

УДК 621.391

ОБНАРУЖЕНИЕ ОШИБОК КОДОМ БЧХ НАД ПОЛЕМ GF(4) НА ОСНОВЕ СПЕКТРАЛЬНОГО ОПИСАНИЯ

В. А. Вершинин

Рыбинский государственный авиационный технический университет

им. П. А. Соловьева

Статья поступила в редакцию 6 сентября 2016 г.

Аннотация. В статье рассматривается спектральное описание кода БЧХ над полем GF(4). Цель кодирования – обнаружение ошибок. Произведена оценка эффективности кодирования, когда число ошибок в кодовом слове больше числа гарантированно обнаруживаемых ошибок.

Моделирование процесса декодирования показало, что наибольшее значение вероятности необнаруженной ошибки получается, когда число ошибок в кодовом слове равно кодовому расстоянию. Эта вероятность используется в статье для оценки сверху вероятности необнаруженной ошибки.

Если число ошибок в кодовом слове больше или равно кодовому расстоянию, то при увеличении длины кодового слова и неизменной величине кодового расстояния можно получить приемлемое значение вероятности необнаруженной ошибки.

Ключевые слова: спектральное описание, обнаружение ошибок, код БЧХ.

Abstract. The article discusses the spectral description of BCH code over the field GF(4). The purpose of the coding – error detection. The assessment of coding efficiency, when the number of errors in the code word greater than the number of guaranteed detectable errors.

Simulation of the decoding process showed that the highest value of the probability of undetected error is obtained when the number of errors in the code word equal to the code distance. This probability is used in the article to estimate from above the probability of undetected error.

If the number of errors in the code word is greater than or equal to the code distance, then increase the length of the code words in the constant value of the code distance it is possible to obtain an acceptable value of probability of undetected error.

Key words: spectral description, error detection, BCH code.

1. Введение

Описать код БЧХ можно [1], исходя из спектрального описания кода Рида-Соломона на основе дискретного преобразования Фурье (ДПФ). Опишем код Рида-Соломона, используя ДПФ над полем $GF(2^m)$, где $m=1, 2, 3, \dots$. Элемент i -ой строки и j -го столбца матрицы F_n прямого ДПФ равен α^{ij} , а такой же элемент матрицы F_n^{-1} обратного ДПФ равен α^{-ij} ; $i=0, 1, 2, \dots, n-1$; $j=0, 1, 2, \dots, n-1$. Здесь α – примитивный элемент поля $GF(2^m)$, $n=2^m-1$. Для примера, при $n=15$ и $\alpha=2$, используя пакет Matlab, можно получить:

$$F_{15} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 8 & 3 & 6 & 12 & 11 & 5 & 10 & 7 & 14 & 15 & 3 & 9 \\ 1 & 4 & 3 & 12 & 5 & 7 & 15 & 9 & 2 & 8 & 6 & 11 & 10 & 14 & 13 \\ 1 & 8 & 12 & 10 & 15 & 1 & 8 & 12 & 10 & 15 & 1 & 8 & 12 & 10 & 15 \\ 1 & 3 & 5 & 15 & 2 & 6 & 10 & 13 & 4 & 12 & 7 & 9 & 8 & 11 & 14 \\ 1 & 6 & 7 & 1 & 6 & 7 & 1 & 6 & 7 & 1 & 6 & 7 & 1 & 6 & 7 \\ 1 & 12 & 15 & 8 & 10 & 1 & 12 & 15 & 8 & 10 & 1 & 12 & 15 & 8 & 10 \\ 1 & 11 & 9 & 12 & 13 & 6 & 15 & 3 & 14 & 8 & 7 & 4 & 10 & 2 & 5 \\ 1 & 5 & 2 & 10 & 4 & 7 & 8 & 14 & 3 & 15 & 6 & 13 & 12 & 9 & 11 \\ 1 & 10 & 8 & 15 & 12 & 1 & 10 & 8 & 15 & 12 & 1 & 10 & 8 & 15 & 12 \\ 1 & 7 & 6 & 1 & 7 & 6 & 1 & 7 & 6 & 1 & 7 & 6 & 1 & 7 & 6 \\ 1 & 14 & 11 & 8 & 9 & 7 & 12 & 4 & 13 & 10 & 6 & 2 & 5 & 15 & 3 \\ 1 & 15 & 10 & 12 & 8 & 1 & 5 & 10 & 12 & 8 & 1 & 15 & 10 & 12 & 8 \\ 1 & 13 & 14 & 10 & 11 & 6 & 8 & 2 & 9 & 15 & 7 & 5 & 12 & 3 & 4 \\ 1 & 9 & 13 & 15 & 14 & 7 & 10 & 5 & 11 & 12 & 6 & 3 & 8 & 4 & 2 \end{bmatrix},$$

