случаем двоичных кодов БЧХ (Боуза – Чоудхури – Хоквингема), и также как и они относятся к классу полиномиальных кодов. В данном случае кодовое слово задается порождающим полиномом g(x):

$$g(x) = \prod_{j=j_0}^{j_0+2t-1} (x - \alpha^j)\,, \qquad (1)$$

где α – примитивный элемент поля $GF(2^m)$, j_0 – некоторое целое число, обычно принимаемое за 1, подбором которого можно упростить схему кодера [4].

Кодовое слово в случае несистематического кодирования задается как произведение информационного многочлена i(x) на порождающий полином:

$$c(x) = i(x)g(x)\,. \qquad (2)$$

В случае систематического кодирования проверочные символы t(x) находятся как остаток от деления информационной последовательности на порождающий полином и добавляются после информационных символов:

$$c(x) = i(x) + t(x)\,,$$
$$t(x) = -R_{g(x)}[i(x)]\,. \qquad (3)$$

Исправляющая способность и границы вероятности ошибки

Коды Рида-Соломона являются оптимальными с точки зрения соотношения длины кодового слова и исправляющей способности – используя 2t проверочных символов, они могут исправлять не менее t ошибок. РС код имеет минимальное кодовое (Хеммингово) расстояние n – k + 1 и является кодом с максимально достижимым расстоянием (МДР). Это следует из следующих соображений: d = 2t + 1 – конструктивное расстояние кода, минимальное расстояние d* удовлетворяет неравенству

$$d^* \ge d = 2t + 1 = n - k + 1\,. \qquad (4)$$

Но для любого линейного кода имеет место граница Синглтона

$$d^* \le n - k + 1\,. \qquad (5)$$

Следовательно, d* = n - k + 1 и d* = d.

Таким образом, при фиксированных n и k не существует кода, у которого минимальное расстояние больше, чем у кода Рида-Соломона. Следовательно он обладает наилучшими исправляющими характеристиками среди кодов с такой же избыточностью [5].

Код Рида-Соломона является одним из наилучших кодов, исправляющих многократные пакеты ошибок. (n, k) РС код над полем $GF(2^m)$ можно представить как (mn, mk) код над полем GF(2), который может исправлять любую комбинацию ошибок в t или меньшем количестве блоков из m символов. Наибольшее число блоков длины m, которые может затронуть пакет длины l_i, где $l_i \le mt_i - (m - 1)$, не превосходит t_i, поэтому код, который может исправить t блоков ошибок, всегда может исправить и любую комбинацию из пакетов общей длины l, если $l + (m - 1) \le mt$.

Для оценки помехоустойчивости (n, k) РС кода над GF(q) используется граница вероятности ошибки на бит P_b

$$P_b \le \frac{2^{m-1}}{2^m - 1} \sum_{i=t+1}^{n} \frac{i+t}{n} \binom{n}{i} P_s^i (1 - P_s)^{n-i}, \quad (6)$$

где P_s – вероятность ошибки на символ на входе декодера РС,

$$P_s = 1 - (1 - p)^m, \quad (7)$$

и p – вероятность ошибки на бит на входе декодера. Вероятность ошибки на кодовое слово ограничена сверху границей

$$P_c = 1 - \sum_{i=0}^{t} \binom{n}{i} P_s^i (1 - P_s)^{n-i}. \quad (8)$$

Исследование канала связи с использованием кода Рида-Соломона на помехоустойчивость

Для исследования свойств недвоичных кодов Рида-Соломона и их сравнения с двоичными кодами была создана модель канала связи в среде моделирования MATLAB (рис.2).

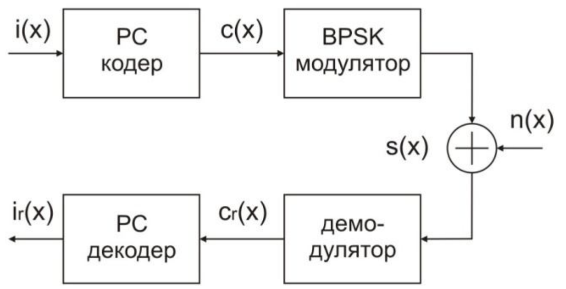

Рис. 2. Модель канала связи с аддитивным гауссовским шумом

В данной модели информационная последовательность i(x), задаваемая случайным образом, кодировалась с помощью кодера Рида-Соломона (при моделировании двоичных кодов – кодером БЧХ). Затем недвоичное кодовое слово c(x) преобразовывалось в двоичную последовательность (рис.3) и модулировалось с помощью двоичной фазовой модуляции (BPSK), т.е. каждый отсчет выходного сигнала представлялся как 1 и -1. К сигналу s(x) добавлялась случайная величина n(x) (гауссовский шум). Принятое сообщение демодулировалось и декодировалось. На основании сравнения декодированной информационной последовательности $i_r(x)$ и переданной i(x) составлялась статистика появления неисправленных ошибок.

