УДК 621.391

ОБНАРУЖЕНИЕ ОШИБОК КОДОМ РИДА – СОЛОМОНА НА ОСНОВЕ СПЕКТРАЛЬНОГО ОПИСАНИЯ

В. А. Вершинин

Рыбинский государственный авиационный технический университет им. П. А. Соловьева

Статья поступила в редакцию 16 ноября 2016 г.

Аннотация. В статье рассматривается спектральное описание кода Рида – Соломона. 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 Рида – Соломона.

Abstract. The article discusses the spectral description of the Reed –Solomon code. The purpose of the coding is error detection. The assessment of coding efficiency, when the number of errors in the code word is greater than the number of guaranteed detectable errors, is given.

Simulation of the decoding process shows that the highest value of the probability of undetected error is obtained when the number of errors in the code word is equal to the code distance. We use this probability 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, it is possible to obtain an acceptable value of probability of undetected value in the

case when the length of the code words increases and the value of the code distance is constant.

Key words: spectral description, error detection, Reed–Solomon code.

1. Введение

Спектральное описание кода Рида – Соломона основано [1] на дискретном преобразовании Фурье (ДПФ). Будем использовать ДПФ над полем $GF\left(2^m\right)$, где $m = 1, 2, 3, \ldots$. 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}; $i = 0, 1, 2, \ldots, n-1$; $j = 0, 1, 2, \ldots, n-1$. Здесь α – примитивный элемент поля $GF\left(2^m\right)$, $n = 2^m - 1$. Для примера, при $n = 15$ и $\alpha = 2$, используя пакет Matlab, можно получить:

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

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

1. Кодирование

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

$$c = bF_n^{-1}. \qquad (1)$$

Элементы сообщения и вектора c могут принимать значения $0, 1, 2, \ldots, n$. Такой код называется кодом Рида – Соломона, его кодовое расстояние $d = n - k + 1$.

2. Декодирование с обнаружением ошибок

Пусть кодовому слову на входе декодера соответствует вектор

$$c' = c + e, \qquad (2)$$

где e – вектор ошибок. Этот вектор связан с наличием помех в канале связи. Если в результате действия помех искажаются элементы кодового слова, то со-

ответствующие элементы вектора ошибок принимают значение $1, 2, \ldots, n$. Неискаженным элементам кодового слова соответствуют нулевые элементы вектора ошибок. В декодере осуществляется прямое ДПФ вектора c', в результате получается вектор $a' = c' F_n$. Здесь F_n – матрица прямого ДПФ, причем $F_n^{-1} F_n = 1$. Учитывая (1) и (2),

$$a' = (c + e) F_n = \left(a F_n^{-1} + e\right) F_n = a F_n^{-1} F_n + e F_n = a + e F_n .$$

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. Гарантированно 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.

3. 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 $1, 2, \ldots, n$.

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. В таблице 1 показаны результаты моделирования при использовании (15,11) кода Рида – Соломона. Было проведено 10^7 испытаний при случайно формируемых размещениях r ненулевых элементов в векторе ошибок с использованием пакета Matlab. Определялось число необнаруженных ошибок N.

Таблица 1

r	4	5	6	7	8	9	10	11	12	13	14	15
N	0	209	123	185	136	161	153	169	145	152	141	162

Рассмотрим матрицу g, состоящую из столбцов матрицы F_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 $r \le d-1$ произведение $eg \ne 0$ 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.

Число линейно независимых строк матрицы g, соответствующих ненулевым элементам вектора e, при $r = d$ равно $d-1$. Число возможных комбинаций ненулевых значений элементов вектора e равно n^d, из них n приводят к $eg = 0$. Тогда

$$P = n/n^d = 1/n^{d-1}. \qquad (3)$$

Значения P, полученные по формуле (3) для кодов с $d = 5$ помещены в таблице 2.

Таблица 2

Код (n,k)	(15,11)	(63,59)	(255,251)
P	$1.98 \cdot 10^{-5}$	$6.35 \cdot 10^{-8}$	$2.37 \cdot 10^{10}$

4. Выводы

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.

Литература

1. Блейхут Р. Теория и практика кодов, контролирующих ошибки. Пер. с англ.– М.: Мир, 1986.– 576 с.