$$F_{15}^{-1} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 9 & 13 & 15 & 14 & 7 & 9 & 5 & 11 & 12 & 6 & 3 & 8 & 4 & 2 \\ 1 & 13 & 14 & 10 & 11 & 6 & 8 & 2 & 9 & 15 & 7 & 5 & 12 & 3 & 4 \\ 1 & 15 & 10 & 12 & 8 & 1 & 15 & 10 & 12 & 8 & 1 & 15 & 10 & 12 & 8 \\ 1 & 14 & 11 & 8 & 9 & 7 & 12 & 4 & 13 & 10 & 6 & 2 & 15 & 5 & 3 \\ 1 & 7 & 6 & 1 & 7 & 6 & 1 & 7 & 6 & 1 & 7 & 6 & 1 & 7 & 6 \\ 1 & 10 & 8 & 15 & 12 & 1 & 10 & 8 & 15 & 12 & 1 & 10 & 8 & 15 & 12 \\ 1 & 5 & 2 & 10 & 4 & 7 & 8 & 14 & 3 & 15 & 6 & 13 & 12 & 9 & 11 \\ 1 & 11 & 9 & 12 & 13 & 6 & 15 & 3 & 14 & 8 & 7 & 4 & 10 & 2 & 5 \\ 1 & 12 & 15 & 8 & 10 & 1 & 12 & 15 & 8 & 10 & 1 & 12 & 15 & 8 & 10 \\ 1 & 6 & 7 & 1 & 6 & 7 & 1 & 6 & 7 & 1 & 6 & 7 & 1 & 6 & 7 \\ 1 & 3 & 5 & 15 & 2 & 6 & 10 & 13 & 4 & 12 & 7 & 9 & 8 & 11 & 14 \\ 1 & 8 & 12 & 10 & 15 & 1 & 8 & 12 & 10 & 15 & 1 & 8 & 12 & 10 & 15 \\ 1 & 4 & 3 & 12 & 5 & 7 & 15 & 9 & 2 & 8 & 6 & 11 & 10 & 14 & 13 \\ 1 & 2 & 4 & 8 & 3 & 6 & 12 & 11 & 5 & 10 & 7 & 14 & 15 & 13 & 9 \end{bmatrix}.$$

ДПФ используется для спектрального описания кода Рида-Соломона следующим образом. Пусть блоку элементов сообщения длиной k соответствует вектор $b = (b_0 b_1 \dots b_{n-1})$, у которого $n - k$ последовательных элементов являются нулевыми и называются проверочными, а остальные k равны элементам сообщения и называются информационными. Кодовый вектор $c = (c_0 c_1 \dots c_{n-1})$ получается с помощью матрицы обратного ДПФ:

$$c = bF_n^{-1}. \tag{1}$$

Элементы сообщения и вектора c могут принимать значения $0, 1, 2, \dots, n$. Такой код называется кодом Рида-Соломона, его кодовое расстояние $d = n - k + 1$. При декодировании используется матрица F_n прямого ДПФ.

Перейдем к описанию кода БЧХ над полем $GF(4)$. Для этого будем использовать код Рида-Соломона над полем $GF(2^s)$ при $s = 2m$. Пусть блоку элементов сообщения длиной k соответствует вектор $a = (a_0 a_1 \dots a_{n-1})$, элементы которого могут принимать 4 значения (нулевое значение и значения элементов поля $GF(2^s)$, порядок которых делит $4^1 - 1 = 3$). По определенному алгоритму

образуется вектор $b = (b_0 b_1 \dots b_{n-1})$ так, чтобы элементы кодового вектора принимали те же 4 значения.