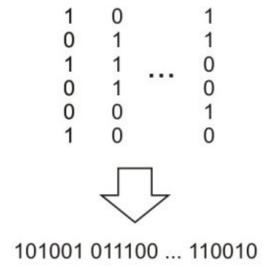

Рис. 3. Преобразование недвоичных символов в двоичную последовательность

Так как коды Рида-Соломона недвоичные, представляет интерес вопрос, какое число бит на символ будет оптимальным. Как показало исследование (рис.4), для кодов с одинаковой избыточностью над разными полями (количество бит на символ 6, 8 и 10 соответственно) разница в величине вероятности ошибки невелика, поэтому для цифровых систем наиболее предпочтительными являются коды над полем GF(2^8), т.к. для них один символ представляется байтом.

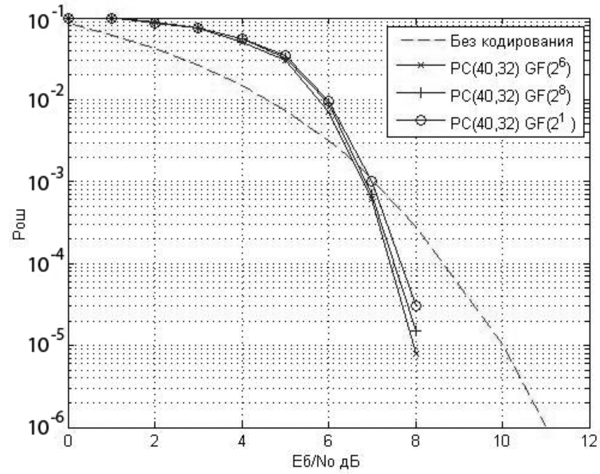

Рис. 4. Помехоустойчивость кодов с различной величиной алфавита

При одинаковой избыточности коды с более длинными кодовыми словами оказываются менее подверженными влиянию ошибок (рис. 5) за счет большего кодового расстояния. На практике обычно используются коды с длинной кодового слова n = 100…255. Наилучшим образом в системах связи проявил себя код с длиной 255 и его укороченные варианты.

В ходе исследования было подтверждено, что коды с большей избыточностью обладают лучшей исправляющей способностью (рис. 6), но при этом уменьшается количество передаваемой полезной информации, поэтому предпочтительны коды с малой избыточностью и относительно высокой исправляющей способностью.

Таким требованиям, например, отвечает (255, 239) код, для которого избыточность составляет всего 6%.

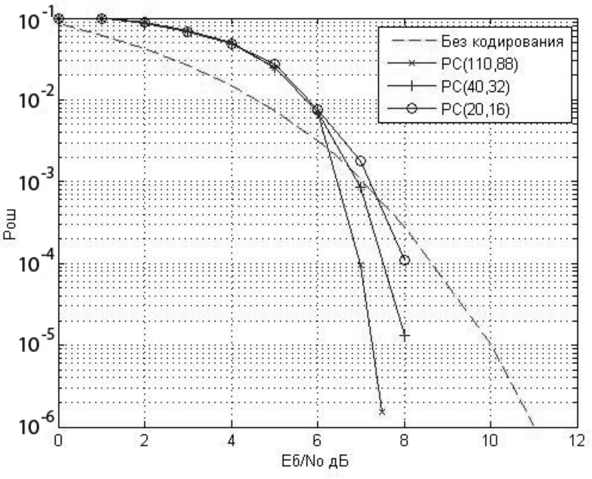

Рис. 5. Помехоустойчивость кодов
с различной длинной кодового слова

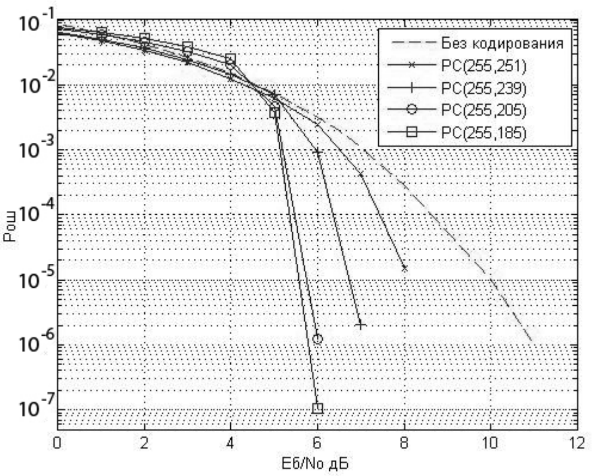

Рис. 6. Помехоустойчивость кодов
с различной избыточностью

Для сравнения показателей двоичных и недвоичных кодов было проведено исследование работы канала связи с использованием БЧХ кодов, с аналогичными показателями по избыточности, как и у кодов Рида-Соломона из предыдущего эксперимента (рис. 7).

Для малых соотношений сигнал/шум (2-5 дБ) разницы в показателях двоичных и недвоичных кодов мала, но в данном диапазоне даже с использованием каскадного кодирования затруднительно обеспечить качественную работу цифрового канала связи. Начиная с соотношения 6 дБ, вероятность ошибки для кодов Рида-Соломона на два порядка ниже, чем для двоичных кодов. Это является важным качеством недвоичных кодов, т.к. они обеспечивают работу систем связи при более низких соотношениях сигнал/шум. Поэтому РС коды давно вытеснили двоичные коды в каналах связи с низкой энергетикой, таких как спутниковое телевидение и связь.