Для осуществления указанного алгоритма вектор b разбивается на группы. Каждая группа состоит из свободных и связанных элементов. Индексы связанных элементов получаются умножением по модулю n индексов свободных элементов на $4^1, 4^2, 4^3, \dots$. Если группа состоит из r элементов, то свободный элемент группы может принимать 4^r значений (нулевое значение и значения элементов поля $GF(2^s)$, порядок которых делит $4^r - 1$). Связанные элементы группы принимают значения, равные степени $4^1, 4^2, 4^3, \dots$ свободного элемента этой группы. При кодировании r элементов вектора a линейно преобразуются в свободный элемент вектора b . Кодовый вектор формируется согласно (1) путем обратного ДПФ вектора b . Сказанное выше поясняется таблицей 1 для $n = 15$.

Таблица 1

Номер группы	Свободные элементы	Связанные элементы	Получение связанных элементов	Значения свободных элементов	Получение свободных элементов
1	b_0			0, 1, 6, 7	$b_0 = a_0$
2	b_1	b_4	$b_4 = b_1^4$	0, 1, 2, ..., 15	$b_1 = a_1 + 2a_2$
3	b_2	b_8	$b_8 = b_2^4$	0, 1, 2, ..., 15	$b_2 = a_3 + 2a_4$
4	b_3	b_{12}	$b_{12} = b_3^4$	0, 1, 2, ..., 15	$b_3 = a_5 + 2a_6$
5	b_5			0, 1, 6, 7	$b_5 = a_7$
6	b_6	b_9	$b_9 = b_6^4$	0, 1, 2, ..., 15	$b_6 = a_8 + 2a_9$
7	b_7	b_{13}	$b_{13} = b_7^4$	0, 1, 2, ..., 15	$b_7 = a_{10} + 2a_{11}$
8	b_{10}			0, 1, 6, 7	$b_{10} = a_{12}$
9	b_{11}	b_{14}	$b_{14} = b_{11}^4$	0, 1, 2, ..., 15	$b_{11} = a_{13} + 2a_{14}$

Здесь элементы вектора a и c могут принимать 4 значения: 0, 1, 6 и 7.

2. Спектральное описание кода БЧХ

Базируясь на изложенном выше описании кода БЧХ, автором предлагается [2], получить матрицу H_n прямого и матрицу H_n^{-1} обратного преобразования над полем $GF(4)$.

Матрица H_n^{-1} получается построчно следующим образом. Формируется вектор $a = (100\dots 00)$ и по формуле (1) определяется значение вектора c , которое и является значением 0-й строки матрицы H_n^{-1} при замене значений элементов поля $GF(2^m)$ на значения элементов поля $GF(4)$. Затем формируется вектор $a = (010\dots 00)$ и по формуле (1) получается 1-я строка матрицы H_n^{-1} и так далее. Последняя строка получается с помощью вектора $a = (000\dots 01)$. Матрица H_n получается как обратная матрице H_n^{-1} .

Для $n = 15$ можно получить:

$$H_{15}^{-1} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 2 & 1 & 2 & 3 & 2 & 0 & 2 & 3 & 2 & 3 & 0 & 3 \\ 1 & 2 & 1 & 1 & 1 & 0 & 2 & 3 & 1 & 3 & 3 & 3 & 2 & 3 & 2 \\ 1 & 2 & 3 & 0 & 2 & 2 & 2 & 1 & 2 & 3 & 0 & 2 & 1 & 2 & 3 \\ 1 & 1 & 1 & 3 & 1 & 1 & 3 & 2 & 2 & 2 & 1 & 2 & 3 & 3 & 3 \\ 1 & 2 & 0 & 3 & 0 & 1 & 0 & 3 & 1 & 0 & 2 & 0 & 2 & 3 & 0 \\ 1 & 0 & 2 & 1 & 3 & 2 & 3 & 1 & 0 & 2 & 1 & 3 & 1 & 0 & 2 \\ 1 & 3 & 2 & 3 & 3 & 0 & 2 & 2 & 1 & 3 & 1 & 1 & 3 & 2 & 1 \\ 1 & 3 & 1 & 0 & 1 & 2 & 2 & 3 & 2 & 3 & 0 & 3 & 2 & 1 & 2 \\ 1 & 2 & 2 & 2 & 3 & 1 & 3 & 1 & 2 & 2 & 2 & 3 & 1 & 2 & 2 \\ 1 & 3 & 0 & 2 & 0 & 1 & 0 & 2 & 1 & 0 & 3 & 0 & 3 & 2 & 0 \\ 1 & 0 & 3 & 3 & 2 & 2 & 3 & 3 & 0 & 2 & 2 & 1 & 2 & 0 & 1 \\ 1 & 1 & 3 & 2 & 2 & 0 & 2 & 1 & 1 & 3 & 2 & 2 & 1 & 1 & 3 \\ 1 & 1 & 2 & 0 & 3 & 2 & 2 & 2 & 2 & 3 & 0 & 1 & 3 & 3 & 1 \\ 1 & 3 & 3 & 1 & 2 & 1 & 3 & 3 & 2 & 2 & 3 & 1 & 2 & 1 & 1 \end{bmatrix},$$

$$H_{15} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 3 & 2 & 3 & 3 & 0 & 2 & 1 & 2 & 2 & 0 & 1 & 3 & 1 & 1 \\ 1 & 0 & 3 & 2 & 3 & 3 & 0 & 2 & 1 & 2 & 2 & 0 & 1 & 3 & 1 \\ 0 & 2 & 3 & 2 & 2 & 0 & 3 & 1 & 3 & 3 & 0 & 1 & 2 & 1 & 1 \\ 1 & 3 & 3 & 0 & 1 & 2 & 1 & 1 & 0 & 2 & 3 & 2 & 2 & 0 & 3 \\ 0 & 3 & 2 & 2 & 3 & 0 & 3 & 2 & 2 & 3 & 0 & 3 & 2 & 2 & 3 \\ 1 & 2 & 0 & 2 & 1 & 1 & 2 & 0 & 2 & 1 & 1 & 2 & 0 & 2 & 1 \\ 1 & 3 & 2 & 1 & 3 & 2 & 1 & 3 & 2 & 1 & 3 & 2 & 1 & 3 & 2 \\ 0 & 2 & 3 & 3 & 2 & 0 & 2 & 3 & 3 & 2 & 0 & 2 & 3 & 3 & 2 \\ 1 & 0 & 1 & 2 & 2 & 1 & 0 & 1 & 2 & 2 & 1 & 0 & 1 & 2 & 2 \\ 0 & 1 & 1 & 2 & 1 & 0 & 3 & 3 & 1 & 3 & 0 & 2 & 2 & 3 & 2 \\ 1 & 2 & 1 & 0 & 3 & 3 & 1 & 3 & 0 & 2 & 2 & 3 & 2 & 0 & 1 \\ 1 & 2 & 3 & 1 & 2 & 3 & 1 & 2 & 3 & 1 & 2 & 3 & 1 & 2 & 3 \\ 0 & 1 & 1 & 3 & 1 & 0 & 2 & 2 & 1 & 2 & 0 & 3 & 3 & 2 & 3 \\ 1 & 0 & 2 & 2 & 1 & 2 & 0 & 3 & 3 & 2 & 3 & 0 & 1 & 1 & 3 \end{bmatrix}.$$

При получении этих матриц значения 0, 1, 6 и 7 элементов поля $GF(2^4)$ заменялись значениями 0, 1, 2 и 3 элементов поля $GF(4)$.

3. Кодирование

Пусть блоку элементов сообщения длиной k соответствует вектор $a = (a_0 a_1 \dots a_{n-1})$, элементы которого могут принимать значения 0, 1, 2, 3. При этом $n - k$ последовательных элементов этого вектора принимаются равными нулю и называются проверочными, а остальные k равны элементам сообщения и называются информационными. От значения $n - k$ зависит кодовое расстояние d кода БЧХ. Величину d принято оценивать конструктивным кодовым расстоянием d^* . При этом $d \geq d^*$, а значение $d^* - 1$ равно количеству последовательно расположенных нулевых элементов вектора b , которые получаются при преобразовании проверочных элементов вектора a .