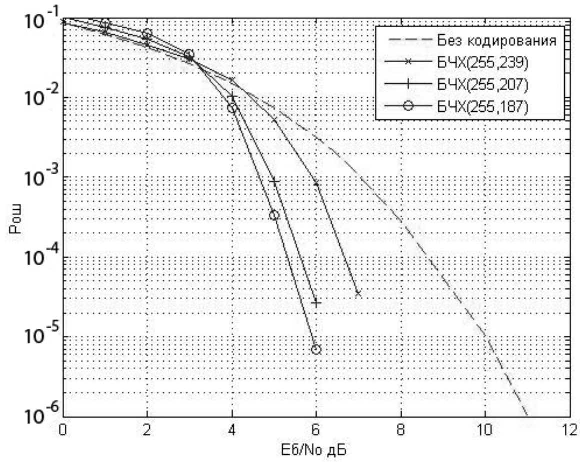

Рис. 7. Помехоустойчивость двоичных кодов

Выводы

Таким образом, в данной работе была дана характеристика недвоичным кодам Рида-Соломона и проведено моделирование работы канала связи с их применением. В ходе исследования определены характеристики РС кодов для различных алфавитов, кодовой длины и избыточности. На основе полученных данных предложены оптимальные варианты кодов. Показано преимущество недвоичных кодов по сравнению с двоичными.

Литература

1. Cipra Barry The ubiquitous Reed-Solomon codes / Barry Cipra // SIAM News. – 1993. – Vol 26, No 1. – P. 77 – 78.

2. Biard Lionel Reed-Solomon codes for low power communications / Lionel Biard, Dominique Noquet // Journal of Communications. – 2008. – Vol 3, No 2. – P. 15 – 16.

3. Скляр Б. Цифровая связь. Теоретические основы и практическое применение / Б. Скляр. – М.: Вильямс, 2003. – 460 с.

4. Блейхут Р. Теория и практика кодов, контролирующих ошибки / Р. Блейхут. – М.: Мир, 1986. – 201 с.

5. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования / Р. Морелос-Сарагоса. – М.: Техносфера, 2005. – 111 с.

6. Reed Irving Error-Control Coding for Data Networks / Irving Reed, Xuemin Chen. – Boston: Kluwer Academic Publishers, 1999. – P. 233.

Поступила в редакцию 2.03.2011

Рецензент: д-р техн. наук, доц., проф. каф. информатики В.А. Гороховатский, Харьковский национальный университет радиоэлектроники, Харьков.

ДОСЛІДЖЕННЯ ЗАВАДОСТІЙКОСТІ ЦИФРОВОГО КАНАЛУ ЗВ'ЯЗКУ З ВИКОРИСТАННЯМ НЕДВІЙКОВИХ КОДІВ РІДА-СОЛОМОНА

І.О. Ратайчук, В.І. Шульгін

Проведено дослідження завадостійкості цифрового каналу зв'язку з використанням недвійкових кодів Ріда-Соломона. Розглянута задача відноситься до класу задач моделювання та статистичної обробки даних. Дана характеристика недвійкових кодів Ріда-Соломона та приведені теоретичні межі імовірності помилки. Побудована модель каналу зв'язку з використанням даних кодів. Визначені залежності імовірності помилки від відношення сигнал/шум для кодів з різними алфавітами, довжиною коду та надлишковістю. Здійснено дослідження якості роботи каналу зв'язку та показана перевага недвійкових кодів Ріда-Соломона над двійковими.

Ключові слова: недвійкові коди Ріда-Соломона, завадостійкість, моделювання каналу зв'язку.

DIGITAL COMMUNICATION CHANNEL WITH NONBINARY REED-SOLOMON CODING INTERFERENCE IMMUNITY RESEARCH

I.A. Rataichuk, V.I. Shulgin

Digital communication channel with nonbinary Reed-Solomon coding was carried out. Considered problem belongs to modeling and statistic analysis problems. Description of nonbinary Reed-Solomon codes and theoretical error probability bounds are given. The model of communication channel with current codes was constructed. The different alphabet, code length and redundancy codes performance was estimated. Communication channel performance was analyzed and was shown nonbinary Reed-Solomon codes advantage over binary codes.

Key words: nonbinary Reed-Solomon codes, interference immunity, communication channel modeling.

Ратайчук Иван Александрович – студент каф. проектирования радиоэлектронных систем летательных аппаратов, Национальный аэрокосмический университет им. Н.Е. Жуковского «Харьковский авиационный институт», Харьков, Украина, e-mail: rataichuk@rambler.ru.

Шульгин Вячеслав Иванович – канд. техн. наук, доцент, доцент каф. проектирования радиоэлектронных систем летательных аппаратов, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Украина, e-mail: vyacheslav.shulgin@gmail.com.