Кодовый вектор получается путем обратного преобразования над полем $GF(4)$:

$$c = aH_n^{-1}, \tag{2}$$

При этом элементы вектора a задаются, а элементы вектора c получаются над полем $GF(4)$.

В таблице 1 приведены параметры некоторых кодов БЧХ, имеющих $d = d^* = 6$.

Таблица 2

Код (n, k)	Проверочные элементы вектора a	Нулевые элементы вектора b , получающиеся из проверочных элементов вектора a
(15,8)	$a_0, a_1, a_2, \dots, a_6$	$b_0, b_1, b_2, b_3, b_4, b_8, b_{12}$
(63,53)	$a_0, a_1, a_2, \dots, a_9$	$b_0, b_1, b_2, b_3, b_4, b_8, b_{12}, b_{16}, b_{32}, b_{48}$
(255,242)	$a_0, a_1, a_2, \dots, a_{12}$	$b_0, b_1, b_2, b_3, b_4, b_8, b_{12}, b_{16}, b_{32}, b_{48}, b_{64}, b_{128}, b_{192}$

4. Декодирование с обнаружением ошибок

Пусть кодовому слову на входе декодера соответствует вектор

$$c' = c + e, \tag{3}$$

где e – вектор ошибок. Этот вектор связан с наличием помех в канале связи. Если в результате действия помех искажаются элементы кодового слова, то соответствующие элементы вектора ошибок принимают значение 1, 2 или 3. Неискаженным элементам кодового слова соответствуют нулевые элементы вектора ошибок. В декодере осуществляется прямое преобразование вектора c' , в результате получается вектор $a' = c' H_n$. Учитывая (2),

$$a' = (c + e)H_n = (aH_n^{-1} + e)H_n = aH_n^{-1}H_n + eH_n = a + eH_n. \tag{4}$$

Очевидно, что при отсутствии ошибок $e = 0$ и $a' = a$. Обнаружение ошибок в кодовом слове осуществляется путем контроля значений проверочных элементов вектора a' . Если хотя бы один из проверочных элементов не равен нулю, то это соответствует обнаружению ошибок. Гарантировано обнаруживаются ошибки, если их количество в кодовом слове не превышает $d - 1$. Если число ошибок больше $d - 1$, то ошибки могут быть не обнаружены с определенной вероятностью. Оценка этой вероятности является целью данной работы.

5. Вероятность необнаруженной ошибки

Будем оценивать вероятность необнаруженной ошибки при фиксированном числе r ненулевых элементов вектора ошибок. При этом предполагаем, что все возможные варианты размещения ненулевых элементов равновероятны и каждый из этих элементов с равной вероятностью принимает значение 1, 2, 3. Очевидно, что вероятность необнаруженной ошибки равна нулю при $r \leq d - 1$.

Моделирование процесса декодирования показало, что наибольшее значение вероятности необнаруженной ошибки получается при $r = d$. Именно эту вероятность P будем использовать для оценки сверху вероятности необнаруженной ошибки при фиксированном значении r .

Образуем матрицу g , состоящую из столбцов матрицы K_n с номерами проверочных элементов. Таким образом, матрица g имеет n строк и $n - k$ столбцов. Любые $d - 1$ строки матрицы g , соответствующие ненулевым элементам вектора e , являются линейно независимыми. Тогда при $r \leq d - 1$ произведение $eg \neq 0$ и такие ошибки всегда обнаруживаются. При $r = d$, для определенных размещений ненулевых элементов вектора e и определенных значений этих элементов возможно $eg = 0$, что соответствует необнаруженным ошибкам.

Пусть u – число линейно независимых строк матрицы g , соответствующих ненулевым элементам вектора e , значение u может быть $d - 1$, либо d . Очевидно, что вероятность размещения P_1 , при котором возможно $eg = 0$ равна вероятности значения $u = d - 1$. Вероятность ненулевых значений элементов вектора e при условии $u = d - 1$, для которых $eg = 0$ равна $P_2 = 1/3^{d-1}$. Выражение для P_2 получено из следующих соображений. Число возможных комбинаций ненулевых значений элементов вектора e равно 3^d , из них 3 (при условии $u = d - 1$) приводят к $eg = 0$. Тогда

$$P = P_1 P_2 = P_1 / 3^{d-1}. \quad (5)$$

Вероятность P_1 определяется путем проведения N испытаний при случайно формируемых размещениях d ненулевых элементов в векторе ошибок с использованием пакета Matlab. При каждом испытании определяется ранг матрицы,

которая получается из матрицы g путем исключения из нее строк, соответствующих нулевым элементам вектора e . При этом определяется число испытаний N_1 с рангом, равным $d - 1$. Затем с помощью функции `binofit(N1,N)` пакета Matlab получаем точечную оценку $P_1^* = N_1/N$ значения P_1 , нижнюю P_{1L} и верхнюю P_{1U} границу оценки с доверительной вероятностью 0.95.

Далее на основании (5) можно определить P^* , P_L , P_U , используя P_1^* , P_{1L} и P_{1U} соответственно.

Результаты, полученные указанным путем, для кодов с $d = 6$ помещены в таблице 3, а для кодов с $d = 7$ – в таблице 4.

Таблица 3

Код (n,k)	(15,8)	(63,53)	(255,242)
N	10^6	10^6	$5 \cdot 10^6$
N_1	20925	399	99
P_1^*	$2.09 \cdot 10^{-2}$	$3.99 \cdot 10^{-4}$	$1.98 \cdot 10^{-5}$
P_{1L}, P_{1U}	$2.06 \cdot 10^{-2}, 2.12 \cdot 10^{-2}$	$3.61 \cdot 10^{-4}, 4.40 \cdot 10^{-4}$	$1.61 \cdot 10^{-5}, 2.41 \cdot 10^{-5}$
P^*	$8.61 \cdot 10^{-5}$	$1.64 \cdot 10^{-6}$	$8.1 \cdot 10^{-8}$
P_L, P_U	$8.50 \cdot 10^{-5}, 8.73 \cdot 10^{-5}$	$1.48 \cdot 10^{-6}, 1.81 \cdot 10^{-6}$	$6.62 \cdot 10^{-8}, 9.92 \cdot 10^{-8}$

Таблица 4

Код (n,k)	(15,7)	(63,50)	(255,238)
N	10^6	10^7	10^8
N_1	20934	21	3
P_1^*	$2.09 \cdot 10^{-2}$	$2.10 \cdot 10^{-6}$	$3.00 \cdot 10^{-8}$
P_{1L}, P_{1U}	$2.06 \cdot 10^{-2}, 2.12 \cdot 10^{-2}$	$1.30 \cdot 10^{-6}, 3.21 \cdot 10^{-6}$	$6.03 \cdot 10^{-9}, 8.76 \cdot 10^{-8}$
P^*	$2.87 \cdot 10^{-5}$	$2.88 \cdot 10^{-9}$	$4.11 \cdot 10^{-11}$
P_L, P_U	$2.83 \cdot 10^{-5}, 2.91 \cdot 10^{-5}$	$1.78 \cdot 10^{-9}, 4.40 \cdot 10^{-9}$	$8.27 \cdot 10^{-12}, 1.20 \cdot 10^{-10}$

6. Выводы

Предлагаемое спектральное описание кода БЧХ позволяет осуществлять кодирование и декодирование над полем $GF(4)$, что ускоряет эти процессы.

Если число ошибок в кодовом слове больше $d - 1$, то с ростом длины кодового слова n и постоянном значении d вероятность необнаруженной ошибки уменьшается и при достаточно большом n можно получить приемлемое значение этой вероятности.

С увеличением n при постоянном значении d увеличивается скорость кода k/n , что также является положительным фактом.

С увеличением d при постоянном значении n вероятность необнаруженной ошибки уменьшается.

Литература

1. Блейхут Р. Теория и практика кодов, контролирующих ошибки. Пер. с англ.– М.: Мир, 1986.– 576 с.
2. Передача дискретных сообщений/ Вершинин В.А. Рыбинская государственная авиационная технологическая академия им. П.А. Соловьева. Рыбинск, 2002.– 82 с.– Деп. в ВИНТИ 17.12.2002 г., № 2196-В2002